aws

Administration Guide

Amazon WorkSpaces

Amazon WorkSpaces: Administration Guide

Table of Contents

What is Amazon WorkSpaces?

Amazon WorkSpaces enables you to provision virtual, cloud-based Microsoft Windows, Amazon Linux 2, Ubuntu Linux, or Red Hat Enterprise Linux desktops for your users, known as *WorkSpaces*. WorkSpaces eliminates the need to procure and deploy hardware or install complex software. You can quickly add or remove users as your needs change. Users can access their virtual desktops from multiple devices or web browsers.

For more information, see Amazon WorkSpaces.

WorkSpaces Personal and WorkSpaces Pools

Amazon WorkSpaces allows you to create the following 2 types of WorkSpaces, depending on your organization and user needs.

- **WorkSpaces Personal** - WorkSpaces Personal offer persistent virtual desktops, tailored for users who need a highly-personalized desktop provisioned for their exclusive use, similar to a physical desktop computer assigned to an individual. For more information, see Create a WorkSpace in WorkSpaces Personal.
- **WorkSpaces Pool** - WorkSpaces Pool offer non-persistent virtual desktops, tailored for users who need access to highly-curated desktop environments hosted on ephemeral infrastructure. For more information, see Administer WorkSpaces Pools.

Pricing

For WorkSpaces pricing details and examples, see WorkSpaces Pricing.

Features

- Choose between WorkSpaces Personal or WorkSpaces Pools. For more information, see WorkSpaces Personal and WorkSpaces Pools.
- Choose your operating system (Windows, Amazon Linux, Ubuntu Linux. Red Hat Enterprise Linux) and select from a range of hardware configurations, software configurations, and AWS Regions. For more information, see Amazon WorkSpaces Bundles and the section called “Create a custom image and bundle”.

- Choose your protocol: PCoIP or WorkSpaces Streaming Protocol (WSP). For more information, see Protocols for WorkSpaces Personal.
- Connect to your WorkSpace and pick up from right where you left off. WorkSpaces Personal provides a persistent desktop experience.
- WorkSpaces provides the flexibility of either monthly or hourly billing for WorkSpaces. For more information, see WorkSpaces Pricing.
- For Windows desktops, you can bring your own licenses and applications, or purchase them from the AWS Marketplace for Desktop Apps.
- Create a standalone managed Microsoft Active Directory for your users, or connect your WorkSpaces to your on-premises Active Directory so that your users can use their existing credentials to obtain seamless access to corporate resources. For more information, see the section called “Directories”.
- Use the same tools to manage WorkSpaces that you use to manage on-premises desktops.
- Use multi-factor authentication (MFA) for additional security.
- Use AWS Key Management Service (AWS KMS) to encrypt data at rest, disk I/O, and volume snapshots.
- Control the IP addresses from which users are allowed to access their WorkSpaces.
- For Windows 10 and 11 WorkSpaces, you can join your WorkSpaces to Microsoft Entra ID so that your users can use their existing Entra ID credentials to obtain seamless access to Microsoft 365 Apps for enterprise. You can also enroll your WorkSpaces into Intune to manage your virtual desktops using Intune. To learn more about Microsoft Entra ID, see What is Microsoft Entra ID?. To learn more about Microsoft Intune, please see Microsoft Intune securely manages identities, manages apps, and manages devices.

Access your WorkSpaces

You can connect to your WorkSpaces by using the client application for a supported device by using a supported web browser on a supported operating system.

> **Note**
>
> You cannot use a web browser to connect to Amazon Linux WorkSpaces.

There are client applications for the following devices:

- Windows computers
- macOS computers
- Ubuntu Linux 18.04 computers
- Chromebooks
- iPads
- Android devices
- Fire tablets
- Zero client devices (Teradici zero client devices are supported only with PCoIP.)

On Windows, macOS, and Linux PCs, you can use the following web browsers to connect to Windows and Ubuntu Linux WorkSpaces:

- Chrome 53 and later (Windows and macOS only)
- Firefox 49 and later

For more information, see WorkSpaces Clients in the *Amazon WorkSpaces User Guide*.

Get started with WorkSpaces

To create a WorkSpace, try one of the following tutorials:

- Get started with WorkSpaces
- Create an AWS Managed Microsoft AD directory
- Create a Simple AD directory
- Create an AD Connector
- Create a trust relationship between your AWS Managed Microsoft AD directory and your on-premises domain
- Create a dedicated Microsoft Entra ID directory with WorkSpaces Personal
- Create a dedicated Custom directory with WorkSpaces Personal

You might also want to explore these resources to learn more about Amazon WorkSpaces:

- Provision Desktops in the Cloud

- Best Practices for Deploying Amazon WorkSpaces
- Amazon WorkSpaces resources — includes whitepapers, blog posts, webinars, and re:Invent sessions
- Amazon WorkSpaces FAQs

Get started with WorkSpaces

As a first-time WorkSpaces user, you can choose to setup your WorkSpaces with quick setup or advanced setup. The following tutorials describes how to provision a cloud-based desktop, known as a *WorkSpace* using WorkSpaces and AWS Directory Service.

To get started with WorkSpaces Pools, see Configure SAML 2.0 and create a WorkSpaces Pools directory.

Get started with WorkSpaces Personal quick setup

In this tutorial, you learn how to provision a virtual, cloud-based Microsoft Windows, Amazon Linux 2, Ubuntu Linux, or Red Hat Enterprise Linux desktop, known as a *WorkSpace*, by using WorkSpaces and AWS Directory Service.

This tutorial uses the quick setup option to launch your WorkSpace. This option is available only if you have never launched a WorkSpace. Alternatively, see Create a directory for WorkSpaces Personal.

Note

This quick setup option and tutorial does not apply to WorkSpaces Pools.

Note

Quick setup is supported in the following AWS Regions:

- US East (N. Virginia)
- US West (Oregon)
- Europe (Ireland)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)

To change your Region, see Choosing a Region.

Tasks

Before you begin

Before you begin, make sure that you meet the following requirements:

- You must have an AWS account to create or administer a WorkSpace. Users do not need an AWS account to connect to and use their WorkSpaces.
- WorkSpaces is not available in every Region. Verify the supported Regions and select a Region for your WorkSpaces. For more information about the supported Regions, see WorkSpaces Pricing by AWS Region.

It's also helpful to review and understand the following before you proceed:

- When you launch a WorkSpace, you must select a WorkSpace bundle. For more information, see Amazon WorkSpaces Bundles and Amazon WorkSpaces Pricing.
- When you launch a WorkSpace, you must select which protocol (PCoIP or WorkSpaces Streaming Protocol [WSP]) you want to use with your bundle. For more information, see Protocols for WorkSpaces Personal.
- When you launch a WorkSpace, you must specify profile information for the user, including a user name and email address. Users complete their profiles by specifying a password. Information about WorkSpaces and users is stored in a directory. For more information, see the section called “Directories”.

What quick setup does

Quick setup completes the following tasks on your behalf:

- **Creates an IAM role** to allow the WorkSpaces service to create elastic network interfaces and list your WorkSpaces directories. This role has the name `workspaces_DefaultRole`.
- **Creates a virtual private cloud (VPC)**. If you want to use an existing VPC instead, make sure it meets the requirements noted in Configure a VPC for WorkSpaces Personal, and then follow the steps in one of the tutorials listed in Create a directory for WorkSpaces Personal. Choose the tutorial that corresponds to the type of Active Directory that you want to use.
- **Sets up a Simple AD directory** in the VPC and enables it for Amazon WorkDocs. This Simple AD directory is used to store user and WorkSpace information. The first AWS account created by quick setup is your admin AWS account. † The directory also has an Administrator account. For more information, see What gets created in the *AWS Directory Service Administration Guide*.
- **Creates the specified AWS accounts and adds them to the directory**.
- **Creates WorkSpaces**. Each WorkSpace receives a public IP address to provide internet access. The running mode is AlwaysOn. For more information, see Manage the running mode in WorkSpaces Personal.
- **Sends invitation emails to the specified users**. If your users don't receive their invitation emails, see Send an invitation email.

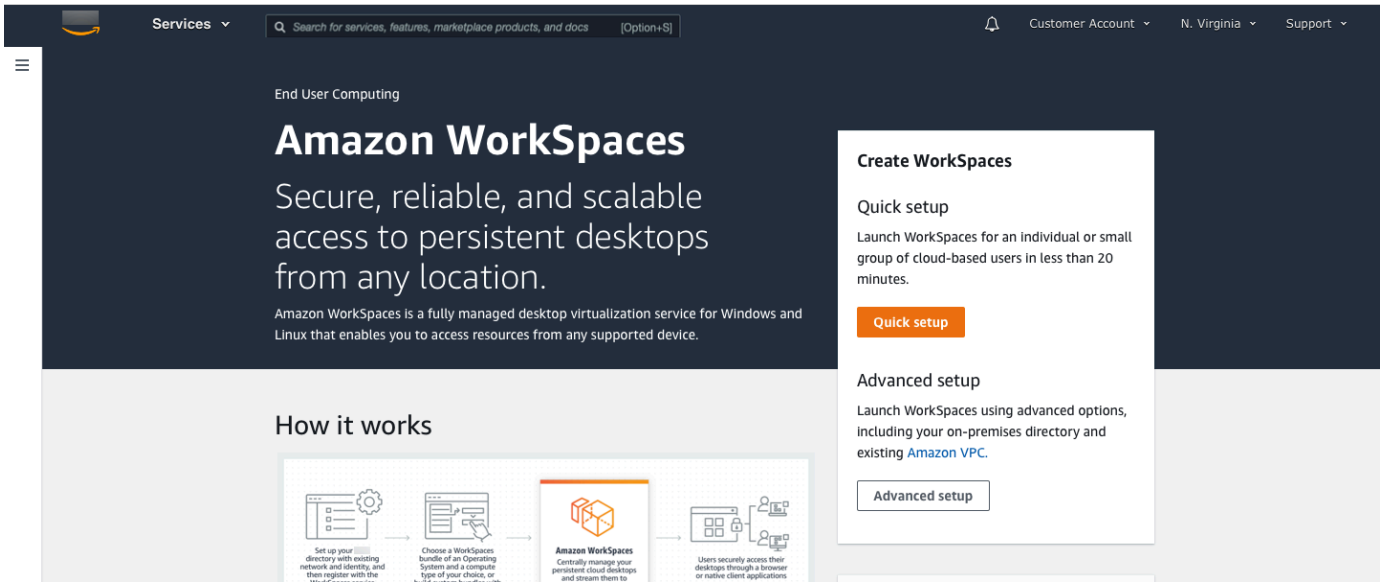
† The first AWS account created by quick setup is your admin AWS account. You can't update this AWS account from the WorkSpaces Console. Don't share the information for this account with anyone else. To invite other users to use WorkSpaces, create new AWS accounts for them.

Step 1: Launch the WorkSpace

Using quick setup, you can launch your first WorkSpace in minutes.

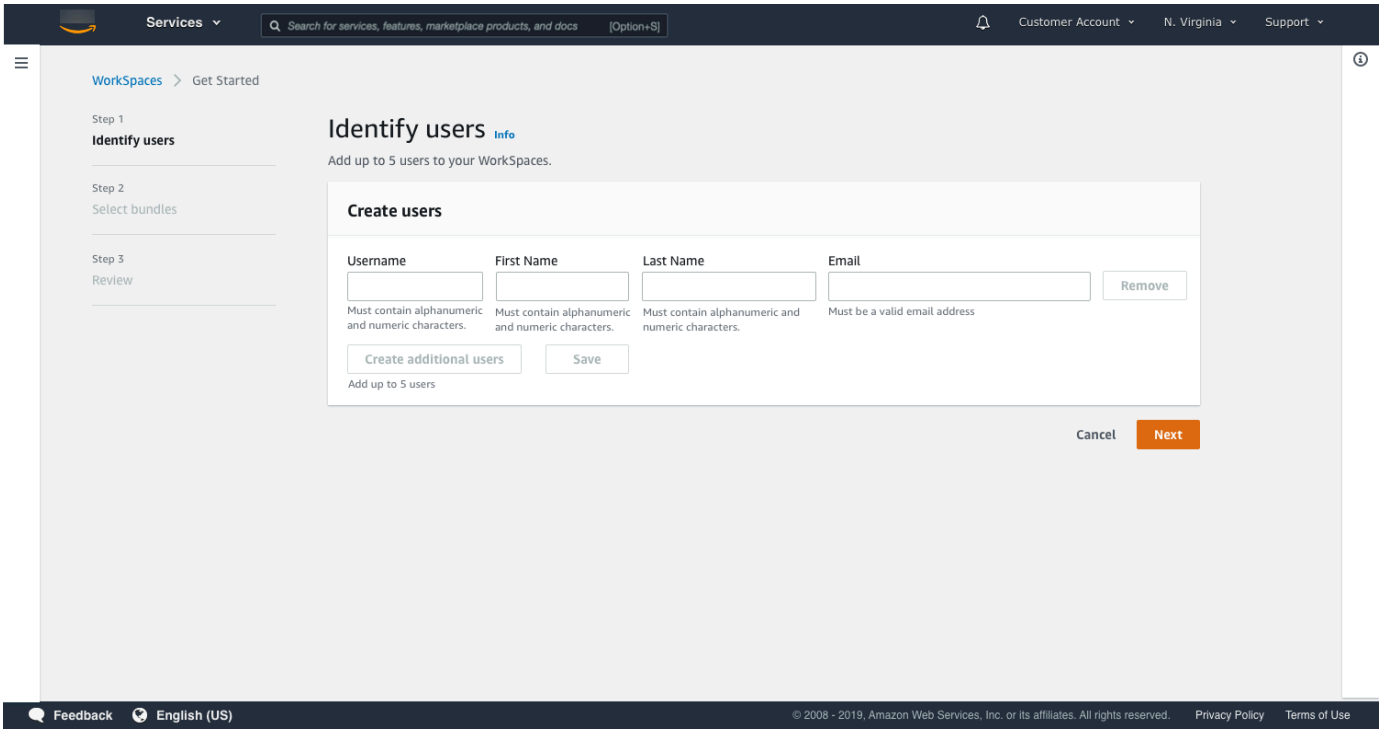
To launch a WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose **Quick setup**. If you don't see this button, either you have already launched a WorkSpace in this Region, or you aren't using one of the Regions that support quick setup. In this case, see Create a directory for WorkSpaces Personal.

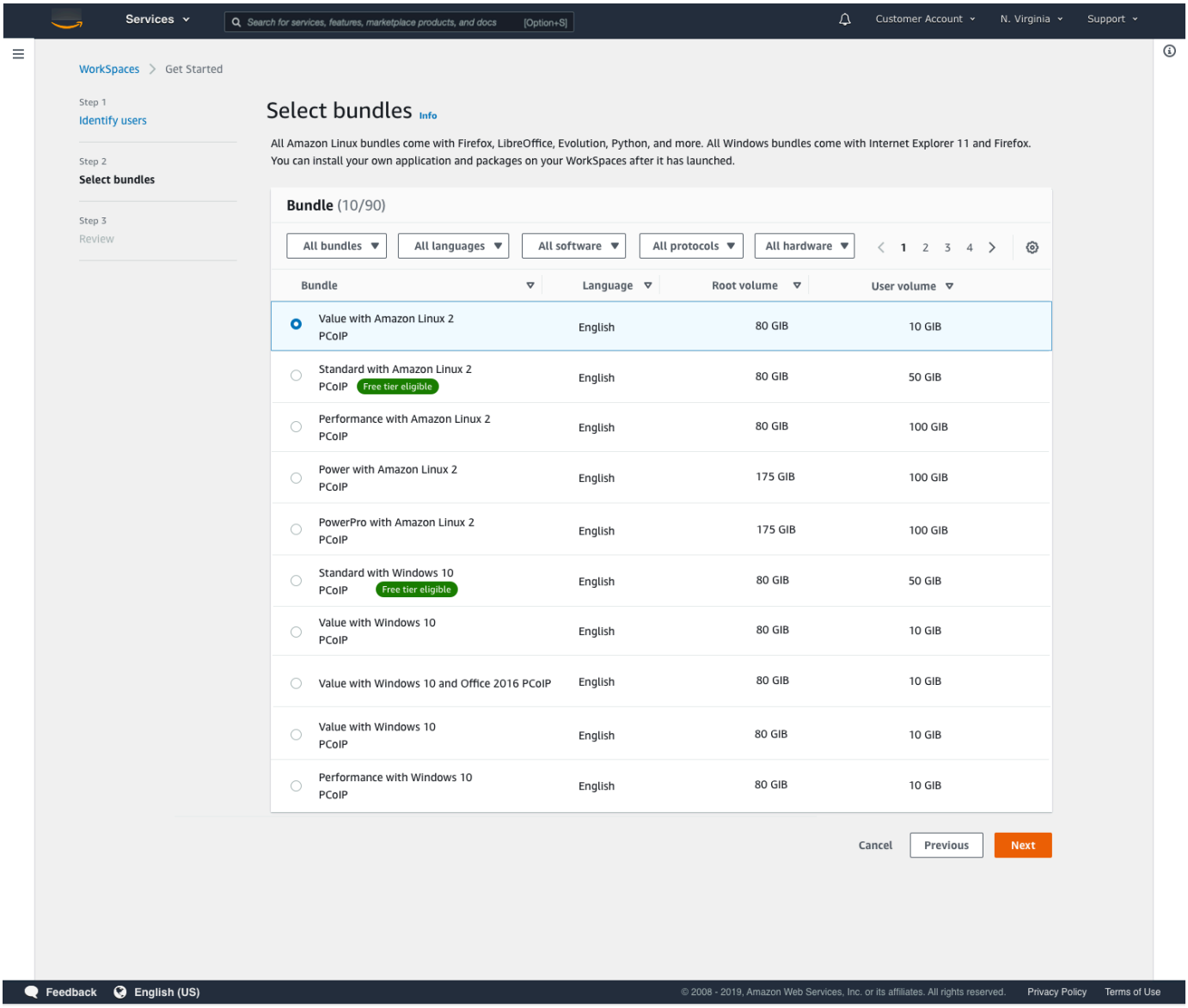


3. For **Identify users**, enter the **Username**, **First Name**. **Last Name**, and **Email**. Then choose **Next**.

> **Note**
>
> If this is your first time using WorkSpaces, we recommend creating a user for yourself for testing purposes.



4. For **Bundles**, select a bundle (hardware and software) for the user with the appropriate protocol (PCoIP or WSP). For more information about the various public bundles available for Amazon WorkSpaces, see Amazon WorkSpaces Bundles.



5. Review your information. Then choose **Create WorkSpace**.

6. It takes approximately 20 minutes for your WorkSpace to launch. To monitor the progress, go to the left navigation pane and choose **Directories**. You will see a directory being created with an initial status of `REQUESTED` and then `CREATING`.

   After the directory has been created and has a status of `ACTIVE`, you can choose **WorkSpaces** in the left navigation pane to monitor the progress of the WorkSpace launch process. The initial status of the WorkSpace is `PENDING`. When the launch is complete, the status is

`AVAILABLE` and an invitation is sent to the email address that you specified for each user. If your users don't receive their invitation emails, see Send an invitation email.

Step 2: Connect to the WorkSpace

After you receive the invitation email, you can connect to the WorkSpace using the client of your choice. After you sign in, the client displays the WorkSpace desktop.

To connect to the WorkSpace

1. If you haven't set up credentials for the user already, open the link in the invitation email and follow the directions. Remember the password that you specify as you will need it to connect to your WorkSpace.

   > **Note**
   >
   > Passwords are case-sensitive and must be between 8 and 64 characters in length, inclusive. Passwords must contain at least one character from each of the following categories: lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9), and the set ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/.

2. Review WorkSpaces Clients in the *Amazon WorkSpaces User Guide* for more information about the requirements for each client, and then do one of the following:

   - When prompted, download one of the client applications or launch **Web Access**.
   - If you aren't prompted and you haven't installed a client application already, open https://clients.amazonworkspaces.com/ and download one of the client applications or launch **Web Access**.

   > **Note**
   >
   > You cannot use a web browser (Web Access) to connect to Amazon Linux WorkSpaces.

3. Start the client, enter the registration code from the invitation email, and choose **Register**.
4. When prompted to sign in, enter the sign-in credentials, and then choose **Sign In**.
5. (Optional) When prompted to save your credentials, choose **Yes**.

For more information about using the client applications, such as setting up multiple monitors or using peripheral devices, see WorkSpaces Clients and Peripheral Device Support in the *Amazon WorkSpaces User Guide*.

Step 3: Clean up (Optional)

If you are finished with the WorkSpace that you created for this tutorial, you can delete it. For more information, see the section called "Delete a WorkSpace".

> **Note**
>
> Simple AD is made available to you free of charge to use with WorkSpaces. If there are no WorkSpaces being used with your Simple AD directory for 30 consecutive days, this directory will be automatically deregistered for use with Amazon WorkSpaces, and you will be charged for this directory as per the AWS Directory Service pricing terms.
> To delete empty directories, see Delete a directory for WorkSpaces Personal. If you delete your Simple AD directory, you can always create a new one when you want to start using WorkSpaces again.

Next steps

You can continue to customize the WorkSpace that you just created. For example, you can install software and then create a custom bundle from your WorkSpace. You can also perform various administrative tasks for your WorkSpaces and your WorkSpaces directory. For more information, see the following documentation.

- Create a custom WorkSpaces image and bundle for WorkSpaces Personal
- Administer WorkSpaces Personal
- Manage directories for WorkSpaces Personal

To create additional WorkSpaces, do one of the following:

- If you want to continue using the VPC and the Simple AD directory that were created by quick setup, you can add WorkSpaces for additional users by following the steps in the Create a WorkSpace in WorkSpaces Personal section of the Launch a WorkSpace Using Simple AD tutorial.
- If you need to use another directory type or if you need to use an existing Active Directory, see the appropriate tutorial in Create a directory for WorkSpaces Personal.

For more information about using the WorkSpaces client applications, such as setting up multiple monitors or using peripheral devices, see WorkSpaces Clients and Peripheral Device Support in the *Amazon WorkSpaces User Guide*.

Get started with WorkSpaces Personal advanced setup

In this tutorial, you learn how to provision a virtual, cloud-based Microsoft Windows, Amazon Linux, Ubuntu Linux, or Red Hat Enterprise Linux desktop desktop, known as a *WorkSpace*, by using WorkSpaces and AWS Directory Service.

This tutorial uses the advanced setup option to launch your WorkSpace.

> **Note**
>
> Advanced setup is supported in all Regions for WorkSpaces.

Tasks

- Before you begin
- Using advanced setup to launch your WorkSpace

Before you begin

Before you begin, make sure you have an AWS account that you can use to create or administer a WorkSpace. Users don't need an AWS account to connect to and use their WorkSpaces.

Review and understand the following concepts before you proceed:

- When you launch a WorkSpace, you must select a WorkSpace bundle. For more information, see Amazon WorkSpaces Bundles.
- When you launch a WorkSpace, you must select which protocol (PCoIP or WorkSpaces Streaming Protocol [WSP]) you want to use with your bundle. For more information, see Protocols for WorkSpaces Personal.
- When you launch a WorkSpace, you must specify profile information for the user, including a user name and email address. Users complete their profiles by specifying a password. Information about WorkSpaces and users is stored in a directory. For more information, see the section called “Directories”.

Using advanced setup to launch your WorkSpace

To use advanced setup to launch your WorkSpace:

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose one of the following directory types, and then choose **Next**:

   - AWS Managed Microsoft AD
   - Simple AD
   - AD Connector

3. Enter the directory information.
4. Choose two subnets in a VPC from two different availability zones. For more information, see Configure a VPC with public subnets.
5. Review your directory's information and choose **Create directory**.

Manage WorkSpaces Personal

WorkSpaces Personal offers persistent virtual desktops, tailored for users who need a highly-personalized desktop provisioned for their exclusive use, similar to a physical desktop computer assigned to an individual. For more information, see Create a WorkSpace in WorkSpaces Personal.

Topics

Architecture for WorkSpaces Personal

Each WorkSpace is associated with a virtual private cloud (VPC), and a directory to store and manage information for your WorkSpaces and users. For more information, see the section called "VPC requirements". Directories are either managed by the WorkSpaces service, or through the AWS Directory Service, which offers the following options: Simple AD, AD Connector, or AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD. For more information, see the AWS Directory Service Administration Guide.

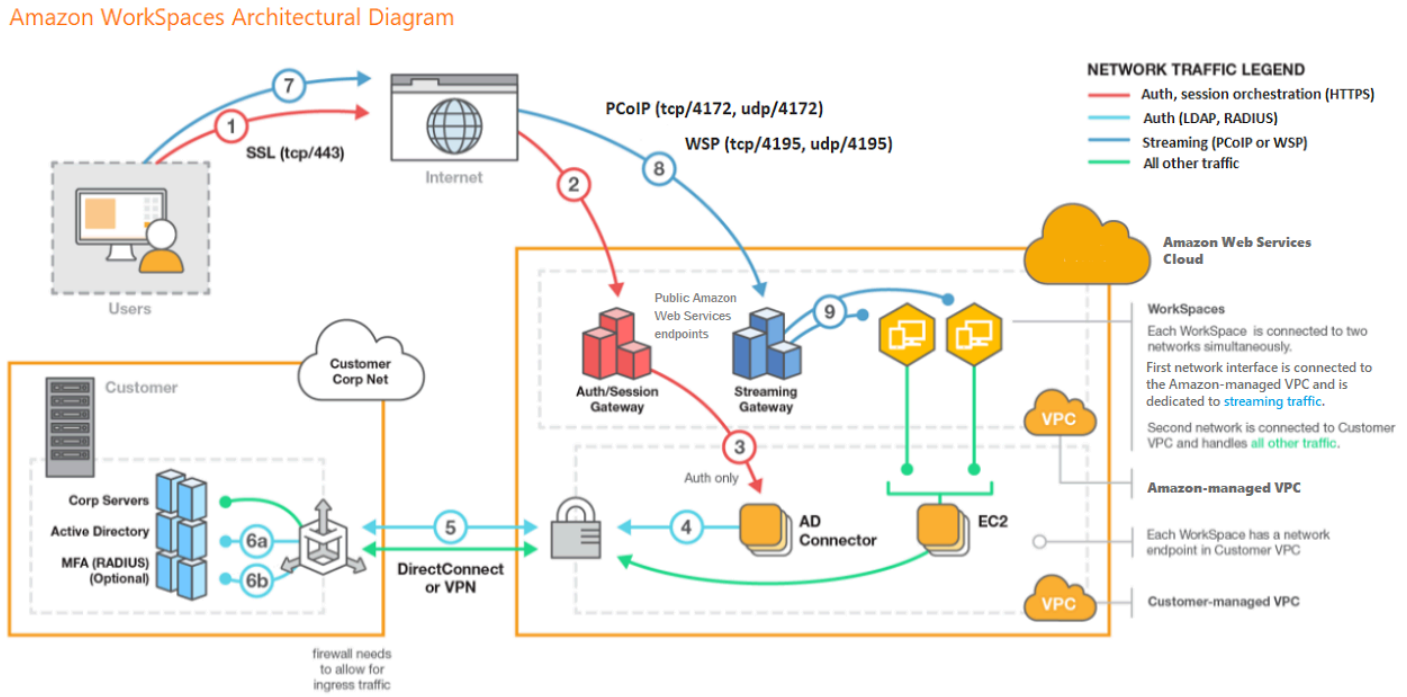
WorkSpaces uses your IAM Identity Center (for directories managed by Amazon WorkSpaces), Simple AD, AD Connector, or AWS Managed Microsoft AD directory to authenticate users. Users access their WorkSpaces by using a client application from a supported device or, for Windows WorkSpaces, a web browser, and they log in by using their directory credentials. The login information is sent to an authentication gateway, which forwards the traffic to the directory for

the WorkSpace. After the user is authenticated, streaming traffic is initiated through the streaming gateway.

Client applications use HTTPS over port 443 for all authentication and session-related information. Client applications use port 4172 (PCoIP) and port 4195 (WSP) for pixel streaming to the WorkSpace and ports 4172 and 4195 for network health checks. For more information, see Ports for client applications.

Each WorkSpace has two elastic network interfaces associated with it: a network interface for management and streaming (eth0) and a primary network interface (eth1). The primary network interface has an IP address provided by your VPC, from the same subnets used by the directory. This ensures that traffic from your WorkSpace can easily reach the directory. Access to resources in the VPC is controlled by the security groups assigned to the primary network interface. For more information, see Network interfaces.

The following diagram shows the architecture of WorkSpaces that use AD Connector.



Networking and access for WorkSpaces Personal

As a WorkSpace administrator, you must understand the following about WorkSpaces networking and access.

Contents

Protocols for WorkSpaces Personal

Amazon WorkSpaces supports two protocols: PCoIP and WorkSpaces Streaming Protocol (WSP). The protocol that you choose depends on several factors, such as the type of devices your users will be accessing their WorkSpaces from, which operating system is on your WorkSpaces, what network conditions your users will be facing, and whether your users require bidirectional video support.

Requirements

WSP WorkSpaces are only supported with the following minimum requirements.

Host agent requirements:

- Windows host agent version 2.0.0.312 or above
- Ubuntu host agent version 2.1.0.501 or above
- Amazon Linux 2 host agent version 2.0.0.596 or above
- Red Hat Enterprise Linux host agent version 2.1.0.1628 or above

Client requirements:

- Windows native client version 5.1.0.329 or higher
- macOS native client version 5.5.0 or higher
- Web Access

For more information about how to check your WorkSpace client version and host agent version, see the FAQ.

When to use WSP

- If you need higher loss/latency tolerance to support your end user network conditions. For example, you have users who are accessing their WorkSpaces across global distances or using unreliable networks.
- If you need your users to authenticate with smart cards or to use smart cards in-session.
- If you need webcam support capabilities in-session.
- If you need to use Web Access with the Windows Server 2022-powered WorkSpaces bundle.
- If you need to use Ubuntu WorkSpaces.
- If you need to use Windows 11 BYOL WorkSpaces.
- If you need to use Windows or Ubuntu GPU-based bundles (Graphics.g4dn and GraphicsPro.g4dn).
- If you need your users to authenticate in-session with WebAuthn authenticators such as YubiKey or Windows Hello.

When to use PCoIP

- If you want to use the iPad or Android Linux clients.
- If you use Teradici zero client devices.

- If you need to use GPU-based bundles (Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro).
- If you need to use a Linux bundle for non-smart card use cases.
- If you need to use WorkSpaces in the China (Ningxia) Region.

Note

- A directory can have a mix of PCoIP and WSP WorkSpaces in it.
- A user can have both a PCoIP and a WSP WorkSpace as long as the two WorkSpaces are located in separate directories. The same user cannot have a PCoIP and a WSP WorkSpace in the same directory. For more information about creating multiple WorkSpaces for a user, see Create multiple WorkSpaces for a user in WorkSpaces Personal.
- You can migrate a WorkSpace between the two protocols by using the WorkSpaces migration feature, which requires a rebuild of the WorkSpace. For more information, see Migrate a WorkSpace in WorkSpaces Personal.
- If your WorkSpace was created with PCoIP bundles you can modify the streaming protocol to migrate between the two protocols without requiring a rebuild, while retaining the root volume. For more information, see Modify protocols.
- For the best experience with video conferencing we recommend using Power or PowerPro bundles only.

Configure a VPC for WorkSpaces Personal

WorkSpaces launches your WorkSpaces in a virtual private cloud (VPC).

You can create a VPC with two private subnets for your WorkSpaces and a NAT gateway in a public subnet. Alternatively, you can create a VPC with two public subnets for your WorkSpaces and associate a public IP address or Elastic IP address with each WorkSpace.

For more information about VPC design considerations, see Best Practices for VPCs and Networking in Amazon WorkSpaces Deployments and Best Practices for Deploying WorkSpaces - VPC Design.

Contents

- Configure a VPC with private subnets and a NAT gateway
- Configure a VPC with public subnets

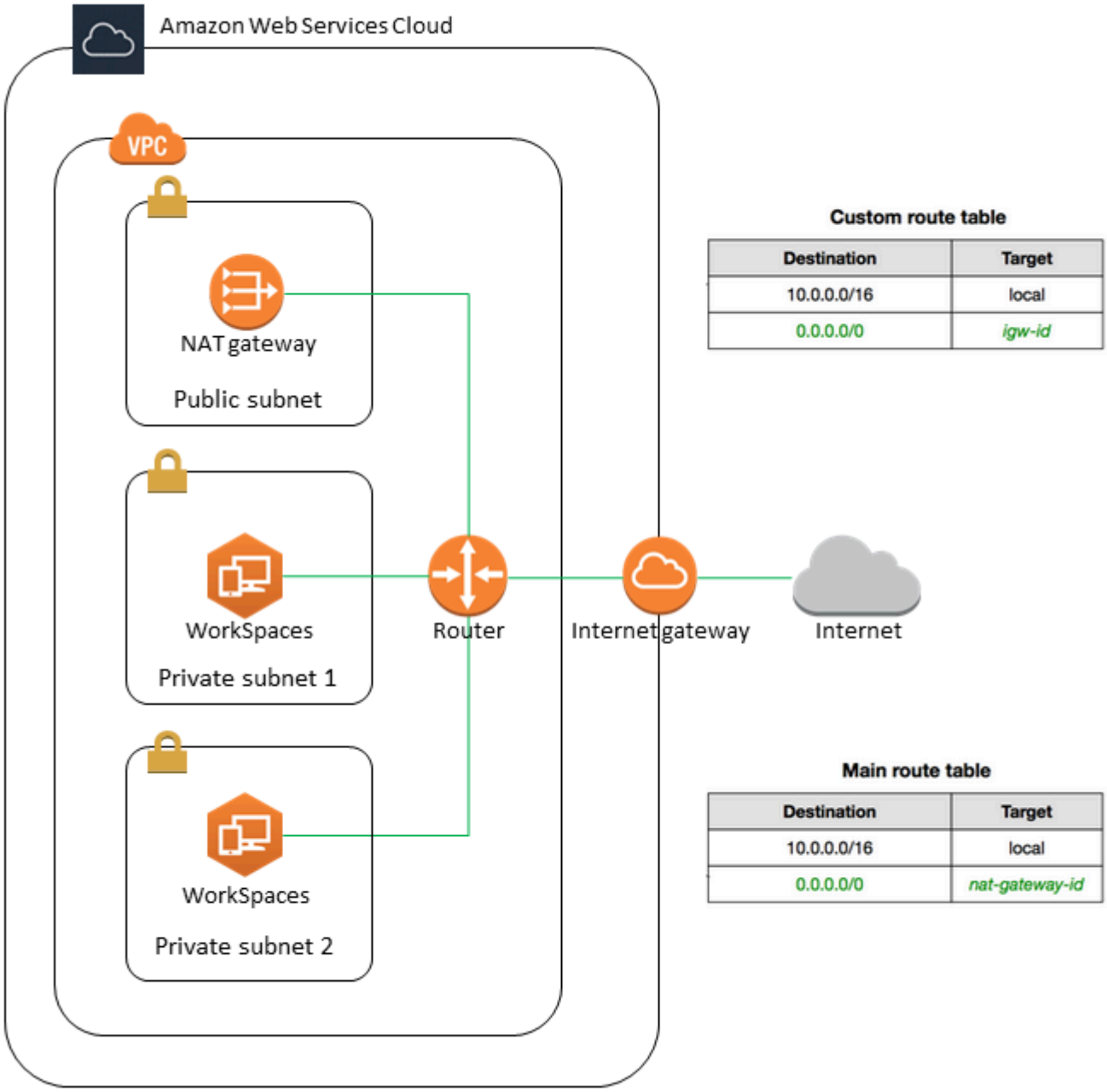
Requirements

Your VPC's subnets must reside in different Availability Zones in the Region where you're launching WorkSpaces. Availability Zones are distinct locations that are engineered to be isolated from failures in other Availability Zones. By launching instances in separate Availability Zones, you can protect your applications from the failure of a single location. Each subnet must reside entirely within one Availability Zone and cannot span zones.

> **Note**
>
> Amazon WorkSpaces is available in a subset of the Availability Zones in each supported Region. To determine which Availability Zones you can use for the subnets of the VPC that you're using for WorkSpaces, see Availability Zones for WorkSpaces Personal.

Configure a VPC with private subnets and a NAT gateway

If you use AWS Directory Service to create an AWS Managed Microsoft or a Simple AD, we recommend that you configure the VPC with one public subnet and two private subnets. Configure your directory to launch your WorkSpaces in the private subnets. To provide internet access to WorkSpaces in a private subnet, configure a NAT gateway in the public subnet.



To create a VPC with one public subnet and two private subnets

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Choose **Create VPC**.
3. Under **Resources to create**, choose **VPC and more**.
4. For **Name tag auto-generation**, enter a name for the VPC.

5. To configure the subnets, do the following:

   a. For **Number of Availability Zones**, choose **1** or **2**, depending on your needs.
   b. Expand **Customize AZs** and choose your Availability Zones. Otherwise, AWS selects them for you. To make an appropriate selection, see Availability Zones for WorkSpaces Personal.
   c. For **Number of public subnets**, ensure that you have one public subnet per Availability Zone.
   d. For **Number of private subnets**, ensure that you have at least one private subnet per Availability Zone.
   e. Enter a CIDR block for each subnet. For more information, see Subnet sizing in the *Amazon VPC User Guide*.
6. For **NAT gateways**, choose **1 per AZ**.
7. Choose **Create VPC**.

IPv6 CIDR blocks

You can associate IPv6 CIDR blocks with your VPC and subnets. However, if you configure your subnets to automatically assign IPv6 addresses to instances launched in the subnet, then you cannot use Graphics bundles. (You can use Graphics.g4dn, GraphicsPro.g4dn, and GraphicsPro bundles, however.) This restriction arises from a hardware limitation of previous-generation instance types that do not support IPv6.

To work around this issue, you can temporarily disable the **auto-assign IPv6 addresses** setting on the WorkSpaces subnets before launching Graphics bundles, and then reenable this setting (if needed) after launching Graphics bundles so that any other bundles receive the desired IP addresses.

By default, the **auto-assign IPv6 addresses** setting is disabled. To check this setting from the Amazon VPC console, in the navigation pane, choose **Subnets**. Select the subnet, and choose **Actions**, **Modify auto-assign IP settings**.

Configure a VPC with public subnets

If you prefer, you can create a VPC with two public subnets. To provide internet access to WorkSpaces in public subnets, configure the directory to assign Elastic IP addresses automatically or manually assign an Elastic IP address to each WorkSpace.

Tasks

- Step 1: Create a VPC
- Step 2: Assign public IP addresses to your WorkSpaces

Step 1: Create a VPC

Create a VPC with one public subnet as follows.

To create the VPC

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Choose **Create VPC**.
3. Under **Resources to create**, choose **VPC and more**.
4. For **Name tag auto-generation**, enter a name for the VPC.
5. To configure the subnets, do the following:
    a. For **Number of Availability Zones**, choose **2**.
    b. Expand **Customize AZs** and choose your Availability Zones. Otherwise, AWS selects them for you. To make an appropriate selection, see Availability Zones for WorkSpaces Personal.
    c. For **Number of public subnets**, choose **2**.
    d. For **Number of private subnets**, choose **0**.
    e. Enter a CIDR block for each public subnet. For more information, see Subnet sizing in the *Amazon VPC User Guide*.
6. Choose **Create VPC**.

IPv6 CIDR blocks

You can associate an IPv6 CIDR block with your VPC and subnets. However, if you configure your subnets to automatically assign IPv6 addresses to instances launched in the subnet, then you cannot use Graphics bundles. (You can use GraphicsPro bundles, however.) This restriction arises from a hardware limitation of previous-generation instance types that do not support IPv6.

To work around this issue, you can temporarily disable the **auto-assign IPv6 addresses** setting on the WorkSpaces subnets before launching Graphics bundles, and then reenable this setting (if needed) after launching Graphics bundles so that any other bundles receive the desired IP addresses.

By default, the **auto-assign IPv6 addresses** setting is disabled. To check this setting from the Amazon VPC console, in the navigation pane, choose **Subnets**. Select the subnet, and choose **Actions**, **Modify auto-assign IP settings**.

Step 2: Assign public IP addresses to your WorkSpaces

You can assign public IP addresses to your WorkSpaces automatically or manually. To use automatic assignment, see the section called “Configure automatic public IP addresses”. To assign public IP addresses manually, use the following procedure.

To assign a public IP address to a WorkSpace manually

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Expand the row (choose the arrow icon) for the WorkSpace and note the value of **WorkSpace IP**. This is the primary private IP address of the WorkSpace.
4. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
5. In the navigation pane, choose **Elastic IPs**. If you do not have an available Elastic IP address, choose **Allocate Elastic IP address** and choose **Amazon's pool of IPv4 addresses** or **Customer owned pool of IPv4 addresses**, and then choose **Allocate**. Make note of the new IP address.
6. In the navigation pane, choose **Network Interfaces**.
7. Select the network interface for your WorkSpace. To find the network interface for your WorkSpace, enter the **WorkSpace IP** value (which you noted earlier) in the search box, and then press **Enter**. The **WorkSpace IP** value matches the primary private IPv4 address for the network interface. Note that the VPC ID of the network interface matches the ID of your WorkSpaces VPC.
8. Choose **Actions**, **Manage IP Addresses**. Choose **Assign new IP**, and then choose **Yes, Update**. Make note of the new IP address.
9. Choose **Actions**, **Associate Address**.
10. On the **Associate Elastic IP Address** page, choose an Elastic IP address from **Address**. For **Associate to private IP address**, specify the new private IP address, and then choose **Associate Address**.

Availability Zones for WorkSpaces Personal

When you are creating a virtual private cloud (VPC) for use with Amazon WorkSpaces, your VPC's subnets must reside in different Availability Zones in the Region where you're launching WorkSpaces. Availability Zones are distinct locations that are engineered to be isolated from failures in other Availability Zones. By launching instances in separate Availability Zones, you can protect your applications from the failure of a single location. Each subnet must reside entirely within one Availability Zone and cannot span zones.

An Availability Zone is represented by a Region code followed by a letter identifier; for example, `us-east-1a`. To ensure that resources are distributed across the Availability Zones for a Region, we independently map Availability Zones to names for each AWS account. For example, the Availability Zone `us-east-1a` for your AWS account might not be the same location as `us-east-1a` for another AWS account.

To coordinate Availability Zones across accounts, you must use the *AZ ID*, which is a unique and consistent identifier for an Availability Zone. For example, `use1-az2` is an AZ ID for the `us-east-1` Region and it has the same location in every AWS account.

Viewing AZ IDs enables you to determine the location of resources in one account relative to the resources in another account. For example, if you share a subnet in the Availability Zone with the AZ ID `use1-az2` with another account, this subnet is available to that account in the Availability Zone whose AZ ID is also `use1-az2`. The AZ ID for each VPC and subnet is displayed in the Amazon VPC console.

Amazon WorkSpaces is only available in a subset of the Availability Zones for each supported Region. The following table lists the AZ IDs that you can use for each Region. To see the mapping of AZ IDs to Availability Zones in your account, see AZ IDs for Your Resources in the *AWS RAM User Guide*.

Region name	Region code	Supported AZ IDs
US East (N. Virginia)	`us-east-1`	`use1-az2`, `use1-az4`, `use1-az6`
US West (Oregon)	`us-west-2`	`usw2-az1`, `usw2-az2`, `usw2-az3`

Region name	Region code	Supported AZ IDs
Asia Pacific (Mumbai)	ap-south-1	aps1-az1, aps1-az2, aps1-az3
Asia Pacific (Seoul)	ap-northeast-2	apne2-az1 , apne2-az3
Asia Pacific (Singapore)	ap-southeast-1	apse1-az1 , apse1-az2
Asia Pacific (Sydney)	ap-southeast-2	apse2-az1 , apse2-az3
Asia Pacific (Tokyo)	ap-northeast-1	apne1-az1 , apne1-az4
Canada (Central)	ca-central-1	cac1-az1, cac1-az2
Europe (Frankfurt)	eu-central-1	euc1-az2, euc1-az3
Europe (Ireland)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
Europe (London)	eu-west-2	euw2-az2, euw2-az3
South America (São Paulo)	sa-east-1	sae1-az1, sae1-az3
Africa (Cape Town)	af-south-1	afs1-az1, afs1-az2, afs1-az3
Israel (Tel Aviv)	il-central-1	ilc1-az1, ilc1-az2, ilc1-az3
AWS GovCloud (US-West)	us-gov-west-1	usgw1-az1 , usgw1-az2 , usgw1-az3
AWS GovCloud (US-East)	us-gov-east-1	usge1-az1 , usge1-az2 , usge1-az3

For more information about Availability Zones and AZ IDs, see Regions, Availability Zones, and Local Zones in the *Amazon EC2 User Guide*.

IP address and port requirements for WorkSpaces Personal

To connect to your WorkSpaces, the network that your WorkSpaces clients are connected to must have certain ports open to the IP address ranges for the various AWS services (grouped in subsets). These address ranges vary by AWS Region. These same ports must also be open on any firewall running on the client. For more information about the AWS IP address ranges for different Regions, see AWS IP Address Ranges in the *Amazon Web Services General Reference*.

For an architecture diagram, see WorkSpaces Architecture. For additional architecture diagrams, see Best Practices for Deploying Amazon WorkSpaces.

Ports for client applications

The WorkSpaces client application requires outbound access on the following ports:

Port 53 (UDP)

This port is used to access DNS servers. It must be open to your DNS server IP addresses so that the client can resolve public domain names. This port requirement is optional if you are not using DNS servers for domain name resolution.

Port 443 (TCP)

This port is used for client application updates, registration, and authentication. The desktop client applications support the use of a proxy server for port 443 (HTTPS) traffic. To enable the use of a proxy server, open the client application, choose **Advanced Settings**, select **Use Proxy Server**, specify the address and port of the proxy server, and choose **Save**.

This port must be open to the following IP address ranges:

- The `AMAZON` subset in the `GLOBAL` Region.
- The `AMAZON` subset in the Region that the WorkSpace is in.
- The `AMAZON` subset in the `us-east-1` Region.
- The `AMAZON` subset in the `us-west-2` Region.
- The `S3` subset in the `us-west-2` Region.

Port 4172 (UDP and TCP)

This port is used for streaming the WorkSpace desktop and health checks for PCoIP WorkSpaces. This port must be open to the PCoIP Gateway and to the health check servers in

the Region that the WorkSpace is in. For more information, see Health check servers and PCoIP gateway servers.

For PCoIP WorkSpaces, the desktop client applications do not support the use of a proxy server nor TLS decryption and inspection for port 4172 traffic in UDP (for desktop traffic). They require a direct connection to ports 4172.

Port 4195 (UDP and TCP)

This port is used for streaming the WorkSpace desktop and health checks for WorkSpaces Streaming Protocol (WSP) WorkSpaces. This port must be open to the WSP Gateway IP address ranges and the health check servers in the Region that the WorkSpace is in. For more information, see Health check servers and WSP gateway servers.

For WSP WorkSpaces, the WorkSpaces Windows client application (version 5.1 and above) and macOS client application (version 5.4 and above) support the use of HTTP proxy servers for port 4195 TCP traffic, but the use of a proxy is not recommended. TLS decryption and inspection are not supported. For more information, see **Configure device proxy server settings for internet access** for Windows WorkSpaces, Amazon Linux WorkSpaces, and Ubuntu WorkSpaces.

Note

- If your firewall uses stateful filtering, ephemeral ports (also known as dynamic ports) are automatically opened to allow return communication. If your firewall uses stateless filtering, you must open ephemeral ports explicitly to allow return communication. The required ephemeral port range that you must open will vary depending on your configuration.
- Proxy server function is not supported for UDP traffic. If you choose to use a proxy server, the API calls that the client application makes to the Amazon WorkSpaces services are also proxied. Both API calls and desktop traffic should pass through the same proxy server.

Ports for Web Access

WorkSpaces Web Access requires outbound access for the following ports:

Port 53 (UDP)

This port is used to access DNS servers. It must be open to your DNS server IP addresses so that the client can resolve public domain names. This port requirement is optional if you are not using DNS servers for domain name resolution.

Port 80 (UDP and TCP)

This port is used for initial connections to `https://clients.amazonworkspaces.com`, which then switch to HTTPS. It must be open to all IP address ranges in the EC2 subset in the Region that the WorkSpace is in.

Port 443 (UDP and TCP)

This port is used for registration and authentication using HTTPS. It must be open to all IP address ranges in the EC2 subset in the Region that the WorkSpace is in.

Port 4195 (UDP and TCP)

For WorkSpaces that are configured for WorkSpaces Streaming Protocol (WSP), this port is used for streaming the WorkSpaces desktop traffic. This port must be open to the WSP Gateway IP address ranges. For more information, see WSP gateway servers.

WSP web access supports the use of a proxy server for port 4195 TCP traffic, but it's not recommended. For more information, see **Configure device proxy server settings for internet access** for Windows WorkSpaces, Amazon Linux WorkSpaces, or Ubuntu WorkSpaces.

> **Note**
>
> If your firewall uses stateful filtering, ephemeral ports (also known as dynamic ports) are automatically opened to allow return communication. If your firewall uses stateless filtering, you must open ephemeral ports explicitly to allow return communication. The required ephemeral port range that you must open varies depending on your configuration.

Typically, the web browser randomly selects a source port in the high range to use for streaming traffic. WorkSpaces Web Access does not have control over the port that the browser selects. You must ensure that return traffic to this port is allowed.

Domains and IP addresses to add to your allow list

For the WorkSpaces client application to be able to access the WorkSpaces service, you must add the following domains and IP addresses to the allow list on the network from which the client is trying to access the service.

Domains and IP addresses to add to your allow list

Category	Domain or IP address
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	• https://d2td7dqidlhjx7.cloudfront.net/ • In the AWS GovCloud (US-West) Region: https://d2td7dqidlhjx7.cloudfront.net/prod/pdt/windows/WorkSpacesAppCastx64.xml
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domains: • https://skylight-client-ds.us-east-1.amazonaws.com • https://skylight-client-ds.us-west-2.amazonaws.com • https://skylight-client-ds.ap-south-1.amazonaws.com • https://skylight-client-ds.ap-northeast-2.amazonaws.com • https://skylight-client-ds.ap-southeast-1.amazonaws.com • https://skylight-client-ds.ap-southeast-2.amazonaws.com • https://skylight-client-ds.ap-northeast-1.amazonaws.com

Category	Domain or IP address
	• https://skylight-client-ds.ca-central-1.amazonaws.com • https://skylight-client-ds.eu-central-1.amazonaws.com • https://skylight-client-ds.eu-west-1.amazonaws.com • https://skylight-client-ds.eu-west-2.amazonaws.com • https://skylight-client-ds.sa-east-1.amazonaws.com • https://skylight-client-ds.af-south-1.amazonaws.com • https://skylight-client-ds.il-central-1.amazonaws.com • In the AWS GovCloud (US-West) Region: https://skylight-client-ds.us-gov-west-1.amazonaws.com • In the AWS GovCloud (US-East) Region: https://skylight-client-ds.us-gov-east-1.amazonaws.com

Category	Domain or IP address
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domains: • https://ws-client-service.us-east-1.amazonaws.com • https://ws-client-service.us-west-2.amazonaws.com • https://ws-client-service.ap-south-1.amazonaws.com • https://ws-client-service.ap-northeast-2.amazonaws.com • https://ws-client-service.ap-southeast-1.amazonaws.com • https://ws-client-service.ap-southeast-2.amazonaws.com • https://ws-client-service.ap-northeast-1.amazonaws.com • https://ws-client-service.ca-central-1.amazonaws.com • https://ws-client-service.eu-central-1.amazonaws.com • https://ws-client-service.eu-west-1.amazonaws.com • https://ws-client-service.eu-west-2.amazonaws.com • https://ws-client-service.sa-east-1.amazonaws.com • https://ws-client-service.af-south-1.amazonaws.com • https://ws-client-service.il-central-1.amazonaws.com • In the AWS GovCloud (US-West) Region:

Category	Domain or IP address
	https://ws-client-service.us-gov-west-1.amazonaws.com • In the AWS GovCloud (US-East) Region: https://ws-client-service.us-gov-east-1.amazonaws.com

Category	Domain or IP address
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/*<region>*/*<directory ID>* Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Login page graphics for customer directory level co-branding: • Legacy — https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> • US East (N. Virginia) — https://d2h1yryv1jxiq.cloudfront.net/ • US West (Oregon) — https://d1fq42e1gi7rtq.cloudfront.net/ • Asia Pacific (Mumbai) — https://d1ctsk4u02kky7.cloudfront.net/ • Asia Pacific (Seoul) — https://dyoj3cw6iktvg.cloudfront.net • Asia Pacific (Singapore) — https://d1525ef92caquk.cloudfront.net/ • Asia Pacific (Sydney) — https://dodwxjr2amr8p.cloudfront.net/

Category	Domain or IP address
	• Asia Pacific (Tokyo) — https://d3v7kcib8ir2e1.cloudfront.net/ • Canada (Central) — https://d1ebdk07rro1qy.cloudfront.net/ • Europe (Frankfurt) — https://d39q4y7cndearu.cloudfront.net/ • Europe (Ireland) — https://d2127w6wvrc6l3.cloudfront.net/ • Europe (London) — https://df4ahgpxbxqy2.cloudfront.net/ • South America (São Paulo) — https://d2nezqurrjvain.cloudfront.net/ • Africa (Cape Town) — https://dr6ry0pwaoy23.cloudfront.net • Israel (Tel Aviv) — https://d2kmf63k5sit88.cloudfront.net CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • US East (N. Virginia) — https://d32i4gd7pg4909.cloudfront.net/ • US West (Oregon) — https://d18af777lco7lp.cloudfront.net/ • Asia Pacific (Mumbai) — https://d78hovzzqqtsb.cloudfront.net/ • Asia Pacific (Seoul) — https://dtyv4uwoh7ynt.cloudfront.net/

Category	Domain or IP address
	• Asia Pacific (Singapore) — https://d3qzmd7y07pz0i.cloudfront.net/ • Asia Pacific (Sydney) — https://dwcpoxuuza83q.cloudfront.net/ • Asia Pacific (Tokyo) — https://d2c2t8mxjhq5z1.cloudfront.net/ • Canada (Central) — https://d2wfbsypmqjmog.cloudfront.net/ • Europe (Frankfurt) — https://d1whcm49570jjw.cloudfront.net/ • Europe (Ireland) — https://d3pgffbf39h4k4.cloudfront.net/ • Europe (London) — https://d16q6638mh01s7.cloudfront.net/ • South America (São Paulo) — https://d2lh2qc5bdoq4b.cloudfront.net/ • Africa (Cape Town) — https://di5ygl2cs0mrh.cloudfront.net/ • Israel (Tel Aviv) — https://d1a3pnge9on3sx.cloudfront.net In the AWS GovCloud (US-West) Region: • Customer directory settings: https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/<directory ID> • Login page graphics for customer directory level co-branding: https://workspace-client-assets-pdt.s3-us-gov-west-1.amazonaws.com • CSS file to style the login pages:

Category	Domain or IP address
	https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css • JavaScript file for the login pages: Not applicable In the AWS GovCloud (US-East) Region: • Customer directory settings: https://s3.amazonaws.com/workspaces-client-properties/prod/osu/<directory ID> • Login page graphics for customer directory level co-branding: https://workspace-client-assets-pdt.s3-us-gov-east-1.amazonaws.com • CSS file to style the login pages: https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css • JavaScript file for the login pages: Not applicable
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers

Category	Domain or IP address
Pre-session Smart Card Authentication Endpoints	• https://smartcard.us-east-1.signin.aws • https://smartcard.us-west-2.signin.aws • https://smartcard.ap-southeast-2.signin.aws • https://smartcard.ap-northeast-1.signin.aws • https://smartcard.eu-west-1.signin.aws • https://smartcard.signin.amazonaws-us-gov.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain) In the AWS GovCloud (US-West) and AWS GovCloud (US-East) Regions: https://login.us-gov-home.awsapps.com/directory/<directory id>/ (where <directory id> is the customer's domain)

Category	Domain or IP address
WS Broker	Domains: • https://ws-broker-service.us-east-1.amazonaws.com • https://ws-broker-service-fips.us-east-1.amazonaws.com • https://ws-broker-service.us-west-2.amazonaws.com • https://ws-broker-service-fips.us-west-2.amazonaws.com • https://ws-broker-service.ap-south-1.amazonaws.com • https://ws-broker-service.ap-northeast-2.amazonaws.com • https://ws-broker-service.ap-southeast-1.amazonaws.com • https://ws-broker-service.ap-southeast-2.amazonaws.com • https://ws-broker-service.ap-northeast-1.amazonaws.com • https://ws-broker-service.ca-central-1.amazonaws.com • https://ws-broker-service.eu-central-1.amazonaws.com • https://ws-broker-service.eu-west-1.amazonaws.com • https://ws-broker-service.eu-west-2.amazonaws.com • https://ws-broker-service.sa-east-1.amazonaws.com • https://ws-broker-service.af-south-1.amazonaws.com

Category	Domain or IP address
	• https://ws-broker-service.il-central-1.amazonaws.com • https://ws-broker-service.us-gov-west-1.amazonaws.com • https://ws-broker-service-fips.us-gov-west-1.amazonaws.com • https://ws-broker-service.us-gov-east-1.amazonaws.com • https://ws-broker-service-fips.us-gov-east-1.amazonaws.com

Category	Domain or IP address
WorkSpaces API Endpoints	Domains: • https://workspaces.us-east-1.amazonaws.com • https://workspaces-fips.us-east-1.amazonaws.com • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com • https://workspaces.ap-south-1.amazonaws.com • https://workspaces.ap-northeast-2.amazonaws.com • https://workspaces.ap-southeast-1.amazonaws.com • https://workspaces.ap-southeast-2.amazonaws.com • https://workspaces.ap-northeast-1.amazonaws.com • https://workspaces.ca-central-1.amazonaws.com • https://workspaces.eu-central-1.amazonaws.com • https://workspaces.eu-west-1.amazonaws.com • https://workspaces.eu-west-2.amazonaws.com • https://workspaces.sa-east-1.amazonaws.com • https://workspaces.af-south-1.amazonaws.com

Category	Domain or IP address
	• https://workspaces.il-central-1.amazonaws.com • https://workspaces.us-gov-west-1.amazonaws.com • https://workspaces-fips.us-gov-west-1.amazonaws.com • https://workspaces.us-gov-east-1.amazonaws.com • https://workspaces-fips.us-gov-east-1.amazonaws.com

Category	Domain or IP address
WorkSpaces Endpoints for SAML Single Sign-On (SSO)	Domains: • https://euc-sso-sm.us-east-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips.us-east-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.us-west-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips.us-west-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-south-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-northeast-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-southeast-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-southeast-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-northeast-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.eu-central-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.eu-west-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.af-south-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.il-central-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.us-gov-west-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips.us-gov-west-1.amazonaws.com/v1/report-heartbeat

Category	Domain or IP address
	• https://euc-sso-sm.us-gov-east-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips.us-gov-east-1.amazonaws.com/v1/report-heartbeat

Domains and IP addresses to add to your allow list for PCoIP

Category	Domain or IP address
PCoIP Session Gateway (PSG)	PCoIP gateway servers
Session Broker (PCM)	Domains: • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws.com • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm-fips.us-west-2.amazonaws.com • https://skylight-cm.ap-south-1.amazonaws.com • https://skylight-cm.ap-northeast-2.amazonaws.com • https://skylight-cm.ap-southeast-1.amazonaws.com • https://skylight-cm.ap-southeast-2.amazonaws.com • https://skylight-cm.ap-northeast-1.amazonaws.com • https://skylight-cm.ca-central-1.amazonaws.com

Category	Domain or IP address
	• https://skylight-cm.eu-central-1.amazonaws.com • https://skylight-cm.eu-west-1.amazonaws.com • https://skylight-cm.eu-west-2.amazonaws.com • https://skylight-cm.sa-east-1.amazonaws.com • https://skylight-cm.af-south-1.amazonaws.com • https://skylight-cm.il-central-1.amazonaws.com • https://skylight-cm.us-gov-west-1.amazonaws.com • https://skylight-cm-fips.us-gov-west-1.amazonaws.com • https://skylight-cm.us-gov-east-1.amazonaws.com • https://skylight-cm-fips.us-gov-east-1.amazonaws.com

Category	Domain or IP address
Web Access TURN Servers for PCoIP	Servers: • turn:*.us-east-1.rdn.amazonaws.com • turn:*.us-west-2.rdn.amazonaws.com • Web Access isn't currently available in the Asia Pacific (Mumbai) Region. • turn:*.ap-northeast-2.rdn.amazonaws.com • turn:*.ap-southeast-1.rdn.amazonaws.com • turn:*.ap-southeast-2.rdn.amazonaws.com • turn:*.ap-northeast-1.rdn.amazonaws.com • turn:*.ca-central-1.rdn.amazonaws.com • turn:*.eu-central-1.rdn.amazonaws.com • turn:*.eu-west-1.rdn.amazonaws.com • turn:*.eu-west-2.rdn.amazonaws.com • turn:*.sa-east-1.rdn.amazonaws.com • Web Access isn't currently available in the Africa (Cape Town) Region • Web Access isn't currently available in the Israel (Tel Aviv) Region.

Domains and IP addresses to add to your allow list for WorkSpaces Streaming Protocol (WSP)

Category	Domain or IP address
WSP Session Gateway (WSG)	WSP gateway servers
Web Access TURN Servers for WSP	WSP gateway servers

Health check servers

The WorkSpaces client applications perform health checks over ports 4172 and 4195. These checks validate whether TCP or UDP traffic streams from the WorkSpaces servers to the client

applications. For these checks to finish successfully, your firewall policies must allow outbound traffic to the IP addresses of the following Regional health check servers.

Region	Health check hostname	IP addresses
US East (N. Virginia)	drp-iad.amazonworkspaces.com	3.209.215.252 3.212.50.30 3.225.55.35 3.226.24.234 34.200.29.95 52.200.219.150
US West (Oregon)	drp-pdx.amazonworkspaces.com	34.217.248.177 52.34.160.80 54.68.150.54 54.185.4.125 54.188.171.18 54.244.158.140
Asia Pacific (Mumbai)	drp-bom.amazonworkspaces.com	13.127.57.82 13.234.250.73
Asia Pacific (Seoul)	drp-icn.amazonworkspaces.com	13.124.44.166 13.124.203.105 52.78.44.253 52.79.54.102
Asia Pacific (Singapore)	drp-sin.amazonworkspaces.com	3.0.212.144

Region	Health check hostname	IP addresses
		18.138.99.116 18.140.252.123 52.74.175.118
Asia Pacific (Sydney)	drp-syd.amazonworkspaces.com	3.24.11.127 13.237.232.125
Asia Pacific (Tokyo)	drp-nrt.amazonworkspaces.com	18.178.102.247 54.64.174.128
Canada (Central)	drp-yul.amazonworkspaces.com	52.60.69.16 52.60.80.237 52.60.173.117 52.60.201.0
Europe (Frankfurt)	drp-fra.amazonworkspaces.com	52.59.191.224 52.59.191.225 52.59.191.226 52.59.191.227
Europe (Ireland)	drp-dub.amazonworkspaces.com	18.200.177.86 52.48.86.38 54.76.137.224

Region	Health check hostname	IP addresses
Europe (London)	drp-lhr.amazonworkspaces.com	35.176.62.54 35.177.255.44 52.56.46.102 52.56.111.36
South America (São Paulo)	drp-gru.amazonworkspaces.com	18.231.0.105 52.67.55.29 54.233.156.245 54.233.216.234
Africa (Cape Town)	drp-cpt.amazonworkspaces.com/	13.244.128.155 13.245.205.255 13.245.216.116
Israel (Tel Aviv)	drp-tlv.amazonworkspaces.com/	51.17.52.90 51.17.109.231 51.16.190.43
AWS GovCloud (US-West)	drp-pdt.amazonworkspaces.com	52.61.60.65 52.61.65.14 52.61.88.170 52.61.137.87 52.61.155.110 52.222.20.88

Region	Health check hostname	IP addresses
AWS GovCloud (US-East)	drp-osu.amazonworkspaces.com	18.253.251.70 18.254.0.118

PCoIP gateway servers

WorkSpaces uses PCoIP to stream the desktop session to clients over port 4172. For its PCoIP gateway servers, WorkSpaces uses a small range of Amazon EC2 public IPv4 addresses. This enables you to set more finely grained firewall policies for devices that access WorkSpaces. Note that the WorkSpaces clients do not support IPv6 addresses as a connectivity option at this time.

Region	Public IP address range
US East (N. Virginia)	3.217.228.0 - 3.217.231.255 3.235.112.0 - 3.235.119.255 52.23.61.0 - 52.23.62.255
US West (Oregon)	35.80.88.0 - 35.80.95.255 44.234.54.0 - 44.234.55.255 54.244.46.0 - 54.244.47.255
Asia Pacific (Mumbai)	13.126.243.0 - 13.126.243.255
Asia Pacific (Seoul)	3.34.37.0 - 3.34.37.255 3.34.38.0 - 3.34.39.255 13.124.247.0 - 13.124.247.255
Asia Pacific (Singapore)	18.141.152.0 - 18.141.152.255 18.141.154.0 - 18.141.155.255 52.76.127.0 - 52.76.127.255

Region	Public IP address range
Asia Pacific (Sydney)	3.25.43.0 - 3.25.43.255 3.25.44.0 - 3.25.45.255 54.153.254.0 - 54.153.254.255
Asia Pacific (Tokyo)	18.180.178.0 - 18.180.178.255 18.180.180.0 - 18.180.181.255 54.250.251.0 - 54.250.251.255
Canada (Central)	15.223.100.0 - 15.223.100.255 15.223.102.0 - 15.223.103.255 35.183.255.0 - 35.183.255.255
Europe (Frankfurt)	18.156.52.0 - 18.156.52.255 18.156.54.0 - 18.156.55.255 52.59.127.0 - 52.59.127.255
Europe (Ireland)	3.249.28.0 - 3.249.29.255 52.19.124.0 - 52.19.125.255
Europe (London)	18.132.21.0 - 18.132.21.255 18.132.22.0 - 18.132.23.255 35.176.32.0 - 35.176.32.255
South America (São Paulo)	18.230.103.0 - 18.230.103.255 18.230.104.0 - 18.230.105.255 54.233.204.0 - 54.233.204.255
Africa (Cape Town)	13.246.120.0 - 13.246.123.255

Region	Public IP address range
Israel (Tel Aviv)	51.17.28.0-51.17.31.255
AWS GovCloud (US-West)	52.61.193.0 - 52.61.193.255
AWS GovCloud (US-East)	18.254.140.0 - 18.254.143.255

WSP gateway servers

Important

Starting in June 2020, WorkSpaces streams the desktop session for WSP WorkSpaces to clients over port 4195 instead of port 4172. If you want to use WSP WorkSpaces, make sure that port 4195 is open to traffic.

WorkSpaces uses a small range of Amazon EC2 public IPv4 addresses for its WSP gateway servers. This enables you to set more finely grained firewall policies for devices that access WorkSpaces. Note that the WorkSpaces clients do not support IPv6 addresses as a connectivity option at this time.

Region	Public IP address range
US East (N. Virginia)	• 3.227.4.0/22 • 44.209.84.0/22
US West (Oregon)	34.223.96.0/22
Asia Pacific (Mumbai)	65.1.156.0/22
Asia Pacific (Seoul)	3.35.160.0/22
Asia Pacific (Singapore)	13.212.132.0/22
Asia Pacific (Sydney)	3.25.248.0/22
Asia Pacific (Tokyo)	3.114.164.0/22

Region	Public IP address range
Canada (Central)	3.97.20.0/22
Europe (Frankfurt)	18.192.216.0/22
Europe (Ireland)	3.248.176.0/22
Europe (London)	18.134.68.0/22
South America (São Paulo)	15.228.64.0/22
Africa (Cape Town)	13.246.108.0/22
Israel (Tel Aviv)	51.17.72.0/22
AWS GovCloud (US-West)	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
AWS GovCloud (US-East)	18.254.148.0/22

WSP gateway domain names

The following table lists the WSP WorkSpace gateway domain names. These domains must be contactable, for the WorkSpaces client application to be able to access the WorkSpace WSP service.

Region	Domain
US East (N. Virginia)	• *.prod.us-east-1.highlander.aws.a2z.com • (FIPS) *.wsp-fips.prod.us-east-1.highlander.aws.a2z.com
US West (Oregon)	• *.prod.us-west-2.highlander.aws.a2z.com • (FIPS) *.wsp-fips.prod.us-west-2.highlander.aws.a2z.com
Asia Pacific (Mumbai)	*.prod.ap-south-1.highlander.aws.a2z.com

Region	Domain
Asia Pacific (Seoul)	*.prod.ap-northeast-2.highlander.aws.a2z.com
Asia Pacific (Singapore)	*.prod.ap-southeast-1.highlander.aws.a2z.com
Asia Pacific (Sydney)	*.prod.ap-southeast-2.highlander.aws.a2z.com
Asia Pacific (Tokyo)	*.prod.ap-northeast-1.highlander.aws.a2z.com
Canada (Central)	*.prod.ca-central-1.highlander.aws.a2z.com
Europe (Frankfurt)	*.prod.eu-central-1.highlander.aws.a2z.com
Europe (Ireland)	*.prod.eu-west-1.highlander.aws.a2z.com
Europe (London)	*.prod.eu-west-2.highlander.aws.a2z.com
South America (São Paulo)	*.prod.sa-east-1.highlander.aws.a2z.com
Africa (Cape Town)	*.prod.af-south-1.highlander.aws.a2z.com
Israel (Tel Aviv)	*.prod.il-central-1.highlander.aws.a2z.com
AWS GovCloud (US-West)	• *.prod.us-gov-west-1.highlander.aws.a2z.com • (FIPS) *.wsp-fips.prod.us-gov-west-1.highlander.aws.a2z.com
AWS GovCloud (US-East)	• *.prod.us-gov-east-1.highlander.aws.a2z.com • (FIPS) *.wsp-fips.prod.us-gov-east-1.highlander.aws.a2z.com

Network interfaces

Each WorkSpace has the following network interfaces:

- The primary network interface (eth1) provides connectivity to the resources within your VPC and on the internet, and is used to join the WorkSpace to the directory.

- The management network interface (eth0) is connected to a secure WorkSpaces management network. It is used for interactive streaming of the WorkSpace desktop to WorkSpaces clients, and to allow WorkSpaces to manage the WorkSpace.

WorkSpaces selects the IP address for the management network interface from various address ranges, depending on the Region that the WorkSpaces are created in. When a directory is registered, WorkSpaces tests the VPC CIDR and the route tables in your VPC to determine if these address ranges create a conflict. If a conflict is found in all available address ranges in the Region, an error message is displayed and the directory is not registered. If you change the route tables in your VPC after the directory is registered, you might cause a conflict.

Warning

Do not modify or delete any of the network interfaces that are attached to a WorkSpace. Doing so might cause the WorkSpace to become unreachable or lose internet access.
For example, if you have enabled automatic assignment of Elastic IP addresses at the directory level, an Elastic IP address (from the Amazon-provided pool) is assigned to your WorkSpace when it is launched. However, if you associate an Elastic IP address that you own to a WorkSpace, and then you later disassociate that Elastic IP address from the WorkSpace, the WorkSpace loses its public IP address, and it doesn't automatically get a new one from the Amazon-provided pool.
To associate a new public IP address from the Amazon-provided pool with the WorkSpace, you must rebuild the WorkSpace. If you don't want to rebuild the WorkSpace, you must associate another Elastic IP address that you own to the WorkSpace.

Management interface IP ranges

The following table lists the IP address ranges used for the management network interface.

Note

- **If you're using Bring Your Own License (BYOL) Windows WorkSpaces**, the IP address ranges in the following table do not apply. Instead, PCoIP BYOL WorkSpaces use the 54.239.224.0/20 IP address range for management interface traffic in all AWS Regions. For WSP BYOL Windows WorkSpaces, both the 54.239.224.0/20 and 10.0.0.0/8 IP

address ranges apply in all AWS Regions. (These IP address ranges are used in addition to the /16 CIDR block that you select for management traffic for your BYOL WorkSpaces.)

- **If you're using WSP WorkSpaces created from public bundles**, the IP address range 10.0.0.0/8 also applies for management interface traffic in all AWS Regions, in addition to the PCoIP/WSP ranges shown in the following table.

Region	IP address range
US East (N. Virginia)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 WSP: 10.0.0.0/8
US West (Oregon)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, and 198.19.0.0/16 WSP: 10.0.0.0/8
Asia Pacific (Mumbai)	PCoIP/WSP: 192.168.0.0/16 WSP: 10.0.0.0/8
Asia Pacific (Seoul)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Asia Pacific (Singapore)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Asia Pacific (Sydney)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, and 198.19.0.0/16 WSP: 10.0.0.0/8
Asia Pacific (Tokyo)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Canada (Central)	PCoIP/WSP: 198.19.0.0/16

Region	IP address range
	WSP: 10.0.0.0/8
Europe (Frankfurt)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Europe (Ireland)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, and 198.19.0.0/16 WSP: 10.0.0.0/8
Europe (London)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
South America (São Paulo)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Africa (Cape Town)	PCoIP/WSP: 172.31.0.0/16 and 198.19.0.0/16 WSP: 10.0.0.0/8
Israel (Tel Aviv)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
AWS GovCloud (US-West)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8 and 192.169.0.0/16
AWS GovCloud (US-East)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8

Management interface ports

The following ports must be open on the management network interface of all WorkSpaces:

- Inbound TCP on port 4172. This is used for establishment of the streaming connection on the PCoIP protocol.
- Inbound UDP on port 4172. This is used for streaming user input on the PCoIP protocol.
- Inbound TCP on port 4489. This is used for access using the web client.
- Inbound TCP on port 8200. This is used for management and configuration of the WorkSpace.
- Inbound TCP on ports 8201-8250. These ports are used for establishment of the streaming connection and for streaming user input on the WSP protocol.
- Inbound UDP on port 8220. This port is used for establishment of the streaming connection and for streaming user input on the WSP protocol
- Outbound TCP on ports 8443 and 9997. This is used for access using the web client.
- Outbound UDP on ports 3478, 4172, and 4195. This is used for access using the web client.
- Outbound UDP on ports 50002 and 55002. This is used for streaming. If your firewall uses stateful filtering, the ephemeral ports 50002 and 55002 are automatically opened to allow return communication. If your firewall uses stateless filtering, you must open ephemeral ports 49152 - 65535 to allow return communication.
- Outbound TCP on port 80, as defined in Management interface IP ranges, to IP address 169.254.169.254 for access to the EC2 metadata service. Any HTTP proxy assigned to your WorkSpaces must also exclude 169.254.169.254.
- Outbound TCP on port 1688 to IP addresses 169.254.169.250 and 169.254.169.251 to allow access to Microsoft KMS for Windows activation for Workspaces that are based on public bundles. If you're using Bring Your Own License (BYOL) Windows WorkSpaces, you must allow access to your own KMS servers for Windows activation.
- Outbound TCP on port 1688 to IP address 54.239.236.220 to allow access to Microsoft KMS for Office activation for BYOL WorkSpaces.

  If you're using Office through one of the WorkSpaces public bundles, the IP address for Microsoft KMS for Office activation varies. To determine that IP address, find the IP address for the management interface of the WorkSpace, and then replace the last two octets with `64.250`. For example, if the IP address of the management interface is 192.168.3.5, the IP address for Microsoft KMS Office activation is 192.168.64.250.
- Outbound TCP to IP address 127.0.0.2 for WSP WorkSpaces when the WorkSpace host is configured to use a proxy server.
- Communications originating from loopback address 127.0.01.

Under normal circumstances, the WorkSpaces service configures these ports for your WorkSpaces. If any security or firewall software is installed on a WorkSpace that blocks any of these ports, the WorkSpace may not function correctly or may be unreachable.

Primary interface ports

No matter which type of directory you have, the following ports must be open on the primary network interface of all WorkSpaces:

- For internet connectivity, the following ports must be open outbound to all destinations and inbound from the WorkSpaces VPC. You need to add these manually to the security group for your WorkSpaces if you want them to have internet access.
  - TCP 80 (HTTP)
  - TCP 443 (HTTPS)
- To communicate with the directory controllers, the following ports must be open between your WorkSpaces VPC and your directory controllers. For a Simple AD directory, the security group created by AWS Directory Service will have these ports configured correctly. For an AD Connector directory, you might need to adjust the default security group for the VPC to open these ports.
  - TCP/UDP 53 - DNS
  - TCP/UDP 88 - Kerberos authentication
  - UDP 123 - NTP
  - TCP 135 - RPC
  - UDP 137-138 - Netlogon
  - TCP 139 - Netlogon
  - TCP/UDP 389 - LDAP
  - TCP/UDP 445 - SMB
  - TCP/UDP 636 - LDAPS (LDAP over TLS/SSL)
  - TCP 1024-65535 - Dynamic ports for RPC

  If any security or firewall software is installed on a WorkSpace that blocks any of these ports, the WorkSpace may not function correctly or may be unreachable.

IP address and port requirements by Region

US East (N. Virginia)

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain: https://skylight-client-ds.us-east-1.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.us-east-1.amazonaws.com
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID>

Category	Details
	Login page graphics for customer directory level co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • US East (N. Virginia) — https://d32i4gd7pg4909.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers
Pre-session Smart Card Authentication Endpoints	https://smartcard.us-east-1.signin.aws
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
WS Broker	Domains: • https://ws-broker-service.us-east-1.amazonaws.com • https://ws-broker-service-fips.us-east-1.amazonaws.com

Category	Details
WorkSpaces API Endpoints	Domains: https://workspaces.us-east-1.amazonaws.com
Session Broker (PCM)	Domains: • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws.com
Web Access TURN Servers for PCoIP	Server: • turn:*.us-east-1.rdn.amazonaws.com
Health check hostname	drp-iad.amazonworkspaces.com
Health check IP addresses	• 3.209.215.252 • 3.212.50.30 • 3.225.55.35 • 3.226.24.234 • 34.200.29.95 • 52.200.219.150
PCoIP gateway servers public IP address ranges	• 3.217.228.0 - 3.217.231.255 • 3.235.112.0 - 3.235.119.255 • 52.23.61.0 - 52.23.62.255
WSP gateway servers IP address range	• 3.227.4.0/22 • 44.209.84.0/22
WSP gateway domain name	*.prod.us-east-1.highlander.aws.a2z.com
Management interface IP address ranges	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

US West (Oregon)

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain: https://skylight-client-ds.us-west-2.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.us-west-2.amazonaws.com
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Login page graphics for customer directory level co-branding:

Category	Details
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • US West (Oregon) — https://d18af777lco7lp.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers
Pre-session Smart Card Authentication Endpoints	https://smartcard.us-west-2.signin.aws
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
WS Broker	Domains: • https://ws-broker-service.us-west-2.amazonaws.com • https://ws-broker-service-fips.us-west-2.amazonaws.com

Category	Details
WorkSpaces API Endpoints	Domains: • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com
Session Broker (PCM)	Domains: • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm-fips.us-west-2.amazonaws.com
Web Access TURN Servers for PCoIP	Server: • turn:*.us-west-2.rdn.amazonaws.com
Health check hostname	drp-pdx.amazonworkspaces.com
Health check IP addresses	• 34.217.248.177 • 52.34.160.80 • 54.68.150.54 • 54.185.4.125 • 54.188.171.18 • 54.244.158.140
PCoIP gateway servers public IP address ranges	• 35.80.88.0 - 35.80.95.255 • 44.234.54.0 - 44.234.55.255 • 54.244.46.0 - 54.244.47.255
WSP gateway servers IP address range	34.223.96.0/22
WSP gateway domain name	*.prod.us-west-2.highlander.aws.a2z.com

Category	Details
Management interface IP address ranges	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

Asia Pacific (Mumbai)

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain: https://skylight-client-ds.ap-south-1.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.ap-south-1.amazonaws.com
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings:

Category	Details
	• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Login page graphics for customer directory level co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • Asia Pacific (Mumbai) — https://d78hovzzqqtsb.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
WS Broker	Domain: • https://ws-broker-service.ap-south-1.amazonaws.com

Category	Details
WorkSpaces API Endpoints	Domain: • https://workspaces.ap-south-1.amazonaws.com
Session Broker (PCM)	Domain: • https://skylight-cm.ap-south-1.amazonaws.com
Web Access TURN Servers for PCoIP	Web Access isn't currently available in the Asia Pacific (Mumbai) Region
Health check hostname	drp-bom.amazonworkspaces.com
Health check IP addresses	• 13.127.57.82 • 13.234.250.73
PCoIP gateway servers public IP address ranges	13.126.243.0 - 13.126.243.255
WSP gateway servers IP address range	65.1.156.0/22
WSP gateway domain name	*.prod.ap-south-1.highlander.aws.a2z.com
Management interface IP address ranges	• PCoIP/WSP: 192.168.0.0/16 • WSP: 10.0.0.0/8

Asia Pacific (Seoul)

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/

Category	Details
Connectivity Check	https://connectivity.amazonworkspaces.com/
Device Metrics (for 1.0+ and 2.0+ WorkSpaces client applications)	https://device-metrics-us-2.amazon.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain: https://skylight-client-ds.ap-northeast-2.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.ap-northeast-2.amazonaws.com

Category	Details
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Login page graphics for customer directory level co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • Asia Pacific (Seoul) — https://dtyv4uwoh7ynt.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers

Category	Details
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
WS Broker	Domain: • https://ws-broker-service.ap-northeast-2.amazonaws.com
WorkSpaces API Endpoints	Domain: • https://workspaces.ap-northeast-2.amazonaws.com
Session Broker (PCM)	Domain: • https://skylight-cm.ap-northeast-2.amazonaws.com
Web Access TURN Servers for PCoIP	Server: • turn:*.ap-northeast-2.rdn.amazonaws.com
Health check hostname	drp-icn.amazonworkspaces.com
Health check IP addresses	• 13.124.44.166 • 13.124.203.105 • 52.78.44.253 • 52.79.54.102
PCoIP gateway servers public IP address ranges	• 3.34.37.0 - 3.34.37.255 • 3.34.38.0 - 3.34.39.255 • 13.124.247.0 - 13.124.247.255
WSP gateway servers IP address range	3.35.160.0/22

Category	Details
WSP gateway domain name	*.prod.ap-northeast-2.highlander.aws.a2z.com
Management interface IP address ranges	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Asia Pacific (Singapore)

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain: https://skylight-client-ds.ap-southeast-1.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.ap-southeast-1.amazonaws.com
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings:

Category	Details
	• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Login page graphics for customer directory level co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • Asia Pacific (Singapore) — https://d3qzmd7y07pz0i.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
WS Broker	Domain: • https://ws-broker-service.ap-southeast-1.amazonaws.com

Category	Details
WorkSpaces API Endpoints	Domain: • https://workspaces.ap-southeast-1.amazonaws.com
Session Broker (PCM)	Domain: • https://skylight-cm.ap-southeast-1.amazonaws.com
Web Access TURN Servers for PCoIP	Server: • turn:*.ap-southeast-1.rdn.amazonaws.com
Health check hostname	drp-sin.amazonworkspaces.com
Health check IP addresses	• 3.0.212.144 • 18.138.99.116 • 18.140.252.123 • 52.74.175.118
PCoIP gateway servers public IP address ranges	• 18.141.152.0 - 18.141.152.255 • 18.141.154.0 - 18.141.155.255 • 52.76.127.0 - 52.76.127.255
WSP gateway servers IP address range	13.212.132.0/22
WSP gateway domain name	*.prod.ap-southeast-1.highlander.aws.a2z.com
Management interface IP address ranges	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Asia Pacific (Sydney)

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain: https://skylight-client-ds.ap-southeast-2.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.ap-southeast-2.amazonaws.com
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Login page graphics for customer directory level co-branding:

Category	Details
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • Asia Pacific (Sydney) — https://dwcpoxuuza83q.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers
Pre-session Smart Card Authentication Endpoints	https://smartcard.ap-southeast-2.signin.aws
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
WS Broker	Domain: • https://ws-broker-service.ap-southeast-2.amazonaws.com
WorkSpaces API Endpoints	Domain: • https://workspaces.ap-southeast-2.amazonaws.com

Category	Details
Session Broker (PCM)	Domain: • https://skylight-cm.ap-southeast-2.amazonaws.com
Web Access TURN Servers for PCoIP	Server: • turn:*.ap-southeast-2.rdn.amazonaws.com
Health check hostname	drp-syd.amazonworkspaces.com
Health check IP addresses	• 3.24.11.127 • 13.237.232.125
PCoIP gateway servers public IP address ranges	• 3.25.43.0 - 3.25.43.255 • 3.25.44.0 - 3.25.45.255 • 54.153.254.0 - 54.153.254.255
WSP gateway servers IP address range	3.25.248.0/22
WSP gateway domain name	*.prod.ap-southeast-2.highlander.aws.a2z.com
Management interface IP address ranges	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, and 198.19.0.0/16 • WSP: 10.0.0.0/8

Asia Pacific (Tokyo)

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/
Connectivity Check	https://connectivity.amazonworkspaces.com/

Category	Details
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain: https://skylight-client-ds.ap-northeast-1.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.ap-northeast-1.amazonaws.com

Category	Details
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Login page graphics for customer directory level co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • Asia Pacific (Tokyo) — https://d2c2t8mxjhq5z1.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers

Category	Details
Pre-session Smart Card Authentication Endpoints	https://smartcard.ap-northeast-1.signin.aws
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
WS Broker	Domain: • https://ws-broker-service.ap-northeast-1.amazonaws.com
WorkSpaces API Endpoints	Domain: • https://workspaces.ap-northeast-1.amazonaws.com
Session Broker (PCM)	Domain: • https://skylight-cm.ap-northeast-1.amazonaws.com
Web Access TURN Servers for PCoIP	Server: • turn:*.ap-northeast-1.rdn.amazonaws.com
Health check hostname	drp-nrt.amazonworkspaces.com
Health check IP addresses	• 18.178.102.247 • 54.64.174.128
PCoIP gateway servers public IP address ranges	• 18.180.178.0 - 18.180.178.255 • 18.180.180.0 - 18.180.181.255 • 54.250.251.0 - 54.250.251.255
WSP gateway servers IP address range	3.114.164.0/22

Category	Details
WSP gateway domain name	*.prod.ap-northeast-1.highlander.aws.a2z.com
Management interface IP address ranges	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Canada (Central)

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain: https://skylight-client-ds.ca-central-1.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.ca-central-1.amazonaws.com
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/

Category	Details
	Customer directory settings: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Login page graphics for customer directory level co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • Canada (Central) — https://d2wfbsypmqjmog.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
WS Broker	Domain: • https://ws-broker-service.ca-central-1.amazonaws.com

Category	Details
WorkSpaces API Endpoints	Domain: • https://workspaces.ca-central-1.amazonaws.com
Session Broker (PCM)	Domain: • https://skylight-cm.ca-central-1.amazonaws.com
Web Access TURN Servers for PCoIP	Server: • turn:*.ca-central-1.rdn.amazonaws.com
Health check hostname	drp-yul.amazonworkspaces.com
Health check IP addresses	• 52.60.69.16 • 52.60.80.237 • 52.60.173.117 • 52.60.201.0
PCoIP gateway servers public IP address ranges	• 15.223.100.0 - 15.223.100.255 • 15.223.102.0 - 15.223.103.255 • 35.183.255.0 - 35.183.255.255
WSP gateway servers IP address range	3.97.20.0/22
WSP gateway domain name	*.prod.ca-central-1.highlander.aws.a2z.com
Management interface IP address ranges	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Europe (Frankfurt)

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain: https://skylight-client-ds.eu-central-1.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.eu-central-1.amazonaws.com
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Login page graphics for customer directory level co-branding:

Category	Details
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • Europe (Frankfurt) — https://d1whcm49570jjw.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
WS Broker	Domain: • https://ws-broker-service.eu-central-1.amazonaws.com
WorkSpaces API Endpoints	Domain: • https://workspaces.eu-central-1.amazonaws.com
Session Broker (PCM)	Domain: • https://skylight-cm.eu-central-1.amazonaws.com

Category	Details
Web Access TURN Servers for PCoIP	Server: • turn:*.eu-central-1.rdn.amazonaws.com
Health check hostname	drp-fra.amazonworkspaces.com
Health check IP addresses	• 52.59.191.224 • 52.59.191.225 • 52.59.191.226 • 52.59.191.227
PCoIP gateway servers public IP address ranges	• 18.156.52.0 - 18.156.52.255 • 18.156.54.0 - 18.156.55.255 • 52.59.127.0 - 52.59.127.255
WSP gateway servers IP address range	18.192.216.0/22
WSP gateway domain name	*.prod.eu-central-1.highlander.aws.a2z.com
Management interface IP address ranges	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Europe (Ireland)

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain:

Category	Details
	https://skylight-client-ds.eu-west-1.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.eu-west-1.amazonaws.com

Category	Details
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Login page graphics for customer directory level co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • Europe (Ireland) — https://d3pgffbf39h4k4.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers

Category	Details
Pre-session Smart Card Authentication Endpoints	https://smartcard.eu-west-1.signin.aws
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
WS Broker	Domain: • https://ws-broker-service.eu-west-1.amazonaws.com
WorkSpaces API Endpoints	Domain: • https://workspaces.eu-west-1.amazonaws.com
Session Broker (PCM)	Domain: • https://skylight-cm.eu-west-1.amazonaws.com
Web Access TURN Servers for PCoIP	Server: • turn:*.eu-west-1.rdn.amazonaws.com
Health check hostname	drp-dub.amazonworkspaces.com
Health check IP addresses	• 18.200.177.86 • 52.48.86.38 • 54.76.137.224
PCoIP gateway servers public IP address ranges	• 3.249.28.0 - 3.249.29.255 • 52.19.124.0 - 52.19.125.255
WSP gateway servers IP address range	3.248.176.0/22

Category	Details
WSP gateway domain name	*.prod.eu-west-1.highlander.aws.a2z.com
Management interface IP address ranges	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, and 198.19.0.0/16 • WSP: 10.0.0.0/8

Europe (London)

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain: https://skylight-client-ds.eu-west-2.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.eu-west-2.amazonaws.com
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/

Category	Details
	Customer directory settings: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Login page graphics for customer directory level co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • Europe (London) — https://d16q6638mh01s7.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
WS Broker	Domain: • https://ws-broker-service.eu-west-2.amazonaws.com

Category	Details
WorkSpaces API Endpoints	Domain: • https://workspaces.eu-west-2.amazonaws.com
Session Broker (PCM)	Domain: • https://skylight-cm.eu-west-2.amazonaws.com
Web Access TURN Servers for PCoIP	Server: • turn:*.eu-west-2.rdn.amazonaws.com
Health check hostname	drp-lhr.amazonworkspaces.com
Health check IP addresses	• 35.176.62.54 • 35.177.255.44 • 52.56.46.102 • 52.56.111.36
PCoIP gateway servers public IP address ranges	• 18.132.21.0 - 18.132.21.255 • 18.132.22.0 - 18.132.23.255 • 35.176.32.0 - 35.176.32.255
WSP gateway servers IP address range	18.134.68.0/22
WSP gateway domain name	*.prod.eu-west-2.highlander.aws.a2z.com
Management interface IP address ranges	• 198.19.0.0/16 • WSP: 10.0.0.0/8

South America (São Paulo)

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain: https://skylight-client-ds.sa-east-1.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.sa-east-1.amazonaws.com
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Login page graphics for customer directory level co-branding:

Category	Details
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • South America (São Paulo) — https://d2lh2qc5bdoq4b.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
WS Broker	Domain: • https://ws-broker-service.sa-east-1.amazonaws.com
WorkSpaces API Endpoints	Domain: • https://workspaces.sa-east-1.amazonaws.com
Session Broker (PCM)	Domain: • https://skylight-cm.sa-east-1.amazonaws.com

Category	Details
Web Access TURN Servers for PCoIP	Server: • turn:*.sa-east-1.rdn.amazonaws.com
Health check hostname	drp-gru.amazonworkspaces.com
Health check IP addresses	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
PCoIP gateway servers public IP address ranges	• 18.230.103.0 - 18.230.103.255 • 18.230.104.0 - 18.230.105.255 • 54.233.204.0 - 54.233.204.255
WSP gateway servers IP address range	15.228.64.0/22
WSP gateway domain name	*.prod.sa-east-1.highlander.aws.a2z.com
Management interface IP address ranges	• 198.19.0.0/16 • WSP: 10.0.0.0/8

Africa (Cape Town)

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain:

Category	Details
	https://skylight-client-ds.af-south-1.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.af-south-1.amazonaws.com

Category	Details
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Login page graphics for customer directory level co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • Africa (Cape Town); — https://di5ygl2cs0mrh.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers

Category	Details
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
WS Broker	Domain: • https://ws-broker-service.af-south-1.amazonaws.com
WorkSpaces API Endpoints	Domain: • https://workspaces.af-south-1.amazonaws.com
Session Broker (PCM)	Domain: • https://skylight-cm.af-south-1.amazonaws.com
Health check hostname	drp-cpt.amazonworkspaces.com
Health check IP addresses	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
PCoIP gateway servers public IP address ranges	• 13.246.120.0 - 13.246.123.255
WSP gateway servers IP address range	15.228.64.0/22
WSP gateway domain name	*.prod.af-south-1.highlander.aws.a2z.com
Management interface IP address ranges	• 172.31.0.0/16 and 198.19.0.0/16 • WSP: 10.0.0.0/8

Israel (Tel Aviv)

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain: https://skylight-client-ds.il-central-1.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.il-central-1.amazonaws.com
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Login page graphics for customer directory level co-branding:

Category	Details
	• CSS file to style the login pages: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript file for the login pages: • Israel (Tel Aviv); —
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
WS Broker	Domain: • https://ws-broker-service.il-central-1.amazonaws.com
WorkSpaces API Endpoints	Domain: • https://workspaces.il-central-1.amazonaws.com
Session Broker (PCM)	Domain: • https://skylight-cm.il-central-1.amazonaws.com

Category	Details
Web Access TURN Servers for PCoIP	Server: • turn:*.il-central-1.rdn.amazonaws.com
Health check hostname	drp-tlv.amazonworkspaces.com
Health check IP addresses	• 51.17.52.90 • 51.17.109.231 • 51.16.190.43
PCoIP gateway servers public IP address ranges	• 51.17.28.0-51.17.31.255
WSP gateway servers IP address range	51.17.72.0/22
WSP gateway domain name	*.prod.il-central-1.highlander.aws.a2z.com
Management interface IP address ranges	• 198.19.0.0/16 • WSP: 10.0.0.0/8

AWS GovCloud (US-West) Region

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://s3.amazonaws.com/workspaces-client-updates/prod/pdt/windows/WorkSpacesAppCast.xml
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain:

Category	Details
	hhttps://skylight-client-ds.us-gov-west-1.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.us-gov-west-1.amazonaws.com

Category	Details
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings: • https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/<directory ID> Login page graphics for customer directory level co-branding: • https://s3.amazonaws.com/workspaces-client-assets/prod/pdt/<directory ID> CSS file to style the login pages: • https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css JavaScript file for the login pages: • Not applicable
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers

Category	Details
Pre-session Smart Card Authentication Endpoints	https://smartcard.signin.amazonaws-us-gov.com
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://login.us-gov-home.awsapps.com/directory/<directory id>/ (where <directory id> is the customer's domain)
WS Broker	Domain: • https://ws-broker-service.us-gov-west-1.amazonaws.com • https://ws-broker-service-fips.us-gov-west-1.amazonaws.com
WorkSpaces API Endpoints	Domain: • https://workspaces.us-gov-west-1.amazonaws.com • https://workspaces-fips.us-gov-west-1.amazonaws.com
Session Broker (PCM)	Domain: • https://skylight-cm.us-gov-west-1.amazonaws.com • https://skylight-cm-fips.us-gov-west-1.amazonaws.com
Health check hostname	drp-pdt.amazonworkspaces.com

Category	Details
Health check IP addresses	• 52.61.60.65 • 52.61.65.14 • 52.61.88.170 • 52.61.137.87 • 52.61.155.110 • 52.222.20.88
PCoIP gateway servers public IP address ranges	• 52.61.193.0 - 52.61.193.255
WSP gateway servers IP address range	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
WSP gateway domain name	*.prod.us-gov-west-1.highlander.aws.a2z.com
Management interface IP address ranges	• 198.19.0.0/16 • WSP: 10.0.0.0/8 and 192.169.0.0/16

AWS GovCloud (US-East) Region

Domains and IP Addresses to add to your allowlist

Category	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Client Auto-update	https://s3.amazonaws.com/workspaces-client-updates/prod/osu/windows/WorkSpacesAppCast.xml
Connectivity Check	https://connectivity.amazonworkspaces.com/
Client Metrics (for 3.0+ WorkSpaces client applications)	Domain:

Category	Details
	hhttps://skylight-client-ds.us-gov-east-1.amazonaws.com
Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)	Domain: https://ws-client-service.us-gov-east-1.amazonaws.com

Category	Details
Directory Settings	Authentication from the client to the customer directory before login to the WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Connections from macOS clients: • https://d32i4gd7pg4909.cloudfront.net/ Customer directory settings: • https://s3.amazonaws.com/workspaces-client-properties/prod/osu/<directory ID> Login page graphics for customer directory level co-branding: • https://s3.amazonaws.com/workspaces-client-assets/prod/osu/<directory ID> CSS file to style the login pages: • https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css JavaScript file for the login pages: • Not applicable
Forrester Log Service	https://fls-na.amazon.com/
Health Check (DRP) Servers	Health check servers

Category	Details
Pre-session Smart Card Authentication Endpoints	https://smartcard.signin.amazonaws-us-gov.com
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
User Login Pages	https://login.us-gov-home.awsapps.com/directory/<directory id>/ (where <directory id> is the customer's domain)
WS Broker	Domain: • https://ws-broker-service.us-gov-east-1.amazonaws.com • https://ws-broker-service-fips.us-gov-east-1.amazonaws.com
WorkSpaces API Endpoints	Domain: • https://workspaces.us-gov-east-1.amazonaws.com • https://workspaces-fips.us-gov-east-1.amazonaws.com
Session Broker (PCM)	Domain: • https://skylight-cm.us-gov-east-1.amazonaws.com • https://skylight-cm-fips.us-gov-east-1.amazonaws.com
Health check hostname	drp-osu.amazonworkspaces.com
Health check IP addresses	• 18.253.251.70 • 18.254.0.118

Category	Details
PCoIP gateway servers public IP address ranges	• 18.254.140.0 - 18.254.143.255
WSP gateway servers IP address range	18.254.148.0/22
WSP gateway domain name	*.prod.us-gov-east-1.highlander.aws.a2z.com
Management interface IP address ranges	• 198.19.0.0/16 • WSP: 10.0.0.0/8

Client network requirements for WorkSpaces Personal

Your WorkSpaces users can connect to their WorkSpaces by using the client application for a supported device. Alternatively, they can use a web browser to connect to WorkSpaces that support this form of access. For a list of WorkSpaces that support web browser access, see "Which Amazon WorkSpaces bundles support web access?" in Client Access, Web Access, and User Experience.

Note

A web browser cannot be used to connect to Amazon Linux WorkSpaces.

Important

Beginning October 1, 2020, customers will no longer be able to use the Amazon WorkSpaces Web Access client to connect to Windows 7 custom WorkSpaces or to Windows 7 Bring Your Own License (BYOL) WorkSpaces.

To provide your users with a good experience with their WorkSpaces, verify that their client devices meet the following network requirements:

- The client device must have a broadband internet connection. We recommend planning for a minimum of 1 Mbps per simultaneous user watching a 480p video window. Depending on your user-quality requirements for video resolution, more bandwidth might be required.

- The network that the client device is connected to, and any firewall on the client device, must have certain ports open to the IP address ranges for various AWS services. For more information, see IP address and port requirements for WorkSpaces Personal.
- For the best performance for PCoIP, the round trip time (RTT) from the client's network to the Region that the WorkSpaces are in should be less than 100ms. If the RTT is between 100ms and 200ms, the user can access the WorkSpace, but performance is affected. If the RTT is between 200ms and 375ms, the performance is degraded. If the RTT exceeds 375ms, the WorkSpaces client connection is terminated.

  For the best performance for WorkSpaces Streaming Protocol (WSP), the RTT from the client's network to the Region that the WorkSpaces are in should be less than 250ms. If the RTT is between 250ms and 400ms, the user can access the WorkSpace, but the performance is degraded.

  To check the RTT to the various AWS Regions from your location, use the Amazon WorkSpaces Connection Health Check.
- To use webcams with WSP, we recommend a minimum upload bandwidth of 1.7 megabits per second.
- If users will access their WorkSpaces through a virtual private network (VPN), the connection must support a maximum transmission unit (MTU) of at least 1200 bytes.

  > **Note**
  >
  > You cannot access WorkSpaces through a VPN connected to your virtual private cloud (VPC). To access WorkSpaces using a VPN, internet connectivity (through the VPN's public IP addresses) is required, as described in IP address and port requirements for WorkSpaces Personal.

- The clients require HTTPS access to WorkSpaces resources hosted by the service and Amazon Simple Storage Service (Amazon S3). The clients do not support proxy redirection at the application level. HTTPS access is required so that users can successfully complete registration and access their WorkSpaces.
- To allow access from PCoIP zero client devices, you must be using a PCoIP protocol bundle for WorkSpaces. You must also enable Network Time Protocol (NTP) in Teradici. For more information, see Set up PCoIP zero clients for WorkSpaces Personal.
- For 3.0+ clients, if you are using single sign-on (SSO) for Amazon WorkDocs, you must follow the instructions in Single Sign-On in the *AWS Directory Service Administration Guide*.

You can verify that a client device meets the networking requirements as follows.

To verify networking requirements for 3.0+ clients

1. Open your WorkSpaces client. If this is the first time you have opened the client, you are prompted to enter the registration code that you received in the invitation email.
2. Depending on which client you're using, do one of the following.

If you're using...	Do this
Windows or Linux clients	In the upper-right corner of the client application, select the **Network** icon  .
macOS client	Choose **Connections**, **Network**.

   The client application tests the network connection, ports, and round-trip time, and reports the results of these tests.
3. Close the **Network** dialog box to return to the sign-in page.

To verify networking requirements for 1.0+ and 2.0+ clients

1. Open your WorkSpaces client. If this is the first time you have opened the client, you are prompted to enter the registration code that you received in the invitation email.
2. Choose **Network** in the lower-right corner of the client application. The client application tests the network connection, ports, and round-trip time, and reports the results of these tests.
3. Choose **Dismiss** to return to the sign-in page.

Restrict access to trusted devices for WorkSpaces Personal

By default, users can access their WorkSpaces from any supported device that is connected to the internet. If your company limits corporate data access to trusted devices (also known as managed devices), you can restrict WorkSpaces access to trusted devices with valid certificates.

> **Note**
>
> This feature is currently available only when your WorkSpaces Personal directories are managed through AWS Directory Service including Simple AD, AD Connector, and AWS Managed Microsoft AD directory.

When you enable this feature, WorkSpaces uses certificate-based authentication to determine whether a device is trusted. If the WorkSpaces client application can't verify that a device is trusted, it blocks attempts to log in or reconnect from the device.

For each directory, you can import up to two root certificates. If you import two root certificates, WorkSpaces presents them both to the client and the client finds the first valid matching certificate that chains up to either of the root certificates.

Supported clients

- Android, running on Android or Android-compatible Chrome OS systems
- macOS
- Windows

> **Important**
>
> This feature is not supported by the following clients:
>
> - WorkSpaces client applications for Linux or iPad
> - Third-party clients, including but not limited to, Teradici PCoIP, RDP clients, and remote desktop applications.

> **Note**
>
> When you enable access for specific clients, make sure that you block access for other device types that you don't need. For more information about how to do this, see Step 3.7 below.

Step 1: Create the certificates

This feature requires two types of certificates: root certificates generated by an internal Certificate Authority (CA) and client certificates that chain up to a root certificate.

Requirements

- Root certificates must be Base64-encoded certificate files in CRT, CERT, or PEM format.
- Root certificates must satisfy the following regular expression pattern, which means that every encoded line, beside the last one, has to be exactly 64 characters long: `-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64} \u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)`.
- Device certificates must include a Common Name.
- Device certificates must include the following extensions: `Key Usage: Digital Signature`, and `Enhanced Key Usage: Client Authentication`.
- All the certificates in the chain from the device certificate to the trusted root Certificate Authority must be installed on the client device.
- The maximum supported length of certificate chain is 4.
- WorkSpaces does not currently support device revocation mechanisms, such as certificate revocation lists (CRL) or Online Certificate Status Protocol (OCSP), for client certificates.
- Use a strong encryption algorithm. We recommend SHA256 with RSA, SHA256 with ECDSA, SHA384 with ECDSA, or SHA512 with ECDSA.
- For macOS, if the device certificate is in the system keychain, we recommend that you authorize the WorkSpaces client application to access those certificates. Otherwise, users must enter keychain credentials when they log in or reconnect.

Step 2: Deploy client certificates to the trusted devices

On the trusted devices for your users, you must install a certificate bundle that includes all the certificates in the chain from the device certificate to the trusted root Certificate Authority. You can use your preferred solution to install certificates to your fleet of client devices; for example, System Center Configuration Manager (SCCM) or mobile device management (MDM). Note that SCCM and MDM can optionally perform a security posture assessment to determine whether the devices meet your corporate policies to access WorkSpaces.

The WorkSpaces client applications search for certificates as follows:

- Android - Go to **Settings**, choose **Security & location**, **Credentials**, then choose **Install from SD card**.
- Android-compatible Chrome OS systems - Open Android settings and choose **Security & location**, **Credentials**, then choose **Install from SD card**.
- macOS - Searches the keychain for client certificates.
- Windows - Searches the user and root certificate stores for client certificates.

Step 3: Configure the restriction

After you have deployed the client certificates on the trusted devices, you can enable restricted access at the directory level. This requires the WorkSpaces client application to validate the certificate on a device before allowing a user to log in to a WorkSpace.

To configure the restriction

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select the directory and then choose **Actions**, **Update Details**.
4. Expand **Access Control Options**.
5. Under **For each device type, specify which devices can access WorkSpaces**, choose **Trusted Devices**.
6. Import up to two root certificates. For each root certificate, do the following:
   a. Choose **Import**.
   b. Copy the body of the certificate to the form.
   c. Choose **Import**.
7. Specify whether other types of devices have access to WorkSpaces.
   a. Scroll down to the **Other Platforms** section. By default, WorkSpaces Linux clients are disabled, and users can access their WorkSpaces from their iOS devices, Android devices, Web Access, Chromebooks, and PCoIP zero client devices.
   b. Select the device types to enable and clear the device types to disable.
   c. To block access from all selected device types, choose **Block**.
8. Choose **Update and Exit**.

Integrate SAML 2.0 with WorkSpaces Personal

> **Note**
>
> SAML 2.0 is available only when your WorkSpaces Personal directories are managed through AWS Directory Service including Simple AD, AD Connector, and AWS Managed Microsoft AD directory. The feature doesn't apply to directories that are managed by Amazon WorkSpaces, which normally use IAM Identity Center for user authentication instead of SAML 2.0 federation.

Integrating SAML 2.0 with your WorkSpaces for desktop session authentication allows your users to use their existing SAML 2.0 identity provider (IdP) credentials and authentication methods through their default web browser. By using your IdP to authenticate users for WorkSpaces, you can protect WorkSpaces by employing IdP features like multi-factor authentication and contextual access policies.

Authentication workflow

The following sections describe the authentication workflow initiated by WorkSpaces client application, WorkSpaces Web Access, and a SAML 2.0 identity provider (IdP):

- When the flow is initiated by the IdP. For example, when users choose an application in the IdP user portal in a web browser.
- When the flow is initiated by the WorkSpaces client. For example, when users open the client application and sign in.
- When the flow is initiated by WorkSpaces Web Access. For example, when users open Web Access in a browser and sign in.

In these examples, users enter `user@example.com`to sign in to the IdP. The IdP has a SAML 2.0 service provider application configured for a WorkSpaces directory and users are authorized for the WorkSpaces SAML 2.0 application. Users create a WorkSpace for their usernames, `user`, in a directory that's enabled for SAML 2.0 authentication. Additionally, users install the WorkSpaces client application on their device or the user uses Web Access in a web browser.

Identity provider (IdP)-initiated flow with client application

The IdP-initiated flow allows users to automatically register the WorkSpaces client application on their devices without having to enter a WorkSpaces registration code. Users don't sign in to their WorkSpaces using the IdP-initiated flow. WorkSpaces authentication must originate from the client application.

1. Using their web browser, users sign in to the IdP.
2. After signing in to the IdP, users choose the WorkSpaces application from the IdP user portal.
3. Users are redirected to this page in the browser, and the WorkSpaces client application is opened automatically.

4. The WorkSpaces client application is now registered and users can continue to sign by clicking **Continue to sign in to WorkSpaces**.

Identity provider (IdP)-initiated flow with Web Access

The IdP-initiated Web Access flow allows users to automatically register their WorkSpaces through a web browser without having to enter a WorkSpaces registration code. Users don't sign in to their WorkSpaces using the IdP-initiated flow. WorkSpaces authentication must originate from Web Access.

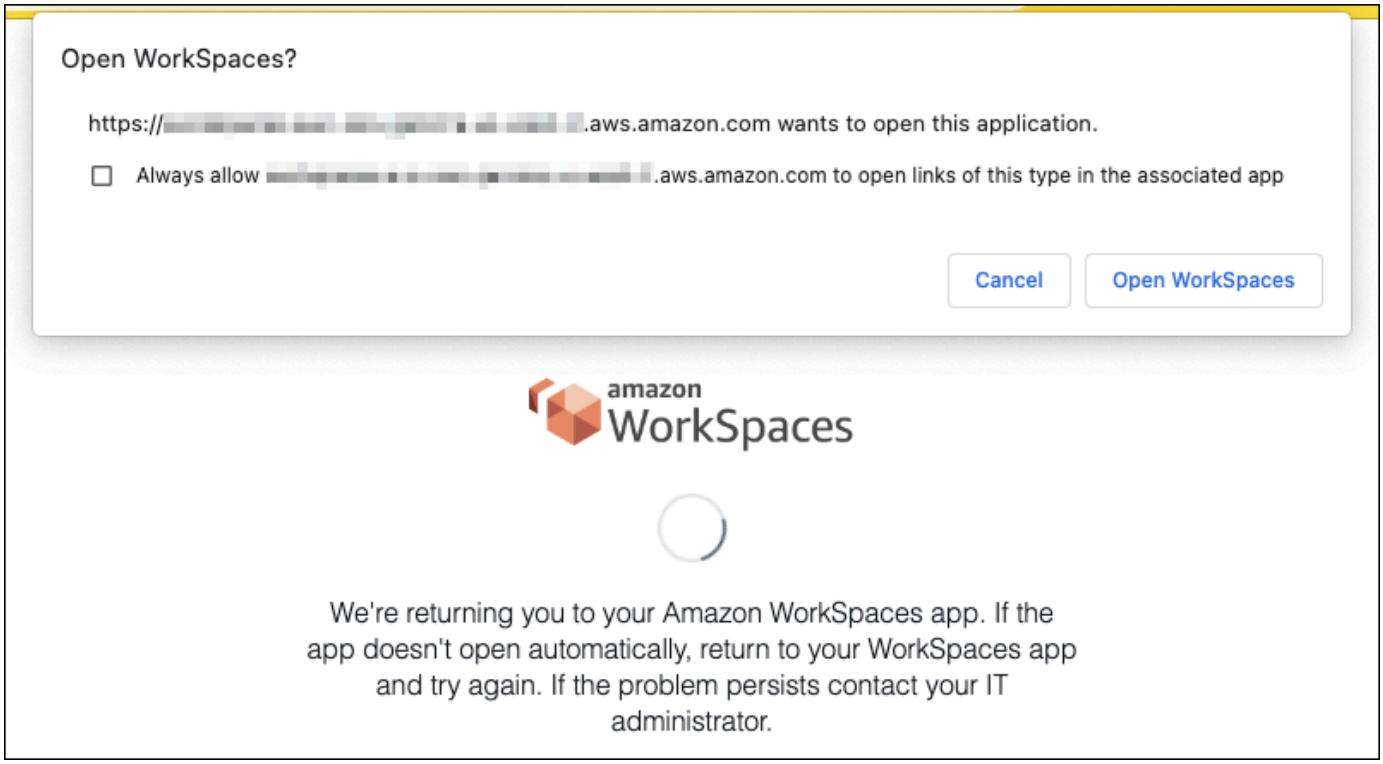
1. Using their web browser, users sign in to the IdP.
2. After signing in to the IdP, users click the WorkSpaces application from the IdP user portal.
3. Users are redirected to this page in the browser. To open WorkSpaces, choose **Amazon WorkSpaces in the browser**.

4. The WorkSpaces client application is now registered and users can continue to sign in through WorkSpaces Web Access.

WorkSpaces client-initiated flow

The client-initiated flow allows users to sign in to their WorkSpaces after signing in to an IdP.

1. Users launch the WorkSpaces client application (if it isn't already running) and clicks **Continue to sign in to WorkSpaces**.
2. Users are redirected to their default web browser to sign in to the IdP. If the users are already signed in to the IdP in their browser, they don't need to sign in again and will skip this step.
3. Once signed in to the IdP, users are redirected to a pop up. Follow the prompts to allow your web browser to open the client application.



4. Users are redirected to the WorkSpaces client application to complete sign in to their WorkSpace. WorkSpaces usernames are populated automatically from the IdP SAML 2.0 assertion. When you use certificate-based authentication (CBA) , users are automatically signed in.
5. Users are signed in to their WorkSpace.

WorkSpaces Web Access-initiated flow

The Web Access-initiated flow allows users to sign in to their WorkSpaces after signing in to an IdP.

1. Users launch the WorkSpaces Web Access and chooses **Sign in**.
2. In the same browser tab, users are redirected to IdP portal. If the users are already signed in to the IdP in their browser, they don't need to sign in again and can skip this step.
3. Once signed in to the IdP, users redirected to this page in the browser, and clicks **Log in to WorkSpaces**.
4. Users redirected to the WorkSpaces client application to complete sign in to their WorkSpace. WorkSpaces usernames are populated automatically from the IdP SAML 2.0 assertion. When you use certificate-based authentication (CBA) , users are automatically signed in.
5. Users are signed in to their WorkSpace.

Setting up SAML 2.0

Enable WorkSpaces client application registration and signing in to WorkSpaces for your users by using their SAML 2.0 identity provider (IdP) credentials and authentication methods by setting up identity federation using SAML 2.0. To set up identity federation using SAML 2.0, use an IAM role and a relay state URL to configure your IdP and enable AWS. This grants your federated users access to a WorkSpaces directory. The relay state is the WorkSpaces directory endpoint to which users are forwarded after successfully signing in to AWS.

Contents

Requirements

- SAML 2.0 authentication is available in the following Regions:
  - US East (N. Virginia) Region
  - US West (Oregon) Region
  - Africa (Cape Town) Region
  - Asia Pacific (Mumbai) Region
  - Asia Pacific (Seoul) Region
  - Asia Pacific (Singapore) Region
  - Asia Pacific (Sydney) Region
  - Asia Pacific (Tokyo) Region
  - Canada (Central) Region
  - Europe (Frankfurt) Region

  - Europe (Ireland) Region
  - Europe (London) Region
  - South America (São Paulo) Region
  - Israel (Tel Aviv) Region
  - AWS GovCloud (US-West)
  - AWS GovCloud (US-East)
- To use SAML 2.0 authentication with WorkSpaces,the IdP must support unsolicited IdP-initiated SSO with a deep link target resource or relay state endpoint URL. Examples of IdPs include ADFS, Azure AD, Duo Single Sign-On, Okta, PingFederate, and PingOne. Consult your IdP documentation for more information.
- SAML 2.0 authentication will function with WorkSpaces launched using Simple AD, but this isn't recommended as Simple AD doesn't integrate with SAML 2.0 IdPs.
- SAML 2.0 authentication is supported on the following WorkSpaces clients. Other client versions are unsupported for SAML 2.0 authentication. Open Amazon WorkSpaces Client Downloads to find the latest versions:
  - Windows client application version 5.1.0.3029 or later
  - macOS client version 5.x or later
  - Linux client for Ubuntu 22.04 version 2024.1 or later, Ubuntu 20.04 version 24.1 or later
  - Web Access

  Other client versions won't be able to connect to WorkSpaces enabled for SAML 2.0 authentication unless fallback is enabled. For more information, see Enable SAML 2.0 authentication on the WorkSpaces directory.

For step-by-step instructions to integrate SAML 2.0 with WorkSpaces using ADFS, Azure AD, Duo Single Sign-On, Okta, OneLogin, PingFederate and PingOne for Enterprise, review the Amazon WorkSpaces SAML Authentication Implementation Guide.

Prerequisites

Complete the following prerequisites before configuring your SAML 2.0 identity provider (IdP) connection to a WorkSpaces directory.

1. Configure your IdP to integrate user identities from the Microsoft Active Directory that is used with the WorkSpaces directory. For a user with a WorkSpace, the **sAMAccountName** and **email**

attributes for the Active Directory user and the SAML claim values must match for the user to sign in to WorkSpaces using the IdP. For more information about integrating Active Directory with your IdP, consult your IdP documentation.

2. Configure your IdP to establish a trust relationship with AWS.

   - See Integrating third-party SAML solution providers with AWS for more information on configuring AWS federation. Relevant examples include IdP integration with AWS IAM to access the AWS management console.
   - Use your IdP to generate and download a federation metadata document that describes your organization as an IdP. This signed XML document is used to establish the relying party trust. Save this file to a location that you can access from the IAM console later.

3. Create or register a directory for WorkSpaces by using the WorkSpaces management console. For more information, see Manage directories for WorkSpaces. SAML 2.0 authentication for WorkSpaces is supported for the following directory types:

   - AD Connector
   - AWS Managed Microsoft AD

4. Create a WorkSpace for a user who can sign in to the IdP using a supported directory type. You can create a WorkSpace using the WorkSpaces management console, AWS CLI, or WorkSpaces API. For more information, see Launch a virtual desktop using WorkSpaces.

Step 1: Create a SAML identity provider in AWS IAM

First, create a SAML IdP in AWS IAM. This IdP defines your organization's IdP-to-AWS trust relationship using the metadata document generated by the IdP software in your organization. For more information, see Creating and managing a SAML identity provider (Amazon Web Services Management Console). For information about working with SAML IdPs in AWS GovCloud (US-West)and AWS GovCloud (US-East), see AWS Identity and Access Management.

Step 2: Create a SAML 2.0 federation IAM role

Next, create a SAML 2.0 federation IAM role. This step establishes a trust relationship between IAM and your organization's IdP, which identifies your IdP as a trusted entity for federation.

To create an IAM role for SAML IdP

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Roles** > **Create role**.

3. For **Role type**, choose **SAML 2.0 federation**.
4. For **SAML Provider** select the SAML IdP that you created.

> **Important**
>
> Don't choose either of the two SAML 2.0 access methods, **Allow programmatic access only** or **Allow programmatic and Amazon Web Services Management Console access**.

5. For **Attribute**, choose **SAML:sub_type**.
6. For **Value** enter `persistent`. This value restricts role access to SAML user streaming requests that include a SAML subject type assertion with a value of persistent. If the SAML:sub_type is persistent, your IdP sends the same unique value for the NameID element in all SAML requests from a particular user. For more information about the SAML:sub_type assertion, see the **Uniquely identifying users in SAML-based federation** section in Using SAML-based federation for API access to AWS.
7. Review your SAML 2.0 trust information, confirming the correct trusted entity and condition, and then choose **Next: Permissions**.
8. On the **Attach permissions policies** page, choose **Next: Tags**.
9. (Optional) Enter a key and value for each tag that you want to add. For more information, see Tagging IAM users and roles.
10. When you're done, choose **Next: Review**. You'll create and embed an inline policy for this role later.
11. For **Role name**, enter a name that identifies the purpose of this role. Because multiple entities might reference the role, you can't edit the role's name once it is created.
12. (Optional) For **Role description**, enter a description for the new role.
13. Review the role details and choose **Create role**.
14. Add the sts:TagSession permission to your new IAM role's trust policy. For more information, see Passing session tags in AWS STS. In your new IAM role's details, choose the **Trust relationships** tab, and then choose **Edit trust relationship***. When Edit Trust Relationship policy editor opens, add the **sts:TagSession*** permission, as follows:

```
{
    "Version": "2012-10-17",
    "Statement": [{
```

```
        "Effect": "Allow",
        "Principal": {
            "Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/
IDENTITY-PROVIDER"
        },
        "Action": [
            "sts:AssumeRoleWithSAML",
            "sts:TagSession"
        ],
        "Condition": {
            "StringEquals": {
                "SAML:aud": "https://signin.aws.amazon.com/saml"
            }
        }
    }]
}
```

Replace `IDENTITY-PROVIDER` with the name of the SAML IdP you created in Step 1. Then choose **Update Trust Policy**.

Step 3: Embed an inline policy for the IAM role

Next, embed an inline IAM policy for the role that you created. When you embed an inline policy, the permissions in that policy can't be accidentally attached to the wrong principal entity. The inline policy provides federated users with access to the WorkSpaces directory.

> **Important**
>
> IAM policies to manage access to AWS based on the source IP are not supported for the `workspaces:Stream` action. To manage IP access controls for WorkSpaces, use IP access control groups. Additionally, when using SAML 2.0 authentication you can use IP access control policies if they are available from your SAML 2.0 IdP.

1. In the details for the IAM role that you created, choose the **Permissions** tab, and then add required permissions to the role's permissions policy. The **Create policy wizard** will start.
2. In **Create policy**, choose the **JSON** tab.
3. Copy and paste the following JSON policy into the JSON window. Then, modify the resource by entering your AWS Region Code, account ID, and directory ID. In the following policy,

`"Action": "workspaces:Stream"` is the action that provides your WorkSpaces users with permissions to connect to their desktop sessions in the WorkSpaces directory.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-
HYPHENS:directory/DIRECTORY-ID",
            "Condition": {
                "StringEquals": {
                    "workspaces:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

Replace `REGION-CODE` with the AWS Region where your WorkSpaces directory exists. Replace `DIRECTORY-ID` with the WorkSpaces directory ID, which can be found in the WorkSpaces management console. For resources in AWS GovCloud (US-West) or AWS GovCloud (US-East), use the following format for the ARN: `arn:aws-us-gov:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-HYPHENS:directory/DIRECTORY-ID`.

4. When you're done, choose **Review policy**. The Policy Validator will report any syntax errors.

Step 4: Configure your SAML 2.0 identity provider

Next, depending on your SAML 2.0 IdP, you may need to manually update your IdP to trust AWS as a service provider by uploading the `saml-metadata.xml` file at https://signin.aws.amazon.com/static/saml-metadata.xml to your IdP. This step updates your IdP's metadata. For some IdPs, the update may already be configured. If this is the case, proceed to the next step.

If this update isn't already configured in your IdP, review the documentation provided by your IdP for information about how to update the metadata. Some providers give you the option to type the URL, and the IdP obtains and installs the file for you. Others require you to download the file from the URL and then provide it as a local file.

> **Important**
>
> At this time, you can also authorize users in your IdP to access the WorkSpaces application you have configured in your IdP. Users who are authorized to access the WorkSpaces application for your directory don't automatically have a WorkSpace created for them. Likewise, users that have a WorkSpace created for them are not automatically authorized to access the WorkSpaces application. To successfully connect to a WorkSpace using SAML 2.0 authentication, a user must be authorized by the IdP and must have a WorkSpace created.

Step 5: Create assertions for the SAML authentication response

Next, configure the information that your IdP sends to AWS as SAML attributes in its authentication response. Depending on your IdP, this is already configured, skip this step and continue to Step 6: Configure the relay state of your federation.

If this information isn't already configured in your IdP, provide the following:

- **SAML Subject NameID** – The unique identifier for the user who is signing in. The value must match the WorkSpaces user name, and is typically the **sAMAccountName** attribute for the Active Directory user.
- **SAML Subject Type** (with a value set to `persistent`) – Setting the value to `persistent` ensures that your IdP sends the same unique value for the `NameID` element in all SAML requests from a particular user. Make sure that your IAM policy includes a condition to only allow SAML requests with a SAML sub_type set to `persistent`, as described in Step 2: Create a SAML 2.0 federation IAM role.
- **`Attribute` element with the `Name` attribute set to `https://aws.amazon.com/SAML/Attributes/Role`** – This element contains one or more `AttributeValue` elements that list the IAM role and SAML IdP to which the user is mapped by your IdP. The role and IdP are specified as a comma-delimited pair of ARNs. An example of the expected value is `arn:aws:iam::ACCOUNTNUMBER:role/ROLENAME,arn:aws:iam::ACCOUNTNUMBER:saml-provider/PROVIDERNAME`.
- **`Attribute` element with the `Name` attribute set to `https://aws.amazon.com/SAML/Attributes/RoleSessionName`** – This element contains one `AttributeValue` element that provides an identifier for the AWS temporary credentials that are issued for SSO. The value in the `AttributeValue` element must be between 2 and 64 characters long, can contain only alphanumeric characters, underscores, and the following characters: **_ . : / = + - @**. It

can't contain spaces. The value is typically an email address or a user principal name (UPN). It shouldn't be a value that includes a space, such as a user's display name.

- **`Attribute` element with the `Name` attribute set to `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`** – This element contains one `AttributeValue` element that provides the email address of the user. The value must match the WorkSpaces user email address as defined in the WorkSpaces directory. Tag values may include combinations of letters, numbers, spaces, and **_ . : / = + - @** characters. For more information, see Rules for tagging in IAM and AWS STS in the *IAM User Guide*.
- **`Attribute` element with the `Name` attribute set to `https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName` (optional)** – This element contains one `AttributeValue` element that provides the Active Directory `userPrincipalName` for the user who is signing in. The value must be provided in the format of `username@domain.com`. This parameter is used with certificate-based authentication as the Subject Alternative Name in the end user certificate. For more information, see Certificate-Based Authentication.
- **`Attribute` element with the `Name` attribute set to `https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid` (optional)** – This element contains one `AttributeValue` element that provides the Active Directory security identifier (SID) for the user who is signing in. This parameter is used with certificate-based authentication to enable strong mapping to the Active Directory user. For more information, see Certificate-Based Authentication.
- **`Attribute` element with the `Name` attribute set to `https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUserName` (optional)** – This element contains one `AttributeValue` element that provides an alternative user name format. Use this attribute if you have use cases that require user name formats such as `corp\username`, `corp.example.com\username`, or `username@corp.example.com` to login using the WorkSpaces client. Tag keys and values can include any combination of letters, numbers, spaces, and **_ : / . + = @ -** characters. For more information, see Rules for tagging in IAM and AWS STS in the *IAM User Guide*. To claim `corp\username` or `corp.example.com\username` formats, replace **** with **/**in the SAML assertion.
- **`Attribute`element with the `Name` attribute set to https://aws.amazon.com/SAML/Attributes/PrincipalTag:Domain (optional)** – This element contains one `AttributeValue` element that provides the Active Directory DNS fully qualified domain name (FQDN) for users signing in. This parameter is used with certificate-based authentication when the Active Directory `userPrincipalName` for the user contains an alternative suffix. The value must be provided in the `domain.com`, including any subdomains.

- **`Attribute` element with the `Name` attribute set to https://aws.amazon.com/SAML/Attributes/SessionDuration (optional)** – This element contains one `AttributeValue` element that specifies the maximum amount of time that a federated streaming session for a user can remain active before reauthentication is required. The default value is 3600 seconds (60 minutes). For more information, see the SAML `SessionDurationAttribute`.

> **Note**
>
> Although `SessionDuration` is an optional attribute, we recommend that you include it in the SAML response. If you don't specify this attribute, the session duration is set to a default value of 3600 seconds (60 minutes). WorkSpaces desktop sessions are disconnected after their session duration expires.

For more information about how to configure these elements, see Configuring SAML assertions for the authentication response in the *IAM User Guide*. For information about specific configuration requirements for your IdP, see your IdP's documentation.

Step 6: Configure the relay state of your federation

Next, use your IdP to configure the relay state of your federation to point to the WorkSpaces directory relay state URL. After successful authentication by AWS, the user is directed to the WorkSpaces directory endpoint, defined as the relay state in the SAML authentication response.

The following is the relay state URL format:

```
https://relay-state-region-endpoint/sso-idp?registrationCode=registration-code
```

Construct your relay state URL from your WorkSpaces directory registration code and the relay state endpoint associated with the Region in which your directory is located. The registration code can be found in the WorkSpaces management console.

Optionally, if you are using cross-region redirection for WorkSpaces, you can substitute the registration code with the fully qualified domain name (FQDN) associated with directories in your primary and failover Regions. For more information, see Cross-region redirection for Amazon WorkSpaces. When using cross-region redirection and SAML 2.0 authentication, both primary and failover directories need to be enabled for SAML 2.0 authentication and independently configured

with the IdP, using the relay state endpoint associated with each Region. This will allow the FQDN to be configured correctly when users register their WorkSpaces client applications before signing in, and will allow users to authenticate during a failover event.

The following table lists the relay state endpoints for the Regions where WorkSpaces SAML 2.0 authentication is available.

Regions where WorkSpaces SAML 2.0 authentication is available

Region	Relay state endpoint
US East (N. Virginia) Region	• workspaces.euc-sso.us-east-1.aws.amazon.com • (FIPS) workspaces.euc-sso-fips.us-east-1.aws.amazon.com
US West (Oregon) Region	• workspaces.euc-sso.us-west-2.aws.amazon.com • (FIPS) workspaces.euc-sso-fips.us-west-2.aws.amazon.com
Africa (Cape Town) Region	workspaces.euc-sso.af-south-1.aws.amazon.com
Asia Pacific (Mumbai) Region	workspaces.euc-sso.ap-south-1.aws.amazon.com
Asia Pacific (Seoul) Region	workspaces.euc-sso.ap-northeast-2.aws.amazon.com
Asia Pacific (Singapore) Region	workspaces.euc-sso.ap-southeast-1.aws.amazon.com
Asia Pacific (Sydney) Region	workspaces.euc-sso.ap-southeast-2.aws.amazon.com
Asia Pacific (Tokyo) Region	workspaces.euc-sso.ap-northeast-1.aws.amazon.com

Region	Relay state endpoint
Canada (Central) Region	workspaces.euc-sso.ca-central-1.aws.amazon.com
Europe (Frankfurt) Region	workspaces.euc-sso.eu-central-1.aws.amazon.com
Europe (Ireland) Region	workspaces.euc-sso.eu-west-1.aws.amazon.com
Europe (London) Region	workspaces.euc-sso.eu-west-2.aws.amazon.com
South America (São Paulo) Region	workspaces.euc-sso.sa-east-1.aws.amazon.com
Israel (Tel Aviv) Region	workspaces.euc-sso.il-central-1.aws.amazon.com
AWS GovCloud (US-West)	• workspaces.euc-sso.us-gov-west-1.amazonaws-us-gov.com • (FIPS) workspaces.euc-sso-fips.us-gov-west-1.amazonaws-us-gov.com **Note** For more information about, see Amazon WorkSpaces in the *AWS GovCloud (US) User Guide*.

Region	Relay state endpoint
AWS GovCloud (US-East)	• workspaces.euc-sso.us-gov-east-1.amazonaws-us-gov.com • (FIPS) workspaces.euc-sso-fips.us-gov-east-1.amazonaws-us-gov.com **Note** For more information about, see Amazon WorkSpaces in the *AWS GovCloud (US) User Guide*.

Step 7: Enable integration with SAML 2.0 on your WorkSpaces directory

You can use the WorkSpaces console to enable SAML 2.0 authentication on the WorkSpaces directory.

To enable integration with SAML 2.0

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Choose on the Directory ID for your WorkSpaces.
4. Under **Authentication**, choose **Edit**.
5. Choose **Edit SAML 2.0 Identity Provider**.
6. Check **Enable SAML 2.0 authentication**.
7. For the **User Access URL** and **IdP deep link parameter name**, enter values that are applicable to your IdP and the application you have configured in Step 1. The default value for the IdP deep link parameter name is “RelayState“ if you omit this parameter. The following table lists user access URL and parameter names that are unique to various identity providers for applications.

Domains and IP addresses to add to your allow list

Identity provider	Parameter	User access URL
ADFS	RelayState	https://<host>/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID=<relaying-party-uri>
Azure AD	RelayState	https://myapps.microsoft.com/signin/<app_id>?tenantId=<tenant_id>
Duo Single Sign-On	RelayState	https://<sub-domain>.sso.duosecurity.com/saml2/sp/<app_id>/sso
Okta	RelayState	https://<sub_domain>.okta.com/app/<app_name>/<app_id>/sso/saml
OneLogin	RelayState	https://<sub-domain>.onelogin.com/trust/saml2/http-post/sso/<app-id>
JumpCloud	RelayState	https://sso.jumpcloud.com/saml2/<app-id>
Auth0	RelayState	https://<DefaultTenatName>.us.auth0.com/samlp/<Client_Id>

Identity provider	Parameter	User access URL
PingFederate	`TargetResource`	`https://<host>/idp/startSSO.ping?PartnerSpId=<sp_id>`
PingOne for Enterprise	`TargetResource`	`https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=<app_id>&idpid=<idp_id>`

The user access URL is usually defined by the provider for unsolicited IdP-initiated SSO. A user can enter this URL in a web browser to federate directly to the SAML application. To test the user access URL and parameter values for your IdP, choose **Test**. Copy and paste the test URL to a private window in your current browser or another browser to test the SAML 2.0 logon without disrupting your current AWS management console session. When IdP-initiated flow opens, you can register your WorkSpaces client. For more information, see Identity provider (IdP)-initiated flow.

8. Manage fallback settings by checking or unchecking **Allow clients that do not support SAML 2.0 to login**. Enable this setting to continue providing your users access to WorkSpaces using client types or versions that do not support SAML 2.0 or if users need time to upgrade to the latest client version.

> **Note**
>
> This setting allows users to bypass SAML 2.0 and log in using directory authentication using older client versions.

9. To use SAML with the web client, enable Web Access. For more information, see Enable and configure Amazon WorkSpaces Web Access.

> **Note**
>
> PCoIP with SAML is not supported on Web Access.

10. Choose **Save**. Your WorkSpaces directory is now enabled with SAML 2.0 integration. You can use the IdP-initiated and client application-initiated flows to register WorkSpaces client applications and sign in to WorkSpaces.

Certificate-based authentication

You can use certificate-based authentication with WorkSpaces to remove the user prompt for the Active Directory domain password. By using certificate-based authentication with your Active Directory domain, you can:

- Rely on your SAML 2.0 identity provider to authenticate the user and provide SAML assertions to match the user in Active Directory.
- Enable a single sign-on logon experience with fewer user prompts.
- Enable passwordless authentication flows using your SAML 2.0 identity provider.

Certificate-based authentication uses AWS Private CA resources in your AWS account. AWS Private CA enables creation of private certificate authority (CA) hierarchies, including root and subordinate CAs. With AWS Private CA, you can create your own CA hierarchy and issue certificates with it for authenticating internal users. For more information, see the AWS Private Certificate Authority User Guide.

When using AWS Private CA for certificate-based authentication, WorkSpaces will request certificates for your users automatically during session authentication. Users are authenticated to Active Directory using a virtual smart card provisioned with the certificates.

Certificate-based authentication is supported with Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) bundles using the latest WorkSpaces Web Access, Windows, and macOS client applications. Open Amazon WorkSpaces Client downloads to find the latest versions:

- Windows client version 5.5.0 or later
- macOS client version 5.6.0 or later

For more information on configuring certificate-based authentication with Amazon WorkSpaces, see How to configure certificate-based authentication for Amazon WorkSpaces and Design considerations in highly regulated environments for Certificate Based Authentication with AppStream 2.0 and WorkSpaces .

Prerequisites

Complete the following steps before enabling certificate-based authentication.

1. Configure your WorkSpaces directory with SAML 2.0 integration to use certificate-based authentication. For more information, see WorkSpaces Integration with SAML 2.0.
2. Configure the `userPrincipalName` attribute in your SAML assertion. For more information, see Create Assertions for the SAML Authentication Response.
3. Configure the `ObjectSid` attribute in your SAML assertion. This is optional to perform strong mapping to the Active Directory user. Certificate-based authentication will fail if the attribute does not match the Active Directory security identifier (SID) for user specified in the SAML_Subject `NameID`. For more information, see Create Assertions for the SAML Authentication Response.
4. Add the sts:TagSession permission to your IAM role trust policy used with your SAML 2.0 configuration if it is not already present. This permission is required to use certificate-based authentication. For more information, see Create a SAML 2.0 Federation IAM Role.
5. Create a private certificate authority (CA) using AWS Private CA if you do not have one configured with your Active Directory. AWS Private CA is required to use certificate-based authentication. For more information, see Planning your AWS Private CA deployment and follow the guidance to configure a CA for certificate-based authentication. The following AWS Private CA settings are the most common for certificate-based authentication use cases:
   a. CA type options:
      i. Short-lived certificate CA usage mode (recommended if you are only using the CA to issue end user certificates for certificate-based authentication)
      ii. Single level hierarchy with a Root CA (alternatively, choose a subordinate CA if you want to integrate with an existing CA hierarchy)
   b. Key algorithm options: RSA 2048
   c. Subject distinguished name options: Use any combination of options to identify the CA in your Active Directory Trusted Root Certification Authorities store.
   d. Certificate revocation options: CRL distribution

> **Note**
>
> Certificate-based authentication requires an online CRL distribution point accessible from desktops and the domain controller. This requires unauthenticated access to the Amazon S3 bucket configured for Private CA CRL entries, or a CloudFront

distribution that will have access to the S3 bucket if it is blocking public access. For more information on these options, see Planning a certificate revocation list (CRL).

6. Tag your private CA with a key entitled `euc-private-ca` to designate the CA for use with EUC certificate-based authentication. The key does not require a value. For more information, see Managing tags for your private CA.
7. Certificate-based authentication utilizes virtual smart cards for logon. Following the Guidelines for enabling smart card logon with third-party certification authorities in Active Directory, perform the following steps:
   - Configure domain controllers with a domain controller certificate to authenticate smart card users. If you have an Active Directory Certificate Services enterprise CA configured in your Active Directory, domain controllers are automatically enrolled with certificates to enable smart card logon. If you don't have Active Directory Certificate Services, see Requirements for domain controller certificates from a third-party CA. You can create a domain controller certificate with AWS Private CA. If you do this, don't use a private CA configured for short-lived certificates.

     Note

     If you are using AWS Managed Microsoft AD, you can configure Certificate Services on an EC2 instance to satisfy the requirement for domain controller certificates. See AWS Launch Wizard for example deployments of AWS Managed Microsoft AD configured with Active Directory Certificate Services. AWS Private CA can be configured as a subordinate to the Active Directory Certificate Services CA, or can be configured as its own root when using AWS Managed Microsoft AD.
     An additional configuration task with AWS Managed Microsoft AD and Active Directory Certificate Services is to create outbound rules from the controllers VPC security group to the EC2 instance running Certificate Services allowing TCP ports 135 and 49152-65535 to enable certificate autoenrollment. In addition, the EC2 instance running must allow inbound access on the same ports from domain instances, including domain controllers. For more information on locating the security group for AWS Managed Microsoft AD see Configure your VPC subnets and security groups.

   - On the AWS Private CA console or using the SDK or CLI, select your CA and under the CA certificate, export the CA private certificate. For more information, see Exporting a private certificate.

- Publish the CA to Active Directory. Logon to a domain controller or a domain-joined machine. Copy the CA private certificate to any <path>\<file> and run the following commands as a domain administrator. Alternatively, you can use Group Policy and the Microsoft PKI Health Tool (PKIView) tool to publish the CA. For more information, see Configuration instructions.

```
certutil -dspublish -f <path>\<file> RootCA
certutil -dspublish -f  <path>\<file> NTAuthCA
```

  Ensure that the commands complete successfully, and then remove the private certificate file. Depending on Active Directory replication settings, it can take several minutes for the CA to be published to your domain controllers and desktop instances.

> **Note**
>
> - It is required that Active Directory distribute the CA to the Trusted Root Certification Authorities and Enterprise NTAuth stores automatically for WorkSpaces desktops when they are joined to the domain.

Enable certificate-based authentication

Complete the following steps to enable certificate-based authentication.

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces.
2. In the navigation pane, choose **Directories**.
3. Choose the Directory ID for your WorkSpaces.
4. Under **Authentication**, click **Edit**.
5. Click **Edit Certificate-Based Authentication**.
6. Check **Enable Certificate-Based Authentication**.
7. Confirm that your private CA ARN is associated in the list. The private CA should be in the same AWS account and AWS Region, and must be tagged with a key entitled euc-private-ca to appear in the list.
8. Click **Save Changes**. Certificate-based authentication is now enabled.
9. Reboot your Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) bundles for the changes to take effect. For more information, see Reboot a WorkSpace.

10. After rebooting, when users authenticate via SAML 2.0 using a supported client, they will no longer receive a prompt for the domain password.

> **Note**
>
> When certificate-based authentication is enabled to sign in to WorkSpaces, users are not prompted for multi-factor authentication (MFA) even if enabled on the Directory. When using certificate-based authentication, MFA can be enabled through your SAML 2.0 identity provider. For more information on AWS Directory Service MFA, see Multi-factor authentication (AD Connector) or Enable multi-factor authentication for AWS Managed Microsoft AD.

Manage certificate-based authentication

CA Certificate

In a typical configuration, the private CA certificate has a validity period of 10 years. See Managing the private CA lifecycle for more information on replacing a CA with an expired certificate, or reissuing the CA with a new validity period.

End User Certificates

End user certificates issued by AWS Private CA for WorkSpaces certificate-based authentication don't require renewal or revocation. These certificates are short-lived. WorkSpaces automatically issues a new certificate every 24 hours. These end user certificates have a shorter validity period than a typical AWS Private CA CRL distribution. As a result, end user certificates don't need to be revoked and won't appear in a CRL.

Audit Reports

You can create an audit report to list all of the certificates that your private CA has issued or revoked. For more information, see Using audit reports with your private CA.

Logging and Monitoring

You can use AWS CloudTrail to record API calls to AWS Private CA by WorkSpaces. For more information, see Using CloudTrail. In CloudTrail Event history you can view `GetCertificate` and `IssueCertificate` event names from `acm-pca.amazonaws.com` event source made by the

WorkSpaces `EcmAssumeRoleSession` user name. These events will be recorded for every EUC certificate-based authentication request.

Enable cross-account PCA sharing

When you use Private CA cross-account sharing, you can grant other accounts permissions to use a centralized CA, which removes the needs for a Private CA in every account. The CA can generate and issue certificates by using AWS Resource Access Manager to manage permissions. Private CA cross-account sharing can be used with WorkSpaces certificate-based Authentication (CBA) within the same AWS Region.

To use a shared Private CA resource with WorkSpaces CBA

1. Configure the Private CA for CBA in a centralized AWS account. For more information, see Certificate-based authentication.
2. Share the Private CA with the resource AWS accounts where WorkSpaces resources utilize CBA by following the steps in How to use AWS RAM to share your ACM Private CA cross-account. You don't need to complete step 3 to create a certificate. You can either share the Private CA with individual AWS accounts, or share through AWS Organizations. To share with individual accounts, you need to accept the shared Private CA in your resource account by using the Resource Access Manager (RAM) console or APIs. When configuring the share, confirm that the RAM resource share for the Private CA in the resource account is using the `AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority` managed permission template. This template aligns with the PCA template used by the WorkSpaces service role when issuing CBA certificates.
3. After the share is successful, you should be able to view the shared Private CA by using the Private CA console in the resource account.
4. Use the API or CLI to associate the Private CA ARN with CBA in your WorkSpaces directory properties. At this time, the WorkSpaces console doesn't support selection of shared Private CA ARNs. Example CLI commands:

```
aws workspaces modify-certificate-based-auth-properties –resource-id <value> –
certificate-based-auth-properties Status=<value>,CertificateAuthorityArn=<value>
```

Access Microsoft Entra ID-joined WorkSpaces Personal

You can create Windows 10 or 11 BYOL personal WorkSpaces that are Microsoft Entra ID-joined and enrolled to Intune. For more details, see Create a dedicated Microsoft Entra ID directory with WorkSpaces Personal.

Authentication workflow

The following sections describe the authentication workflow initiated by WorkSpaces client application, WorkSpaces Web Access, and a SAML 2.0 identity provider (IdP), Microsoft Entra ID:

- When the flow is initiated by the IdP. For example, when users choose an application in the Entra ID's user portal in a web browser..
- When the flow is initiated by the WorkSpaces client. For example, when users open the client application and sign in.
- When the flow is initiated by WorkSpaces Web Access. For example, when users open Web Access in a browser and sign in.

In these examples, users enter `user@example.onmicrosoft.com`to sign in to the IdP. On Entra ID, an enterprise application is configured to integrate with IAM Identity Center. Users create a WorkSpace for their user names in a directory that uses IAM Identity Center as the identity source to connect to an Entra ID tenant. Additionally, users install the WorkSpaces client application on their device or the user uses Web Access in a web browser.

Identity provider (IdP)-initiated flow with client application

The IdP-initiated flow allows users to automatically register the WorkSpaces client application on their devices without having to enter a WorkSpaces registration code. Users don't sign in to their WorkSpaces using the IdP-initiated flow. WorkSpaces authentication must originate from the client application.

1. Using their web browser, users sign in to the IdP (Microsoft Entra ID).
2. After signing in to the IdP, users choose the AWS IAM Identity Center application from the IdP user portal.
3. Users are redirected to the AWS access portal in the browser. Then, users choose the WorkSpaces icon.

4. Users are redirected to the page below and the WorkSpaces client application is opened automatically. Choose **Open Amazon WorkSpaces app** if the client application doesn't opened automatically.

5. The WorkSpaces client application is now registered and users can continue to sign by clicking **Continue to sign in to WorkSpaces**.

Identity provider (IdP)-initiated flow with Web Access

The IdP-initiated Web Access flow allows users to automatically register their WorkSpaces through a web browser without having to enter a WorkSpaces registration code. Users don't sign in to their WorkSpaces using the IdP-initiated flow. WorkSpaces authentication must originate from Web Access.

1. Using their web browser, users sign in to the IdP.
2. After signing in to the IdP, users click the AWS IAM Identity Center application from the IdP user portal.
3. Users are redirected to AWS access portal in the browser. Then, users choose the WorkSpaces icon.
4. Users are redirected to this page in the browser. To open WorkSpaces, choose **Amazon WorkSpaces in the browser**.

5. The WorkSpaces client application is now registered and users can continue to sign in through WorkSpaces Web Access.

WorkSpaces client-initiated flow

The client-initiated flow allows users to sign in to their WorkSpaces after signing in to an IdP.

1. Users launch the WorkSpaces client application (if it isn't already running) and clicks **Continue to sign in to WorkSpaces**.
2. Users are redirected to their default web browser to sign in to the IdP. If the users are already signed in to the IdP in their browser, they don't need to sign in again and will skip this step.
3. Once signed in to the IdP, users are redirected to a pop up. Follow the prompts to allow your web browser to open the client application.
4. Users are redirected to the WorkSpaces client application, on Windows login screen.
5. Users complete sign-in to Windows using their Entra ID username and credentials.

WorkSpaces Web Access-initiated flow

The Web Access-initiated flow allows users to sign in to their WorkSpaces after signing in to an IdP.

1. Users launch the WorkSpaces Web Access and chooses **Sign in**.
2. In the same browser tab, users are redirected to IdP portal. If the users are already signed in to the IdP in their browser, they don't need to sign in again and can skip this step.

3. Once signed in to the IdP, users redirected to this page in the browser, and clicks **Log in to WorkSpaces**.
4. Users are redirected to the WorkSpaces client application, on the Windows login screen.
5. Users complete sign-in to Windows using their Entra ID username and credentials.

First-time user experience

If you're logging in for the first time to a Microsoft Entra ID-joined Windows WorkSpaces, you must go through the out-of-box experience (OOBE). During OOBE, the WorkSpaces are joined to Entra ID. You can customize the OOBE experience by configuring the Autopilot profile assigned to the Microsoft Intune device group that you create for your WorkSpaces. For more information, see Step 3: Configure Windows Autopilot user-driven mode.

Use smart cards for authentication in WorkSpaces Personal

Windows and Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) bundles allow the use of Common Access Card (CAC) and Personal Identity Verification (PIV) smart cards for authentication.

Amazon WorkSpaces supports the use of smart cards for both *pre-session authentication* and *in-session authentication*. Pre-session authentication refers to smart card authentication that's performed while users are logging in to their WorkSpaces. In-session authentication refers to authentication that's performed after logging in.

For example, users can use smart cards for in-session authentication while working with web browsers and applications. They can also use smart cards for actions that require administrative permissions. For example, if the user has administrative permissions on their Linux WorkSpace, they can use smart cards to authenticate themselves when running `sudo` and `sudo -i` commands.

Contents

Requirements

- An Active Directory Connector (AD Connector) directory is required for pre-session authentication. AD Connector uses certificate-based mutual Transport Layer Security (mutual TLS) authentication to authenticate users to Active Directory using a hardware or software-based smart card certificate. For more information about how to configure your AD Connector and your on-premises directory, see Directory configuration.
- To use a smart card with a Windows or Linux WorkSpace, the user must use the Amazon WorkSpaces Windows client version 3.1.1 or later or the WorkSpaces macOS client version 3.1.5 or later. For more information about using smart cards with the Windows and macOS clients, see Smart Card Support in the *Amazon WorkSpaces User Guide*.
- The root CA and smart card certificates must meet certain requirements. For more information, see Enable mTLS authentication in AD Connector for use with smart cards in the *AWS Directory Service Administration Guide* and Certificate Requirements in the Microsoft documentation.

  In addition to those requirements, user certificates employed for smart card authentication to Amazon WorkSpaces must include the following attributes:

  - The AD user's userPrincipalName (UPN) in the subjectAltName (SAN) field of the certificate. We recommend issuing smart card certificates for the user's default UPN.
  - The Client Authentication (1.3.6.1.5.5.7.3.2) Extended Key Usage (EKU) attribute.
  - The Smart Card Logon (1.3.6.1.4.1.311.20.2.2) EKU attribute.
- For pre-session authentication, Online Certificate Status Protocol (OCSP) is required for certificate revocation checking. For in-session authentication, OCSP is recommended, but not required.

Limitations

- Only the WorkSpaces Windows client application version 3.1.1 or later and the macOS client application version 3.1.5 or later are currently supported for smart card authentication.
- The WorkSpaces Windows client application 3.1.1 or later supports smart cards only when the client is running on a 64-bit version of Windows.
- Ubuntu WorkSpaces does not currently support smart card authentication.
- Only AD Connector directories are currently supported for smart card authentication.
- In-session authentication is available in all Regions where WSP is supported. Pre-session authentication is available in the following Regions:

- Asia Pacific (Sydney) Region
- Asia Pacific (Tokyo) Region
- Europe (Ireland) Region
- AWS GovCloud (US-East) Region
- AWS GovCloud (US-West) Region
- US East (N. Virginia) Region
- US West (Oregon) Region

- For in-session authentication and pre-session authentication on Linux or Windows WorkSpaces, only one smart card is currently allowed at a time.
- For pre-session authentication, enabling both smart card authentication and sign-in authentication on the same directory is not currently supported.
- Only CAC and PIV cards are supported at this time. Other types of hardware or software-based smart cards might also work, but they haven't been fully tested for use with WSP.

Directory configuration

To enable smart card authentication, you must configure your AD Connector directory and your on-premises directory in the following manner.

AD Connector directory configuration

Before you begin, make sure your AD Connector directory has been set up as described in AD Connector Prerequisites in the *AWS Directory Service Administration Guide*. In particular, make sure that you have opened up the necessary ports in your firewall.

To finish configuring your AD Connector directory, follow the instructions in Enable mTLS authentication in AD Connector for use with smart cards in the *AWS Directory Service Administration Guide*.

> **Note**
>
> Smart card authentication requires Kerberos Constrained Delegation (KCD) to function properly. KCD requires the username portion of the AD Connector service account to match the sAMAccountName of the same user. A sAMAccountName can't exceed 20 characters.

On-premises directory configuration

In addition to configuring your AD Connector directory, you must also make sure that the certificates that are issued to the domain controllers for your on-premises directory have the "KDC Authentication" extended key usage (EKU) set. To do this, use the Active Directory Domain Services (AD DS) default Kerberos Authentication certificate template. Do not use a Domain Controller certificate template or a Domain Controller Authentication certificate template because those templates don't contain the necessary settings for smart card authentication.

Enable smart cards for Windows WorkSpaces

For general guidance on how to enable smart card authentication on Windows, see Guidelines for enabling smart card logon with third-party certification authorities in the Microsoft documentation.

To detect the Windows lock screen and disconnect the session

To allow users to unlock Windows WorkSpaces that are enabled for smart card pre-session authentication when the screen is locked, you can enable Windows lock screen detection in users' sessions. When the Windows lock screen is detected, the WorkSpace session is disconnected, and the user can reconnect from the WorkSpaces client by using their smart card.

You can enable disconnecting the session when the Windows lock screen is detected by using Group Policy settings. For more information, see Enable or disable disconnect session on screen lock for WSP.

To enable in-session or pre-session authentication

By default, Windows WorkSpaces are not enabled to support the use of smart cards for pre-session or in-session authentication. If needed, you can enable in-session and pre-session authentication for Windows WorkSpaces by using Group Policy settings. For more information, see Enable or disable smart card redirection for WSP.

To use pre-session authentication, in addition to updating the Group Policy settings, you must also enable pre-session authentication through your AD Connector directory settings. For more information, follow the instructions in Enable mTLS authentication in AD Connector for use in smart cards in the *AWS Directory Service Administration Guide*.

To enable users to use smart cards in a browser

If your users are using Chrome as their browser, no special configuration is required to use smart cards.

If your users are using Firefox as their browser, you can enable your users to use smart cards in Firefox through Group Policy. You can use these Firefox Group Policy templates in GitHub.

For example, you can install the 64-bit version of OpenSC for Windows to support PKCS #11, and then use the following Group Policy setting, where *NAME_OF_DEVICE* is whatever value you want to use to identify PKCS #11, such as OpenSC, and where *PATH_TO_LIBRARY_FOR_DEVICE* is the path to the PKCS #11 module. This path should point to a library with a .DLL extension, such as `C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`.

```
Software\Policies\Mozilla\Firefox\SecurityDevices\NAME_OF_DEVICE
 = PATH_TO_LIBRARY_FOR_DEVICE
```

Tip

If you're using OpenSC, you can also load the OpenSC `pkcs11` module into Firefox by running the `pkcs11-register.exe` program. To run this program, either double-click the file at `C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe`, or open a Command Prompt window and run the following command:

```
"C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe"
```

To verify that the OpenSC `pkcs11` module has been loaded into Firefox, do the following:

1. If Firefox is already running, close it.
2. Open Firefox. Choose the menu button ☰ in the upper-right corner, and then choose **Options**.
3. On the **about:preferences** page, in the left navigation pane, choose **Privacy & Security**.
4. Under **Certificates**, choose **Security Devices**.
5. In the **Device Manager** dialog box, you should see **OpenSC smartcard framework (0.21)** in the left navigation, and it should have the following values when you select it:

   Module: `OpenSC smartcard framework (0.21)`

Path: `C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`

Troubleshooting

For information about troubleshooting smart cards, see Certificate and configuration problems in the Microsoft documentation.

Some common issues that can cause problems:

- Incorrect mapping of the slots to the certificates.
- Having multiple certificates on the smart card that can match the user. Certificates are matched using the following criteria:
  - The root CA for the certificate.
  - The <KU> and <EKU> fields of the certificate.
  - The UPN in the certificate subject.
- Having multiple certificates that have `<EKU>msScLogin` in their key usage.

In general, it's best to have only one certificate for smart card authentication that is mapped to the very first slot in the smart card.

The tools for managing the certificates and keys on the smart card (such as removing or remapping the certificates and keys) might be manufacturer-specific. For more information, see the documentation provided by the manufacturer of your smart cards.

Enable smart cards for Linux WorkSpaces

Note

Linux WorkSpaces on WSP currently have the following limitations:

- Clipboard, audio-in, video-in, and time zone redirection aren't supported.
- Multiple monitors aren't supported.
- You must use the WorkSpaces Windows client application to connect to Linux WorkSpaces on WSP.

To enable the use of smart cards on Linux WorkSpaces, you need to include a root CA certificate file in the PEM format in the WorkSpace image.

To obtain your root CA certificate

You can obtain your root CA certificate in several ways:

- You can use a root CA certificate operated by a third-party certification authority.
- You can export your own root CA certificate by using the Web Enrollment site, which is either `http://`*`ip_address`*`/certsrv` or `http://`*`fqdn`*`/certsrv`, where *`ip_address`* and *`fqdn`* are the IP address and the fully qualified domain name (FQDN) of the root certification CA server. For more information about using the Web Enrollment site, see How to export a Root Certification Authority Certificate in the Microsoft documentation.
- You can use the following procedure to export the root CA certificate from a root CA certification server that is running Active Directory Certificate Services (AD CS). For information about installing AD CS, see Install the Certification Authority in the Microsoft documentation.

  1. Log into the root CA server using an administrator account.
  2. From the Windows **Start** menu, open a command prompt window (**Start** > **Windows System** > **Command Prompt**).
  3. Use the following command to export the root CA certificate to a new file, where *`rootca`*`.cer` is the name of the new file:

     ```
     certutil -ca.cert rootca.cer
     ```

     For more information about running certutil, see certutil in the Microsoft documentation.
  4. Use the following OpenSSL command to convert the exported root CA certificate from DER format to PEM format, where *`rootca`* is the name of the certificate. For more information about OpenSSL, see www.openssl.org.

     ```
     openssl x509 -inform der -in rootca.cer -out /tmp/rootca.pem
     ```

To add your root CA certificate to your Linux WorkSpaces

To assist you with enabling smart cards, we've added the `enable_smartcard` script to our Amazon Linux WSP bundles. This script performs the following actions:

- Imports your root CA certificate into the Network Security Services (NSS) database.
- Installs the `pam_pkcs11` module for Pluggable Authentication Module (PAM) authentication.
- Performs a default configuration, which includes enabling `pkinit` during WorkSpace provisioning.

The following procedure explains how to use the `enable_smartcard` script to add your root CA certificate to your Linux WorkSpaces and to enable smart cards for your Linux WorkSpaces.

1. Create a new Linux WorkSpace with the WSP protocol enabled. When launching the WorkSpace in the Amazon WorkSpaces console, on the **Select Bundles** page, be sure to select **WSP** for the protocol, and then select one of the Amazon Linux 2 public bundles.
2. On the new WorkSpace, run the following command as root, where *`pem-path`* is the path to the root CA certificate file in PEM format.

   ```
   /usr/lib/skylight/enable_smartcard --ca-cert pem-path
   ```

   Note

   Linux WorkSpaces assume that the certificates on the smart cards are issued for the user's default user principal name (UPN), such as *`sAMAccountName`*@*`domain`*, where *`domain`* is a fully qualified domain name (FQDN).
   To use alternate UPN suffixes, `run /usr/lib/skylight/enable_smartcard --help` for more information. The mapping for alternate UPN suffixes is unique to each user. Therefore, that mapping must be performed individually on each user's WorkSpace.
3. (Optional) By default, all services are enabled to use smart card authentication on Linux WorkSpaces. To limit smart card authentication to only specific services, you must edit `/etc/pam.d/system-auth`. Uncomment the `auth` line for `pam_succeed_if.so` and edit the list of services as needed.

   After the `auth` line is uncommented, to allow a service to use smart card authentication, you must add it to the list. To make a service use only password authentication, you must remove it from the list.
4. Perform any additional customizations to the WorkSpace. For example, you might want to add a system-wide policy to enable users to use smart cards in Firefox. (Chrome users must enable

smart cards on their clients themselves. For more information, see Smart Card Support in the *Amazon WorkSpaces User Guide*.)

5. Create a custom WorkSpace image and bundle from the WorkSpace.
6. Use the new custom bundle to launch WorkSpaces for your users.

To enable users to use smart cards in Firefox

You can enable your users to use smart cards in Firefox by adding a SecurityDevices policy to your Linux WorkSpace image. For more information about adding system-wide policies to Firefox, see the Mozilla policy templates on GitHub.

1. On the WorkSpace that you're using to create your WorkSpace image, create a new file named `policies.json` in `/usr/lib64/firefox/distribution/`.
2. In the JSON file, add the following SecurityDevices policy, where *`NAME_OF_DEVICE`* is whatever value you want to use to identify the `pkcs` module. For example, you might want to use a value such as `"OpenSC"`:

```
{
    "policies": {
        "SecurityDevices": {
            "NAME_OF_DEVICE": "/usr/lib64/opensc-pkcs11.so"
        }
    }
}
```

Troubleshooting

For troubleshooting, we recommend adding the `pkcs11-tools` utility. This utility allows you to perform the following actions:

- List each smart card.
- List the slots on each smart card.
- List the certificates on each smart card.

Some common issues that can cause problems:

- Incorrect mapping of the slots to the certificates.

- Having multiple certificates on the smart card that can match the user. Certificates are matched using the following criteria:
  - The root CA for the certificate.
  - The <KU> and <EKU> fields of the certificate.
  - The UPN in the certificate subject.
- Having multiple certificates that have <EKU>msScLogin in their key usage.

In general, it's best to have only one certificate for smart card authentication that is mapped to the very first slot in the smart card.

The tools for managing the certificates and keys on the smart card (such as removing or remapping the certificates and keys) might be manufacturer-specific. Additional tools that you can use to work with smart cards are:

- opensc-explorer
- opensc-tool
- pkcs11_inspect
- pkcs11_listcerts
- pkcs15-tool

To enable debug logging

To troubleshoot your pam_pkcs11 and pam-krb5 configuration, you can enable debug logging.

1. In the /etc/pam.d/system-auth-ac file, edit the auth action and change the nodebug parameter of pam_pksc11.so to debug.
2. In the /etc/pam_pkcs11/pam_pkcs11.conf file, change debug = false; to debug = true;. The debug option applies separately to each mapper module, so you might need to change it both directly under the pam_pkcs11 section and also under the appropriate mapper section (by default, this is mapper generic).
3. In the /etc/pam.d/system-auth-ac file, edit the auth action and add the debug or the debug_sensitive parameter to pam_krb5.so.

After you've enabled debug logging, the system prints out pam_pkcs11 debug messages directly in the active terminal. Messages from pam_krb5 are logged in /var/log/secure.

To check which username a smart card certificate maps to, use the following `pklogin_finder` command:

```
sudo pklogin_finder debug config_file=/etc/pam_pkcs11/pam_pkcs11.conf
```

When prompted, enter the smart card PIN. `pklogin_finder` outputs on `stdout` the username on the smart card certificate in the form *`NETBIOS`*`\`*`username`*. This username should match the WorkSpace username.

In Active Directory Domain Services (AD DS), the NetBIOS domain name is the pre-Windows 2000 domain name. Typically (but not always), the NetBIOS domain name is the subdomain of the Domain Name System (DNS) domain name. For example, if the DNS domain name is `example.com`, the NetBIOS domain name is usually `EXAMPLE`. If the DNS domain name is `corp.example.com`, the NetBIOS domain name is usually `CORP`.

For example, for the user `mmajor` in the domain `corp.example.com`, the output from `pklogin_finder` is `CORP\mmajor`.

> **Note**
>
> If you receive the message "`ERROR:pam_pkcs11.c:504: verify_certificate() failed`", this message indicates that `pam_pkcs11` has found a certificate on the smart card that matches the username criteria but that doesn't chain up to a root CA certificate that is recognized by the machine. When that happens, `pam_pkcs11` outputs the above message and then tries the next certificate. It allows authentication only if it finds a certificate that both matches the username and chains up to a recognized root CA certificate.

To troubleshoot your `pam_krb5` configuration, you can manually invoke `kinit` in debug mode with the following command:

```
KRB5_TRACE=/dev/stdout kinit -V
```

This command should successfully obtain a Kerberos Ticket Granting Ticket (TGT). If it fails, try adding the correct Kerberos principal name explicitly to the command. For example, for the user `mmajor` in the domain `corp.example.com`, use this command:

```
KRB5_TRACE=/dev/stdout kinit -V mmajor
```

If this command succeeds, the issue is most likely in the mapping from the WorkSpace username to the Kerberos principal name. Check the `[appdefaults]/pam/mappings` section in the `/etc/krb5.conf` file.

If this command doesn't succeed, but a password-based `kinit` command does succeed, check the `pkinit_`-related configurations in the `/etc/krb5.conf` file. For example, if the smart card contains more than one certificate, you might need to make changes to `pkinit_cert_match`.

Provide internet access for WorkSpaces Personal

Your WorkSpaces must have access to the internet so that you can install updates to the operating system and deploy applications. You can use one of the following options to allow your WorkSpaces in a virtual private cloud (VPC) to access the internet.

Options

- Launch your WorkSpaces in private subnets and configure a NAT gateway in a public subnet in your VPC.
- Launch your WorkSpaces in public subnets and automatically or manually assign public IP addresses to your WorkSpaces.

For more information about these options, see the corresponding sections in Configure a VPC for WorkSpaces Personal.

With any of these options, you must ensure that the security group for your WorkSpaces allows outbound traffic on ports 80 (HTTP) and 443 (HTTPS) to all destinations (`0.0.0.0/0`).

Amazon Linux extras library

If you are using the Amazon Linux repository, your Amazon Linux WorkSpaces must either have internet access or you must configure VPC endpoints to this repository and to the main Amazon Linux repository. For more information, see the *Example: Enabling Access to the Amazon Linux AMI Repositories* section in Endpoints for Amazon S3. The Amazon Linux AMI repositories are Amazon S3 buckets in each Region. If you want instances in your VPC to access the repositories through an endpoint, create an endpoint policy that enables access to these buckets. The following policy allows access to the Amazon Linux repositories.

```
{
  "Statement": [
    {
        "Sid": "AmazonLinux2AMIRepositoryAccess",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amazonlinux.*.amazonaws.com/*"
        ]
    }
  ]
}
```

Security groups for WorkSpaces Personal

When you register a directory with WorkSpaces, it creates two security groups, one for directory controllers and another for WorkSpaces in the directory. The security group for directory controllers has a name that consists of the directory identifier followed by **_controllers** (for example, d-12345678e1_controllers). The security group for WorkSpaces has a name that consists of the directory identifier followed by **_workspacesMembers** (for example, d-123456fc11_workspacesMembers).

> **Warning**
>
> Avoid modifying, deleting, or detaching the **_controllers** and the **_workspacesMembers** security groups. Be cautious when modifying or deleting these security groups, because you will not be able to recreate these groups and add them back after they have been modified or deleted. For more information, see Amazon EC2 security groups for Linux instance or Amazon EC2 security groups for Windows instances.

You can add a default WorkSpaces security group to a directory. After you associate a new security group with a WorkSpaces directory, new WorkSpaces that you launch or existing WorkSpaces that you rebuild will have the new security group. You can also add this new default security group to existing WorkSpaces without rebuilding them, as explained later in this topic.

When you associate multiple security groups with a WorkSpaces directory, the rules from each security group are effectively aggregated to create one set of rules. We recommend condensing your security group rules as much as possible.

For more information about security groups, see Security Groups for Your VPC in the *Amazon VPC User Guide*.

To add a security group to a WorkSpaces directory

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select the directory and choose **Actions**, **Update Details**.
4. Expand **Security Group** and select a security group.
5. Choose **Update and Exit**.

To add a security group to an existing WorkSpace without rebuilding it, you assign the new security group to the elastic network interface (ENI) of the WorkSpace.

To add a security group to an existing WorkSpace

1. Find the IP address for each WorkSpace that needs to be updated.
   a. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
   b. Expand each WorkSpace and record its WorkSpace IP address.
2. Find the ENI for each WorkSpace and update its security group assignment.
   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. Under **Network & Security**, choose **Network Interfaces**.
   c. Search for the first IP address that you recorded in Step 1.
   d. Select the ENI associated with the IP address, choose **Actions**, and then choose **Change Security Groups**.
   e. Select the new security group, and choose **Save**.
   f. Repeat this process as needed for any other WorkSpaces.

IP access control groups for WorkSpaces Personal

Amazon WorkSpaces allows you to control which IP addresses your WorkSpaces can be accessed from. By using IP address-based control groups, you can define and manage groups of trusted IP addresses, and only allow users to access their WorkSpaces when they're connected to a trusted network.

An *IP access control group* acts as a virtual firewall that controls the IP addresses from which users are allowed to access their WorkSpaces. To specify the CIDR address ranges, add rules to your IP access control group, and then associate the group with your directory. You can associate each IP access control group with one or more directories. You can create up to 100 IP access control groups per Region per AWS account. However, you can only associate up to 25 IP access control groups with a single directory.

A default IP access control group is associated with each directory. This default group includes a default rule that allows users to access their WorkSpaces from anywhere. You cannot modify the default IP access control group for your directory. If you don't associate an IP access control group with your directory, the default group is used. If you associate an IP access control group with a directory, the default IP access control group is disassociated.

To specify the public IP addresses and ranges of IP addresses for your trusted networks, add rules to your IP access control groups. If your users access their WorkSpaces through a NAT gateway or VPN, you must create rules that allow traffic from the public IP addresses for the NAT gateway or VPN.

Note

- IP access control groups do not allow the use of dynamic IP addresses for NATs. If you're using a NAT, configure it to use a static IP address instead of a dynamic IP address. Make sure the NAT routes all the UDP traffic through the same static IP address for the duration of the WorkSpaces session.
- IP access control groups control the IP addresses from which users can connect their streaming sessions to WorkSpaces. Users can still execute functionalities, such as restart, rebuild, shutdown, from any IP address using Amazon WorkSpaces public APIs.

You can use this feature with Web Access, PCoIP zero clients, and the client applications for macOS, iPad, Windows, Chromebook, and Android.

Create an IP access control group

You can create an IP access control group as follows. Each IP access control group can contain up to 10 rules.

To create an IP access control group

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **IP Access Controls**.
3. Choose **Create IP Group**.
4. In the **Create IP Group** dialog box, enter a name and description for the group and choose **Create**.
5. Select the group and choose **Edit**.
6. For each IP address, choose **Add Rule**. For **Source**, enter the IP address or IP address range. For **Description**, enter a description. When you are done adding rules, choose **Save**.

Associate an IP access control group with a directory

You can associate an IP access control group with a directory to ensure that WorkSpaces are accessed only from trusted networks.

If you associate an IP access control group that has no rules with a directory, this blocks all access to all WorkSpaces.

To associate an IP access control group with a directory

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select the directory and choose **Actions**, **Update Details**.
4. Expand **IP Access Control Groups** and select one or more IP access control groups.
5. Choose **Update and Exit**.

Copy an IP access control group

You can use an existing IP access control group as a base for creating a new IP access control group.

To create an IP access control group from an existing one

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **IP Access Controls**.
3. Select the group and choose **Actions**, **Copy to New**.
4. In the **Copy IP Group** dialog box, enter a name and description for the new group and choose **Copy Group**.
5. (Optional) To modify the rules copied from the original group, select the new group and choose **Edit**. Add, update, or remove rules as needed. Choose **Save**.

Delete an IP access control group

You can delete a rule from an IP access control group at any time. If you remove a rule that was used to allow a connection to a WorkSpace, the user is disconnected from the WorkSpace.

Before you can delete an IP access control group, you must disassociate it from any directories.

To delete an IP access control group

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. For each directory that is associated with the IP access control group, select the directory and choose **Actions**, **Update Details**. Expand **IP Access Control Groups**, clear the check box for the IP access control group, and choose **Update and Exit**.
4. In the navigation pane, choose **IP Access Controls**.
5. Select the group and choose **Actions**, **Delete IP Group**.

Set up PCoIP zero clients for WorkSpaces Personal

PCoIP zero clients are compatible only with WorkSpaces bundles that are using the PCoIP protocol.

If your zero client device has firmware version 6.0.0 or later, your users can connect to their WorkSpaces directly. When your users are connecting directly to their WorkSpaces using a zero client device, we recommend using multi-factor authentication (MFA) with your WorkSpaces directory. For more information about using MFA with your directory, see the following documentation:

- **AWS Managed Microsoft AD** — Enable multi-factor authentication for AWS Managed Microsoft AD in the *AWS Directory Service Administration Guide*
- **AD Connector** — Enable multi-factor authentication for AD Connector in the *AWS Directory Service Administration Guide* and Multi-factor authentication (AD Connector)
- **Trusted domains** — Enable multi-factor authentication for AWS Managed Microsoft AD in the *AWS Directory Service Administration Guide*
- **Simple AD** — Multi-factor authentication is not available for Simple AD.

As of April 13, 2021, PCoIP Connection Manager is no longer supported for use with zero client device firmware versions between 4.6.0 and 6.0.0. If your zero client firmware is not version 6.0.0 or later, you can get the latest firmware through a Desktop Access subscription at https://www.teradici.com/desktop-access.

Important

- In the Teradici PCoIP Administrative Web Interface (AWI) or the Teradici PCoIP Management Console (MC), make sure you enable Network Time Protocol (NTP). For the NTP host DNS name, use **`pool.ntp.org`**, and set the NTP host port to **123**. If NTP isn't enabled, your PCoIP zero client users might receive certificate failure errors, such as "The supplied certificate is invalid due to timestamp."
- Starting with version 20.10.4 of the PCoIP agent, Amazon WorkSpaces disables USB redirection by default through the Windows registry. This registry setting affects the behavior of USB peripherals when your users are using PCoIP zero client devices to connect to their WorkSpaces. For more information, see USB printers and other USB peripherals aren't working for PCoIP zero clients.

For information about setting up and connecting with a PCoIP zero client device, see PCoIP Zero Client in the *Amazon WorkSpaces User Guide*. For a list of approved PCoIP zero client devices, see PCoIP Zero Clients on the Teradici website.

Set up Android for Chromebooks for WorkSpaces Personal

Version 2.4.13 is the final release of the Amazon WorkSpaces Chromebook client application. Because Google is phasing out support for Chrome Apps, there will be no further updates to the WorkSpaces Chromebook client application, and its use is unsupported.

For Chromebooks that support installing Android applications, we recommend using the WorkSpaces Android client application instead.

Some Chromebooks launched before 2019 must be enabled to install Android apps before users can install the Amazon WorkSpaces Android client application. For more information, see Chrome OS Systems Supporting Android Apps.

To remotely manage enabling your users' Chromebooks to install Android apps, see Set up Android on Chrome devices.

Enable and configure WorkSpaces Web Access for WorkSpaces Personal

Most WorkSpaces bundles support Amazon WorkSpaces Web Access. For a list of WorkSpaces that support web browser access, see "Which Amazon WorkSpaces bundles support Web Access?" in Client Access, Web Access, and User Experience.

Note

- Web Access with WSP for Windows and Ubuntu WorkSpaces is supported in all Regions where WSP WorkSpaces are available. WSP for Amazon Linux WorkSpaces is only available in AWS GovCloud (US-West).
- We strongly recommend using Web Access with WSP WorkSpaces for best streaming quality and user experience. The following are limitations when using Web Access with PCoIP WorkSpaces:
  - Web Access with PCoIP is not supported in the AWS GovCloud (US) Regions, Asia Pacific (Mumbai), Africa (Cape Town), Europe (Frankfurt), and Israel (Tel Aviv)
  - Web Access with PCoIP is only supported for Windows WorkSpaces, not with Amazon Linux or Ubuntu WorkSpaces.
  - Web Access is not available for some Windows 10 WorkSpaces that are using the PCoIP protocol. If your PCoIP WorkSpaces are powered by Windows Server 2019 or 2022, Web Access is not available.
  - Web Access with PCoIP is limited in feature functionality. It supports video-out, audio-out, keyboard and mouse. It does not support many features, including video-in, audio-in, clipboard redirection, and web cams.
- You can't use a web browser to connect to GPU-enabled WorkSpaces.

- If you are using macOS on VPN and using the Firefox web browser, the web browser will not support streaming PCoIP WorkSpaces using WorkSpaces Web Access. This is due to a limitation in Firefox implementation of the WebRTC protocol.

Important

Beginning October 1, 2020, customers will no longer be able to use the Amazon WorkSpaces Web Access client to connect to Windows 7 custom WorkSpaces or to Windows 7 Bring Your Own License (BYOL) WorkSpaces.

Step 1: Enable Web Access to your WorkSpaces

You control Web Access to your WorkSpaces at the directory level. For each directory containing WorkSpaces that you want to allow users to access through the Web Access client, do the following steps.

To enable Web Access to your WorkSpaces

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Under the **Directory ID** column, choose the directory ID of the directory you want to enable Web Access for.
4. On the **Directory Details** page, scroll down to the **Other platforms** section and choose **Edit**.
5. Choose **Web Access**.
6. Choose **Save**.

Note

After you enable Web Access, reboot your WorkSpace for the change to apply.

Step 2: Configure inbound and outbound access to ports for Web Access

Amazon WorkSpaces Web Access requires inbound and outbound access for certain ports. For more information, see Ports for Web Access.

Step 3: Configure Group Policy and security policy settings to enable users to log on

Amazon WorkSpaces relies on a specific logon screen configuration to enable users to successfully log on from their Web Access client.

To enable Web Access users to log on to their WorkSpaces, you must configure a Group Policy setting and three Security Policy settings. If these settings are not correctly configured, users might experience long logon times or black screens when they try to log on to their WorkSpaces. To configure these settings, use the following procedures.

You can use Group Policy Objects (GPOs) to apply settings to manage Windows WorkSpaces or users that are part of your Windows WorkSpaces directory. We recommend that you create an organizational unit for your WorkSpaces Computer Objects and an organizational unit for your WorkSpaces User Objects.

For information about using the Active Directory administration tools to work with GPOs, see Installing the Active Directory Administration Tools in the *AWS Directory Service Administration Guide*.

To enable the WorkSpaces logon agent to switch users

In most cases, when a user attempts to log on to a WorkSpace, the user name field is prepopulated with the name of that user. However, if an administrator has established an RDP connection to the WorkSpace to perform maintenance tasks, the user name field is populated with the name of the administrator instead.

To avoid this issue, disable the **Hide entry points for Fast User Switching** Group Policy setting. When you disable this setting, the WorkSpaces logon agent can use the **Switch User** button to populate the user name field with the correct name.

1. Open the Group Policy Management tool (**gpmc.msc**) and navigate to and select a GPO at the domain or domain controller level of the directory that you use for your WorkSpaces. (If you have the WorkSpaces Group Policy administrative template installed in your domain, you can use the WorkSpaces GPO for your WorkSpaces machine accounts.)
2. Choose **Action**, **Edit** in the main menu.
3. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **System**, and **Logon**.
4. Open the **Hide entry points for Fast User Switching** setting.

5. In the **Hide entry points for Fast User Switching** dialog box, choose **Disabled**, and then choose **OK**.

To hide the last logged on user name

By default, the list of last logged on users is displayed instead of the **Switch User** button. Depending on the configuration of the WorkSpace, the list might not display the **Other User** tile. When this situation occurs, if the prepopulated user name isn't correct, the WorkSpaces logon agent can't populate the field with the correct name.

To avoid this issue, enable the Security Policy setting **Interactive logon: Don't display last signed-in** or **Interactive logon: Do not display last user name** (depending on which version of Windows you're using).

1. Open the Group Policy Management tool (**gpmc.msc**) and navigate to and select a GPO at the domain or domain controller level of the directory that you use for your WorkSpaces. (If you have the WorkSpaces Group Policy administrative template installed in your domain, you can use the WorkSpaces GPO for your WorkSpaces machine accounts.)
2. Choose **Action**, **Edit** in the main menu.
3. In the Group Policy Management Editor, choose **Computer Configuration**, **Windows Settings**, **Security Settings**, **Local Policies**, and **Security Options**.
4. Open one of the following settings:
   - For Windows 7 — **Interactive logon: Don't display last signed-in**
   - For Windows 10 — **Interactive logon: Do not display last user name**
5. In the **Properties** dialog box for the setting, choose **Enabled**, and then choose **OK**.

To require pressing CTRL+ALT+DEL before users can log on

For WorkSpaces Web Access, you need to require that users press CTRL+ALT+DEL before they can log on. Requiring users to press CTRL+ALT+DEL before they log on ensures that users are using a trusted path when they're entering their passwords.

1. Open the Group Policy Management tool (**gpmc.msc**) and navigate to and select a GPO at the domain or domain controller level of the directory that you use for your WorkSpaces. (If you have the WorkSpaces Group Policy administrative template installed in your domain, you can use the WorkSpaces GPO for your WorkSpaces machine accounts.)

2. Choose **Action**, **Edit** in the main menu.
3. In the Group Policy Management Editor, choose **Computer Configuration**, **Windows Settings**, **Security Settings**, **Local Policies**, and **Security Options**.
4. Open the **Interactive logon: Do not require CTRL+ALT+DEL** setting.
5. On the **Local Security Setting** tab, choose **Disabled**, and then choose **OK**.

To display the domain and user information when the session is locked

The WorkSpaces logon agent looks for the user's name and domain. After this setting is configured, the lock screen will display the user's full name (if it is specified in Active Directory), their domain name, and their user name.

1. Open the Group Policy Management tool (**gpmc.msc**) and navigate to and select a GPO at the domain or domain controller level of the directory that you use for your WorkSpaces. (If you have the WorkSpaces Group Policy administrative template installed in your domain, you can use the WorkSpaces GPO for your WorkSpaces machine accounts.)
2. Choose **Action**, **Edit** in the main menu.
3. In the Group Policy Management Editor, choose **Computer Configuration**, **Windows Settings**, **Security Settings**, **Local Policies**, and **Security Options**.
4. Open the **Interactive logon: Display user information when the session is locked** setting.
5. On the **Local Security Setting** tab, choose **User display name, domain and user names**, and then choose **OK**.

To apply the Group Policy and Security Policy settings changes

Group Policy and Security Policy settings changes take effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy and Security Policy changes in the prior procedures, do one of the following:

- Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
- From an administrative command prompt, enter **gpupdate /force**.

Configure FedRAMP authorization or DoD SRG compliance for WorkSpaces Personal

To comply with the Federal Risk and Authorization Management Program (FedRAMP) or the Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG), you must configure Amazon WorkSpaces to use Federal Information Processing Standards (FIPS) endpoint encryption at the directory level. You must also use a US AWS Region that has FedRAMP authorization or is DoD SRG compliant.

The level of FedRAMP authorization (Moderate or High) or DoD SRG Impact Level (2, 4, or 5) depends on the US AWS Region in which Amazon WorkSpaces is being used. For the levels of FedRAMP authorization and DoD SRG compliance that apply to each Region, see AWS Services in Scope by Compliance Program.

> **Note**
>
> In addition to using FIPS endpoint encryption, you can also encrypt your WorkSpaces. For more information, see Encrypted WorkSpaces in WorkSpaces Personal.

Requirements

- You must create your WorkSpaces in a US AWS Region that has FedRAMP authorization or is DoD SRG-compliant.
- The WorkSpaces directory must be configured to use **FIPS 140-2 Validated Mode** for endpoint encryption.

  > **Note**
  >
  > To use the **FIPS 140-2 Validated Mode** setting, the WorkSpaces directory must either be new, or all existing WorkSpaces in the directory must be using **FIPS 140-2 Validated Mode** for endpoint encryption. Otherwise, you cannot use this setting, and therefore the WorkSpaces that you create will not comply with FedRAMP or DoD security requirements. Refer to step 3 below for details on how to verify the directory.

- Users must access their WorkSpaces from one of the following WorkSpaces client applications:
  - Windows: 2.4.3 or later

- macOS: 2.4.3 or later for PCoIP WorkSpaces, and 5.21.0 or later for WSP WorkSpaces
- Linux: 3.0.0 or later
- iOS: 2.4.1 or later
- Android: 2.4.1 or later
- Fire Tablet: 2.4.1 or later
- ChromeOS: 2.4.1 or later
- Web Access

To use FIPS endpoint encryption

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Verify that the directory where you want to create FedRAMP-authorized and DoD SRG-compliant WorkSpaces does not have any existing WorkSpaces associated with it. If there are WorkSpaces associated with the directory and the directory is not already enabled to use FIPS 140-2 Validated Mode, either terminate the WorkSpaces or create a new directory.
4. Choose the directory that meets the above criteria, and then choose **Actions**, **Update Details**.
5. On the **Update Directory Details** page, choose the arrow to expand the **Access Control Options** section.
6. For **Endpoint Encryption**, choose **FIPS 140-2 Validated Mode** instead of **TLS Encryption Mode (Standard)**.
7. Choose **Update and Exit**.
8. You can now create WorkSpaces from this directory that are FedRAMP authorized and DoD SRG compliant. To access these WorkSpaces, users must use one of the WorkSpaces client applications listed earlier in the Requirements section.

Enable SSH connections for your Linux WorkSpaces in WorkSpaces Personal

If you or your users want to connect to your Linux WorkSpaces by using the command line, you can enable SSH connections. You can enable SSH connections to all WorkSpaces in a directory or to individual WorkSpaces in a directory.

To enable SSH connections, you create a new security group or update an existing security group and add a rule to allow inbound traffic for this purpose. Security groups act as a firewall for associated instances, controlling both inbound and outbound traffic at the instance level. After you create or update your security group, your users and others can use PuTTY or other terminals to connect from their devices to your Linux WorkSpaces. For more information, see the section called "Security groups".

For a video tutorial, see How can I connect to my Linux Amazon WorkSpaces using SSH? on the AWS Knowledge Center. This tutorial is for Amazon Linux 2 WorkSpaces only.

Contents

Prerequisites for SSH connections to Linux WorkSpaces

- Enabling inbound SSH traffic to a WorkSpace — To add a rule to allow inbound SSH traffic to one or more Linux WorkSpaces, make sure that you have the public or private IP addresses of the devices that require SSH connections to your WorkSpaces. For example, you can specify the public IP addresses of devices outside your virtual private cloud (VPC) or the private IP address of another EC2 instance in the same VPC as your WorkSpace.

  If you plan to connect to a WorkSpace from your local device, you can use the search phrase "what is my IP address" in an internet browser or use the following service: Check IP.
- Connecting to a WorkSpace — The following information is required to initiate an SSH connection from a device to a Linux WorkSpace.
  - The NetBIOS name of the Active Directory domain that you are connected to.
  - Your WorkSpace user name.
  - The public or private IP address of the WorkSpace that you want to connect to.

    Private: If your VPC is attached to a corporate network and you have access to that network, you can specify the private IP address of the WorkSpace.

Public: If your WorkSpace has a public IP address, you can use the WorkSpaces console to find the public IP address, as described in the following procedure.

To find the IP addresses for the Linux WorkSpace you want to connect to and your user name

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. In the list of WorkSpaces, choose the WorkSpace that you want to enable SSH connections to.
4. In the **Running mode** column, confirm that the WorkSpace status is **Available**.
5. Click the arrow to the left of the WorkSpace name to display the inline summary, and note the following information:

   - The **WorkSpace IP**. This is the private IP address of the WorkSpace.

     The private IP address is required for obtaining the elastic network interface associated with the WorkSpace. The network interface is required to retrieve information such as the security group or public IP address associated with the WorkSpace.
   - The WorkSpace **Username**. This is the user name that you specify to connect to the WorkSpace.
6. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
7. In the navigation pane, choose **Network Interfaces**.
8. In the search box, type the **WorkSpace IP** that you noted in Step 5.
9. Select the network interface associated with the **WorkSpace IP**.
10. If your WorkSpace has a public IP address, it is displayed in the **IPv4 Public IP** column. Make a note of this address, if applicable.

To find the NetBIOS name of the Active Directory domain that you are connected to

1. Open the AWS Directory Service console at https://console.aws.amazon.com/directoryservicev2/.
2. In the list of directories, click the **Directory ID** link of the directory for the WorkSpace.
3. In the **Directory details** section, note the **Directory NetBIOS name**.

Enable SSH connections to all Linux WorkSpaces in a directory

To enable SSH connections to all Linux WorkSpaces in a directory, do the following.

To create a security group with a rule to allow inbound SSH traffic to all Linux WorkSpaces in a directory

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose **Security Groups**.
3. Choose **Create Security Group**.
4. Type a name and optionally, a description for your security group.
5. For **VPC**, choose the VPC that contains the WorkSpaces that you want to enable SSH connections to.
6. On the **Inbound** tab, choose **Add Rule**, and do the following:
   - For **Type**, choose **SSH**.
   - For **Protocol**, TCP is automatically specified when you choose **SSH**.
   - For **Port Range**, 22 is automatically specified when you choose **SSH**.
   - For **Source**, specify the CIDR range of the public IP addresses for the computers that users will use to connect to their WorkSpaces. For example, a corporate network or a home network.
   - For **Description** (optional), type a description for the rule.
7. Choose **Create**.
8. Attach this security group to your WorkSpaces. For more information on adding this security group to your WorkSpaces, see Security groups for WorkSpaces Personal. If you want to automatically attach additional security groups to your WorkSpaces, refer to this blog post.

Password-based authentication in WorkSpaces

To enable password authentication in newly created Linux WorkSpaces

1. Launch the WorkSpaces client and login to your WorkSpace.
2. Open the Terminal window.
3. In the Terminal window, run the following command to enable SSH Password Authentication in cloud-init.

```
sudo bash -c 'touch /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && echo "ssh_pwauth:
 true" > /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && sudo rm /var/lib/cloud/
instance/sem/config_set_passwords && sudo cloud-init single --name set-passwords'
```

This script will do the following:

- Create a configuration file in the cloud-init directory `/etc/cloud/cloud.cfg.d/`.
- Modify the configuration file to tell cloud-init to enable SSH password authentication.
- Reset the `set-passwords` cloud-init module so that it can be run again.
- Run the `set-passwords` cloud-init module by itself. This will write a file that enables SSH password authentication to the SSH configuration directory, `/etc/ssh/sshd_config.d/`, and restart SSHD so that the setting will take place immediately.

This enables SSH password authentication on your WorkSpace and will persist through custom images. If you enable SSH password authentication only in the SSHD configuration file, without configuring cloud-init, the setting will not persist through imaging on some Linux WorkSpaces. For more information, see Set Passwords in the cloud-init module documentation.

To disable password authentication in existing Linux WorkSpaces

1. Launch the WorkSpaces client and login to your WorkSpace.
2. Open the Terminal window.
3. In the Terminal window, run the following command to disable SSH Password Authentication in cloud-init.

```
sudo bash -c 'touch /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && echo "ssh_pwauth:
 false" > /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && sudo rm /var/lib/cloud/
instance/sem/config_set_passwords && sudo cloud-init single –name set-passwords'
```

This script will do the following:

- Create a configuration file in the cloud-init directory `/etc/cloud/cloud.cfg.d/`.
- Modify the configuration file to tell cloud-init to disable SSH password authentication.
- Reset the `set-passwords` cloud-init module so that it can be run again.

- Run the `set-passwords` cloud-init module by itself. This will write a file that enables SSH password authentication to the SSH configuration directory, `/etc/ssh/sshd_config.d/`, and restart SSHD so that the setting will take place immediately.

This immediately disables SSH in the WorkSpace and will persist through custom images.

Enable SSH connections to a specific Linux WorkSpace

To enable SSH connections to a specific Linux WorkSpace, do the following.

To add a rule to an existing security group to allow inbound SSH traffic to a specific Linux WorkSpace

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, under **Network & Security**, choose **Network Interfaces**.
3. In the search bar, type the private IP address of the WorkSpace that you want to enable SSH connections to.
4. In the **Security groups** column, click the link for the security group.
5. On the **Inbound** tab, choose **Edit**.
6. Choose **Add Rule**, and then do the following:
   - For **Type**, choose **SSH**.
   - For **Protocol**, TCP is automatically specified when you choose **SSH**.
   - For **Port Range**, 22 is automatically specified when you choose **SSH**.
   - For **Source**, choose **My IP** or **Custom**, and specify a single IP address or an IP address range in CIDR notation. For example, if your IPv4 address is `203.0.113.25`, specify `203.0.113.25/32` to list this single IPv4 address in CIDR notation. If your company allocates addresses from a range, specify the entire range, such as `203.0.113.0/24`.
   - For **Description** (optional), type a description for the rule.
7. Choose **Save**.

Connect to a Linux WorkSpace using Linux or PuTTY

After you create or update your security group and add the required rule, your users and others can use Linux or PuTTY to connect from their devices to your WorkSpaces.

Note

Before completing either of the following procedures, make sure that you have the following:

- The NetBIOS name of the Active Directory domain that you are connected to.
- The username that you use to connect to the WorkSpace.
- The public or private IP address of the WorkSpace that you want to connect to.

For instructions on how to obtain this information, see "Prerequisites for SSH Connections to Linux WorkSpaces" earlier in this topic.

To connect to an Linux WorkSpace using Linux

1. Open the command prompt as an administrator and enter the following command. For *NetBIOS name*, *Username*, and *WorkSpace IP*, enter the applicable values.

   ```
   ssh "NetBIOS_NAME\Username"@WorkSpaceIP
   ```

   The following is an example of the SSH command where:

   - The *NetBIOS_NAME* is anycompany
   - The *Username* is janedoe
   - The *WorkSpace IP* is 203.0.113.25

   ```
   ssh "anycompany\janedoe"@203.0.113.25
   ```

2. When prompted, enter the same password that you use when authenticating with the WorkSpaces client (your Active Directory password).

To connect to an Linux WorkSpace using PuTTY

1. Open PuTTY.
2. In the **PuTTY Configuration** dialog box, do the following:

- For **Host Name (or IP address)**, enter the following command. Replace the values with the NetBIOS name of the Active Directory domain that you are connected to, the user name that you use to connect to the WorkSpace, and the IP address of the WorkSpace that you want to connect to.

  ```
  NetBIOS_NAME\Username@WorkSpaceIP
  ```

- For **Port**, enter **22**.
- For **Connection type**, choose **SSH**.

For an example of the SSH command, see step 1 in the previous procedure.

3. Choose **Open**.
4. When prompted, enter the same password that you use when authenticating with the WorkSpaces client (your Active Directory password).

Required configuration and service components for WorkSpaces Personal

As a WorkSpace administrator, you must understand the following about required configuration and service components.

- the section called “Routing table configuration”
- the section called “Components for Windows”
- the section called “Components for Linux”
- the section called “Components for Ubuntu”
- the section called “Components for Red Hat Enterprise Linux ”

Required routing table configuration

We recommend that you not modify the operating system-level routing table for a WorkSpace. The WorkSpaces service requires the preconfigured routes in this table to monitor the system state and update system components. If routing table changes are required for your organization, contact AWS Support or your AWS account team before applying any changes.

Required service components for Windows

On Windows WorkSpaces, the service components are installed in the following locations. Do not delete, change, block, or quarantine these objects. If you do so, the WorkSpace will not function correctly.

If antivirus software is installed on the WorkSpace, make sure it does not interfere with the service components installed in the following locations.

- `C:\Program Files\Amazon`
- `C:\Program Files\NICE`
- `C:\Program Files\Teradici`
- `C:\Program Files (x86)\Teradici`
- `C:\ProgramData\Amazon`
- `C:\ProgramData\NICE`
- `C:\ProgramData\Teradici`

If antivirus software is installed on the WorkSpaces Core, make sure it does not interfere with the service components installed in the following locations.

- C:\Program Files\Amazon
- C:\ProgramData\Amazon

32-bit PCoIP agent

As of March 29, 2021, we updated the PCoIP agent from 32-bit to 64-bit. For Windows WorkSpaces that are using the PCoIP protocol, this means that the location of the Teradici files changed from `C:\Program Files (x86)\Teradici` to `C:\Program Files\Teradici`. Because we updated PCoIP agents during regular maintenance windows, some of your WorkSpaces might have used the 32-bit agent longer than others during the transition.

If you've configured firewall rules, antivirus software exclusions (on the client side and host side), Group Policy Object (GPO) settings, or settings for Microsoft System Center Configuration Manager (SCCM), Microsoft Endpoint Configuration Manager, or similar configuration management tools based on the full path to the 32-bit agent, you must also add the full path to the 64-bit agent to those settings.

If you're filtering on the paths to any 32-bit PCoIP components, be sure to add the paths to the 64-bit versions of the components. Because your WorkSpaces might not all be updated at the same time, do not replace the 32-bit path with the 64-bit path, or some of your WorkSpaces might not work. For example, if you're basing your exclusions or communication filters on `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_server_win32.exe`, you must also add `C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_server.exe`. Likewise, if you're basing your exclusions or communications filters on `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_agent.exe`, you must also add `C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_agent.exe`.

PCoIP arbiter service change — Be aware that the PCoIP arbiter service (`C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_arbiter_win32.exe`) is removed when your WorkSpaces are updated to use the 64-bit agent.

PCoIP zero clients and USB devices — Starting with version 20.10.4 of the PCoIP agent, Amazon WorkSpaces disables USB redirection by default through the Windows registry. This registry setting affects the behavior of USB peripherals when your users are using PCoIP zero client devices to connect to their WorkSpaces. For more information, see USB printers and other USB peripherals aren't working for PCoIP zero clients.

Required service components for Linux

On Amazon Linux WorkSpaces, the service components are installed in the following locations. Do not delete, change, block, or quarantine these objects. If you do so, the WorkSpace will not function correctly.

> **Note**
>
> Making changes to files other than `/etc/pcoip-agent/pcoip-agent.conf` might cause your WorkSpaces to stop working and might require you to rebuild them. For information about modifying `/etc/pcoip-agent/pcoip-agent.conf`, see Manage your Amazon Linux WorkSpaces in WorkSpaces Personal.

- `/etc/dhcp/dhclient.conf`
- `/etc/logrotate.d/pcoip-agent`
- `/etc/logrotate.d/pcoip-server`

- /etc/os-release
- /etc/pam.d/pcoip
- /etc/pam.d/pcoip-session
- /etc/pcoip-agent
- /etc/profile.d/system-restart-check.sh
- /etc/X11/default-display-manager
- /etc/yum/pluginconf.d/halt_os_update_check.conf
- /etc/systemd/system/euc-analytic-agent.service
- /lib/systemd/system/pcoip.service
- /lib/systemd/system/pcoip-agent.service
- /lib64/security/pam_self.so
- /usr/bin/pcoip-fne-view-license
- /usr/bin/pcoip-list-licenses
- /usr/bin/pcoip-validate-license
- /usr/bin/euc-analytics-agent
- /usr/lib/firewalld/services/pcoip-agent.xml
- /usr/lib/modules-load.d/usb-vhci.conf
- /usr/lib/pcoip-agent
- /usr/lib/skylight
- /usr/lib/systemd/system/pcoip.service
- /usr/lib/systemd/system/pcoip.service.d/
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/tmpfiles.d/pcoip-agent.conf
- /usr/lib/yum-plugins/halt_os_update_check.py
- /usr/sbin/pcoip-agent
- /usr/sbin/pcoip-register-host
- /usr/sbin/pcoip-support-bundler
- /usr/share/doc/pcoip-agent
- /usr/share/pcoip-agent

- /usr/share/selinux/packages/pcoip-agent.pp
- /usr/share/X11
- /var/crash/pcoip-agent
- /var/lib/pcoip-agent
- /var/lib/skylight
- /var/log/pcoip-agent
- /var/log/skylight
- /var/logs/wsp
- /var/log/eucanalytics

Required service components for Ubuntu

On Ubuntu WorkSpaces, the service components are installed in the following locations. Do not delete, change, block, or quarantine these objects. If you do so, the WorkSpace will not function correctly.

- /etc/X11/default-display-manager
- /etc/dcv
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan
- /etc/os-release
- /etc/pam.d/dcv
- /etc/pam.d/dcv-graphical-sso
- /etc/sssd/sssd.conf
- /etc/wsp
- /etc/systemd/system/euc-analytic-agent.service
- /lib64/security/pam_self.so
- /usr/lib/skylight
- /usr/lib/systemd/system/dcvserver.service
- /usr/lib/systemd/system/dcvsessionlauncher.service
- /usr/lib/systemd/system/skylight-agent.service

- /usr/lib/systemd/system/wspdcvhostadapter.service
- /usr/share/X11
- /usr/bin/euc-analytics-agent
- /var/lib/skylight
- /var/log/skylight
- /var/log/eucanalytics

Required service components for Red Hat Enterprise Linux

On Red Hat Enterprise Linux WorkSpaces, the service components are installed in the following locations. Do not delete, change, block, or quarantine these objects. If you do so, the WorkSpace will not function correctly.

- /etc/dcv
- /etc/os-release
- /etc/pam.d/dcv-graphical-sso
- /etc/pam.d/dcv
- /etc/systemd/system/euc-analytic-agent.service
- /etc/wsp
- /usr/bin/euc-analytics-agent
- /usr/lib/skylight
- /usr/lib/systemd/system/dcvserver.service
- /usr/lib/systemd/system/dcvsessionlauncher.service
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/systemd/system/wspdcvhostadapter.service
- /usr/lib/systemd/system/xdcv-console.path
- /usr/lib/systemd/system/xdcv-console.service
- /usr/lib/systemd/system/xdcv-console-update.service
- /usr/share/X11
- /var/log/eucanalytics
- /var/log/skylight

Manage directories for WorkSpaces Personal

WorkSpaces uses a directory to store and manage information for your WorkSpaces and users. You can use one of the following options:

- AD Connector — Use your existing on-premises Microsoft Active Directory. Users can sign into their WorkSpaces using their on-premises credentials and access on-premises resources from their WorkSpaces.
- AWS Managed Microsoft AD — Create a Microsoft Active Directory hosted on AWS.
- Simple AD — Create a directory that is compatible with Microsoft Active Directory, powered by Samba 4, and hosted on AWS.
- Cross trust — Create a trust relationship between your AWS Managed Microsoft AD directory and your on-premises domain.
- Microsoft Entra ID — Create a directory that uses Microsoft Entra ID as its identity source (through IAM Identity Center). Personal WorkSpaces in the directory are joined using Microsoft Entra's native authentication and are enrolled into Microsoft Intune through Microsoft Windows Autopilot user-driven mode. Directories using Microsoft Entra ID only support Windows 10 and 11 Bring Your Own Licenses WorkSpaces.
- Custom — Create a directory that use an identity provider of your choice (through IAM Identity Center). WorkSpaces in the directory are managed using the device management solution of your choice such as JumpCloud. Directories using custom identity providers only support Windows 10 and 11 Bring Your Own Licenses WorkSpaces.

For tutorials that demonstrate how to set up these directories and launch WorkSpaces, see Create a directory for WorkSpaces Personal.

> **Tip**
>
> For a detailed exploration of directory and virtual private cloud (VPC) design considerations for various deployment scenarios, see Best Practices for Deploying Amazon WorkSpaces.

After you create a directory, you'll perform most directory administration tasks using tools such as the Active Directory Administration Tools. You can perform some directory administration tasks using the WorkSpaces console and other tasks using Group Policy. For more information about

managing users and groups, see Manage users in WorkSpaces Personal and Set up Active Directory Administration Tools for WorkSpaces Personal.

Note

- Shared directories are not currently supported for use with Amazon WorkSpaces.
- If you configure your AWS Managed Microsoft AD directory for multi-Region replication, only the directory in the primary Region can be registered for use with Amazon WorkSpaces. Attempts to register the directory in a replicated Region for use with Amazon WorkSpaces will fail. Multi-Region replication with AWS Managed Microsoft AD isn't supported for use with Amazon WorkSpaces within replicated Regions.
- Simple AD and AD Connector are made available to you free of charge to use with WorkSpaces. If there are no WorkSpaces being used with your Simple AD or AD Connector directory for 30 consecutive days, this directory will be automatically deregistered for use with Amazon WorkSpaces, and you will be charged for this directory as per the AWS Directory Service pricing terms.

  To delete empty directories, see Delete a directory for WorkSpaces Personal. If you delete your Simple AD or AD Connector directory, you can always create a new one when you want to start using WorkSpaces again.

Contents

Register an existing AWS Directory Service directory with WorkSpaces Personal

To allow WorkSpaces to use an existing AWS Directory Service directory, you must register it with WorkSpaces. After you register a directory, you can launch WorkSpaces in the directory.

Requirements

To register a directory for use with WorkSpaces, it must meet the following requirement:

- If you're using AWS Managed Microsoft AD or Simple AD, your directory can be in a dedicated private subnet, as long as the directory has access to the VPC where the WorkSpaces are located.

For more information about directory and VPC design, see the *Best Practices for Deploying Amazon WorkSpaces* whitepaper.

> **Note**
>
> Simple AD and AD Connector are made available to you free of charge to use with WorkSpaces. If there are no WorkSpaces being used with your Simple AD or AD Connector directory for 30 consecutive days, this directory will be automatically deregistered for use with Amazon WorkSpaces, and you will be charged for this directory as per the AWS Directory Service pricing terms.
> To delete empty directories, see Delete a directory for WorkSpaces Personal. If you delete your Simple AD or AD Connector directory, you can always create a new one when you want to start using WorkSpaces again.

To register an existing AWS Directory Service directory

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Choose **Create directory**.
4. On the **Create directory** page, for **WorkSpaces type** choose **Personal**. For **WorkSpace device management**, choose **AWS Directory Service**.
5. Select the directory you want to register in the **Directories in AWS Directory Service** table

6. Select two subnets of your VPC that are not from the same Availability Zone. These subnets will be used to launch your WorkSpaces. For more information, see Availability Zones for WorkSpaces Personal.

   > **Note**
   >
   > If you do not know which subnets to choose, select **No Preference**.

7. For **Enable Self Service Permissions**, choose **Yes** to enable your users to rebuild their WorkSpaces, change volume size, compute type and running mode. Enabling may impact how much you pay for Amazon WorkSpaces. Choose **No** otherwise.
8. For **Enable Amazon WorkDocs**, choose **Yes** to register the directory for use with Amazon WorkDocs or **No** otherwise.

   > **Note**
   >
   > This option is displayed only if Amazon WorkDocs is available in the Region and if you're not using AWS Managed Microsoft AD. If you're using AWS Managed Microsoft AD, finish registering your directory, and then see Enable Amazon WorkDocs for AWS Managed Microsoft AD.

9. Choose **Register**. Initially the value of **Registered** is `REGISTERING`. After registration is complete, the value is `Yes`.

After you've registered the AWS Directory Service directory, you can create a personal WorkSpace. For more information, see Create a WorkSpace in WorkSpaces Personal.

When you are finished using the directory with WorkSpaces, you can deregister it. Note that you must deregister a directory before you can delete it. If you want to deregister and delete a directory, you must first find and remove all the applications and services that are registered to the directory. For more information, see Delete Your Directory in the *AWS Directory Service Administration Guide*.

To deregister a directory

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select the directory.

4. Choose **Actions**, **Deregister**.
5. When prompted for confirmation, choose **Confirm**. After deregistration is complete, the directory becomes unregistered and is removed from the list.

Update directory details for WorkSpaces Personal

You can complete the following directory management tasks using the WorkSpaces console.

Tasks

- Select an organizational unit
- Configure automatic public IP addresses
- Control device access
- Manage local administrator permissions
- Update the AD Connector account (AD Connector)
- Multi-factor authentication (AD Connector)

Select an organizational unit

> **Note**
>
> This feature is only available for directories managed through AWS Directory Service, including AD Connector, AWS Managed Microsoft AD, and Simple AD.

WorkSpace machine accounts are placed in the default organizational unit (OU) for the WorkSpaces directory. Initially, the machine accounts are placed in the Computers OU of your directory or the directory that your AD Connector is connected to. You can select a different OU from your directory or connected directory, or specify an OU in a separate target domain. Note that you can select only one OU per directory.

After you select a new OU, the machine accounts for all WorkSpaces that are created or rebuilt are placed in the newly selected OU.

To select an organizational unit

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.

2. In the navigation pane, choose **Directories**.
3. Choose your directory.
4. Under Target domain and organizational unit, choose **Edit**.
5. To find an OU, under Target and organizational unit, you can start typing all or part of the OU name and choose the OU you want to use.
6. (Optional) Choose an OU distiguished name to overwrite your selected OU with a custom OU.
7. Choose **Save**.
8. (Optional) Rebuild the existing WorkSpaces to update the OU. For more information, see Rebuild a WorkSpace in WorkSpaces Personal.

Configure automatic public IP addresses

After you enable automatic assignment of public IP addresses, each WorkSpace that you launch is assigned a public IP address from the Amazon-provided pool of public addresses. A WorkSpace in a public subnet can access the internet through the internet gateway if it has a public IP address. WorkSpaces that already exist before you enable automatic assignment do not receive public addresses until you rebuild them.

Note that you do not need to enable automatic assignment of public addresses if your WorkSpaces are in private subnets and you configured a NAT gateway for the virtual private cloud (VPC), or if your WorkSpaces are in public subnets and you assigned them Elastic IP addresses. For more information, see Configure a VPC for WorkSpaces Personal.

> **Warning**
>
> If you associate an Elastic IP address that you own to a WorkSpace, and then you later disassociate that Elastic IP address from the WorkSpace, the WorkSpace loses its public IP address, and it doesn't automatically get a new one from the Amazon-provided pool. To associate a new public IP address from the Amazon-provided pool with the WorkSpace, you must rebuild the WorkSpace. If you don't want to rebuild the WorkSpace, you must associate another Elastic IP address that you own to the WorkSpace.

To configure Elastic IP addresses

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.

2. In the navigation pane, choose **Directories**.
3. Select the directory for your WorkSpaces.
4. Choose **Actions**, **Update Details**.
5. Expand **Access to Internet** and select **Enable** or **Disable**.
6. Choose **Update**.

Control device access

You can specify the types of devices that have access to WorkSpaces. In addition, you can restrict access to WorkSpaces to trusted devices (also known as managed devices).

To control device access to WorkSpaces

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Choose your directory.
4. Under Access control options, choose **Edit**.
5. Under Trusted devices, specify which device types can access WorkSpaces by selecting either **Allow all**, **Trusted devices**, or **Deny all**. For more information, see Restrict access to trusted devices for WorkSpaces Personal.
6. Choose **Save**.

Manage local administrator permissions

> **Note**
>
> This feature is only available for directories managed through AWS Directory Service, including AD Connector, AWS Managed Microsoft AD, and Simple AD.

You can specify whether users are local administrators on their WorkSpaces, which enables them to install application and modify settings on their WorkSpaces. Users are local administrators by default. If you modify this setting, the change applies to all new WorkSpaces that you create and any WorkSpaces that you rebuild.

To modify local administrator permissions

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Choose your directory.
4. Under Local administrator settings, choose **Edit**.
5. To ensure that users are local administrators, choose **Enable local administrator setting**.
6. Choose **Save**.

Update the AD Connector account (AD Connector)

You can update the AD Connector account that is used to read users and groups and join WorkSpaces machine accounts to your AD Connector directory.

To update the AD Connector account

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory and then choose **View details**.
4. Under AD connector account, choose **Edit**.
5. Enter the sign-in credentials for the new account.
6. Choose **Save**.

Multi-factor authentication (AD Connector)

You can enable multi-factor authentication (MFA) for your AD Connector directory. For more information about using multi-factor authentication with AWS Directory Service, see Enable multi-factor authentication for AD Connector and AD Connector prerequisites.

Note

- Your RADIUS server can either be hosted by AWS or it can be on-premises.
- The usernames must match between Active Directory and your RADIUS server.

To enable multi-factor authentication

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory and then choose **Actions**, **Update Details**.
4. Expand **Multi-Factor Authentication** and then select **Enable Multi-Factor Authentication**.
5. For **RADIUS server IP address(es)**, type the IP addresses of your RADIUS server endpoints separated by commas, or type the IP address of your RADIUS server load balancer.
6. For **Port**, type the port that your RADIUS server is using for communications. Your on-premises network must allow inbound traffic over the default RADIUS server port (UDP:1812) from AD Connector.
7. For **Shared secret code** and **Confirm shared secret code**, type the shared secret code for your RADIUS server.
8. For **Protocol**, choose the protocol for your RADIUS server.
9. For **Server timeout**, type the time, in seconds, to wait for the RADIUS server to respond. This value must be between 1 and 50.
10. For **Max retries**, type the number of times to attempt communication with the RADIUS server. This value must be between 0 and 10.
11. Choose **Update and Exit**.

Multi-factor authentication is available when **RADIUS status** is **Enabled**. While multi-factor authentication is being set up, users cannot log in to their WorkSpaces.

Create a directory for WorkSpaces Personal

Personal WorkSpaces allows you to use directories managed through AWS Directory Service to store and manage information for your WorkSpaces and users. The following are options for creating a WorkSpaces Personal directory:

- Create a Simple AD directory.
- Create an AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD.
- Connect to an existing Microsoft Active Directory by using Active Directory Connector.
- Create a trust relationship between your AWS Managed Microsoft AD directory and your on-premises domain.

- Create a dedicated Microsoft Entra ID WorkSpaces directory.
- Create a dedicated Custom WorkSpaces directory.

Contents

Identify the computer name

The **Computer Name** value shown for a WorkSpace in the Amazon WorkSpaces console varies, depending on which type of WorkSpace you've launched (Amazon Linux, Ubuntu, or Windows). The computer name for a WorkSpace can be in one of these formats:

- **Amazon Linux**: A-*xxxxxxxxxxxxx*
- **Red Hat Enterprise Linux**: R-*xxxxxxxxxxxxx*
- **Ubuntu**: U-*xxxxxxxxxxxxx*
- **Windows**: IP-C*xxxxxx* or WSAMZN-*xxxxxxx* or EC2AMAZ-*xxxxxxx*

For Windows WorkSpaces, the computer name format is determined by the bundle type, and in the case of WorkSpaces created from public bundles or from custom bundles based on public images, by when the public images were created.

Starting June 22, 2020, Windows WorkSpaces launched from public bundles have the WSAMZN-*xxxxxxx* format for their computer names instead of the IP-C*xxxxxx* format.

For custom bundles based on a public image, if the public image was created before June 22, 2020, the computer names are in the EC2AMAZ-*xxxxxxx* format. If the public image was created on or after June 22, 2020, the computer names are in the WSAMZN-*xxxxxxx* format.

For Bring Your Own License (BYOL) bundles, either the DESKTOP-*xxxxxxx* or the EC2AMAZ-*xxxxxxx* format is used for the computer names by default.

If you've specified a custom format for the computer names in your custom or BYOL bundles, your custom format overrides these defaults. To specify a custom format, see Create a custom WorkSpaces image and bundle for WorkSpaces Personal.

Important

If you change the computer name for a WorkSpace through the Windows system settings, you will no longer be able to access the WorkSpace.

Note

- Shared directories are not currently supported for use with Amazon WorkSpaces.
- If you configure your AWS Managed Microsoft AD directory for multi-Region replication, only the directory in the primary Region can be registered for use with Amazon WorkSpaces. Attempts to register the directory in a replicated Region for use with Amazon WorkSpaces will fail. Multi-Region replication with AWS Managed Microsoft AD isn't supported for use with Amazon WorkSpaces within replicated Regions.
- Simple AD and AD Connector are made available to you free of charge to use with WorkSpaces. If there are no WorkSpaces being used with your Simple AD or AD Connector directory for 30 consecutive days, this directory will be automatically deregistered for use with Amazon WorkSpaces, and you will be charged for this directory as per the AWS Directory Service pricing terms.

The following tutorials show you how to create a WorkSpaces Personal directory.

Before you begin creating a directory

- WorkSpaces is not available in every Region. Verify the supported Regions and select a Region for your WorkSpaces. For more information about the supported Regions, see WorkSpaces Pricing by AWS Region.
- Create a virtual private cloud with at least two private subnets. For more information, see Configure a VPC for WorkSpaces Personal. The VPC must be connected to your on-premises

network through a virtual private network (VPN) connection or AWS Direct Connect. For more information, see AD Connector Prerequisites in the *AWS Directory Service Administration Guide*.

- Provide access to the internet from the WorkSpace. For more information, see Provide internet access for WorkSpaces Personal.

Create an AWS Managed Microsoft AD directory

In this tutorial, we create an AWS Managed Microsoft AD directory. For tutorials that use the other options, see Create a directory for WorkSpaces Personal.

First, create an AWS Managed Microsoft AD directory. AWS Directory Service creates two directory servers, one in each of the private subnets of your VPC. Note that there are no users in the directory initially. You will add a user in the next step when you launch the WorkSpace.

> **Note**
>
> - Shared directories are not currently supported for use with Amazon WorkSpaces.
> - If your AWS Managed Microsoft AD directory has been configured for multi-Region replication, only the directory in the primary Region can be registered for use with Amazon WorkSpaces. Attempts to register the directory in a replicated Region for use with Amazon WorkSpaces will fail. Multi-Region replication with AWS Managed Microsoft AD isn't supported for use with Amazon WorkSpaces within replicated Regions.

To create an AWS Managed Microsoft AD directory

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Choose **Create directory**.
4. On the **Create directory** page, for **WorkSpaces type** choose **Personal**. Then, for **WorkSpace device management** choose **AWS Directory Service**.
5. Choose **Create directory**, which opens the **Set up a directory** page on the AWS Directory Service
6. Choose **AWS Managed Microsoft AD**, and then **Next**.
7. Configure the directory as follows:

a. For **Organization name**, enter a unique organization name for your directory (for example, my-demo-directory). This name must be at least four characters in length, consist of only alphanumeric characters and hyphens (-), and begin or end with a character other than a hyphen.

b. For **Directory DNS**, enter the fully-qualified name for the directory (for example, workspaces.demo.com).

> **Important**
>
> If you need to update your DNS server after launching your WorkSpaces, follow the procedure in Update DNS servers for WorkSpaces Personal to ensure that your WorkSpaces get properly updated.

c. For **NetBIOS name**, enter a short name for the directory (for example, workspaces).

d. For **Admin password** and **Confirm password**, enter a password for the directory administrator account. For more information about the password requirements, see Create Your AWS Managed Microsoft AD Directory in the *AWS Directory Service Administration Guide*.

e. (Optional) For **Description**, enter a description for the directory.

f. For **VPC**, select the VPC that you created.

g. For **Subnets**, select the two private subnets (with the CIDR blocks `10.0.1.0/24` and `10.0.2.0/24`).

h. Choose **Next Step**.

8. Choose **Create directory**.

9. You will be brought back to the Create directory page on WorkSpaces console. The initial status of the directory is `Requested` and then `Creating`. When directory creation is complete (this might take a few minutes), the status is `Active`.

After you've created an AWS Managed Microsoft AD directory, you can register it with Amazon WorkSpaces. For more information, see Register an existing AWS Directory Service directory with WorkSpaces Personal

Create a Simple AD directory

In this tutorial, we launch a WorkSpace that uses Simple AD. For tutorials that use the other options, see Create a directory for WorkSpaces Personal.

> **Note**
>
> - Simple AD is not available in every Region. Verify the supported Regions and select a Region for your Simple AD directory. For more information about the supported Regions for Simple AD, see Region Availability for AWS Directory Service.
> - Simple AD is made available to you free of charge to use with WorkSpaces. If there are no WorkSpaces being used with your Simple AD directory for 30 consecutive days, this directory will be automatically deregistered for use with Amazon WorkSpaces, and you will be charged for this directory as per the AWS Directory Service pricing terms.

When you create a Simple AD directory. AWS Directory Service creates two directory servers, one in each of the private subnets of your VPC. There are no users in the directory initially. Add a user after you create the WorkSpace. For more information, see Create a WorkSpace in WorkSpaces Personal

To create a Simple AD directory

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Choose **Create directory**.
4. On the **Create directory** page, for **WorkSpaces type** choose **Personal**. Then, for **WorkSpace device management** choose **AWS Directory Service**.
5. Choose **Create directory**, which opens the **Set up a directory** page on the AWS Directory Service
6. Choose **Simple AD**, and then **Next**.
7. Configure the directory as follows:

    a. For **Organization name**, enter a unique organization name for your directory (for example, my-example-directory). This name must be at least four characters in length, consist of only alphanumeric characters and hyphens (-), and begin or end with a character other than a hyphen.

b. For **Directory DNS name**, enter the fully-qualified name for the directory (for example, example.com).

> **Important**
>
> If you need to update your DNS server after launching your WorkSpaces, follow the procedure in Update DNS servers for WorkSpaces Personal to ensure that your WorkSpaces get properly updated.

c. For **NetBIOS name**, enter a short name for the directory (for example, example).

d. For **Admin password** and **Confirm password**, enter a password for the directory administrator account. For more information about the password requirements, see How to Create a Microsoft AD Directory in the *AWS Directory Service Administration Guide*.

e. (Optional) For **Description**, enter a description for the directory.

f. For **Directory size**, choose **Small**.

g. For **VPC**, select the VPC that you created.

h. For **Subnets**, select the two private subnets (with the CIDR blocks `10.0.1.0/24` and `10.0.2.0/24`).

i. Choose **Next**.

8. Choose **Create directory**.
9. You will be brought back to the Create directory page on WorkSpaces console. The initial status of the directory is `Requested` and then `Creating`. When directory creation is complete (this might take a few minutes), the status is `Active`.

What happens during directory creation

WorkSpaces completes the following tasks on your behalf:

- Creates an IAM role to allow the WorkSpaces service to create elastic network interfaces and list your WorkSpaces directories. This role has the name `workspaces_DefaultRole`.
- Sets up a Simple AD directory in the VPC that is used to store user and WorkSpace information. The directory has an administrator account with the user name Administrator and the specified password.
- Creates two security groups, one for directory controllers and another for WorkSpaces in the directory.

After you've created an Simple AD directory, you can register it with Amazon WorkSpaces. For more information, see Register an existing AWS Directory Service directory with WorkSpaces Personal

Create an AD Connector

In this tutorial, we create an AD Connector. For tutorials that use the other options, see Create a directory for WorkSpaces Personal.

Create an AD Connector

> **Note**
>
> AD Connector is made available to you free of charge to use with WorkSpaces. If there are no WorkSpaces being used with your AD Connector directory for 30 consecutive days, this directory will be automatically deregistered for use with Amazon WorkSpaces, and you will be charged for this directory as per the AWS Directory Service pricing terms.
> To delete empty directories, see Delete a directory for WorkSpaces Personal. If you delete your AD Connector directory, you can always create a new one when you want to start using WorkSpaces again.

To create an AD Connector

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Choose **Create directory**.
4. On the **Create directory** page, for **WorkSpaces type** choose **Personal**. Then, for **WorkSpace device management** choose **AWS Directory Service**.
5. Choose **Create directory**, which opens the **Set up a directory** page on the AWS Directory Service
6. Choose **AWS Managed Microsoft AD**, and then **Next**.
7. For **Organization name**, enter a unique organization name for your directory (for example, my-example-directory). This name must be at least four characters in length, consist of only alphanumeric characters and hyphens (-), and begin or end with a character other than a hyphen.
8. For **Connected directory DNS**, enter the fully-qualified name of your on-premises directory (for example, example.com).

9. For **Connected directory NetBIOS name**, enter the short name of your on-premises directory (for example, example).
10. For **Connector account username**, enter the user name of a user in your on-premises directory. The user must have permissions to read users and groups, create computer objects, and join computers to the domain.
11. For **Connector account password** and **Confirm password**, enter the password for the on-premises user.
12. For **DNS address**, enter the IP address of at least one DNS server in your on-premises directory.

> **Important**
>
> If you need to update your DNS server IP address after launching your WorkSpaces, follow the procedure in Update DNS servers for WorkSpaces Personal to ensure that your WorkSpaces get properly updated.

13. (Optional) For **Description**, enter a description for the directory.
14. Keep **Size** as **Small**.
15. For **VPC**, select your VPC.
16. For **Subnets**, select your subnets. The DNS servers that you specified must be accessible from each subnet.
17. Choose **Create directory**.
18. You will be brought back to the Create directory page on WorkSpaces console. The initial status of the directory is `Requested` and then `Creating`. When directory creation is complete (this might take a few minutes), the status is `Active`.

Create a trust relationship between your AWS Managed Microsoft AD directory and your on-premises domain

In this tutorial, we create a trust relationship between your AWS Managed Microsoft AD directory and your on-premises domain. For tutorials that use the other options, see Create a directory for WorkSpaces Personal.

> **Note**
>
> Launching WorkSpaces with AWS accounts in a separate trusted domain works with AWS Managed Microsoft AD when it is configured with a trust relationship to your on-

premises directory. However, WorkSpaces using Simple AD or AD Connector cannot launch WorkSpaces for users from a trusted domain.

To set up the trust relationship

1. Set up AWS Managed Microsoft AD in your virtual private cloud (VPC). For more information, see Create Your AWS Managed Microsoft AD directory in the *AWS Directory Service Administration Guide*.

   Note

   - Shared directories are not currently supported for use with Amazon WorkSpaces.
   - If your AWS Managed Microsoft AD directory has been configured for multi-Region replication, only the directory in the primary Region can be registered for use with Amazon WorkSpaces. Attempts to register the directory in a replicated Region for use with Amazon WorkSpaces will fail. Multi-Region replication with AWS Managed Microsoft AD isn't supported for use with Amazon WorkSpaces within replicated Regions.

2. Create a trust relationship between your AWS Managed Microsoft AD and your on-premises domain. Ensure that the trust is configured as a two-way trust. For more information, see Tutorial: Create a Trust Relationship Between Your AWS Managed Microsoft AD and Your On-Premises Domain in the *AWS Directory Service Administration Guide*.

A one-way or two-way trust can be used to manage and authenticate with WorkSpaces, and so that WorkSpaces can be provisioned to on-premises users and groups. For more information, see Deploy Amazon WorkSpaces using a One-Way Trust Resource Domain with AWS Directory Service.

Note

- Red Hat Enterprise Linux and Ubuntu WorkSpaces use System Security Services Daemon (SSSD) for Active Directory integration, and SSSD does not support forest trust. Configure external trust instead. Two-way trust is recommended for Amazon Linux, Ubuntu, and Red Hat Enterprise Linux WorkSpaces.
- You cannot use a web browser (Web Access) to connect to Linux WorkSpaces.

Create a dedicated Microsoft Entra ID directory with WorkSpaces Personal

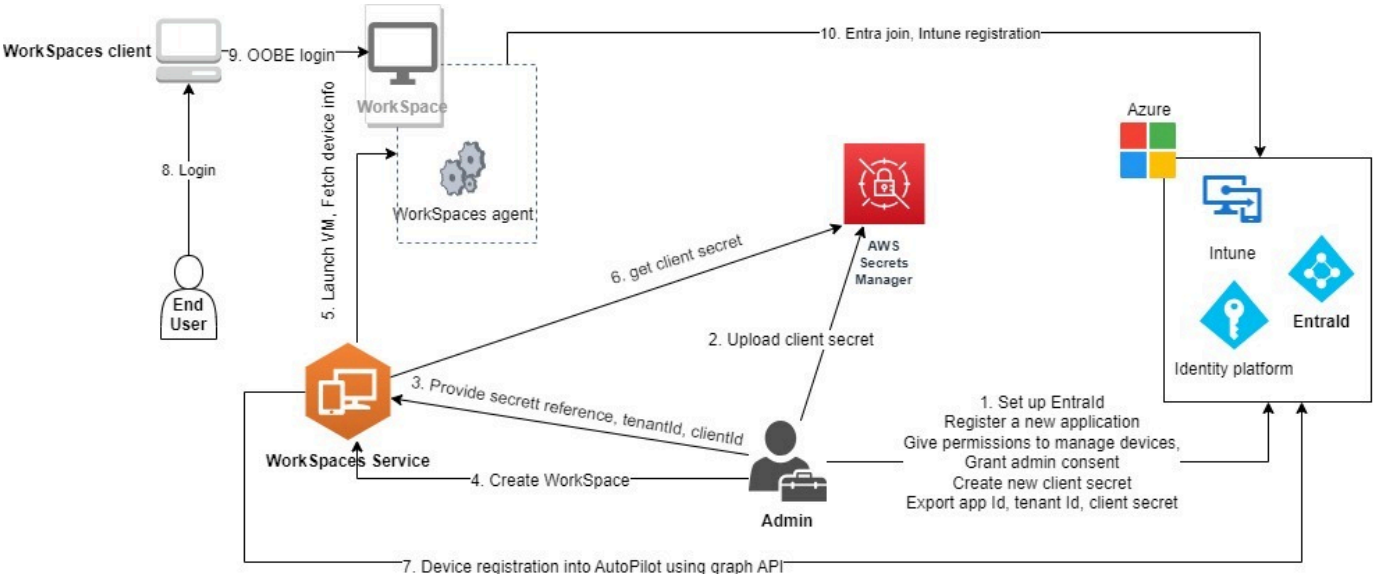
In this tutorial, we create Bring Your Own License (BYOL) Windows 10 and 11 personal WorkSpaces that are Microsoft Entra ID joined and enrolled to Microsoft Intune. Before creating such WorkSpaces, you need to first create a dedicated WorkSpaces Personal directory for Entra ID-joined WorkSpaces.

> **Note**
>
> Microsoft Entra joined personal WorkSpaces are available in all AWS regions where Amazon WorkSpaces is offered except for Africa (Cape Town), Israel (Tel Aviv), and China (Ningxia).

Contents

Overview

A Microsoft Entra ID personal WorkSpaces directory contains all the information needed to launch Microsoft Entra ID-joined WorkSpaces that are assigned to your users managed with Microsoft Entra ID. User information is made available to WorkSpaces through AWS IAM Identity Center, which acts as an identity broker to bring your workforce identity from Entra ID to AWS. Microsoft Windows Autopilot user-driven mode is used to accomplish WorkSpaces Intune enrollment and Entra join. The following diagram illustrates the Autopilot process.



Requirements and limitations

- Microsoft Entra ID P1 plan or higher.
- Microsoft Entra ID and Intune is enabled and have role assignments.
- Intune administrator - Required for managing Autopilot deployment profiles.
- Global administrator - Required for granting admin consent for the API permissions assigned to the application created in step 3. The application can be created without this permission. However, a Global Administrator would need to provide admin consent on the application permissions.
- Assign VDA E3/E5 user subscription licenses to users so their Windows 10 or 11 WorkSpaces can be joined to Entra ID.
- Entra ID directories only support Windows 10 or 11 Bring Your Own License personal WorkSpaces. The following are supported versions.
  - Windows 10 Version 21H2 (December 2021 Update)
  - Windows 10 Version 22H2 (November 2022 Update)
  - Windows 11 Enterprise 23H2 (October 2023 release)
  - Windows 11 Enterprise 22H2 (October 2022 release)
- Bring Your Own License (BYOL) is enabled for your AWS account and you have a valid Windows 10 or 11 BYOL image imported in your account. For more information, see Bring Your Own Windows desktop licenses in WorkSpaces.
- Microsoft Entra ID directories only support Windows 10 or 11 BYOL personal WorkSpaces.

- Microsoft Entra ID directories support only WSP protocol.

Step 1: Enable IAM Identity Center and synchronize with Microsoft Entra ID

To create Microsoft Entra ID-joined personal WorkSpaces and assign them to your Entra ID users, you have to make the user information available to AWS through IAM Identity Center. IAM Identity Center is the recommended AWS service for managing user access to AWS resources. For more information, see What is IAM Identity Center?. This is a one-time setup.

> **Note**
>
> A WorkSpaces Personal directory and its associated IAM Identity Center instance must be in the same AWS region.

1. Enable IAM Identity Center with your AWS Organizations, especially if you are using a multi-account environment. You can also create an account instance of IAM Identity Center. To learn more, see Enabling AWS IAM Identity Center. Each WorkSpaces directory can be associated with one IAM Identity Center instance, organization or account.

   If you are using an organization instance and trying to create a WorkSpaces directory in one of the member accounts, make sure you have the following IAM Identity Center permissions.

   - `"sso:DescribeInstance"`
   - `"sso:CreateApplication"`
   - `"sso:PutApplicationGrant"`
   - `"sso:PutApplicationAuthenticationMethod"`
   - `"sso:DeleteApplication"`
   - `"sso:DescribeApplication"`
   - `"sso:getApplicationGrant"`

   For more information, see Overview of managing access permissions to your IAM Identity Center resources. Also, ensure that no Service Control Policies (SCPs) are blocking these permissions. To learn more about SCPs, see Service control policies (SCPs).
2. Configure IAM Identity Center and Microsoft Entra ID to automatically synchronize selected or all users from your Entra ID tenant to your IAM Identity Center instance. For more information,

see Configure SAML and SCIM with Microsoft Entra ID and IAM Identity Center and Tutorial: Configure AWS IAM Identity Center for automatic user provisioning.

3. Verify that the users you configured on Microsoft Entra ID are synchronized correctly to AWS IAM Identity Center instance. If you see an error message, "Request is unparsable, syntactically incorrect, or violates schema", from Microsoft Entra ID, it indicates that the user in Entra ID is configured in a way that IAM Identity Center doesn't support. For example, the user object in Entra ID lacks a first name, a last name, and/or a display name. For more information, see Specific users fail to synchronize into IAM Identity Center from an external SCIM provider.

> **Note**
>
> WorkSpaces uses Entra ID UserPrincipalName (UPN) attribute to identify individual users and the following are its limitations:
>
> - UPNs cannot exceed 63 characters in length.
> - If you change the UPN after assigning a WorkSpace to a user, the user won't be able to connect to their WorkSpace unless you change the UPN back to what it was before.

Step 2: Register a Microsoft Entra ID application to grant permissions for Windows Autopilot

WorkSpaces Personal uses Microsoft Windows Autopilot user-driven mode to enroll WorkSpaces to Microsoft Intune and join them to Microsoft Entra ID.

To allow Amazon WorkSpaces to register WorkSpaces Personal into Autopilot, you must register a Microsoft Entra ID application that grants necessary Microsoft Graph API permissions. For more information about registering an Entra ID application, see Quickstart: Register an application with the Microsoft identity platform.

We recommend providing the following API permissions in your Entra ID application.

- To create a new personal WorkSpace that needs to be joined to Entra ID, following API permission is required.
  - `DeviceManagementServiceConfig.ReadWrite.All`
- When you terminate a personal WorkSpace or rebuild it, the following permissions are used.

> **Note**
>
> If you don't provide these permissions, WorkSpace will be terminated but it will not be removed from your Intune and Entra ID tenants and you will have to remove them separately.

- `DeviceManagementServiceConfig.ReadWrite.All`
- `Device.ReadWrite.All`
- `DeviceManagementManagedDevices.ReadWrite.All`
- These permissions require admin consent. For more information, see Grant tenant-wide admin consent to an application .

Next, you must add a client secret for the Entra ID application. For more information, see Add credentials. Make sure you remember the client secret string as you will need it when creating the AWS Secrets Manager secret in Step 4.

Step 3: Configure Windows Autopilot user-driven mode

Ensure you are familiar with the Step by step tutorial for Windows Autopilot user-driven Microsoft Entra join in Intune.

To configure your Microsoft Intune for Autopilot

1. Sign into the Microsoft Intune admin center
2. Create a new Autopilot device group for personal WorkSpaces. For more information, see Create device groups for Windows Autopilot.
   a. Choose **Groups**, **New group**
   b. For **Group type**, choose **Security**.
   c. For **Membership type**, choose **Dynamic Device**.
   d. Choose **Edit dynamic query** to create a dynamic membership rule. The rule should be in the following format:

```
(device.devicePhysicalIds -any (_ -eq "[OrderID]:WorkSpacesDirectoryName"))
```

> **Important**
>
> `WorkSpacesDirectoryName` should match the directory name of the Entra ID WorkSpaces Personal directory you create in step 5. This is because the directory name string is used as group tag when WorkSpaces registers virtual desktops into Autopilot. Additionally, group tag maps to the `OrderID` attribute on Microsoft Entra devices.

3. Choose **Devices**, **Windows**, **Enrollment**. For **Enrollment Options**, choose **Automatic Enrollment**. For **MDM user scope** select **All**.
4. Create an Autopilot deployment profile. For more information, see Create an Autopilot deployment profile.
   a. For **Windows Autopilot**, choose **Deployment profiles**, **Create profile**.
   b. In the **Windows Autopilot deployment profiles** screen, select the **Create Profile** drop down menu and then select **Windows PC**.
   c. In the **Create profile** screen, on **On the Out-of-box experience (OOBE)** page. For **Deployment mode**, select **User-driven**. For **Join to Microsoft Entra ID**, select **Microsoft Entra joined**. You can customize the computer names for your Entra ID-joined personal WorkSpaces by selecting **Yes** for **Apply device name template**, to create a template to use when naming a device during enrollment.
   d. On the **Assignments** page, for **Assign to**, choose **Selected groups**. Choose **Select groups to include**, and select the Autopilot device group you've just created in 2.

Step 4: Create an AWS Secrets Manager secret

You must create a secret in AWS Secrets Manager to securely store the information, including the application ID and client secret, for the Entra ID application you created in Step 2: Register a Microsoft Entra ID application to grant permissions for Windows Autopilot. This is a one-time setup.

To create an AWS Secrets Manager secret

1. Create a customer managed key on AWS Key Management Service. The key will later be used to encrypt the AWS Secrets Manager secret. Don't use the default key to encrypt your secret

as the default key cannot be accessed by the WorkSpaces service. Follow the steps below to create the key.

a. Open the AWS KMS console at https://console.aws.amazon.com/kms.

b. To change the AWS Region, use the Region selector in the upper-right corner of the page.

c. Choose **Create key**.

d. On the **Configure key** page, for **Key type** choose **Symmetric**. For **Key usage**, choose **Encrypt and decrypt**.

e. On the **Review** page, in the Key policy editor, ensure you allow the WorkSpaces service's principal `workspaces.amazonaws.com` access to the key by including following permissions in the key policy.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "workspaces.amazonaws.com"
        ]
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "*"
 }
```

2. Create the secret on AWS Secrets Manager, using the AWS KMS key created in previous step.

a. Open the Secrets Manager console at https://console.aws.amazon.com/secretsmanager/.

b. Choose **Store a new secret**.

c. On the **Choose secret type** page, for **Secret type**, select **Other type of secret**.

d. For **Key/value pairs**, in the key box, enter “application_id” into the key box, then copy the Entra ID application ID from Step 2 and paste it into the value box.

e. Choose **Add row**, in the key box, enter “application_password”, then copy the Entra ID application client secret from Step 2 and paste it into the value box.

f. Choose the AWS KMS key that you created in the previous step from the **Encryption key** drop-down list.

g. Choose **Next**.

h. On the **Configure secret** page, enter a **Secret name** and **Description**.

i. In the **Resource permissions** section, choose **Edit permissions**.

j. Make sure you allow the WorkSpaces service's principal `workspaces.amazonaws.com` access to the secret by including following resource policy in the resource permissions.

```
{
  "Version" : "2012-10-17",
  "Statement" : [ {
    "Effect" : "Allow",
    "Principal" : {
      "Service" : [ "workspaces.amazonaws.com"]
    },
    "Action" : "secretsmanager:GetSecretValue",
    "Resource" : "*"
  } ]
}
```

Step 5: Create a dedicated Microsoft Entra ID WorkSpaces directory

Create a dedicated WorkSpaces directory that stores information for your Microsoft Entra ID-joined WorkSpaces and Entra ID users.

To create an Entra ID WorkSpaces directory

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. On the **Create directory** page, for **WorkSpaces type** choose **Personal**. For **WorkSpace device management**, choose **Microsoft Entra ID**.
4. For **Microsoft Entra tenant ID**, enter your Microsoft Entra ID tenant ID that you want your directory's WorkSpace to join to. You won't be able to change the tenant ID after the directory is created.
5. For **Entra ID Application ID and password**, select the AWS Secrets Manager secret that you created in Step 4 from the drop down list. You won't be able to change the secret associated with the directory after the directory is created. However, you can always update the content of the secret, including the Entra ID Application ID and its password through the AWS Secrets Manager console at https://console.aws.amazon.com/secretsmanager/.

6. For **User identity source**, select the IAM Identity Center instance that you configured in Step 1from the drop down list. You won't be able to change the IAM Identity Center instance associated with the directory after the directory is created.
7. For **Directory name**, enter a unique name for the directory (For example, `WorkSpacesDirectoryName`).

> **Important**
>
> The directory name should match the `OrderID` used to construct the dynamic query for the Autopilot device group that you created with Microsoft Intune in Step 3. The directory name string is used as the group tag when registering personal WorkSpaces into Windows Autopilot. The group tag maps to the `OrderID` attribute on Microsoft Entra devices.

8. (Optional) For **Description**, enter a description for the directory.
9. For **VPC**, select the VPC that you used to launch your WorkSpaces. For more information, see Configure a VPC for WorkSpaces Personal.
10. For **Subnets**, select two subnets of your VPC that are not from the same Availability Zone. These subnets will be used to launch your personal WorkSpaces. For more information, see Availability Zones for WorkSpaces Personal.

> **Important**
>
> Make sure the WorkSpaces launched in the subnets have internet access, which is needed when users login to the Windows desktops. For more information, see Provide internet access for WorkSpaces Personal.

11. For **Configuration**, select **Enable dedicated WorkSpace**. You must enable it to create a dedicated WorkSpaces Personal directory to launch Bring Your Own License (BYOL) Windows 10 or 11 personal WorkSpaces.

> **Note**
>
> If you don't see the **Enable dedicated WorkSpace** option under **Configuration**, your account hasn't been enabled for BYOL. To enable BYOL for your account, see Bring Your Own Windows desktop licenses in WorkSpaces.

12. (Optional) For **Tags**, specify the key pair value that you want to use for personal WorkSpaces in the directory.
13. Review the directory summary and choose **Create directory**. It takes several minutes for your directory to be connected. The initial status of the directory is `Creating`. When directory creation is complete, the status is `Active`.

An IAM Identity Center application is also automatically created on your behalf once the directory is created. To find the application's ARN go to the directory's summary page.

You can now use the directory to launch Windows 10 or 11 personal WorkSpaces that are enrolled to Microsoft Intune and joined to Microsoft Entra ID. For more information, see Create a WorkSpace in WorkSpaces Personal.

After you've created a WorkSpaces Personal directory, you can create a personal WorkSpace. For more information, see Create a WorkSpace in WorkSpaces Personal

Configure the IAM Identity Center application for a WorkSpaces directory (optional)

A corresponding IAM Identity Center application is automatically created once a directory is created. You can find the application's ARN in the Summary section on the directory detail page. By default, all users in the Identity Center instance can access their assigned WorkSpaces without configuring the corresponding Identity Center application. However, you can manage user access to WorkSpaces in a directory by configuring the user assignment for the IAM Identity Center application.

To configure the user assignment for the IAM Identity Center application

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. On the **AWS managed applications** tab, choose the application for the WorkSpaces directory. The application names are in the following format: `WorkSpaces.wsd-xxxxx`, where `wsd-xxxxx` is the WorkSpaces directory ID.
3. Choose **Actions**, **Edit details**.
4. Change the **User and group assignment method** from **Do not require assignments** to **Require assignments**.
5. Choose **Save changes**.

After you make this change, users in the Identity Center instance will lose access their assign WorkSpaces unless they are assigned to the application. To assign your users to the application, use the AWS CLI command `create-application-assignment` to assign users or groups to an application. For more information, see the AWS CLI Command Reference.

Create a dedicated Custom directory with WorkSpaces Personal

Before you create Windows 10 and 11 BYOL personal WorkSpaces and assign them to your users, managed with AWS IAM Identity Center Identity Providers (IdPs), you must create a dedicated Custom WorkSpaces directory. Personal WorkSpaces are not joined to any Microsoft Active Directory but can be managed with a Mobile Device Management (MDM) solution of your choice, such as JumpCloud. For more information about JumpCloud, see this article. For tutorials that use the other options, see Create a directory for WorkSpaces Personal.

Note

- Amazon WorkSpaces can't create or manage user accounts on personal WorkSpaces launched in a Custom directory. As an administrator, you will have to manage them.
- Custom WorkSpaces directory is available in all AWS regions where Amazon WorkSpaces is offered except for Africa (Cape Town), Israel (Tel Aviv), and China (Ningxia).
- Amazon WorkSpaces can't create or manage user accounts on WorkSpaces using Custom directories. To ensure the MDM agent software you use can create the user profile on the Windows WorkSpaces, contact the MDM solution providers. Creating the user profile allows your users to sign into the Windows desktop from Windows login screen.

Contents

Requirements and limitations

- Custom WorkSpaces directories only support Windows 10 or 11 Bring Your Own License personal WorkSpaces.
- Custom WorkSpaces directories only support WSP protocol.

- Ensure you enable BYOL for your AWS account and you have your own AWS KMS server that your personal WorkSpaces can access for Windows 10 and 11 activation. For details, see Bring Your Own Windows desktop licenses in WorkSpaces.
- Ensure you pre-install the MDM agent software on the BYOL image that you imported to your AWS account.

Step 1: Enable IAM Identity Center and connect with your Identity Provider

To assign WorkSpaces to your users managed with your Identity Providers, the user information must be made available to AWS through AWS IAM Identity Center. We recommend using IAM Identity Center to manage your user's access to AWS resources. For more information, see What is IAM Identity Center?. This is a one-time setup.

To make user information available to AWS

1. Enable IAM Identity Center on AWS. You can enable IAM Identity Center with your AWS organizations, especially if you are using a multi-account environment. You can also create an account instance of IAM Identity Center. For more information, see Enabling AWS IAM Identity Center. Each WorkSpaces directory can associate with one IAM Identity Center organization or account instance. Each IAM Identity Center instance can be associated with one or more WorkSpaces Personal directory.

   If you are using an organization instance and trying to create a WorkSpaces directory in one of the member accounts, ensure you have the following IAM Identity Center permissions.

   - `"sso:DescribeInstance"`
   - `"sso:CreateApplication"`
   - `"sso:PutApplicationGrant"`
   - `"sso:PutApplicationAuthenticationMethod"`
   - `"sso:DeleteApplication"`
   - `"sso:DescribeApplication"`
   - `"sso:getApplicationGrant"`

   For more information, see Overview of managing access permissions to your IAM Identity Center resources. Ensure that no Service Control Policies (SCPs) are blocking these permissions. To learn more about SCPs, see Service control policies (SCPs).

2. Configure IAM Identity Center and your Identity Provider (IdP) to automatically synchronize users from your IdP to your IAM Identity Center instance. For more information, see Getting started tutorials and choose the specific tutorial for the IdP that you want to use. For example, Using IAM Identity Center to connect with your JumpCloud Directory Platform.
3. Verify that the users you configured on your IdP are synchronized correctly to AWS IAM Identity Center instance. The first synchronization can take up to an hour depending the configuration of your IdP.

Step 2: Create a dedicated Custom WorkSpaces directory

Create a dedicated WorkSpaces Personal directory that stores information about your personal WorkSpaces and your users.

To create a dedicated Custom WorkSpaces directory

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Choose **Create directory**.
4. On the **Create directory** page, for **WorkSpaces** type, choose **Personal**. For **WorkSpace device management**, choose **Custom**.
5. For **User identity source**, select the IAM Identity Center instance that you configured in Step 1 from the dropdown list. You won't be able to change the IAM Identity Center instance associated with the directory once the directory is created.

   > **Note**
   >
   > You have to specify an IAM Identity Center instance for the directory or you won't be able to launch personal WorkSpaces with the directory using the WorkSpaces console. WorkSpaces directories with no associated Identity Center are only compatible with WorkSpaces Core partner solutions.

6. For **Directory name**, enter a unique name for the directory.
7. For **VPC**, select the VPC that you used to launch your WorkSpaces. For more information, see Configure a VPC for WorkSpaces Personal.

8. For **Subnets**, select two subnets of your VPC that are not from the same Availability Zone. These subnets will be used to launch your personal WorkSpaces. For more information, see Availability Zones for WorkSpaces Personal.

   > **Important**
   >
   > Make sure the WorkSpaces launched in the subnets have internet access, which is needed when users login to the Windows desktops. For more information, see Provide internet access for WorkSpaces Personal.

9. For **Configuration**, select **Enable dedicated WorkSpace**. You must enable it to create a dedicated WorkSpaces Personal directory to launch Bring Your Own License (BYOL) Windows 10 or 11 personal WorkSpaces.
10. (Optional) For **Tags**, specify the key pair value that you want to use for personal WorkSpaces in the directory.
11. Review the directory summary and choose **Create directory**. It takes several minutes for your directory to be connected. The initial status of the directory is `Creating`. When directory creation is complete, the status is `Active`.

An IAM Identity Center application is also automatically created on your behalf once the directory is created. To find the application's ARN go to the directory's summary page.

You can now use the directory to launch Windows 10 or 11 personal WorkSpaces that are enrolled to Microsoft Intune and joined to Microsoft Entra ID. For more information, see Create a WorkSpace in WorkSpaces Personal.

After you've created a WorkSpaces Personal directory, you can create a personal WorkSpace. For more information, see Create a WorkSpace in WorkSpaces Personal

To delete empty directories, see Delete a directory for WorkSpaces Personal. If you delete your Simple AD or AD Connector directory, you can always create a new one when you want to start using WorkSpaces again.

Update DNS servers for WorkSpaces Personal

If you need to update the DNS server IP addresses for your Active Directory after launching your WorkSpaces, you must also update your WorkSpaces with the new DNS server settings.

You can update your WorkSpaces with the new DNS settings in one of the following ways:

- Update the DNS settings on the WorkSpaces **before** you update the DNS settings for Active Directory.
- Rebuild the WorkSpaces **after** you update the DNS settings for Active Directory.

We recommend updating the DNS settings on the WorkSpaces before updating the DNS settings in Active Directory (as explained in Step 1 of the following procedure).

If you want to rebuild the WorkSpaces instead, update one of the DNS server IP addresses in your Active Directory (Step 2), and then follow the procedure in Rebuild a WorkSpace in WorkSpaces Personal to rebuild your WorkSpaces. After you've rebuilt your WorkSpaces, follow the procedure in Step 3 to test your DNS server updates. After completing that step, update the IP address of your second DNS server in Active Directory, and then rebuild your WorkSpaces again. Be sure to follow the procedure in Step 3 to test your second DNS server update. As noted in the Best Practices section, we recommend updating your DNS server IP addresses one at a time.

Best practices

When you're updating your DNS server settings, we recommend the following best practices:

- To avoid disconnections and inaccessibility of domain resources, we strongly recommend performing DNS server updates during off-peak hours or during a planned maintenance period.
- Don't launch any new WorkSpaces during the 15 minutes before and the 15 minutes after changing your DNS server settings.
- When updating your DNS server settings, change one DNS server IP address at a time. Verify that the first update is correct before updating the second IP address. We recommend performing the following procedure (Step 1, Step 2, and Step 3) twice to update the IP addresses one at a time.

Step 1: Update the DNS server settings on your WorkSpaces

In the following procedure, the current and new DNS server IP address values are referred to as follows:

- Current DNS IP addresses: *`OldIP1`*, *`OldIP2`*
- New DNS IP addresses: *`NewIP1`*, *`NewIP2`*

> **Note**
>
> If this is the second time you're performing this procedure, replace *OldIP1* with *OldIP2* and *NewIP1* with *NewIP2*.

Update the DNS server settings for Windows WorkSpaces

If you have multiple WorkSpaces, you can deploy the following registry update to the WorkSpaces by applying a Group Policy Object (GPO) on the Active Directory OU for your WorkSpaces. For more information about working with GPOs, see Manage your Windows WorkSpaces in WorkSpaces Personal.

You can make these updates either by using the Registry Editor or by using Windows PowerShell. Both procedures are described in this section.

To update the DNS registry settings using the Registry Editor

1. On your Windows WorkSpace, open the Windows search box, and enter **`registry editor`** to open the Registry Editor (**regedit.exe**).
2. When asked "Do you want to allow this app to make changes to your device?", choose **Yes**.
3. In the Registry Editor, navigate to the following registry entry:

   HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\SkyLight
4. Open the **DomainJoinDns** registry key. Update *OldIP1* with *NewIP1*, and then choose **OK**.
5. Close the Registry Editor.
6. Reboot the WorkSpace, or restart the service SkyLightWorkspaceConfigService.

   > **Note**
   >
   > After you restart the service SkyLightWorkspaceConfigService, it can take up to 1 minute for the network adapter to reflect the change.
7. Proceed to Step 2, and update your DNS server settings in Active Directory to replace *OldIP1* with *NewIP1*.

To update the DNS registry settings using PowerShell

The following procedure uses PowerShell commands to update your registry and restart the service SkyLightWorkspaceConfigService.

1. On your Windows WorkSpace, open the Windows search box, and enter **`powershell`**. Choose **Run as Administrator**.
2. When asked "Do you want to allow this app to make changes to your device?", choose **Yes**.
3. In the PowerShell window, run the following command to retrieve the current DNS server IP addresses.

   ```
   Get-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS
   ```

   You should receive the following output.

   ```
   DomainJoinDns : OldIP1,OldIP2
   PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
   \Amazon\SkyLight
   PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
   \Amazon
   PSChildName   : SkyLight
   PSDrive       : HKLM
   PSProvider    : Microsoft.PowerShell.Core\Registry
   ```

4. In the PowerShell window, run the following command to change *`OldIP1`* to *`NewIP1`*. Be sure to leave *`OldIP2`* as is for now.

   ```
   Set-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS -Value
    "NewIP1,OldIP2"
   ```

5. Run the following command to restart the service SkyLightWorkspaceConfigService.

   ```
   restart-service -Name SkyLightWorkspaceConfigService
   ```

   Note

   After you restart the service SkyLightWorkspaceConfigService, it can take up to 1 minute for the network adapter to reflect the change.

6. Proceed to Step 2, and update your DNS server settings in Active Directory to replace *OldIP1* with *NewIP1*.

Update the DNS server settings for Amazon Linux 2 WorkSpaces

If you have more than one Amazon Linux 2 WorkSpace, we recommend that you use a configuration management solution to distribute and enforce policy. For example, you can use Ansible.

To update the DNS server settings on a Amazon Linux 2 WorkSpace

1. On your Linux WorkSpace, open a Terminal window.
2. Use the following Linux command to edit the `/etc/dhcp/dhclient.conf` file. You must have root user privileges to edit this file. Either become root by using the `sudo -i` command, or run all commands with `sudo` as shown.

   ```
   sudo vi /etc/dhcp/dhclient.conf
   ```

   In the `/etc/dhcp/dhclient.conf` file, you will see the following `prepend` command, where *OldIP1* and *OldIP2* are the IP addresses of your DNS servers.

   ```
   prepend domain-name-servers OldIP1, OldIP2; # skylight
   ```
3. Replace *OldIP1* with *NewIP1*, and leave *OldIP2* as is for now.
4. Save your changes to `/etc/dhcp/dhclient.conf`.
5. Reboot the WorkSpace.
6. Proceed to Step 2, and update your DNS server settings in Active Directory to replace *OldIP1* with *NewIP1*.

Update the DNS server settings for Ubuntu WorkSpaces

If you have more than one Ubuntu WorkSpace, we recommend that you use a configuration management solution to distribute and enforce policy. For example, you can use Landscape.

To update the DNS server settings on a Ubuntu WorkSpace

1. On your Ubuntu WorkSpace, open a Terminal window and run the following command. You must have root user privileges to edit this file. Either become root by using the `sudo -i` command, or run all commands with `sudo` as shown.

   ```
   sudo vi /etc/netplan/zz-workspaces-domain.yaml
   ```

2. In the yaml file, you will see the following `nameserver` command.

   ```
   nameservers:
       search:[Your domain FQDN]
       addresses:[OldIP1, OldIP2]
   ```

   Replace the *OldIP1* and *OldIP2* with the *NewIP1* and *NewIP2*.

   If you have multiple DNS servers IP addesses, add them as comma separated values. For example, [*NewDNSIP1*, *NewDNSIP2*, *NewDNSIP3*].

3. Save the yaml file.
4. Run the command `sudo netplan apply` to apply the changes.
5. Run the command `resolvectl status` to verify that the new DNS IP address is being used.
6. Proceed to Step 2, and update your DNS server settings in Active Directory.

Update the DNS server settings for Red Hat Enterprise Linux WorkSpaces

If you have more than one Red Hat Enterprise Linux WorkSpace, we recommend that you use a configuration management solution to distribute and enforce policy. For example, you can use Ansible.

To update the DNS server settings on a Red Hat Enterprise Linux WorkSpace

1. On your Red Hat Enterprise Linux WorkSpace, open a Terminal window and run the command below. You must have root user privileges to edit this file. Either become root by using the `sudo -i` command, or run all commands with `sudo` as shown.

   ```
   sudo nmcli conn modify CustomerNIC ipv4.dns 'NewIP1 NewIP2'
   ```

2. Run the following command.

```
sudo systemctl restart NetworkManager
```

3. To check the updated DNS and network configuration run the following command.

```
nmcli device show eth1
```

4. Proceed to Step 2, and update your DNS server settings in Active Directory.

Step 2: Update the DNS server settings for Active Directory

In this step, you update your DNS server settings for Active Directory. As noted in the Best Practices section, we recommend updating your DNS server IP addresses one at a time.

To update your DNS server settings for Active Directory, see the following documentation in the *AWS Directory Service Administration Guide*:

- **AD Connector**: Update the DNS Address for Your AD Connector
- **AWS Managed Microsoft AD**: Configure DNS Conditional Forwarders for Your On-premises Domain
- **Simple AD**: Configure DNS

After updating your DNS server settings, proceed to Step 3.

Step 3: Test the updated DNS server settings

After completing Step 1 and Step 2, use the following procedure to verify that your updated DNS server settings are working as expected.

In the following procedure, the current and new DNS server IP address values are referred to as follows:

- Current DNS IP addresses: *OldIP1*, *OldIP2*
- New DNS IP addresses: *NewIP1*, *NewIP2*

> **Note**
>
> If this is the second time you're performing this procedure, replace *OldIP1* with *OldIP2* and *NewIP1* with *NewIP2*.

Test the updated DNS server settings for Windows WorkSpaces

1. Shut down the *OldIP1* DNS server.
2. Log in to a Windows WorkSpace.
3. On the Windows **Start** menu, choose **Windows System**, then choose **Command Prompt**.
4. Run the following command, where *AD_Name* is the name of your Active Directory (for example, `corp.example.com`).

   ```
   nslookup AD_Name
   ```

   The `nslookup` command should return the following output. (If this is the second time you're performing this procedure, you should see *NewIP2* in place of *OldIP2*.)

   ```
   Server:  Full_AD_Name
   Address:  NewIP1

   Name:    AD_Name
   Addresses:  OldIP2
             NewIP1
   ```

5. If the output is not what you were expecting or if you receive any errors, repeat Step 1.
6. Wait for an hour and confirm that no user issues have been reported. Verify that *NewIP1* is getting DNS queries and responding with answers.
7. After you've verified that the first DNS server is working properly, repeat Step 1 to update the second DNS server, this time replacing *OldIP2* with *NewIP2*. Then repeat Step 2 and Step 3.

Test the updated DNS server settings for Linux WorkSpaces

1. Shut down the *OldIP1* DNS server.
2. Log in to a Linux WorkSpace.
3. On your Linux WorkSpace, open a Terminal window.

4. The DNS server IP addresses returned in the DHCP response are written to the local `/etc/resolv.conf` file on the WorkSpace. Run the following command to view the contents of the `/etc/resolv.conf` file.

   ```
   cat /etc/resolv.conf
   ```

   You should see the following output. (If this is the second time you're performing this procedure, you should see *NewIP2* in place of *OldIP2*.)

   ```
   ; This file is generated by Amazon WorkSpaces
   ; Modifying it can make your WorkSpace inaccessible until reboot
   options timeout:2 attempts:5
   ; generated by /usr/sbin/dhclient-script
   search region.compute.internal
   nameserver NewIP1
   nameserver OldIP2
   nameserver WorkSpaceIP
   ```

   > **Note**
   >
   > If you make manual modifications to the `/etc/resolv.conf` file, those changes are lost when the WorkSpace is restarted.

5. If the output is not what you were expecting or if you receive any errors, repeat Step 1.

6. The actual DNS server IP addresses are stored in the `/etc/dhcp/dhclient.conf` file. To see the contents of this file, run the following command.

   ```
   sudo cat /etc/dhcp/dhclient.conf
   ```

   You should see the following output. (If this is the second time you're performing this procedure, you should see *NewIP2* in place of *OldIP2*.)

   ```
   # This file is generated by Amazon WorkSpaces
   # Modifying it can make your WorkSpace inaccessible until rebuild
   prepend domain-name-servers NewIP1, OldIP2; # skylight
   ```

7. Wait for an hour and confirm that no user issues have been reported. Verify that *NewIP1* is getting DNS queries and responding with answers.

8. After you've verified that the first DNS server is working properly, repeat Step 1 to update the second DNS server, this time replacing *OldIP2* with *NewIP2*. Then repeat Step 2 and Step 3.

Delete a directory for WorkSpaces Personal

> **Note**
>
> Simple AD and AD Connector are made available to you free of charge to use with WorkSpaces. If there are no WorkSpaces being used with your Simple AD or AD Connector directory for 30 consecutive days, this directory will be automatically deregistered for use with Amazon WorkSpaces, and you will be charged for this directory as per the AWS Directory Service pricing terms.
> If you delete your Simple AD or AD Connector directory, you can always create a new one when you want to start using WorkSpaces again.

What happens when you delete a directory

When a Simple AD or AWS Directory Service for Microsoft Active Directory directory is deleted, all of the directory data and snapshots are deleted and cannot be recovered. After the directory is deleted, any Amazon EC2 instances that are joined to the directory remain intact. You cannot, however, use your directory credentials to log in to these instances. You need to log in to these instances with an AWS account that is local to the instance.

When an AD Connector directory is deleted, your on-premises directory remains intact. Any Amazon EC2 instances that are joined to the directory also remain intact and remain joined to your on-premises directory. You can still use your directory credentials to log in to these instances.

Delete an Entra ID or Custom WorkSpaces directory

Entra ID WorkSpaces directory allows you to create Entra ID-joined Windows 10 or 11 BYOL WorkSpaces. For more information, see Create a dedicated Microsoft Entra ID directory with WorkSpaces Personal.

Custom WorkSpaces directory allows you to create WorkSpaces that are not Active Directory domain-joined, but use your own device management software and IAM Identity Center. For more information, see Create a dedicated Custom directory with WorkSpaces Personal.

To delete an Entra ID or Custom WorkSpaces directory

1. Delete all the WorkSpaces in the directory. For more information, see Delete a WorkSpace in WorkSpaces Personal.
2. In the navigation pane, choose **Directories**.
3. Select the directory.
4. Choose **Actions**, **Delete**.
5. When prompted for confirmation, enter **delete**.

Delete an AWS Directory Service directory

You can delete the AWS Directory Service directory for your WorkSpaces if it is no longer in use by other WorkSpaces or other applications, such as Amazon WorkDocs, Amazon WorkMail, or Amazon Chime. Note that you must deregister a directory before you can delete it.

To deregister a directory

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select the directory.
4. Choose **Actions**, **Deregister**.
5. When prompted for confirmation, choose **Deregister**. After deregistration is complete, the value of **Registered** is No.

To delete a directory

1. Delete all WorkSpaces in the directory. For more information, see Delete a WorkSpace in WorkSpaces Personal.
2. Find and remove all of the applications and services that are registered to the directory. For more information, see Delete Your Directory in the *AWS Directory Service Administration Guide*.
3. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
4. In the navigation pane, choose **Directories**.
5. Select the directory and choose **Actions**, **Deregister**.
6. When prompted for confirmation, choose **Deregister**.
7. Select the directory again and choose **Actions**, **Delete**.

8. When prompted for confirmation, choose **Delete**.

> **Note**
>
> Removing application assignments can sometimes take more time than expected. If you receive the following error message, verify that you've removed all application assignments, and then wait 30 to 60 minutes before trying again to delete the directory:
>
> ```
> An Error Has Occurred
> Cannot delete the directory because it still has authorized applications.
> Additional directory details can be viewed at the Directory Service console.
> ```

9. (Optional) After you delete all resources in the virtual private cloud (VPC) for your directory, you can delete the VPC and release the Elastic IP address used for the NAT gateway. For more information, see Deleting your VPC and Working with Elastic IP addresses in the *Amazon VPC User Guide*.
10. (Optional) To delete any custom bundles and images that you are finished with, see Delete a custom bundle or image in WorkSpaces Personal.

Enable Amazon WorkDocs for AWS Managed Microsoft AD

If you're using AWS Managed Microsoft AD with Amazon WorkSpaces, you can enable Amazon WorkDocs for your directory through either the Amazon WorkDocs console or the AWS Directory Service console.

> **Note**
>
> Amazon WorkDocs is not available in all of the AWS Regions where Amazon WorkSpaces is available. For more information, see Amazon WorkDocs Pricing.

To enable WorkDocs through the Amazon WorkDocs console

1. Open the Amazon WorkDocs console at https://console.aws.amazon.com/zocalo/.
2. Choose **Create a New WorkDocs Site**.
3. Under **Standard Setup**, choose **Launch**.

4. Select the directory and create your site name.
5. Specify the user who will administer the WorkDocs site. You can use the admin or any user created in the directory.

For more information, see Getting Started with AWS Managed Microsoft AD in the *Amazon WorkDocs Administration Guide*.

To enable WorkDocs through the AWS Directory Service console

1. Open the AWS Directory Service console at https://console.aws.amazon.com/directoryservicev2/.
2. In the navigation pane, choose **Directories**.
3. On the **Directories** page, choose your directory.
4. On the **Directory details** page, choose the **Application management** tab.
5. In the **Application access URL** section, if an access URL has not been assigned to the directory, the **Create** button is displayed. Enter a directory alias and choose **Create**. For more information, see Creating an Access URL in the *AWS Directory Service Administration Guide*.
6. In the **Application access URL** section, choose **Enable** to enable single sign-on for Amazon WorkDocs. For more information, see Single Sign-On in the *AWS Directory Service Administration Guide*.

Set up Active Directory Administration Tools for WorkSpaces Personal

You'll perform most administrative tasks for your WorkSpaces directory using directory management tools, such as the Active Directory Administration Tools. However, you'll use the WorkSpaces console to perform some directory-related tasks. For more information, see Manage directories for WorkSpaces Personal.

If you create a directory with AWS Managed Microsoft AD or Simple AD that includes five or more WorkSpaces, we recommend that you centralize administration on an Amazon EC2 instance. Although you can install the directory management tools on a WorkSpace, using an Amazon EC2 instance is a more robust solution.

To set up the Active Directory Administration Tools

1. Launch an Amazon EC2 Windows instance and join it to your WorkSpaces directory by using one of the following options:

- If you don't already have an existing Amazon EC2 Windows instance, you can join the instance to your directory domain when you launch the instance. For more information, see Seamlessly join a Windows EC2 instance in the *AWS Directory Service Administration Guide*.
- If you already have an existing Amazon EC2 Windows instance, you can join it to your directory manually. For more information, see Manually Add a Windows Instance in the *AWS Directory Service Administration Guide*.

2. Install the Active Directory Administration Tools on the Amazon EC2 Windows instance. For more information, see Installing the Active Directory Administration Tools in the *AWS Directory Service Administration Guide*.

   > **Note**
   >
   > When you're installing the Active Directory Administration Tools, make sure to also select **Group Policy Management** to install the Group Policy Management Editor (**gpmc.msc**) tool.

   When the feature installation is finished, the Active Directory tools are available on the Windows **Start** menu under **Windows Administrative Tools**.

3. Run the tools as a directory administrator as follows:

   a. On the Windows **Start** menu, open **Windows Administrative Tools**.

   b. Hold down the Shift key, right-click the shortcut for the tool you want to use, and choose **Run as different user**.

   c. Enter the sign-in credentials for the administrator. With Simple AD, the username is **`Administrator`** and with AWS Managed Microsoft AD, the administrator is **`Admin`**.

You can now perform directory administration tasks using the Active Directory tools that you are familiar with. For example, you can use the Active Directory Users and Computers Tool to add users, remove users, promote a user to directory administrator, or reset a user password. Note that you must be logged into your Windows instance as a user that has permissions to manage users in the directory.

To promote a user to a directory administrator

> **Note**
>
> This procedure applies only to directories created with Simple AD, not AWS Managed AD. For directories created with AWS Managed AD, see Manage Users and Groups in AWS Managed Microsoft AD in the *AWS Directory Service Administration Guide*.

1. Open the Active Directory Users and Computers tool.
2. Navigate to the **Users** folder under your domain and select the user to promote.
3. Choose **Action**, **Properties**.
4. In the ***username*** **Properties** dialog box, choose **Member Of**.
5. Add the user to the following groups and choose **OK**.
   - **Administrators**
   - **Domain Admins**
   - **Enterprise Admins**
   - **Group Policy Creator Owners**
   - **Schema Admins**

To add or remove users

You can create new users from the Amazon WorkSpaces console only during the process of launching a WorkSpace, and you cannot delete users through the Amazon WorkSpaces console. Most user management tasks, including managing user groups, must be performed through your directory.

> **Important**
>
> Before you can remove a user, you must delete the WorkSpace assigned to that user. For more information, see Delete a WorkSpace in WorkSpaces Personal.

The process you use for managing users and groups depends on which type of directory you're using.

- If you're using AWS Managed Microsoft AD, see Manage Users and Groups in AWS Managed Microsoft AD in the *AWS Directory Service Administration Guide*.
- If you're using Simple AD, see Manage Users and Groups in Simple AD in the *AWS Directory Service Administration Guide*.
- If you use Microsoft Active Directory through AD Connector or a trust relationship, you can manage users and groups using the Active Directory module.

To reset a user password

When you reset the password for an existing user, do not set **User must change password at next logon**. Otherwise, the users cannot connect to their WorkSpaces. Instead, assign a secure temporary password to each user and then ask the users to manually change their passwords from within the WorkSpace the next time they log on.

> **Note**
>
> If you're using AD Connector or if your users are in the AWS GovCloud (US-West) Region, your users won't be able to reset their own passwords. (The **Forgot password?** option on the WorkSpaces client application login screen won't be available .)

Create a WorkSpace in WorkSpaces Personal

WorkSpaces enables you to provision virtual, cloud-based Windows and Linux desktops for your users, known as *WorkSpaces*.

Before creating a personal WorkSpace, create a directory by doing one of the following:

- Create a Simple AD directory.
- Create an AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD.
- Connect to an existing Microsoft Active Directory by using Active Directory Connector.
- Create a trust relationship between your AWS Managed Microsoft AD directory and your on-premises domain.
- Create a dedicated directory that uses Microsoft Entra ID as the identity source (through IAM Identity Center). WorkSpaces in the directory are native Entra ID-joined and enrolled into Microsoft Intune through Microsoft Windows Autopilot user-driven mode.

> **Note**
>
> Such directories currently only support Windows 10 and 11 Bring Your Own Licenses personal WorkSpaces.

- Create a dedicated directory that uses an identity provider of your choice as the identity source (through IAM Identity Center). WorkSpaces in the directory are native Entra ID-joined and enrolled into Microsoft Intune through Microsoft Windows Autopilot user-driven mode.

> **Note**
>
> Such directories currently only support Windows 10 and 11 Bring Your Own Licenses personal WorkSpaces.

Now that you have created a directory, you are ready to create a personal WorkSpace.

To create a personal WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Choose **Launch WorkSpaces**, **Personal**.
4. Choose **Create WorkSpaces**
5. Under **Onboarding** (optional), you can choose **Recommend options to me based on my use case** to get recommendations on the type of WorkSpace you want to use. You can skip this step if you know that you want to use personal WorkSpaces.
6. Choose **Next**. WorkSpaces registers your AD Connector.
7. Under **Configure WorkSpaces**, enter the following details:
   - For **Bundle**, choose from the following the bundle type that you want to use for your WorkSpaces.
     - **Use a base WorkSpaces bundle** - Choose one of the bundles from the drop down. For more information about the bundle type you selected, choose **Bundle details**. To compare bundles offered for pools, choose **Compare all bundles**.

- **Use your own custom or BYOL bundle** - Choose a bundle that you previously created. To create a custom bundle, see Create a custom WorkSpaces image and bundle for WorkSpaces Personal.

> **Note**
>
> Review the recommended uses and specifications of each bundle to help ensure you select the bundle that works best for your users. For more information about each use case, see Amazon WorkSpaces Bundles. For more information about bundle specifications, recommended uses, and pricing, see Amazon WorkSpaces pricing.

- For **Running mode**, choose from the following to configure your personal WorkSpace's immediate availability and how you pay for it (monthly or hourly):
  - **AlwaysOn** — Bills monthly fee for unlimited usage of your WorkSpaces. This mode is best for users who use their WorkSpace full time as their primary desktop.
  - **AutoStop** — Bills by the hour. With this mode, your WorkSpaces stop after a specified period of disconnection, and the state of apps and data is saved.
- For **Tags**, specify the key pair value that you want to use. A key can be a general category, such as "project," "owner," or "environment," with specific associated values.

8. Under **Select directory**, enter the following details:
   - Choose the directory that you created. To create a directory, choose **Create directory**. For more information about creating personal directories, see Register an existing AWS Directory Service directory with WorkSpaces Personal.
   - Choose the users from that directory you want to provision personal WorkSpaces for by doing the following.
     1. Choose **Create users**.
     2. Enter the user's **Username**, **First name**, **Last name**, and **Email**. To add additional users, choose **Create additional user** and enter their information.
9. Under **Customization** (optional), you can customize bundles, root and user volume encryption, and user volume for all users or specific users.
10. Choose Create WorkSpaces. The initial status of the WorkSpace is PENDING. When the creation is complete, the status is AVAILABLE and an invitation is sent to the email address that you specified for the users.

11. Send invitations to the email address for each user. For more information, see Send an invitation email.

> **Note**
>
> - These invitations aren't sent automatically if you're using AD Connector or a trust relationship.
> - Invitation emails aren't sent if the user already exists in Active Directory. Instead, make sure you manually send the user an invitation email. For more information, see Send an invitation email.

Connect to the WorkSpace

You can connect to your WorkSpace using the client of your choice. After you sign in, the client displays the WorkSpace desktop.

To connect to the WorkSpace

1. Open the link in the invitation email.
2. Review WorkSpaces Clients in the *Amazon WorkSpaces User Guide* for more information about the requirements for each client, and then do one of the following:
   - When prompted, download one of the client applications or launch Web Access.
   - If you aren't prompted and you haven't installed a client application already, open https://clients.amazonworkspaces.com/ and download one of the client applications or launch Web Access.

> **Note**
>
> You cannot use a web browser (Web Access) to connect to Amazon Linux WorkSpaces.

3. Start the client, enter the registration code from the invitation email, and choose **Register**.
4. When prompted to sign in, enter the the user's sign-in credentials, and then choose **Sign In**.
5. (Optional) When prompted to save your credentials, choose **Yes**.

> **Note**
>
> Because you're using AD Connector, your users won't be able to reset their own passwords. (The **Forgot password?** option on the WorkSpaces client application login screen won't be available.) For information about how to reset user passwords, see Set up Active Directory Administration Tools for WorkSpaces Personal.

Next steps

You can continue to customize the WorkSpace that you just created. For example, you can install software and then create a custom bundle from your WorkSpace. You can also perform various administrative tasks for your WorkSpaces and your WorkSpaces directory. If you are finished with your WorkSpace, you can delete it. For more information, see the following documentation.

- Create a custom WorkSpaces image and bundle for WorkSpaces Personal
- Administer WorkSpaces Personal
- Manage directories for WorkSpaces Personal
- Delete a WorkSpace in WorkSpaces Personal

For more information about using the WorkSpaces client applications, such as setting up multiple monitors or using peripheral devices, see WorkSpaces Clients and Peripheral Device Support in the *Amazon WorkSpaces User Guide*.

Administer users in WorkSpaces Personal

Each WorkSpace is assigned to a single user and cannot be shared by multiple users. By default, only one WorkSpace per user per directory is allowed.

Contents

- Enable diagnostic log uploads in WorkSpaces Personal

Manage users in WorkSpaces Personal

As an administrator for WorkSpaces, you can perform the following tasks to manage WorkSpaces users.

Edit user information

You can use the WorkSpaces console to edit the user information for a WorkSpace.

> **Note**
>
> This feature is available only if you use AWS Managed Microsoft AD or Simple AD. If you use Microsoft Active Directory through AD Connector or a trust relationship, you can manage users and groups using the Active Directory module. If you use Microsoft Entra ID or Custom WorkSpaces directory, you can manage users and groups with Microsoft Entra ID or your Identity Providers.

To edit user information

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select a user and choose **Actions**, **Edit users**.
4. Update **First name**, **Last name**, and **Email** as needed.
5. Choose **Update**.

Add or delete users

You can create users from the Amazon WorkSpaces console only during the process of launching a WorkSpace, and you cannot delete users through the Amazon WorkSpaces console. Most user management tasks, including managing user groups, must be performed through your directory.

To add or delete users and groups

To add, delete, or otherwise manage users and groups, you must do this through your directory. You'll perform most administrative tasks for your WorkSpaces directory using directory

management tools, such as the Active Directory Administration Tools. For more information, see Set up Active Directory Administration Tools for WorkSpaces Personal.

> **Important**
>
> Before you can remove a user, you must delete the WorkSpace assigned to that user. For more information, see Delete a WorkSpace in WorkSpaces Personal.

The process you use for managing users and groups depends on which type of directory you're using.

- If you're using AWS Managed Microsoft AD, see Manage Users and Groups in AWS Managed Microsoft AD in the *AWS Directory Service Administration Guide*.
- If you're using Simple AD, see Manage Users and Groups in Simple AD in the *AWS Directory Service Administration Guide*.
- If you use Microsoft Active Directory through AD Connector or a trust relationship, you can manage users and groups by using the Active Directory module.

Send an invitation email

You can send an invitation email to a user manually if needed.

> **Note**
>
> If you're using AD Connector or a trusted domain, invitation emails aren't automatically sent to your users, so you must send them manually. Invitation emails also aren't sent automatically if the user already exists in Active Directory.

To resend an invitation email

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. On the **WorkSpaces** page, use the search box to search for the user you want to send an invitation to, and then select the corresponding WorkSpace from the search results. You can select only one WorkSpace at a time.

4. Choose **Actions**, **Invite users**.
5. On the **Invite users to the WorkSpace** page, choose **Send invite**.

Create multiple WorkSpaces for a user in WorkSpaces Personal

By default, you can create only one WorkSpace per user per directory. However, if needed, you can create more than one WorkSpace for a user, depending on your directory setup.

- If you have only one directory for your WorkSpaces, create multiple usernames for the user. For example, a user named Mary Major can have mmajor1, mmajor2, and so on as usernames. Each username is associated with a different WorkSpace in the same directory, but the WorkSpaces have the same registration code, as long as the WorkSpaces are all created in the same directory in the same AWS Region.
- If you have multiple directories for your WorkSpaces, create the WorkSpaces for the user in separate directories. You can use the same username in the directories, or you can use different usernames in the directories. The WorkSpaces will have different registration codes.

Tip

So that you can easily locate all the WorkSpaces that you've created for a user, use the same base username for each WorkSpace.
For example, if you have a user named Mary Major with the Active Directory username mmajor, create WorkSpaces for her with usernames such as mmajor, mmajor1, mmajor2, mmajor3, or other variants, such as mmajor_windows or mmajor_linux. As long as all the WorkSpaces have the same starting base username (mmajor), you can sort on the username in your WorkSpaces console to group all of the WorkSpaces for that user together.

Important

- A user can have both a PCoIP and a WSP WorkSpace as long as the two WorkSpaces are located in separate directories. The same user cannot have a PCoIP and a WSP WorkSpace in the same directory.

- If you are setting up multiple WorkSpaces for use with cross-Region redirection, you must set up the WorkSpaces in different directories in different AWS Regions, and you must use the same usernames in each directory. For more information about cross-Region redirection, see Cross-Region redirection for WorkSpaces Personal.

To switch between the WorkSpaces, the user logs in with the username and registration code associated with a particular Workspace. If the user is using a 3.0+ version of the WorkSpaces client applications for Windows, macOS, or Linux, the user can assign different names to the WorkSpaces by going to **Settings**, **Manage Login Information** in the client application.

Customize how users log in to their WorkSpaces in WorkSpaces Personal

Customize your users' access to WorkSpaces by using uniform resource identifiers (URIs) to provide a simplified login experience that integrates with existing workflows in your organization. For example, you can automatically generate login URIs that register your users by using their WorkSpaces registration code. As a result:

- Users can bypass the manual registration process.
- Their usernames are automatically entered on their WorkSpaces client login page.
- If multi-factor authentication (MFA) is used in your organization, their usernames and MFA codes are automatically entered on their client login page.

URI access works with both Region-based registration codes (for example, `WSpdx+ABC12D`) and fully qualified domain name (FQDN) based registration codes (for example, `desktop.example.com`). For more information about creating and using FQDN-based registration codes, see Cross-Region redirection for WorkSpaces Personal.

You can configure URI access to WorkSpaces for client applications on the following supported devices:

- Windows computers
- macOS computers
- Ubuntu Linux 18.04, 20.04, and 22.04 computers
- iPads

- Android devices

To use URIs to access their WorkSpaces, users must first install the client application for their device by opening https://clients.amazonworkspaces.com/ and following the directions.

URI access is supported on the Firefox and Chrome browsers on Windows and macOS computers, on the Firefox browser on Ubuntu Linux 18.04, 20.04, and 22.04 computers, and on the Internet Explorer and Microsoft Edge browsers on Windows computers. For more information about WorkSpaces clients, see WorkSpaces Clients in the *Amazon WorkSpaces User Guide*.

Note

On Android devices, URI access works only with the Firefox browser, not with the Google Chrome browser.

To configure URI access to WorkSpaces, use any of the URI formats described in the following table.

Note

If the data component of your URI includes any of the following reserved characters, we recommend that you use percent-encoding in the data component to avoid ambiguity:
`@ : / ? & =`
For example, if you have usernames that include any of these characters, you should percent-encode those usernames in your URI. For more information, see Uniform Resource Identifier (URI): Generic Syntax.

Supported syntax	Description
workspaces://	Opens the WorkSpaces client application. (Note: Using workspaces:// by itself is not currently supported in the Linux client application.)
workspaces://@registrationcode	Registers a user by using their WorkSpaces registration code. Also displays the client login page.

Supported syntax	Description
workspaces://username@registrationcode	Registers a user by using their WorkSpaces registration code. Also automatically enters the username in the **username** field on the client login page.
workspaces://username@registrationcode?MFACode=mfa	Registers a user by using their WorkSpaces registration code. Also automatically enters the username in the **username** field and the multi-factor authentication (MFA) code in the **MFA code** field on the client login page.
workspaces://@registrationcode?MFACode=mfa	Registers a user by using their WorkSpaces registration code. Also automatically enters the multi-factor authentication (MFA) code in the **MFA code** field on the client login page.

Note

If users open a URI link when they are already connected to a WorkSpace from a Windows client, a new WorkSpaces session opens and their original WorkSpaces session remains open. If users open a URI link when they are connected to a WorkSpace from a macOS, iPad, or Android client, no new session opens; only their original WorkSpaces session remains open.

Enable self-service WorkSpaces management capabilities for your users in WorkSpaces Personal

In WorkSpaces, you can enable self-service WorkSpace management capabilities for your users to provide them with more control over their experience. It can also reduce your IT support staff workload for WorkSpaces. When you enable self-service capabilities, users can perform one or more of the following tasks directly from their WorkSpaces client:

- Cache their credentials on their client. This lets them reconnect to their WorkSpace without re-entering their credentials.

- Restart (reboot) their WorkSpace.
- Increase the size of the root and user volumes on their WorkSpace.
- Change the compute type (bundle) for their WorkSpace.
- Switch the running mode of their WorkSpace.
- Rebuild their WorkSpace.

Supported clients

- Android, running on Android or Android-compatible Chrome OS systems
- Linux
- macOS
- Windows

To enable self-service management capabilities for your users

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Choose the directory you want to enable self-service management capabilities.
4. Scroll down to Self-service permissions and choose **Edit**. Enable or disable the following options as required to determine the WorkSpace management tasks that users can perform from their client:

   - **Remember me** — Users can choose whether to cache their credentials on their client by selecting the **Remember Me** or **Keep me logged in** check box on the login screen. The credentials are cached in RAM only. When users choose to cache their credentials, they can reconnect to their WorkSpaces without re-entering their credentials. To control how long users can cache their credentials, see Set the maximum lifetime for a Kerberos ticket.
   - **Restart WorkSpace from client** — Users can restart (reboot) their WorkSpace. Restarting disconnects the user from their WorkSpace, shuts it down, and reboots it. The user data, operating system, and system settings are not affected.
   - **Increase volume size** — Users can expand the root and user volumes on their WorkSpace to a specified size without contacting IT support. Users can increase the size of the root volume (for Windows, the C: drive; for Linux, /) up to 175 GB, and the size of the user volume (for Windows, the D: drive; for Linux, /home) up to 100 GB. WorkSpace root and user volumes

come in set groups that can't be changed. The available groups are [Root(GB), User(GB)]: [80, 10], [80, 50], [80, 100], [175 to 2000, 100 to 2000]. For more information, see Modify a WorkSpace in WorkSpaces Personal.

For a newly created WorkSpace, users must wait 6 hours before they can increase the size of these drives. After that, they can do so only once in a 6-hour period. While a volume size increase is in progress, users can perform most tasks on their WorkSpace. The tasks that they can't perform are: changing their WorkSpace compute type, switching their WorkSpace running mode, restarting their WorkSpace, or rebuilding their WorkSpace. When the process is finished, the WorkSpace must be rebooted for the changes to take effect. This process might take up to an hour.

> **Note**
>
> If users increase the volume size on their WorkSpace, this increases the billing rate for their WorkSpace.

- **Change compute type** — Users can switch their WorkSpace between compute types (bundles). For a newly created WorkSpace, users must wait 6 hours before they can switch to a different bundle. After that, they can switch to a larger bundle only once in a 6-hour period, or to a smaller bundle once in a 30-day period. When a WorkSpace compute type change is in progress, users are disconnected from their WorkSpace, and they can't use or change the WorkSpace. The WorkSpace is automatically rebooted during the compute type change process. This process might take up to an hour.

  > **Note**
  >
  > If users change their WorkSpace compute type, this changes the billing rate for their WorkSpace.

- **Switch running mode** — Users can switch their WorkSpace between the **AlwaysOn** and **AutoStop** running modes. For more information, see Manage the running mode in WorkSpaces Personal.

> **Note**
>
> If users switch the running mode of their WorkSpace, this changes the billing rate for their WorkSpace.

- **Rebuild WorkSpace from client** — Users can rebuild the operating system of a WorkSpace to its original state. When a WorkSpace is rebuilt, the user volume (D: drive) is recreated from the latest backup. Because backups are completed every 12 hours, users' data might be up to 12 hours old. For a newly created WorkSpace, users must wait 12 hours before they can rebuild their WorkSpace. When a WorkSpace rebuild is in progress, users are disconnected from their WorkSpace, and they can't use or make changes to their WorkSpace. This process might take up to an hour.
- **Diagnostic log uploads** — Users can upload WorkSpaces client log files directly to WorkSpaces to troubleshoot issues without interrupting use of the WorkSpaces client. If you enable diagnostic log uploads for your users, or let your users do so themselves, the log files are sent to WorkSpaces automatically. You can enable diagnostic log uploads before or during a WorkSpaces streaming session.

5. Choose **Save**.

Enable Amazon Connect audio optimization for your users in WorkSpaces Personal

In the WorkSpaces management console, you can enable Amazon Connect Contact Control Panel (CCP) audio optimization for your WorkSpaces fleets to enhance security and to enable native-quality audio. After enabling CCP audio optimization, the CCP audio will be processed by the client endpoints, while WorkSpaces users can interact with the CCP from within their WorkSpaces.

Amazon Connect Contact Control Panel (CCP) audio optimization works with:

- The WorkSpaces Windows client.
- Amazon Linux and Windows WorkSpaces.
- WorkSpaces using PCoIP or WSP.

Requirements

- You must be set up with Amazon Connect.
- You must build a custom CCP with the Amazon Connect Stream API by creating a CCP with no media for call signaling. This way, the media is handled on the local desktop using standard CCP, and the signaling and call controls are handled on the remote connection with the CCP with no media. For more information about the Amazon Connect streams API, see the GitHub repository at https://github.com/aws/amazon-connect-streams. The custom CCP that you build is the CCP your Amazon Connect agents will use within their WorkSpaces.
- You must have a web browser installed onto WorkSpaces client endpoints that's supported by Amazon Connect. For the list of supported browsers, see Browsers supported by Amazon Connect.

> **Note**
>
> If your users use browsers that are not supported, they will be asked to download a supported browser when they attempt to log in to the CCP.

Enable Amazon Connect audio optimization

To enable Amazon Connect audio optimization for your users:

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory, and choose **Actions**, **Update Details**.
4. Expand **Amazon Connect Audio Optimization**.

> **Note**
>
> Before configuring with Amazon Connect, choose **Update** to save any unsaved changes made previously in the management console.

5. Choose **Configure Amazon Connect**.
6. Enter an Amazon Connect Contact Control Panel (CCP) name.

> **Note**
>
> The name that you give your CCP will be used in the user add-in menu. Choose a name that will be meaningful to your users.

7. Enter the Amazon Connect Contact Control Panel URL that's generated by Amazon Connect. See Provide access to the Contact Control Panel for more information on getting the URL.
8. Choose **Create Amazon Connect**.

Update directory's Amazon Connect audio optimization details

To update a directory's Amazon Connect audio optimization details:

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory, and choose **Actions**, **Update Details**.
4. Expand **Amazon Connect Audio Optimization**.

> **Note**
>
> Before configuring with Amazon Connect, choose **Update** to save any unsaved changes made previously in the management console.

5. Choose **Configure Amazon Connect**.
6. Choose **Edit**.
7. Select your directory, and choose **Actions**, **Update Details**.
8. Update the Amazon Connect Contact Control Panel name and URL.
9. Choose **Save**.

Delete directory's Amazon Connect audio optimization

To delete a directory's Amazon Connect audio optimization:

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.

3. Select your directory, and choose **Actions**, **Update Details**.
4. Expand **Amazon Connect Audio Optimization**.

> **Note**
>
> Before configuring with Amazon Connect, choose **Update** to save any unsaved changes made previously in the management console.

5. Choose **Configure Amazon Connect**.
6. Choose **Delete Amazon Connect**.

See the Agent training guide for more information.

Enable diagnostic log uploads in WorkSpaces Personal

To troubleshoot WorkSpaces client issues, enable automatic diagnostic log uploads. This is currently supported for Windows, macOS, Linux, and Web Access clients.

> **Note**
>
> The WorkSpaces client diagnostic log uploads feature is currently unavailable in the AWS GovCloud (US-West) Region.

Diagnostic log uploads

With Diagnostic log uploads, you can upload WorkSpaces client log files directly to WorkSpaces to troubleshoot issues without interrupting use of the WorkSpaces client. If you enable diagnostic log uploads for your users, or let your users do so themselves, the log files are sent to WorkSpaces automatically. You can enable diagnostic log uploads before or during a WorkSpaces streaming session.

To automatically upload diagnostic logs from managed devices, install a WorkSpaces client that supports diagnostic uploads. Log uploading is enabled by default. You can modify the settings in either of the following ways:

Option 1: Using the AWS console

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.

2. In the navigation pane, choose **Directories**.
3. Choose the directory name that you want to enable diagnostic logging for.
4. Scroll down to **Self-service permission**.
5. Choose **View details**
6. Choose **Edit**.
7. Choose **Diagnostic log uploads**.
8. Choose **Save**.

Option 2: Using an API call

You can edit the directory settings to enable or disable the WorkSpaces Windows, macOS, and Linux client to upload diagnostic logs automatically using an API call. If enabled, when a client issue occurs, the logs are sent to WorkSpaces without user interaction. For more information, see the WorkSpaces API reference.

You can also let your users choose whether to enable automatic diagnostic log uploads after client installation. For more information, see WorkSpaces Windows client application , WorkSpaces macOS client application, and WorkSpaces Linux client application.

Note

- Diagnostic logs don't contain sensitive information. You can disable automatic diagnostic log uploads for your users at the directory level, or allow your users to disable these features themselves.
- To access the diagnostic log uploads feature, you need to install the following versions of the WorkSpaces clients:
  - 5.4.0 or later of the Windows client
  - 5.8.0 or later of the macOS client
  - 2023.1 of the Ubuntu 22.04 client
  - 2023.1 of the Ubuntu 20.04 client
  - You can also access the diagnostic log upload feature with the Web Access client

Administer WorkSpaces Personal

You can administer your WorkSpaces using the WorkSpaces console.

To perform directory administration tasks, see the section called “Set up Directory Administration”.

Note

- Ensure you update networking dependency drivers like ENA, NVMe, and PV drivers on your WorkSpaces. You should do this at least once every 6 months. For more information, see Install or upgrade Elastic Network Adapter (ENA) driver , AWS NVMe drivers for Windows instances, and Upgrade PV drivers on Windows instances.
- Ensure you update the EC2Config, EC2Launch, and EC2Launch V2 agents to the latest versions periodically. You should do this at least once every 6 months. For more information, see Update EC2Config and EC2Launch.

Contents

- Microsoft 365 Bring Your Own License (BYOL) in WorkSpaces Personal
- Upgrade Windows BYOL WorkSpaces in WorkSpaces Personal
- Migrate a WorkSpace in WorkSpaces Personal
- Delete a WorkSpace in WorkSpaces Personal

Manage your Windows WorkSpaces in WorkSpaces Personal

You can use Group Policy Objects (GPOs) to apply settings to manage Windows WorkSpaces or users that are part of your Windows WorkSpaces directory.

Note

- If you use Microsoft Entra ID or Custom WorkSpaces directory, you can manage users and groups with Microsoft Entra ID or your Identity Providers. For more inforamtion, see Create a dedicated Microsoft Entra ID directory with WorkSpaces Personal.
- Linux instances do not adhere to Group Policy. For information about managing Amazon Linux WorkSpaces, see Manage your Amazon Linux WorkSpaces in WorkSpaces Personal.

We recommend that you create an organizational unit for your WorkSpaces Computer Objects and an organizational unit for your WorkSpaces User Objects.

To use the Group Policy settings that are specific to Amazon WorkSpaces, you must install the Group Policy administrative template for the protocol or protocols that you are using, either PCoIP or WorkSpaces Streaming Protocol (WSP).

Warning

Group Policy settings can affect the experience of your WorkSpace users as follows:

- **Implementing an interactive logon message to display a logon banner prevents users from being able to access their WorkSpaces.** The interactive logon message Group Policy setting is not currently supported by PCoIP WorkSpaces. The logon message is supported on WSP WorkSpaces, and users have to login again after accepting the logon banner.
- **Disabling removable storage through Group Policy settings causes a login failure** that results in users being logged in to temporary user profiles with no access to drive D.

- **Removing users from the Remote Desktop Users local group through Group Policy settings prevents those users from being able to authenticate** through the WorkSpaces client applications. For more information about this Group Policy setting, see Allow log on through Remote Desktop Services in the Microsoft documentation.
- **If you remove the built-in Users group from the Allow log on locally security policy, your PCoIP WorkSpaces users won't be able to connect to their WorkSpaces through the WorkSpaces client applications.** Your PCoIP WorkSpaces also won't receive updates to the PCoIP agent software. PCoIP agent updates might contain security and other fixes, or they might enable new features for your WorkSpaces. For more information about working with this security policy, see Allow log on locally in the Microsoft documentation.
- Group Policy settings can be used to restrict drive access. **If you configure Group Policy settings to restrict access to drive C or to drive D, users can't access their WorkSpaces.** To prevent this issue from occurring, make sure that your users can access drive C and drive D.
- **The WorkSpaces audio-in feature requires local logon access inside the WorkSpace.** The audio-in feature is enabled by default for Windows WorkSpaces. However, if you have a Group Policy setting that restricts users' local logon in their WorkSpaces, audio-in won't work on your WorkSpaces. If you remove that Group Policy setting, the audio-in feature is enabled after the next reboot of the WorkSpace. For more information about this Group Policy setting, see Allow log on locally in the Microsoft documentation.

  For more information about enabling or disabling audio-in redirection, see Enable or disable audio-in redirection for PCoIP or Enable or disable audio-in redirection for WSP.
- Using Group Policy to set the Windows power plan to **Balanced** or **Power saver** might cause your WorkSpaces to sleep when they're left idle. We strongly recommend using Group Policy to set the Windows power plan to **High performance**. For more information, see My Windows WorkSpace goes to sleep when it's left idle.
- Some Group Policy settings force users to log off when they are disconnected from a session. Any applications that users have open on their WorkSpaces are closed.
- "Set time limit for active but idle Remote Desktop Services sessions" is currently not supported on WSP WorkSpaces. Avoid using it during WSP sessions as it causes a disconnect even when there is activity and the session is not idle.

For information about using the Active Directory administration tools to work with GPOs, see Set up Active Directory Administration Tools for WorkSpaces Personal.

Contents

Install the Group Policy administrative template files for the WorkSpaces Streaming Protocol (WSP)

To use the Group Policy settings that are specific to WorkSpaces when using the WorkSpaces Streaming Protocol (WSP), you must add the Group Policy administrative template `wsp.admx` and `wsp.adml` files for WSP to the Central Store of the domain controller for your WorkSpaces directory. For more information about `.admx` and `.adml` files, see How to create and manage the Central Store for Group Policy Administrative Templates in Windows.

The following procedure describes how to create the Central Store and add the administrative template files to it. Perform the following procedure on a directory administration WorkSpace or Amazon EC2 instance that is joined to your WorkSpaces directory.

To install the Group Policy administrative template files for WSP

1. From a running Windows WorkSpace, make a copy of the `wsp.admx` and `wsp.adml` files in the `C:\Program Files\Amazon\WSP` directory.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open Windows File Explorer, and in the address bar, enter your organization's fully qualified domain name (FQDN), such as `\\example.com`.
3. Open the `sysvol` folder.
4. Open the folder with the *FQDN* name.
5. Open the `Policies` folder. You should now be in `\\`*FQDN*`\sysvol\`*FQDN*`\Policies`.
6. If it doesn't already exist, create a folder named `PolicyDefinitions`.
7. Open the `PolicyDefinitions` folder.
8. Copy the `wsp.admx` file into the `\\`*FQDN*`\sysvol\`*FQDN*`\Policies\PolicyDefinitions` folder.
9. Create a folder named `en-US` in the `PolicyDefinitions` folder.
10. Open the `en-US` folder.
11. Copy the `wsp.adml` file into the `\\`*FQDN*`\sysvol\`*FQDN*`\Policies\PolicyDefinitions\en-US` folder.

To verify that the administrative template files are correctly installed

1. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**).
2. Expand the forest (**Forest:*FQDN***).
3. Expand **Domains**.
4. Expand your FQDN (for example, `example.com`).
5. Expand **Group Policy Objects**.
6. Select **Default Domain Policy**, open the context (right-click) menu, and choose **Edit**.

> **Note**
>
> If the domain backing the WorkSpaces is an AWS Managed Microsoft AD directory, you cannot use the Default Domain Policy to create your GPO. Instead, you must create and link the GPO under the domain container that has delegated privileges.
> When you create a directory with AWS Managed Microsoft AD, AWS Directory Service creates a *yourdomainname* organizational unit (OU) under the domain root. The name of this OU is based on the NetBIOS name that you typed when you created your directory. If you didn't specify a NetBIOS name, it will default to the first part of your Directory DNS name (for example, in the case of `corp.example.com`, the NetBIOS name is `corp`).
> To create your GPO, instead of selecting **Default Domain Policy**, select the *yourdomainname* OU (or any OU under that one), open the context (right-click) menu, and choose **Create a GPO in this domain, and Link it here**.
> For more information about the *yourdomainname* OU, see What Gets Created in the *AWS Directory Service Administration Guide*.

7. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
8. You can now use this **WSP** Group Policy object to modify the Group Policy settings that are specific to WorkSpaces when using WSP.

Manage Group Policy settings for WorkSpaces Streaming Protocol (WSP)

To use Group Policy settings to manage your Windows WorkSpaces that use WSP

1. Make sure that the most recent WorkSpaces Group Policy administrative template for WSP is installed in the Central Store of the domain controller for your WorkSpaces directory.
2. Verify the adminisitrative template files are correctly installed. For more information, see To verify that the administrative template files are correctly installed.

Configure printer support for WSP

By default, WorkSpaces enables Basic remote printing, which offers limited printing capabilities because it uses a generic printer driver on the host side to ensure compatible printing.

Advanced remote printing for Windows clients (not available for WSP) lets you use specific features of your printer, such as double-sided printing, but it requires installation of the matching printer driver on the host side.

Remote printing is implemented as a virtual channel. If virtual channels are disabled, remote printing does not function.

For Windows WorkSpaces, you can use Group Policy settings to configure printer support as needed.

To configure printer support

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Configure remote printing** setting.
3. In the **Configure remote printing** dialog box, do one of the following:
   - To enable local printer redirection, choose **Enabled**, and then for **Printing options**, choose **Basic**. To automatically use the client computer's current default printer, select **Map local default printer to the remote host**.
   - To disable printing, choose **Disabled**.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.

Configure clipboard redirection (copy/paste) for WSP

By default, WorkSpaces supports two-way (copy/paste) clipboard redirection. For Windows WorkSpaces, you can use Group Policy settings to disable this feature or configure the direction where clipboard redirection is allowed.

To configure clipboard redirection for Windows WorkSpaces

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Configure clipboard redirection** setting.
3. In the **Configure clipboard redirection** dialog box, choose **Enabled** or **Disabled**.

   When **Configure clipboard redirection** is **Enabled**, the following **Clipboard redirection options** will become available:

   - Choose **Copy and Paste** to allow two-way clipboard copy and paste redirection.
   - Choose **Copy Only** to allow copying data from the server clipboard to the client clipboard only.
   - Choose **Paste Only** to allow pasting data from the client clipboard to the server clipboard only.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.

Known limitation

With clipboard redirection enabled on the WorkSpace, if you copy content that is larger than 890 KB from a Microsoft Office application, the application might become slow or unresponsive for up to 5 seconds.

Set the session resume timeout for WSP

When you lose network connectivity, your active WorkSpaces client session is disconnected. WorkSpaces client applications for Windows and macOS attempt to reconnect the session automatically if network connectivity is restored within a certain amount of time. The default session resume timeout is 20 minutes (1200 seconds), but you can modify that value for WorkSpaces that are controlled by your domain's Group Policy settings.

To set the automatic session resume timeout value

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Enable/disable automatic reconnect** setting.
3. In the **Enable/disable automatic reconnect** dialog box, choose **Enabled**, and then set **Reconnect timeout (seconds)** to the desired timeout in seconds.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.

Enable or disable video-in redirection for WSP

By default, WorkSpaces supports redirecting data from a local camera. If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

To enable or disable video-in redirection for Windows WorkSpaces

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Enable/disable video-in redirection** setting.
3. In the **Enable/disable video-in redirection** dialog box, choose **Enabled** or **Disabled**.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.

Enable or disable audio-in redirection for WSP

By default, WorkSpaces supports redirecting data from a local microphone. If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

To enable or disable audio-in redirection for Windows WorkSpaces

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Enable/disable audio-in redirection** setting.
3. In the **Enable/disable audio-in redirection** dialog box, choose **Enabled** or **Disabled**.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.

Enable or disable audio-out redirection for WSP

By default, WorkSpaces redirects data to a local speaker. If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

To enable or disable audio-out redirection for Windows WorkSpaces

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Enable/disable audio-out redirection** setting.
3. In the **Enable/disable audio-out redirection** dialog box, choose **Enabled** or **Disabled**.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

- Reboot the WorkSpace. In the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions** > **Reboot WorkSpaces**.
- In an administrative command prompt, enter **`gpupdate /force`**.

Disable time zone redirection for WSP

By default, the time within a Workspace is set to mirror the time zone of the client that is being used to connect to the WorkSpace. This behavior is controlled through time zone redirection. You might want to turn off time zone direction for various reasons. For example:

- Your company wants all employees to work in a certain time zone (even if some employees are in other time zones).
- You have scheduled tasks in a WorkSpace that are meant to run at a certain time in a specific time zone.
- Your users who travel a lot want to keep their WorkSpaces in one time zone for consistency and personal preference.

If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

To disable time zone redirection for Windows WorkSpaces

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Enable/disable time zone redirection** setting.
3. In the **Enable/disable time zone redirection** dialog box, choose **Disabled**.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.
6. Set the time zone for the WorkSpaces to the desired time zone.

The time zone of the WorkSpaces is now static and no longer mirrors the time zone of the client machines.

Configure WSP security settings

For WSP, data in transit is encrypted using TLS 1.2 encryption. By default, all of the following ciphers are allowed for encryption, and the client and server negotiate which cipher to use:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384

For Windows WorkSpaces, you can use Group Policy settings to modify the TLS Security Mode and to add new or block certain cipher suites. A detailed explanation of these settings and the supported cipher suites is provided in the **Configure security settings Group Policy** dialog box.

To configure WSP security settings

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open **Configure security settings**.
3. In the **Configure security settings** dialog box, choose **Enabled**. Add cipher suites that you want to allow and remove cipher suites that you want to block. For more information about these settings, see the descriptions provided in the **Configure security settings** dialog box.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace, and after you restart the WorkSpace session. To apply the Group Policy changes, do one of the following:
   - To reboot the WorkSpace, in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**.
   - In an administrative command prompt, enter **`gpupdate /force`**.

Configure extensions for WSP

By default, support for WorkSpaces extensions is disabled. If needed, you can configure your WorkSpace to use extensions in the following ways:

- Server and client – Enable extensions for both server and client
- Server only – Enable extensions for server only
- Client only – Enable extensions for client only

For Windows WorkSpaces, you can use Group Policy settings to configure the use of extensions.

To configure extensions for WSP

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Configure extensions** setting.
3. In the **Configure extensions** dialog box, choose **Enabled** and then set the desired support option. Choose **Client Only**, **Server and Client**, or **Server only**.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after you restart the WorkSpace session. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace. In the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**.
   - In an administrative command prompt, enter **`gpupdate /force`**.

Enable or disable smart card redirection for WSP

By default, Amazon WorkSpaces are not enabled to support the use of smart cards for either *pre-session authentication* or *in-session authentication*. Pre-session authentication refers to smart card authentication that's performed while users are logging in to their WorkSpaces. In-session authentication refers to authentication that's performed after logging in.

If needed, you can enable pre-session and in-session authentication for Windows WorkSpaces by using Group Policy settings. Pre-session authentication must also be enabled through your AD Connector directory settings by using the **EnableClientAuthentication** API action or the

enable-client-authentication AWS CLI command. For more information, see Enable Smart Card Authentication for AD Connector in the *AWS Directory Service Administration Guide*.

> **Note**
>
> To enable the use of smart cards with Windows WorkSpaces, additional steps are required. For more information, see Use smart cards for authentication in WorkSpaces Personal.

To enable or disable smart card redirection for Windows WorkSpaces

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Enable/disable smart card redirection** setting.
3. In the **Enable/disable smart card redirection** dialog box, choose **Enabled** or **Disabled**.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the WorkSpace session is restarted. To apply the Group Policy change, reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).

Enable or disable WebAuthn (FIDO2) redirection for WSP

By default, Amazon WorkSpaces enables the use of WebAuthn authenticators for in-session authentication. In-session authentication refers to WebAuthn authentication that's performed after logging in and requested by the web applications running within the session.

Requirements

WebAuthn (FIDO2) redirection for WSP requires the following:

- WSP host agent version 2.0.0.1425 or higher
- WorkSpaces clients:
  - Linux Ubuntu 22.04 2023.3 or higher
  - Windows 5.19.0 or higher
  - Mac client 5.19.0 or higher
- Web browsers installed on your WorkSpaces running the Amazon DCV WebAuthn Redirection Extension:

- Google Chrome 116+
- Microsoft Edge 116+

Enabling or disabling WebAuthn (FIDO2) redirection for Windows WorkSpaces

If needed, you can enable or disable support for in-session authentication with WebAuthn authenticators for Windows WorkSpaces by using Group Policy settings. If you enable or do not configure this setting, WebAuthn redirection will be enabled and users can utilize local authenticators within the remote WorkSpace.

When feature is enabled, all WebAuthn requests from the browser in the session are redirected to the local client. Users can use Windows Hello or locally attached security devices like YubiKey or other FIDO2 compliant authenticators to complete the authentication process.

To enable or disable WebAuthn (FIDO2) redirection for Windows WorkSpaces

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Enable/disable WebAuthn redirection** setting.
3. In the **Enable/disable WebAuthn redirection** dialog box, choose **Enabled** or **Disabled**.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the WorkSpace session is restarted. To apply the Group Policy changes, reboot the WorkSpace by going to the Amazon WorkSpaces console and selecting the WorkSpace. Then, choose **Actions**, **Reboot WorkSpaces**).

Installing the Amazon DCV WebAuthn Redirection Extension

Users will need install the Amazon DCV WebAuthn Redirection Extension to use WebAuthn after the feature is enabled by doing either of the following:

- Your users will be prompted to enable the browser extension in their browser.

> **Note**
>
> This is a one-time browser prompt. Your users will get the notification when you update the WSP agent version to 2.0.0.1425 or higher. If your end users don't need the

WebAuthn redirection, they can just remove the extension from the browser. You can also block the WebAuthn Redirection Extension installation prompt using below GPO policy.

- You can force install the redirection extension for your users using below GPO policy. If you enable the GPO policy, the extension will automatically be installed when your users launch the supported browsers with internet access.
- Your users can install the extension manually with Microsoft Edge Add-ons or the Chrome Web Store.

Manage and install the browser extension using Group Policy

You can install the Amazon DCV WebAuthn Redirection Extension using Group Policy, either centrally from your domain for session hosts that are joined to an Active Directory (AD) domain or using the Local Group Policy Editor for each session host. This process will change depending on which browser you're using.

For Microsoft Edge

1. Download and install the Microsoft Edge administrative template.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**).
3. Expand the forest (**Forest:*FQDN***).
4. Expand **Domains**.
5. Expand your FQDN (for example, `example.com`).
6. Expand **Group Policy Objects**.
7. Select **Default Domain Policy**, open the context (right-click) menu, and choose **Edit**.
8. Choose **Computer Configuration** , **Administrative Templates**, **Microsoft Edge**, and **Extensions**
9. Open **Configure extension management settings** and set it to **Enabled**.
10. Under **Configure extension management settings**, enter the following:

```
{"ihejeaahjpbegmaaegiikmlphghlfmeh":
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

11. Choose **OK**.

12. The Group Policy setting change takes effect after the WorkSpace session is restarted. To apply the Group Policy changes, reboot the WorkSpace by going to the Amazon WorkSpaces console and selecting the WorkSpace. Then, choose **Actions**, **Reboot WorkSpaces**).

> **Note**
>
> You can block the installation of the extension by applying the following configuration management setting:
>
> ```
> {"ihejeaahjpbegmaaegiikmlphghlfmeh":
> {"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
> extensionwebstorebase/v1/crx"}}
> ```

For Google Chrome

1. Download and install the Google Chrome administrative template. For more information, see Set Chrome Browser policies on managed PCs.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**).
3. Expand the forest (**Forest:*FQDN***).
4. Expand **Domains**.
5. Expand your FQDN (for example, `example.com`).
6. Expand **Group Policy Objects**.
7. Select **Default Domain Policy**, open the context (right-click) menu, and choose **Edit**.
8. Choose **Computer Configuration** , **Administrative Templates**, **Google Chrome**, and **Extensions**
9. Open **Configure extension management settings** and set it to **Enabled**.
10. Under **Configure extension management settings**, enter the following:

    ```
    {"mmiioagbgnbojdbcjoddlefhmcocfpmn":
    { "installation_mode":"force_installed","update_url":"https://clients2.google.com/
    service/update2/crx"}}
    ```

11. Choose **OK**.

12. The Group Policy setting change takes effect after the WorkSpace session is restarted. To apply the Group Policy changes, reboot the WorkSpace by going to the Amazon WorkSpaces console and selecting the WorkSpace. Then, choose **Actions**, **Reboot WorkSpaces**).

> **Note**
>
> You can block the installation of the extension by applying the following configuration management setting:
>
> ```
> {"mmiioagbgnbojdbcjoddlefhmcocfpmn":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

Enable or disable WebRTC redirection for WSP

WebRTC redirection enhances real-time communication by offloading audio and video processing from WorkSpaces to your local client, which improves performance and reduces latency. However, WebRTC redirection isn't universal and requires third-party application vendors to develop specific integrations with WorkSpaces. By default, WebRTC redirection isn't enabled on WorkSpaces. To use WebRTC redirection, ensure the following:

- Third-party application vendor integration
- WorkSpaces extensions are enabled through Group Policy settings
- WebRTC redirection is enabled
- WebRTC redirection Browser extension is installed and enabled

> **Note**
>
> This redirection is implemented as an extension and requires you to enable support for WorkSpaces extensions using Group Policy settings. If the extensions are disabled, WebRTC redirection will not function.

Requirements

WebRTC redirection for WSP requires the following:

- WSP host agent version 2.0.0.1622 or higher
- WorkSpaces clients:
  - Windows 5.21.0 or higher
  - Web client
- Web browsers installed on your WorkSpaces running the Amazon DCV WebRTC Redirection Extension:
  - Google Chrome 116+
  - Microsoft Edge 116+

Enabling or disabling WebRTC redirection for Windows WorkSpaces

If needed, you can enable or disable support for WebRTC redirection for Windows WorkSpaces by using Group Policy settings. If you disable or don't configure this setting, WebRTC redirection will be disabled.

When feature is enabled, web applications that have integration with Amazon WorkSpaces will be able to redirect WebRTC API calls to the local client.

To enable or disable WebRTC redirection for Windows WorkSpaces

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Configure WebRTC Redirection** setting.
3. In the **Configure WebRTC Redirection** dialog box, choose **Enabled** or **Disabled**.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the WorkSpace session is restarted. To apply the Group Policy changes, reboot the WorkSpace by going to the Amazon WorkSpaces console and selecting the WorkSpace. Then, choose **Actions**, **Reboot WorkSpaces**).

Installing the Amazon DCV WebRTC Redirection Extension

Users install the Amazon DCV WebRTC Redirection Extension to use WebRTC redirection after the feature is enabled by doing either of the following:

- Users will be prompted to enable the browser extension in their browser.

> **Note**
>
> As a one-time browser prompt, users will get the notification when you enable WebRTC redirection.

- You can force install the redirection extension for users using the following GPO policy. If you enable the GPO policy, the extension will automatically be installed when users launch the supported browsers with internet access.
- Users can install the extension manually with Microsoft Edge Add-ons or the Chrome Web Store.

Manage and install the browser extension using Group Policy

You can install the Amazon DCV WebRTC Redirection Extension using Group Policy, either centrally from your domain, for session hosts joined to an Active Directory (AD) domain, or using the Local Group Policy Editor for each session host. This process will be different depending on which browser you're using.

For Microsoft Edge

1. Download and install the Microsoft Edge administrative template.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**).
3. Expand the forest (**Forest:*FQDN***).
4. Expand **Domains**.
5. Expand your FQDN (for example, `example.com`).
6. Expand **Group Policy Objects**.
7. Select **Default Domain Policy**, open the context (right-click) menu, and choose **Edit**.
8. Choose **Computer Configuration** , **Administrative Templates**, **Microsoft Edge**, and **Extensions**
9. Open **Configure extension management settings** and set it to **Enabled**.
10. Under **Configure extension management settings**, enter the following:

```
{"kjbbkjjiecchbcdoollhgffghfjnbhef":
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

11. Choose **OK**.
12. The Group Policy setting change takes effect after the WorkSpace session is restarted. To apply the Group Policy changes, reboot the WorkSpace by going to the Amazon WorkSpaces console and selecting the WorkSpace. Then, choose **Actions**, **Reboot WorkSpaces**).

> **Note**
>
> You can block the installation of the extension by applying the following configuration management setting:
>
> ```
> {"kjbbkjjiecchbcdoollhgffghfjnbhef":
> {"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
> extensionwebstorebase/v1/crx"}}
> ```

For Google Chrome

1. Download and install the Google Chrome administrative template. For more information, see Set Chrome Browser policies on managed PCs.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**).
3. Expand the forest (**Forest:*FQDN***).
4. Expand **Domains**.
5. Expand your FQDN (for example, `example.com`).
6. Expand **Group Policy Objects**.
7. Select **Default Domain Policy**, open the context (right-click) menu, and choose **Edit**.
8. Choose **Computer Configuration** , **Administrative Templates**, **Google Chrome**, and **Extensions**
9. Open **Configure extension management settings** and set it to **Enabled**.
10. Under **Configure extension management settings**, enter the following:

```
{"diilpfplcnhehakckkpmcmibmhbingnd":
{ "installation_mode":"force_installed","update_url":"https://clients2.google.com/
service/update2/crx"}}
```

11. Choose **OK**.
12. The Group Policy setting change takes effect after the WorkSpace session is restarted. To apply the Group Policy changes, reboot the WorkSpace by going to the Amazon WorkSpaces console and selecting the WorkSpace. Then, choose **Actions**, **Reboot WorkSpaces**).

> **Note**
>
> You can block the installation of the extension by applying the following configuration management setting:
>
> ```
> {"diilpfplcnhehakckkpmcmibmhbingnd":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

Enable or disable disconnect session on screen lock for WSP

If needed, you can disconnect users' WorkSpaces sessions when the Windows lock screen is detected. To reconnect from the WorkSpaces client, users can use their passwords or their smart cards to authenticate themselves, depending on which type of authentication has been enabled for their WorkSpaces.

This Group Policy setting is disabled by default. If needed, you can enable disconnecting the session when the Windows lock screen is detected for Windows WorkSpaces by using Group Policy settings.

> **Note**
>
> - This Group Policy setting applies to both password-authenticated and smart card-authenticated sessions.
> - To enable the use of smart cards with Windows WorkSpaces, additional steps are required. For more information, see Use smart cards for authentication in WorkSpaces Personal.

To enable or disable disconnect session on screen lock for Windows WorkSpaces

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Enable/disable disconnect session on screen lock** setting.
3. In the **Enable/disable disconnect session on screen lock** dialog box, choose **Enabled** or **Disabled**.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.

Enable or disable Indirect Display Driver (IDD) for WSP

By default, WorkSpaces supports supports using Indirect Display Driver (IDD). If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

To enable or disable Indirect Display Driver (IDD) for Windows WorkSpaces

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Enable the AWS Indirect Display Driver** setting.
3. In the **Enable the AWS Indirect Display Driver** dialog box, choose **Enabled** or **Disabled**.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

   a. Reboot the WorkSpace (in the WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).

   b. In an administrative command prompt, enter `gpupdate /force`.

Configure display settings for WSP

WorkSpaces allows you to configure several different display settings, including the maximum frame rate, minimum image quality, maximum image quality, and YUV encoding. Adjust these settings based on the image quality, responsiveness, and color accuracy that you need.

By default, the maximum frame rate value is 25. The maximum frame rate value specifies the maximum allowed frames per second (fps). A value of 0 means no limit.

By default, the minimum image quality value is 30. The minimum image quality can be optimized for best image responsiveness, or best image quality. For best responsiveness, reduce the minimum quality. For best quality, increase the minimum quality.

- Ideal values for best responsiveness are between 30 and 90.
- Ideal values for best quality are between 60 and 90.

By default, the maximum image quality value is 80. The maximum image quality doesn't affect the image responsiveness or quality, but sets a maximum to limit network usage.

By default, image encoding is set to YUV420. Selecting **Enable YUV444 encoding** enables YUV444 encoding for high color accuracy.

For Windows WorkSpaces, you can use Group Policy settings to configure the maximum frame rate, minimum image quality, and maximum image quality values.

To configure display settings for Windows WorkSpaces

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Configure display settings** setting.
3. In the **Configure display settings** dialog box, choose **Enabled** and then set the **Maximum frame rate (fps)**, **minimum image quality**, and **maximum image quality** values to the desired levels.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after you restart the WorkSpace session. To apply the Group Policy changes, do one of the following:

- Reboot the WorkSpace. the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**
- In an administrative command prompt, enter **`gpupdate /force`**.

Enable or disable VSync for the AWS Virtual Display-Only Driver for WSP

By default, WorkSpaces supports using the VSync feature for the AWS Virtual Display-Only Driver. If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

To enable or disable VSync for Windows WorkSpaces

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Enable VSync feature of the AWS Virtual Display Only Driver** setting.
3. In the **Enable VSync feature of the AWS Virtual Display Only Driver** dialog box, choose **Enabled** or **Disabled**.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do the following:

    a. Restart the WorkSpace by doing the either of the following:

        i. Option 1 — In the WorkSpaces console, choose the WorkSpace you want to reboot. Then, choose **Actions**, **Reboot WorkSpaces**.

        ii. Option 2 — In an administrative command prompt, enter `gpupdate /force`.

    b. Reconnect to the WorkSpace in order to apply the setting.

    c. Reboot the Workspace again.

Configure log verbosity for WSP

By default, the log verbosity level for WSP WorkSpaces is set to **Info**. You can set log levels to verbosity levels ranging from least verbose to most verbose, as detailed here:

- Error – least verbose
- Warning

- Info – default
- Debug – most verbose

For Windows WorkSpaces, you can use Group Policy settings to configure the log verbosity levels.

To configure log verbosity levels for Windows WorkSpaces

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Configure log verbosity** setting.
3. In the **Configure log verbosity** dialog box, choose **Enabled** and then set the log verbosity level to **debug**, **error**, **info**, or **warning**.
4. Choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after you restart the WorkSpace session. To apply the Group Policy changes, do one of the following:

   - Reboot the WorkSpace. In the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**.
   - In an administrative command prompt, enter **`gpupdate /force`**.

Configure idle disconnect timeout for WSP

WorkSpaces allows you to configure how long a user can be inactive, while connected to a WorkSpace, before they are disconnected. Examples of user activity input include the following:

- Keyboard events
- Mouse events (cursor movement, scrolling, clicking)
- Stylus events
- Touch events (tapping touchscreens, tablets)
- Gamepad events
- File storage operations (uploads, downloads, directory creation, list items)
- Webcam streaming

Audio in, audio out, and pixels changing don't qualify as user activity.

When enabling idle disconnect timeout will, you can optionally notify your user that their session will disconnect within the configured time unless they engage.

> **Note**
>
> Only users using Linux and Web Access clients will receive this notification.

By default, idle disconnect timeout is disabled, the timeout value is set to 0 minutes, and the notification is disabled. If you enable this policy setting, the idle disconnect timeout value defaults to 60 minutes and the idle disconnect warning value defaults to 60 seconds. For Windows WorkSpaces, you can use Group Policy settings to configure this feature.

To configure idle disconnect timeout for Windows WorkSpaces

1. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
2. Open the **Configure Idle Disconnect Timeout** setting.
3. In the **Configure Idle Disconnect Timeout** dialog box, choose **Enabled** and then set the desired disconnect timeout value (in minutes), and optionally the warning timer value (in seconds).
4. Choose **Apply**, **OK**.
5. The Group Policy setting change takes effect immediately after you apply the change.

Install the Group Policy administrative template for PCoIP

To use the Group Policy settings that are specific to Amazon WorkSpaces when using the PCoIP protocol, you must add the Group Policy administrative template that is appropriate to the version of the PCoIP agent (either 32-bit or 64-bit) that is being used for your WorkSpaces.

> **Note**
>
> If you have a mix of WorkSpaces with 32-bit and 64-bit agents, you can use the Group Policy administrative templates for 32-bit agents, and your Group Policy settings will be applied to both 32-bit and 64-bit agents. When all of your WorkSpaces are using the 64-bit agent, you can switch to using the administrative template for 64-bit agents.

To determine whether your WorkSpaces have the 32-bit agent or the 64-bit agent

1. Log in to a WorkSpace, and then open the Task Manager by choosing **View**, **Send Ctrl + Alt + Delete** or by right-clicking the task bar and choosing **Task Manager**.
2. In the Task Manager, go to the **Details** tab, right-click the column headers, and choose **Select Columns**.
3. In the **Select Columns** dialog box, select **Platform**, and then choose **OK**.
4. On the **Details** tab, find `pcoip_agent.exe`, and then check its value in the **Platform** column to determine if the PCoIP agent is 32-bit or 64-bit. (You might see a mix of 32-bit and 64-bit WorkSpaces components; this is normal.)

Install the Group Policy administrative template for PCoIP (32-Bit)

To use the Group Policy settings that are specific to WorkSpaces when using the PCoIP protocol with the 32-bit PCoIP agent, you must install the Group Policy administrative template for PCoIP. Perform the following procedure on a directory administration WorkSpace or Amazon EC2 instance that is joined to your directory.

For more information about working with .adm files, see Recommendations for managing Group Policy administrative template (.adm) files in the Microsoft documentation.

To install the Group Policy administrative template for PCoIP

1. From a running Windows WorkSpace, make a copy of the `pcoip.adm` file in the `C:\Program Files (x86)\Teradici\PCoIP Agent\configuration` directory.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**) and navigate to the organizational unit in your domain that contains your WorkSpaces machine accounts.
3. Open the context (right-click) menu for the machine account organizational unit and choose **Create a GPO in this domain, and link it here**.
4. In the **New GPO** dialog box, enter a descriptive name for the GPO, such as **WorkSpaces Machine Policies**, and leave **Source Starter GPO** set to **(none)**. Choose **OK**.
5. Open the context (right-click) menu for the new GPO and choose **Edit**.
6. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, and **Administrative Templates**. Choose **Action**, **Add/Remove Templates** from the main menu.

7. In the **Add/Remove Templates** dialog box, choose **Add**, select the `pcoip.adm` file copied previously, and then choose **Open**, **Close**.
8. Close the Group Policy Management Editor. You can now use this GPO to modify the Group Policy settings that are specific to WorkSpaces.

To verify that the administrative template file is correctly installed

1. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**) and navigate to and select the WorkSpaces GPO for your WorkSpaces machine accounts. Choose **Action**, **Edit** in the main menu.
2. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Classic Administrative Templates**, and **PCoIP Session Variables**.
3. You can now use this **PCoIP Session Variables** Group Policy object to modify the Group Policy settings that are specific to Amazon WorkSpaces when using PCoIP.

> **Note**
>
> To allow the user to override your settings, choose **Overridable Administrator Settings**; otherwise, choose **Not Overridable Administrator Settings**.

Install the Group Policy administrative template for PCoIP (64-Bit)

To use the Group Policy settings that are specific to WorkSpaces when using the PCoIP protocol, you must add the Group Policy administrative template `PCoIP.admx` and `PCoIP.adml` files for PCoIP to the Central Store of the domain controller for your WorkSpaces directory. For more information about `.admx` and `.adml` files, see How to create and manage the Central Store for Group Policy Administrative Templates in Windows.

The following procedure describes how to create the Central Store and add the administrative template files to it. Perform the following procedure on a directory administration WorkSpace or Amazon EC2 instance that is joined to your WorkSpaces directory.

To install the Group Policy administrative template files for PCoIP

1. From a running Windows WorkSpace, make a copy of the `PCoIP.admx` and `PCoIP.adml` files in the `C:\Program Files\Teradici\PCoIP Agent\configuration`

\policyDefinitions directory. The PCoIP.adml file is in the en-US subfolder of that directory.

2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open Windows File Explorer, and in the address bar, enter your organization's fully qualified domain name (FQDN), such as \\example.com.
3. Open the sysvol folder.
4. Open the folder with the *FQDN* name.
5. Open the Policies folder. You should now be in *FQDN*\sysvol*FQDN*\Policies.
6. If it doesn't already exist, create a folder named PolicyDefinitions.
7. Open the PolicyDefinitions folder.
8. Copy the PCoIP.admx file into the *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions folder.
9. Create a folder named en-US in the PolicyDefinitions folder.
10. Open the en-US folder.
11. Copy the PCoIP.adml file into the *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions\en-US folder.

To verify that the administrative template files are correctly installed

1. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**).
2. Expand the forest (**Forest:*FQDN***).
3. Expand **Domains**.
4. Expand your FQDN (for example, example.com).
5. Expand **Group Policy Objects**.
6. Select **Default Domain Policy**, open the context (right-click) menu, and choose **Edit**.

> **Note**
>
> If the domain backing the WorkSpaces is an AWS Managed Microsoft AD directory, you cannot use the Default Domain Policy to create your GPO. Instead, you must create and link the GPO under the domain container that has delegated privileges.
> When you create a directory with AWS Managed Microsoft AD, AWS Directory Service creates a *yourdomainname* organizational unit (OU) under the domain root. The

name of this OU is based on the NetBIOS name that you typed when you created your directory. If you didn't specify a NetBIOS name, it will default to the first part of your Directory DNS name (for example, in the case of `corp.example.com`, the NetBIOS name is `corp`).
To create your GPO, instead of selecting **Default Domain Policy**, select the *`yourdomainname`* OU (or any OU under that one), open the context (right-click) menu, and choose **Create a GPO in this domain, and Link it here**.
For more information about the *`yourdomainname`* OU, see What Gets Created in the *AWS Directory Service Administration Guide*.

7. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, and **PCoIP Session Variables**.
8. You can now use this **PCoIP Session Variables** Group Policy object to modify the Group Policy settings that are specific to WorkSpaces when using PCoIP.

> **Note**
>
> To allow the user to override your settings, choose **Overridable Administrator Settings**; otherwise, choose **Not Overridable Administrator Settings**.

Manage Group Policy settings for PCoIP

Use Group Policy settings to manage your Windows WorkSpaces that use PCoIP.

Configure printer support for PCoIP

By default, WorkSpaces enables Basic remote printing, which offers limited printing capabilities because it uses a generic printer driver on the host side to ensure compatible printing.

Advanced remote printing for Windows clients lets you use specific features of your printer, such as double-sided printing, but it requires installation of the matching printer driver on the host side.

Remote printing is implemented as a virtual channel. If virtual channels are disabled, remote printing does not function.

For Windows WorkSpaces, you can use Group Policy settings to configure printer support as needed.

To configure printer support

1. Make sure that you've installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit).
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**) and navigate to **PCoIP Session Variables**.
3. Open the **Configure remote printing** setting.
4. In the **Configure remote printing** dialog box, do one of the following:
   - To enable Advanced remote printing, choose **Enabled**, and then under **Options, Configure remote printing**, choose **Basic and Advanced printing for Windows clients**. To automatically use the client computer's current default printer, select **Automatically set default printer**.
   - To disable printing, choose **Enabled**, and then under **Options, Configure remote printing**, choose **Printing disabled**.
5. Choose **OK**.
6. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.

By default, local printer auto-redirection is disabled. You can use Group Policy settings to enable this feature so that your local printer is set as the default printer every time that you connect to your WorkSpace.

> **Note**
>
> Local printer redirection is not available for Amazon Linux WorkSpaces.

To enable local printer auto-redirection

1. Make sure that you've installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit).
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**) and navigate to **PCoIP Session Variables**.
3. Open the **Configure remote printing** setting.
4. Choose **Enabled**, and then under **Options**, **Configure remote printing**, choose one of the following:
   - **Basic and Advanced printing for Windows clients**
   - **Basic printing**
5. Select **Automatically set default printer**, and then choose **OK**.
6. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.

Enable or disable clipboard redirection (copy/paste) for PCoIP

By default, WorkSpaces supports clipboard redirection. If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

To enable or disable clipboard redirection

1. Make sure that you've installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit).
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**) and navigate to **PCoIP Session Variables**.

3. Open the **Configure clipboard redirection** setting.
4. In the **Configure clipboard redirection** dialog box, choose **Enabled** and then choose one of the following settings to determine the direction in which clipboard redirection is allowed. When you're done, choose **OK**.
   - Disabled in both directions
   - Enabled agent to client only (WorkSpace to local computer)
   - Enabled client to agent only (local computer to WorkSpace)
   - Enabled in both directions
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.

Known limitation

With clipboard redirection enabled on the WorkSpace, if you copy content that is larger than 890 KB from a Microsoft Office application, the application might become slow or unresponsive for up to 5 seconds.

Set the session resume timeout for PCoIP

When you lose network connectivity, your active WorkSpaces client session is disconnected. WorkSpaces client applications for Windows and macOS attempt to reconnect the session automatically if network connectivity is restored within a certain amount of time. The default session resume timeout is 20 minutes, but you can modify that value for WorkSpaces that are controlled by your domain's Group Policy settings.

To set the automatic session resume timeout value

1. Make sure that you've installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit).

2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**) and navigate to **PCoIP Session Variables**.
3. Open the **Configure Session Automatic Reconnection Policy** setting.
4. In the **Configure Session Automatic Reconnection Policy** dialog box, choose **Enabled**, set the **Configure Session Automatic Reconnection Policy** option to the desired timeout, in minutes, and choose **OK**.
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.

Enable or disable audio-in redirection for PCoIP

By default, Amazon WorkSpaces supports redirecting data from a local microphone. If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

> **Note**
>
> If you have a Group Policy setting that restricts users' local logon in their WorkSpaces, audio-in won't work on your WorkSpaces. If you remove that Group Policy setting, the audio-in feature is enabled after the next reboot of the WorkSpace. For more information about this Group Policy setting, see Allow logon locally in the Microsoft documentation.

To enable or disable audio-in redirection

1. Make sure that you've installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit).
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**) and navigate to **PCoIP Session Variables**.
3. Open the **Enable/disable audio in the PCoIP session** setting.

4. In the **Enable/disable audio in the PCoIP session** dialog box, choose **Enabled** or **Disabled**.
5. Choose **OK**.
6. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.

Disable time zone redirection for PCoIP

By default, the time within a Workspace is set to mirror the time zone of the client that is being used to connect to the WorkSpace. This behavior is controlled through time zone redirection. You might want to turn off time zone direction for various reasons:

- Your company wants all employees to work in a certain time zone (even if some employees are in other time zones).
- You have scheduled tasks in a WorkSpace that are meant to run at a certain time in a specific time zone.
- Your users who travel a lot want to keep their WorkSpaces in one time zone for consistency and personal preference.

If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

To disable time zone redirection

1. Make sure that you've installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit).
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**) and navigate to **PCoIP Session Variables**.
3. Open the **Configure timezone redirection** setting.
4. In the **Configure timezone redirection** dialog box, choose **Disabled**.
5. Choose **OK**.

6. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.

7. Set the time zone for the WorkSpaces to the desired time zone.

The time zone of the WorkSpaces is now static and no longer mirrors the time zone of the client machines.

Configure PCoIP security settings

For PCoIP, data in transit is encrypted using TLS 1.2 encryption and SigV4 request signing. The PCoIP protocol uses encrypted UDP traffic, with AES encryption, for streaming pixels. The streaming connection, using port 4172 (TCP and UDP), is encrypted by using AES-128 and AES-256 ciphers, but the encryption defaults to 128-bit. You can change this default to 256-bit by using the **Configure PCoIP Security Settings** Group Policy setting.

You can also use this Group Policy setting to modify the TLS Security Mode and to block certain cipher suites. A detailed explanation of these settings and the supported cipher suites is provided in the **Configure PCoIP Security Settings** Group Policy dialog box.

To configure PCoIP security settings

1. Make sure that you've installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit).
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**) and navigate to **PCoIP Session Variables**.
3. Open the **Configure PCoIP Security Settings** setting.
4. In the **Configure PCoIP Security Settings** dialog box, choose **Enabled**. To set the default encryption for streaming traffic to 256-bit, go to the **PCoIP Data Encryption Ciphers** option, and select **AES-256-GCM only**.

5. (Optional) Adjust the **TLS Security Mode** setting, and then list any cipher suites that you want to block. For more information about these settings, see the descriptions provided in the **Configure PCoIP Security Settings** dialog box.
6. Choose **OK**.
7. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.

Enable USB redirection for YubiKey U2F

> **Note**
>
> Amazon WorkSpaces currently supports USB redirection only for YubiKey U2F. Other types of USB devices might be redirected but they are not supported and might not work properly.

To enable USB redirection for YubiKey U2F

1. Make sure that you've installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit).
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**) and navigate to **PCoIP Session Variables**.
3. Open the **Enable/disable USB in the PCOIP session** setting.
4. Choose **Enabled**, and then choose **OK**.
5. Open the **Configure PCoIP USB allowed and unallowed device rules** setting.
6. Choose **Enabled**, and under **Enter the USB authorization table (maximum ten rules)**, configure your USB device allow list rules.

- Authorization rule - 110500407. This value is a combination of a Vendor ID (VID) and a Product ID (PID). The format for a VID/PID combination is 1xxxxyyyy, where xxxx is the VID in hexadecimal format and yyyy is the PID in hexadecimal format. For this example, 1050 is the VID, and 0407 is the PID. For more YubiKey USB values, see YubiKey USB ID Values.

7. Under **Enter the USB authorization table (maximum ten rules)**, configure your USB device block list rules.

   - For **Unauthorization Rule**, set an empty string. This means that only USB devices in the authorization list are allowed.

   > **Note**
   >
   > You can define a maximum of 10 USB authorization rules and a maximum of 10 USB unauthorization rules. Use the vertical bar (|) character to separate multiple rules. For detailed information about the authorization/unauthorization rules, see Teradici PCoIP Standard Agent for Windows.

8. Choose **OK**.
9. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter **`gpupdate /force`**.

After the setting takes effect, all supported USB devices can redirect to WorkSpaces unless restrictions are configured through the USB device rules setting.

Set the maximum lifetime for a Kerberos ticket

If you have not disabled the **Remember Me** feature of your Windows WorkSpaces, your WorkSpace users can use the **Remember Me** or **Keep me logged in** check box in their WorkSpaces client application to save their credentials. This feature allows users to easily connect to their WorkSpaces

while the client application remains running. Their credentials are securely cached up to the maximum lifetime of their Kerberos tickets.

If your WorkSpace uses an AD Connector directory, you can modify the maximum lifetime of the Kerberos tickets for your WorkSpaces users through Group Policy by following the steps in Maximum Lifetime for a User Ticket in the Microsoft Windows documentation.

To enable or disable the **Remember Me** feature, see Enable self-service WorkSpaces management capabilities for your users in WorkSpaces Personal.

Configure device proxy server settings for internet access

By default, the WorkSpaces client applications use the proxy server that's specified in the device operating system settings for HTTPS (port 443) traffic. The Amazon WorkSpaces client applications use the HTTPS port for updates, registration, and authentication.

> **Note**
>
> Proxy servers that require authentication with sign-in credentials are not supported.

You can configure the device proxy server settings for your Windows WorkSpaces through Group Policy by following the steps in Configure device proxy and internet connectivity settings in the Microsoft documentation.

For more information about configuring the proxy settings in the WorkSpaces Windows client application, see Proxy Server in the *Amazon WorkSpaces User Guide*.

For more information about configuring the proxy settings in the WorkSpaces macOS client application, see Proxy Server in the *Amazon WorkSpaces User Guide*.

For more information about configuring the proxy settings in the WorkSpaces Web Access client application, see Proxy Server in the *Amazon WorkSpaces User Guide*.

Proxying desktop traffic

For PCoIP WorkSpaces, the desktop client applications do not support the use of a proxy server nor TLS decryption and inspection for port 4172 traffic in UDP (for desktop traffic). They require a direct connection to ports 4172.

For WSP WorkSpaces, the WorkSpaces Windows client application (version 5.1 and above) and macOS client application (version 5.4 and above) support the use of HTTP proxy servers for port 4195 TCP traffic. TLS decryption and inspection are not supported.

WSP does not support the use of proxy for desktop traffic over UDP. Only WorkSpaces Windows and macOS desktop client applications and WSP web access support the use of proxy, for TCP traffic.

> **Note**
>
> If you choose to use a proxy server, the API calls that the client application makes to the WorkSpaces services are also proxied. Both API calls and desktop traffic should pass through the same proxy server.

Recommendation on the use of proxy servers

We do not recommend the use of a proxy server with your WorkSpaces desktop traffic.

Amazon WorkSpaces desktop traffic is already encrypted, so proxies do not improve security. A proxy represents an additional hop in the network path that could impact streaming quality by introducing latency. Proxies could also potentially reduce throughput if a proxy is not properly sized to handle desktop streaming traffic. Furthermore, most proxies are not designed for supporting long running WebSocket (TCP) connections and may affect streaming quality and stability.

If you must use a proxy, please locate your proxy server as close to the WorkSpace client as possible, preferably in the same network, to avoid adding network latency, which could negatively impact streaming quality and responsiveness.

Enable Amazon WorkSpaces for Zoom Meeting Media Plugin support

Zoom supports optimized real-time communication for WSP and PCoIP Windows-based WorkSpaces, with the Zoom VDI Plugin. Direct client communication allows video calls to bypass the cloud-based virtual desktop and provide a local-like Zoom experience when the meeting is running inside the your user's WorkSpace.

Enable Zoom Meeting Media Plugin for WSP

Before installing the Zoom VDI components, update your WorkSpaces configuration to support Zoom optimization.

Prerequisites

Before using the plugin, make sure the following requirements are met.

- Windows WorkSpaces client version 5.10.0+ with Zoom VDI Plugin version 5.17.10+
- Within your WorkSpaces — Zoom VDI Meeting client version 5.17.10+

Before you begin

1. Enable the **Extensions** Group Policy setting. For more information, see Configure extensions for WSP.
2. Disable the **Automatic reconnect** Group Policy setting. For more information, see Set the session resume timeout for WSP.

Installing the Zoom components

To enable Zoom optimization, install two components, provided by Zoom, on your Windows WorkSpaces. For more information, see Using Zoom for Amazon Web Services.

1. Install the Zoom VDI Meeting client version 5.12.6+ within your WorkSpace.
2. Install the Zoom VDI Plugin (Windows Universal Installer) version 5.12.6+ on the client where your WorkSpace is installed
3. Validate the plugin is optimizing the Zoom traffic, by confirming that your VDI Plugin Status shows as **Connected** within the Zoom VDI client. For more information, see How to confirm Amazon WorkSpaces optimization .

Enable Zoom Meeting Media Plugin for PCoIP

Users with administrative permission to Active Directory can generate a registry key using their Group Policy Object (GPO). This allows users to send the registry key to all the Windows WorkSpaces within your domain using a forced update. Alternatively, users with administrative rights can also install registry keys individually on their WorkSpaces host.

Prerequisites

Before using the plugin, make sure the following requirements are met.

- Windows WorkSpaces client version 5.4.0+ with Zoom VDI Plugin version 5.12.6+.

- Within your WorkSpaces — Zoom VDI Meeting client version 5.12.6+.

Create the registry key on a Windows WorkSpaces host

Complete the following procedure to create a registry key on a Windows WorkSpaces host. The registry key is required to use Zoom on Windows WorkSpaces.

1. Open Windows Registry Editor as an administrator.
2. Go to `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon`.
3. If the **Extension** key doesn't exist, right-click and choose **New** > **Key** and name it **Extension**.
4. In the new **Extension** key, right-click and choose **New** > **DWORD** and name it **enable**. The name must be in lower-case.
5. Choose the new **DWORD** and change the **Value** to **1**.
6. Reboot the computer to complete the process.
7. On your WorkSpaces host, download and install the latest Zoom VDI client. On your WorkSpaces client (5.4 or higher), download and install the latest Zoom VDI client plugin for Amazon WorkSpaces. For more information, see VDI releases and downloads on the *Zoom support website*.

Launch Zoom to start your video call.

Troubleshooting

Complete the following actions to troubleshoot Zoom on Windows WorkSpaces.

- Confirm that The Registry Key Activation and Applied Correctly.
- Go to `C:\ProgramData\Amazon\Amazon WorkSpaces Extension`. You should see `wse_core_dll`.
- Make sure that the versions on the host and clients are correct and the same.

If you continue to experience difficulty, contact AWS Support using the AWS Support Center.

You can use the following examples to apply a GPO as an administrator of your directory.

- **WSE.adml**

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
 schemaVersion="1.0" xmlns="http://www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <!-- 'displayName' and 'description' don't appear anywhere. All Windows native
 GPO template files have them set like this. -->
    <displayName>enter display name here</displayName>
    <description>enter description here</description>

    <resources>
    <stringTable>
        <string id="SUPPORTED_ProductOnly">N/A</string>
        <string id="Amazon">Amazon</string>
        <string id="Amazon_Help">Amazon Group Policies</string>
        <string id="WorkspacesExtension">Workspaces Extension</string>
        <string id="WorkspacesExtension_Help">Workspace Extension Group Policies</
string>

        <!-- Extension Itself -->
        <string id="ToggleExtension">Enable/disable Extension Virtual Channel</
string>
        <string id="ToggleExtension_Help">
Allows two-way Virtual Channel data communication for multiple purposes

By default, Extension is disabled.</string>

    </stringTable>
    </resources>
</policyDefinitionResources>
```

- **WSE.admx**

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" revision="1.0" schemaVersion="1.0" xmlns="http://
www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <policyNamespaces>
        <target prefix="WorkspacesExtension"
 namespace="Microsoft.Policies.Amazon.WorkspacesExtension" />
    </policyNamespaces>
    <supersededAdm fileName="wse.adm" />
    <resources minRequiredRevision="1.0" />
    <supportedOn>
        <definitions>
```

```
            <definition name="SUPPORTED_ProductOnly"
 displayName="$(string.SUPPORTED_ProductOnly)"/>
        </definitions>
    </supportedOn>
    <categories>
        <category name="Amazon" displayName="$(string.Amazon)"
 explainText="$(string.Amazon_Help)" />
        <category name="WorkspacesExtension"
 displayName="$(string.WorkspacesExtension)"
 explainText="$(string.WorkspacesExtension_Help)">
            <parentCategory ref="Amazon" />
        </category>
    </categories>

    <policies>
        <policy name="ToggleExtension" class="Machine"
 displayName="$(string.ToggleExtension)" explainText="$(string.ToggleExtension_Help)"
 key="Software\Policies\Amazon\Extension" valueName="enable">
            <parentCategory ref="WorkspacesExtension" />
            <supportedOn ref="SUPPORTED_ProductOnly" />
            <enabledValue>
                <decimal value="1" />
            </enabledValue>
            <disabledValue>
                <decimal value="0" />
            </disabledValue>
        </policy>
    </policies>
</policyDefinitions>
```

Manage your Amazon Linux WorkSpaces in WorkSpaces Personal

As with Windows WorkSpaces, Amazon Linux WorkSpaces are domain joined, so you can use Active Directory Users and Groups to:

- Administer your Amazon Linux WorkSpaces
- Provide access to those WorkSpaces for users

Because Linux instances do not adhere to Group Policy, we recommend that you use a configuration management solution to distribute and enforce policy. For example, you can use AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise, or Ansible.

> **Note**
>
> Local printer redirection is not available for Amazon Linux WorkSpaces.

Control WorkSpaces Streaming Protocol (WSP) behavior on Amazon Linux WorkSpaces

The behavior of WSP is controlled by configuration settings in the `wsp.conf` file, which is located in the `/etc/wsp/` directory. To deploy and enforce changes to the policy, use a configuration management solution that supports Amazon Linux. Any changes take effect when the agent starts up.

> **Note**
>
> - If you make incorrect or unsupported changes to the `wsp.conf` file, policy changes may not be applied to the newly established connections on your WorkSpace.
> - Amazon Linux WorkSpaces on WSP bundles currently have the following limitations:
>   - Currently only available in the AWS GovCloud (US-West) and AWS GovCloud (US-East).
>   - Video-in is not supported.
>   - Disconnect session on screen lock is not supported.

The following sections describe how to enable or disable certain features.

Configure clipboard redirection for WSP Amazon Linux WorkSpaces

By default, WorkSpaces supports clipboard redirection. Use the WSP configuration file to configure this feature, if needed. This setting takes effect when you disconnect and reconnect the WorkSpace.

To configure clipboard redirection for WSP Amazon Linux WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2.
```
clipboard = X
```

Where the possible values for *X* are:

`enabled` — Clipboard redirection is enabled in both directions (default)

`disabled` — Clipboard redirection is disabled in both directions

`paste-only` — Clipboard redirection is enabled but only allows you to copy contents from the local client device and paste it to the remote host desktop

`copy-only` — Clipboard redirection is enabled but only allows you to copy contents from the remote host desktop and paste it to the local client device

Enable or disable audio-in redirection for WSP Amazon Linux WorkSpaces

By default, WorkSpaces supports audio-in redirection. Use the WSP configuration file to disable this feature, if needed. This setting takes effect when you disconnect and reconnect to the WorkSpace.

To enable or disable audio-in redirection for WSP Amazon Linux WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Add the following line to the end of the file.

```
audio-in = X
```

Where the possible values for *X* are:

`enabled` — Audio-in redirection is enabled (default)

`disabled` — Audio-in redirection is disabled

Enable or disable time zone redirection for WSP Amazon Linux WorkSpaces

By default, the time within a Workspace is set to mirror the time zone of the client that is being used to connect to the WorkSpace. This behavior is controlled through time zone redirection. You might want to turn off time zone direction for reasons such as the following:

- Your company wants all employees to work in a certain time zone (even if some employees are in other time zones).
- You have scheduled tasks in a WorkSpace that are meant to run at a certain time in a specific time zone.
- Your users who travel a lot want to keep their WorkSpaces in one time zone for consistency and personal preference.

Use the WSP configuration file to configure this feature, if needed. This setting takes effect after you disconnect and reconnect to the WorkSpace.

To enable or disable time zone redirection for WSP Amazon Linux WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp-agent/wsp.conf
   ```

2. Add the following line to the end of the file.

   ```
   timezone_redirect= X
   ```

   Where the possible values for *X* are:

   enabled — Time zone redirection is enabled (default)

   disabled — Time zone redirection is disabled

Control PCoIP Agent behavior on Amazon Linux WorkSpaces

The behavior of the PCoIP Agent is controlled by configuration settings in the `pcoip-agent.conf` file, which is located in the `/etc/pcoip-agent/` directory. To deploy and enforce changes to the policy, use a configuration management solution that supports Amazon Linux. Any changes take

effect when the agent starts up. Restarting the agent ends any open connections and restarts the window manager. To apply any changes, we recommend rebooting the WorkSpace.

> **Note**
>
> If you make incorrect or unsupported changes to the `pcoip-agent.conf` file, you might cause your WorkSpace to stop working. If your WorkSpace stops working, you might need to either connect to your WorkSpace using SSH to roll back the changes, or you might have to rebuild the WorkSpace.

The following sections describe how to enable or disable certain features. For a full listing of the available settings, run `man pcoip-agent.conf` from the terminal on any Amazon Linux WorkSpace.

Configure clipboard redirection for PCoIP Amazon Linux WorkSpaces

By default, WorkSpaces supports clipboard redirection. Use the PCoIP Agent conf to disable this feature, if needed. This setting takes effect when you reboot the WorkSpace.

To configure clipboard redirection for PCoIP Amazon Linux WorkSpaces

1. Open the `pcoip-agent.conf` file in an editor with elevated rights by using the following command.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Add the following line to the end of the file.

   ```
   pcoip.server_clipboard_state = X
   ```

   Where the possible values for *X* are:

   0 — Clipboard redirection is disabled in both directions

   1 — Clipboard redirection is enabled in both directions

   2 — Clipboard redirection is enabled client to agent only (allow copy and paste only from local client device to the remote host desktop)

3 — Clipboard redirection is enabled agent to client only (allow copy and paste only from the remote host desktop to the local client device)

> **Note**
>
> Clipboard redirection is implemented as a virtual channel. If virtual channels are disabled, clipboard redirection doesn't work. To enable virtual channels, see PCoIP Virtual Channels in the Teradici documentation.

Enable or disable audio-in redirection for PCoIP Amazon Linux WorkSpaces

By default, WorkSpaces supports audio-in redirection. Use the PCoIP Agent conf to disable this feature, if needed. This setting takes effect when you reboot the WorkSpace.

To enable or disable audio-in redirection for PCoIP Amazon Linux WorkSpaces

1. Open the `pcoip-agent.conf` file in an editor with elevated rights by using the following command.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Add the following line to the end of the file.

   ```
   pcoip.enable_audio = X
   ```

   Where the possible values for *X* are:

   0 — Audio-in redirection is disabled

   1 — Audio-in redirection is enabled

Enable or disable time zone redirection for PCoIP Amazon Linux WorkSpaces

By default, the time within a Workspace is set to mirror the time zone of the client that is being used to connect to the WorkSpace. This behavior is controlled through time zone redirection. You might want to turn off time zone direction for reasons such as the following:

- Your company wants all employees to work in a certain time zone (even if some employees are in other time zones).
- You have scheduled tasks in a WorkSpace that are meant to run at a certain time in a specific time zone.
- Your users who travel a lot want to keep their WorkSpaces in one time zone for consistency and personal preference.

If needed for Linux WorkSpaces, you can use the PCoIP Agent conf to disable this feature. This setting takes effect when you reboot the WorkSpace.

To enable or disable time zone redirection for PCoIP Amazon Linux WorkSpaces

1. Open the `pcoip-agent.conf` file in an editor with elevated rights by using the following command.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Add the following line to the end of the file.

   ```
   pcoip.enable_timezone_redirect= X
   ```

   Where the possible values for *X* are:

   0 — Time zone redirection is disabled

   1 — Time zone redirection is enabled

Grant SSH access to Amazon Linux WorkSpaces administrators

By default, only assigned users and accounts in the Domain Admins group can connect to Amazon Linux WorkSpaces by using SSH.

We recommend that you create a dedicated administrators group for your Amazon Linux WorkSpaces administrators in Active Directory.

To enable sudo access for members of the Linux_Workspaces_Admins Active Directory group

1. Edit the `sudoers` file by using `visudo`, as shown in the following example.

```
[example\username@workspace-id ~]$ sudo visudo
```

2. Add the following line.

```
%example.com\\Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

After you create the dedicated administrators group, follow these steps to enable login for members of the group.

To enable login for members of the Linux_WorkSpaces_Admins Active Directory group

1. Edit `/etc/security/access.conf` with elevated rights.

```
[example\username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Add the following line.

```
+:(example\Linux_WorkSpaces_Admins):ALL
```

For more information about enabling SSH connections, see Enable SSH connections for your Linux WorkSpaces in WorkSpaces Personal.

Override the default shell for Amazon Linux WorkSpaces

To override the default shell for Linux WorkSpaces, we recommend that you edit the user's `~/.bashrc` file. For example, to use `Z shell` instead of `Bash` shell, add the following lines to `/home/`*`username`*`/.bashrc`.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> After making this change, you must either reboot the WorkSpace or log out of the WorkSpace (not just disconnect) and then log back in for the change to take effect.

Protect custom repositories from unauthorized access

To control access to your custom repositories, we recommend using the security features built into Amazon Virtual Private Cloud (Amazon VPC) rather than using passwords. For example, use network access control lists (ACLs) and security groups. For more information about these features, see Security in the *Amazon VPC User Guide*.

If you must use passwords to protect your repositories, be sure to create your `yum` repository definition files as shown in Repository Definition Files in the Fedora documentation.

Use the Amazon Linux Extras Library repository

With Amazon Linux, you can use the Extras Library to install application and software updates on your instances. For information about using the Extras Library, see Extras Library (Amazon Linux) in the *Amazon EC2 User Guide for Linux Instances*.

> **Note**
>
> If you are using the Amazon Linux repository, your Amazon Linux WorkSpaces must have internet access, or you must configure virtual private cloud (VPC) endpoints to this repository and to the main Amazon Linux repository. For more information, see Provide internet access for WorkSpaces Personal.

Use smart cards for authentication on Linux WorkSpaces

Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) bundles allow the use of Common Access Card (CAC) and Personal Identity Verification (PIV) smart cards for authentication. For more information, see Use smart cards for authentication in WorkSpaces Personal.

Configure device proxy server settings for internet access

By default, the WorkSpaces client applications use the proxy server that's specified in the device operating system settings for HTTPS (port 443) traffic. The Amazon WorkSpaces client applications use the HTTPS port for updates, registration, and authentication.

> **Note**
>
> Proxy servers that require authentication with sign-in credentials are not supported.

You can configure the device proxy server settings for your Linux WorkSpaces through Group Policy by following the steps in Configure device proxy and internet connectivity settings in the Microsoft documentation.

For more information about configuring the proxy settings in the WorkSpaces Windows client application, see Proxy Server in the *Amazon WorkSpaces User Guide*.

For more information about configuring the proxy settings in the WorkSpaces macOS client application, see Proxy Server in the *Amazon WorkSpaces User Guide*.

For more information about configuring the proxy settings in the WorkSpaces Web Access client application, see Proxy Server in the *Amazon WorkSpaces User Guide*.

Proxying desktop traffic

For PCoIP WorkSpaces, the desktop client applications do not support the use of a proxy server nor TLS decryption and inspection for port 4172 traffic in UDP (for desktop traffic). They require a direct connection to ports 4172.

For WSP WorkSpaces, the WorkSpaces Windows client application (version 5.1 and above) and macOS client application (version 5.4 and above) support the use of HTTP proxy servers for port 4195 TCP traffic. TLS decryption and inspection are not supported.

WSP does not support the use of proxy for desktop traffic over UDP. Only WorkSpaces Windows and macOS desktop client applications and WSP web access support the use of proxy, for TCP traffic.

> **Note**
>
> If you choose to use a proxy server, the API calls that the client application makes to the WorkSpaces services are also proxied. Both API calls and desktop traffic should pass through the same proxy server.

Recommendation on the use of proxy servers

We do not recommend the use of a proxy server with your WorkSpaces desktop traffic.

Amazon WorkSpaces desktop traffic is already encrypted, so proxies do not improve security. A proxy represents an additional hop in the network path that could impact streaming quality by

introducing latency. Proxies could also potentially reduce throughput if a proxy is not properly sized to handle desktop streaming traffic. Furthermore, most proxies are not designed for supporting long running WebSocket (TCP) connections and may affect streaming quality and stability.

If you must use a proxy, please locate your proxy server as close to the WorkSpace client as possible, preferably in the same network, to avoid adding network latency, which could negatively impact streaming quality and responsiveness.

Manage your Ubuntu WorkSpaces in WorkSpaces Personal

As with Windows and Amazon Linux WorkSpaces, Ubuntu WorkSpaces are domain joined, so you can use Active Directory Users and Groups to:

- Administer your Ubuntu WorkSpaces
- Provide access to those WorkSpaces for users

You can manage Ubuntu WorkSpaces with Group Policy by using ADsys. See the Ubuntu Active Directory integration FAQ for more information. You can also use other configuration and management solutions, such as Landscape and Ansible.

Control WorkSpaces Streaming Protocol (WSP) behavior on Ubuntu WorkSpaces

The behavior of WSP is controlled by configuration settings in the `wsp.conf` file, which is located in the `/etc/wsp/` directory. To deploy and enforce changes to the policy, use a configuration management solution that supports Ubuntu. Any changes take effect when the agent starts up.

> **Note**
>
> If you make incorrect or unsupported changes to the `wsp.conf` policies may not be applied to the new established connections to your WorkSpace.

The following sections describe how to enable or disable certain features.

Enable or disable clipboard redirection for Ubuntu WorkSpaces

By default, WorkSpaces supports clipboard redirection. Use the WSP configuration file to disable this feature, if needed.

To enable or disable clipboard redirection for Ubuntu WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Add the following line to the end of the `[policies]` group.

```
clipboard = X
```

Where the possible values for *X* are:

enabled — Clipboard redirection is enabled in both directions (default)

disabled — Clipboard redirection is disabled in both directions

paste-only — Clipboard redirection is enabled and only allows you to copy contents from the local client device and paste it to the remote host desktop

copy-only — Clipboard redirection is enabled and only allows you to copy contents from the remote host desktop and paste it to the local client device

Enable or disable audio-in redirection for Ubuntu WorkSpaces

By default, WorkSpaces supports audio-in redirection. Use the WSP configuration file to disable this feature, if needed.

To enable or disable audio-in redirection for Ubuntu WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Add the following line to the end of the `[policies]` group.

```
audio-in = X
```

Where the possible values for *X* are:

enabled — Audio-in redirection is enabled (default)

disabled — Audio-in redirection is disabled

Enable or disable video-in redirection for Ubuntu WorkSpaces

By default, WorkSpaces supports video-in redirection. Use the WSP configuration file to disable this feature, if needed.

To enable or disable video-in redirection for Ubuntu WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Add the following line to the end of the `[policies]` group.

   ```
   video-in = X
   ```

   Where the possible values for *X* are:

   enabled — Video-in redirection is enabled (default)

   disabled — Video-in redirection is disabled

Enable or disable time zone redirection for Ubuntu WorkSpaces

By default, the time within a Workspace is set to mirror the time zone of the client that is being used to connect to the WorkSpace. This behavior is controlled through time zone redirection. You might want to turn off time zone direction for reasons such as the following:

- Your company wants all employees to work in a certain time zone (even if some employees are in other time zones).
- You have scheduled tasks in a WorkSpace that are meant to run at a certain time in a specific time zone.
- Your users travel a lot and want to keep their WorkSpaces in one time zone for consistency and personal preference.

Use the WSP configuration file to configure this feature, if needed.

To enable or disable time zone redirection for Ubuntu WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Add the following line to the end of the `[policies]` group.

```
timezone-redirection = X
```

Where the possible values for *X* are:

enabled — Time zone redirection is enabled (default)

disabled — Time zone redirection is disabled

Enable or disable printer redirection for Ubuntu WorkSpaces

By default, WorkSpaces supports printer redirection. Use the WSP configuration file to disable this feature, if needed.

To enable or disable printer redirection for Ubuntu WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Add the following line to the end of the `[policies]` group.

```
remote-printing = X
```

Where the possible values for *X* are:

enabled — Printer redirection is enabled (default)

disabled — Printer redirection is disabled

Enable or disable disconnect session on screen lock for WSP

Enable disconnect session on screen lock to allow your users to end their WorkSpaces session when the lock screen is detected. To reconnect from the WorkSpaces client, users can use their passwords or their smart cards to authenticate themselves, depending on which type of authentication has been enabled for their WorkSpaces.

By default, WorkSpaces doesn't support disconnecting session on screen lock. Use the WSP configuration file to enable this feature, if needed.

To enable or disable disconnect session on screen lock for Ubuntu WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Add the following line to the end of the `[policies]` group.

   ```
   disconnect-on-lock = X
   ```

   Where the possible values for *X* are:

   enabled — Disconnect on screen lock is enabled

   disabled — Disconnect on screen lock is disabled (default)

Grant SSH access to Ubuntu WorkSpaces administrators

By default, only assigned users and accounts in the Domain Admins group can connect to Ubuntu WorkSpaces by using SSH. To enable other users and accounts to connect to Ubuntu WorkSpaces using SSH, we recommend that you create a dedicated administrators group for your Ubuntu WorkSpaces administrators in Active Directory.

To enable sudo access for members of the `Linux_WorkSpaces_Admins` Active Directory group

1. Edit the `sudoers` file by using `visudo`, as shown in the following example.

   ```
   [username@workspace-id ~]$ sudo visudo
   ```

2. Add the following line.

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

After you create the dedicated administrators group, follow these steps to enable login for members of the group.

To enable login for members of the `Linux_WorkSpaces_Admins` Active Directory group

1. Edit `/etc/security/access.conf` with elevated rights.

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Add the following line.

```
+:(Linux_WorkSpaces_Admins):ALL
```

With Ubuntu WorkSpaces you do not need to add a domain name when specifying username for SSH connection, and by default, password authentication is disabled. To connect via SSH, you needs to either add your SSH public key to `$HOME/.ssh/authorized_keys` on your Ubuntu WorkSpace, or edit `/etc/ssh/sshd_config` to set PasswordAuthentication to `yes`. For more information about enabling SSH connections, see Enable SSH connections for your Linux WorkSpaces.

Override the default shell for Ubuntu WorkSpaces

To override the default shell for Ubuntu WorkSpaces, we recommend that you edit the user's `~/.bashrc` file. For example, to use `Z shell` instead of `Bash` shell, add the following lines to `/home/username/.bashrc`.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> After making this change, you must either reboot the WorkSpace or log out of the WorkSpace (not just disconnect) and then log back in for the change to take effect.

Configure device proxy server settings for internet access

By default, the WorkSpaces client applications use the proxy server that's specified in the device operating system settings for HTTPS (port 443) traffic. The Amazon WorkSpaces client applications use the HTTPS port for updates, registration, and authentication.

> **Note**
>
> Proxy servers that require authentication with sign-in credentials are not supported.

You can configure the device proxy server settings for your Ubuntu WorkSpaces through Group Policy by following the steps in Configure device proxy and internet connectivity settings in the Microsoft documentation.

For more information about configuring the proxy settings in the WorkSpaces Windows client application, see Proxy Server in the *Amazon WorkSpaces User Guide*.

For more information about configuring the proxy settings in the WorkSpaces macOS client application, see Proxy Server in the *Amazon WorkSpaces User Guide*.

For more information about configuring the proxy settings in the WorkSpaces Web Access client application, see Proxy Server in the *Amazon WorkSpaces User Guide*.

Proxying desktop traffic

For PCoIP WorkSpaces, the desktop client applications do not support the use of a proxy server nor TLS decryption and inspection for port 4172 traffic in UDP (for desktop traffic). They require a direct connection to ports 4172.

For WSP WorkSpaces, the WorkSpaces Windows client application (version 5.1 and above) and macOS client application (version 5.4 and above) support the use of HTTP proxy servers for port 4195 TCP traffic. TLS decryption and inspection are not supported.

WSP does not support the use of proxy for desktop traffic over UDP. Only WorkSpaces Windows and macOS desktop client applications and WSP web access support the use of proxy, for TCP traffic.

> **Note**
>
> If you choose to use a proxy server, the API calls that the client application makes to the WorkSpaces services are also proxied. Both API calls and desktop traffic should pass through the same proxy server.

Recommendation on the use of proxy servers

We do not recommend the use of a proxy server with your WorkSpaces desktop traffic.

Amazon WorkSpaces desktop traffic is already encrypted, so proxies do not improve security. A proxy represents an additional hop in the network path that could impact streaming quality by introducing latency. Proxies could also potentially reduce throughput if a proxy is not properly sized to handle desktop streaming traffic. Furthermore, most proxies are not designed for supporting long running WebSocket (TCP) connections and may affect streaming quality and stability.

If you must use a proxy, please locate your proxy server as close to the WorkSpace client as possible, preferably in the same network, to avoid adding network latency, which could negatively impact streaming quality and responsiveness.

Manage your Red Hat Enterprise Linux WorkSpaces

As with Windows and Amazon Linux WorkSpaces, Red Hat Enterprise Linux WorkSpaces are domain joined, so you can use Active Directory Users and Groups to:

- Administer your Red Hat Enterprise Linux WorkSpaces
- Provide access to those WorkSpaces for users

You can manage Red Hat Enterprise Linux WorkSpaces with Group Policy by using ADsys. See the Red Hat Enterprise Linux Active Directory integration FAQ for more information. You can also use other configuration and management solutions, such as Landscape and Ansible.

Control WorkSpaces Streaming Protocol (WSP) behavior on Red Hat Enterprise Linux WorkSpaces

The behavior of WSP is controlled by configuration settings in the `wsp.conf` file, which is located in the `/etc/wsp/` directory. To deploy and enforce changes to the policy, use a configuration management solution that supports Red Hat Enterprise Linux. Any changes take effect when the agent starts up.

> **Note**
>
> If you make incorrect or unsupported changes to the `wsp.conf` policies may not be applied to the new established connections to your WorkSpace.

The following sections describe how to enable or disable certain features.

Enable or disable clipboard redirection for Red Hat Enterprise Linux WorkSpaces

By default, WorkSpaces supports clipboard redirection. Use the WSP configuration file to disable this feature, if needed.

To enable or disable clipboard redirection for Red Hat Enterprise Linux WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Add the following line to the end of the `[policies]` group.

   ```
   clipboard = X
   ```

   Where the possible values for *X* are:

   enabled — Clipboard redirection is enabled in both directions (default)

   disabled — Clipboard redirection is disabled in both directions

paste-only — Clipboard redirection is enabled and only allows you to copy contents from the local client device and paste it to the remote host desktop

copy-only — Clipboard redirection is enabled and only allows you to copy contents from the remote host desktop and paste it to the local client device

Enable or disable audio-in redirection for Red Hat Enterprise Linux WorkSpaces

By default, WorkSpaces supports audio-in redirection. Use the WSP configuration file to disable this feature, if needed.

To enable or disable audio-in redirection for Red Hat Enterprise Linux WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Add the following line to the end of the `[policies]` group.

```
audio-in = X
```

Where the possible values for *X* are:

enabled — Audio-in redirection is enabled (default)

disabled — Audio-in redirection is disabled

Enable or disable video-in redirection for Red Hat Enterprise Linux WorkSpaces

By default, WorkSpaces supports video-in redirection. Use the WSP configuration file to disable this feature, if needed.

To enable or disable video-in redirection for Red Hat Enterprise Linux WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Add the following line to the end of the `[policies]` group.

```
video-in = X
```

Where the possible values for *X* are:

enabled — Video-in redirection is enabled (default)

disabled — Video-in redirection is disabled

Enable or disable time zone redirection for Red Hat Enterprise Linux WorkSpaces

By default, the time within a Workspace is set to mirror the time zone of the client that is being used to connect to the WorkSpace. This behavior is controlled through time zone redirection. You might want to turn off time zone direction for reasons such as the following:

- Your company wants all employees to work in a certain time zone (even if some employees are in other time zones).
- You have scheduled tasks in a WorkSpace that are meant to run at a certain time in a specific time zone.
- Your users travel a lot and want to keep their WorkSpaces in one time zone for consistency and personal preference.

Use the WSP configuration file to configure this feature, if needed.

To enable or disable time zone redirection for Red Hat Enterprise Linux WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Add the following line to the end of the `[policies]` group.

```
timezone-redirection = X
```

Where the possible values for *X* are:

enabled — Time zone redirection is enabled (default)

disabled — Time zone redirection is disabled

Enable or disable printer redirection for Red Hat Enterprise Linux WorkSpaces

By default, WorkSpaces supports printer redirection. Use the WSP configuration file to disable this feature, if needed.

To enable or disable printer redirection for Red Hat Enterprise Linux WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Add the following line to the end of the `[policies]` group.

```
remote-printing = X
```

Where the possible values for *X* are:

enabled — Printer redirection is enabled (default)

disabled — Printer redirection is disabled

Enable or disable disconnect session on screen lock for WSP

Enable disconnect session on screen lock to allow your users to end their WorkSpaces session when the lock screen is detected. To reconnect from the WorkSpaces client, users can use their passwords or their smart cards to authenticate themselves, depending on which type of authentication has been enabled for their WorkSpaces.

By default, WorkSpaces doesn't support disconnecting session on screen lock. Use the WSP configuration file to enable this feature, if needed.

To enable or disable disconnect session on screen lock for Red Hat Enterprise Linux WorkSpaces

1. Open the `wsp.conf` file in an editor with elevated rights by using the following command.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Add the following line to the end of the `[policies]` group.

```
disconnect-on-lock = X
```

Where the possible values for *X* are:

enabled — Disconnect on screen lock is enabled

disabled — Disconnect on screen lock is disabled (default)

Grant SSH access to Red Hat Enterprise Linux WorkSpaces administrators

By default, only assigned users and accounts in the Domain Admins group can connect to Red Hat Enterprise Linux WorkSpaces by using SSH. To enable other users and accounts to connect to Red Hat Enterprise Linux WorkSpaces using SSH, we recommend that you create a dedicated administrators group for your Red Hat Enterprise Linux WorkSpaces administrators in Active Directory.

To enable sudo access for members of the `Linux_WorkSpaces_Admins` Active Directory group

1. Edit the `sudoers` file by using `visudo`, as shown in the following example.

```
[username@workspace-id ~]$ sudo visudo
```

2. Add the following line.

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

After you create the dedicated administrators group, follow these steps to enable login for members of the group.

To enable login for members of the `Linux_WorkSpaces_Admins` Active Directory group

1. Edit `/etc/security/access.conf` with elevated rights.

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Add the following line.

```
+:(Linux_WorkSpaces_Admins):ALL
```

With Red Hat Enterprise Linux WorkSpaces you do not need to add a domain name when specifying username for SSH connection, and by default, password authentication is disabled. To connect via SSH, you needs to either add your SSH public key to `$HOME/.ssh/authorized_keys` on your Red Hat Enterprise Linux WorkSpace, or edit `/etc/ssh/sshd_config` to set PasswordAuthentication to `yes`. For more information about enabling SSH connections, see Enable SSH connections for your Linux WorkSpaces.

Override the default shell for Red Hat Enterprise Linux WorkSpaces

To override the default shell for Red Hat Enterprise Linux WorkSpaces, we recommend that you edit the user's `~/.bashrc` file. For example, to use `Z shell` instead of `Bash` shell, add the following lines to `/home/username/.bashrc`.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> After making this change, you must either reboot the WorkSpace or log out of the WorkSpace (not just disconnect) and then log back in for the change to take effect.

Optimize WorkSpaces for real-time communication in WorkSpaces Personal

Amazon WorkSpaces offers a diverse range of techniques to facilitate the deployment of Unified Communication (UC) applications like Microsoft Teams, Zoom, Webex and others. In contemporary application landscapes, most UC applications consist of a variety of features, including 1:1 chat rooms, collaborative group chat channels, seamless file storage and exchange, live events, webinars, broadcasts, interactive screen sharing and control, whiteboarding, and offline audio/video messaging capabilities. Most of this functionality is seamlessly available on WorkSpaces as standard features, without the need for additional fine-tuning or enhancement. However, it's worth noting that real-time communication elements, particularly one-on-one calling and collective group meetings, represent an exception to this rule. The successful incorporation of such functionality frequently demands dedicated focus and planning during the process of WorkSpaces deployment.

When planning your implementation of real-time communication functionalities of UC applications on Amazon WorkSpaces, you have three distinct Real-Time Communication (RTC) configuration modes to choose from. The selection of which depends on the specific application or applications that you intend to provide to your users and the client devices you plan to use.

This document focus on optimizing the user experience for the most common UC applications in Amazon WorkSpaces. For WorkSpaces Core specific optimizations, please refer to the partner-specific documentation.

Topics

Overview of media optimization modes

Following are the media optimization options available.

Option 1: Media Optimized Real-Time Communication (Media Optimized RTC)

In this mode, third-party UC and VoIP applications are executed on the remote WorkSpace, while their media framework is offloaded to the supported client for direct communication. The following UC applications use this approach on Amazon WorkSpaces:

- Zoom meetings
- Cisco Webex meetings

For Media Optimized RTC mode to function, the UC application vendor should develop the integration with WorkSpaces using one of the available Software Development Kits (SDK), such as the DCV Extension SDK. This mode requires the UC components to be installed on the client device.

For more information about configuring this mode, see Configure Media Optimized RTC.

Option 2: In-Session Optimized Real-Time Communication (In-session Optimized RTC)

In this mode, the unaltered UC application runs on the WorkSpace, channeling audio and video traffic via the WorkSpaces Streaming Protocol to the client device. Local audio from the microphone and video stream from a webcam are redirected to the WorkSpace, where they are consumed by the UC application. This mode provides broad application compatibility and efficiently delivers the UC application from the remote WorkSpace to a variety of client platforms. You don't need to deploy the UC application components to the client device.

For more information about configuring this mode, see Configure In-session Optimized RTC.

Option 3: Direct Real-Time Communication (Direct RTC)

In this mode, the application operating within the WorkSpace takes control over the physical or virtual telephone set located on the user's desk or client OS. This results in the audio traffic traversing directly from the physical telephone at the user's workstation or the virtual phone operating on the client device to the remote call peer. Notable instances of applications functioning within this mode encompass:

- Amazon Connect Optimization for Amazon WorkSpaces
- Genesys Cloud WebRTC media helper
- Microsoft Teams SIP Gateway
- Microsoft Teams Desk phones and Teams displays
- Participation in audio conferencing through the dial-in or "dial my phone" features of the UC application.

For more information about configuring this mode, see Configure Direct RTC.

Which RTC optimization mode to use?

Different RTC optimization modes can be employed concurrently or set up to complement each other as a fallback. For instance, consider enabling Media Optimized RTC for Cisco Webex meetings. This configuration ensures that users experience optimized communication when accessing WorkSpace through a desktop client. However, in scenarios where Webex is accessed from a shared internet kiosk lacking UC optimization components, Webex will seamlessly transition to In-session Optimized RTC mode to maintain functionality. When users engage with multiple UC applications, the RTC configuration modes may vary based on their unique requirements.

The following table represents common UC application features and defines which RTC configuration mode provides the best result.

Feature	Direct RTC	Media Optimized RTC	In-session Optimized RTC
1:1 chat	Does not require RTC configuration		
Group chat rooms	Does not require RTC configuration		
Group audio conferencing	Best	Best	Good
Group video conferencing	Good	Best	Good
1:1 audio calls	Best	Best	Good
1:1 video calls	Good	Best	Good
Whiteboarding	Does not require RTC configuration		
Audio/video clips/ messaging	Not applicable	Good	Best
File Sharing	Not applicable	Depends on UC application	Best
Screen sharing and control	Not applicable	Depends on UC application	Best

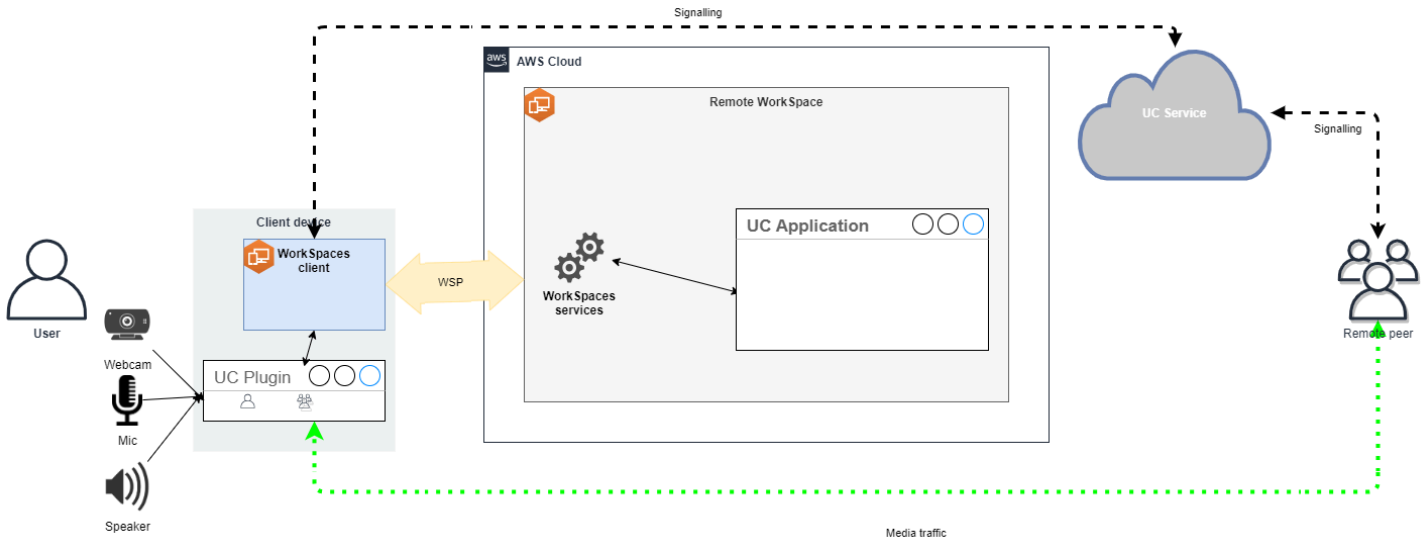
Feature	Direct RTC	Media Optimized RTC	In-session Optimized RTC
Webinars/Broadcast events	Not applicable	Good	Best

RTC Optimization Guidance

Configure Media Optimized RTC

Media Optimized RTC mode is made possible by the UC application vendor use of the SDKs provided by Amazon. The architecture requires UC vendor to develop a UC-specific plugin or extension and deploy it to the client.

The SDK, which includes publicly available options like the DCV Extension SDK and customized private versions, establishes a control channel between the UC application module operating within the WorkSpace and a plugin on the client side. Typically, this control channel instructs the client extension to initiate or join a call. Once the call is established through the client-side extension, the UC plugin captures audio from the microphone and video from the webcam, which are then transmitted directly to the UC cloud or a call peer. The incoming audio is played locally, and video is overlaid on the remote client UI. The control channel is responsible for communicating the call's status.



Amazon WorkSpaces currently supports following applications with Media Optimized RTC mode:

- Zoom meetings (for PCoIP and WSP WorkSpaces)

- Cisco Webex meetings (for WSP WorkSpaces only)

If you are using an application that is not on the list, it is advisable to engage the application vendor and request support for WorkSpaces Media Optimized RTC. To expedite this process, encourage them to contact aws-av-offloading@amazon.com.

While Media Optimized RTC mode enhances call performance and minimizes WorkSpace resource utilization, it does possess certain limitations:

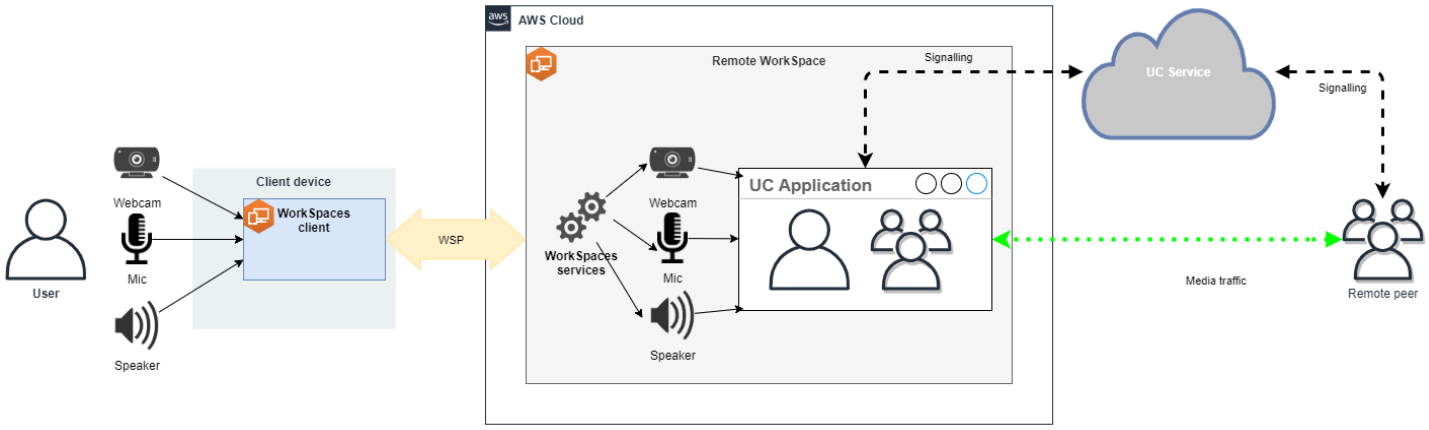
- The UC client extension must be installed on the client device.
- The UC client extension requires independent management and updates.
- UC client extensions might not be available on certain client platforms, such as, mobile platforms, or web clients.
- Some UC application functionalities could be constrained in this mode; for instance, screen sharing behavior might differ.
- Usage of client-side extensions might not be suitable for scenarios like Bring Your Own Device (BYOD) or shared kiosks.

If Media Optimized RTC mode proves unsuitable for your environment or certain users are unable to install the client extension, configuring In-session Optimized RTC mode as a fallback option is recommended.

Configure In-session Optimized RTC

In the In-session Optimized RTC mode, the UC application operates on the WorkSpace without any modifications, providing a like-local experience. The audio and video streams generated by the application are captured by the WorkSpaces Streaming Protocol (WSP) and transmitted to the client side. At the client, the microphone (on both WSP and PCoIP WorkSpaces) and webcam (only on WSP WorkSpaces) signals are captured, redirected back to the WorkSpace, and seamlessly passed to the UC application.

Notably, this option ensures exceptional compatibility, even with legacy applications, offering a cohesive user experience regardless of the application's origin. In-session optimization works with web client as well.



WorkSpaces Streaming Protocol (WSP) has been meticulously optimized to enhance the performance of Remote RTC mode. The optimization measures encompass:

- Utilization of an Adaptive UDP-based QUIC transport, ensuring efficient data transmission.
- Establishment of a low-latency audio path, facilitating fast audio input and output.
- Implementation of voice-optimized audio codecs to maintain audio quality while reducing CPU and network utilization.
- Webcam redirection, enabling the integration of webcam functionalities.
- Configuration of webcam resolution to optimize performance.
- Integration of adaptive display codecs to balance speed and visual quality.
- Audio jitter correction, guaranteeing smooth audio transmission.

These optimizations collectively contribute to a robust and fluid experience in Remote RTC mode.

Sizing recommendations

To effectively support Remote RTC mode, it's crucial to ensure proper sizing of Amazon WorkSpaces. The remote WorkSpace must meet or exceed the system requirements of the respective Unified Communication (UC) application. The following table outlines the minimum supported and recommended WorkSpaces configurations for popular UC applications when used for video and audio calls:

			Video calls		Audio calls		
Application	**CPU requirements for RTC app**	**RAM requirements for RTC app**	**Minimally supported WorkSpace**	**Recommended WorkSpace**	**Minimally supported WorkSpace**	**Recommended WorkSpace**	**Reference**
Microsoft Teams	2 core required, 4 core recommended	4.0 GB RAM	Power (4 vCPU, 16 GB memory)	PowerPro (8 vCPU, 32 GB memory)	Performance (2 vCPU, 8 GB memory)	Power (4 vCPU, 16 GB memory)	Hardware requirements for Microsoft Teams
Zoom	2 core required, 4 core recommended	4.0 GB RAM	Power (4 vCPU, 16 GB memory)	PowerPro (8 vCPU, 32 GB memory)	Performance (2 vCPU, 8 GB memory)	Power (4 vCPU, 16 GB memory)	Zoom system requirements: Windows, macOS, Linux
Webex	2 core required	4.0 GB RAM	Power (4 vCPU, 16 GB memory)	PowerPro (8 vCPU, 32 GB memory)	Performance (2 vCPU, 8 GB memory)	Power (4 vCPU, 16 GB memory)	System requirements for Webex services

It's important to note that video conferencing involves significant resource usage for video encoding and decoding. In physical machine scenarios, these tasks are offloaded to the GPU. In non-GPU WorkSpaces, these tasks are performed on the CPU in parallel with remote protocol encoding. Therefore, for users regularly engaged in video streaming or video calls, opting for the PowerPro configuration is highly recommended.

Screen sharing also consumes notable resources, with resource consumption increasing with higher resolutions. As result, on non-GPU WorkSpaces, screen sharing is often limited to a lower frame rate.

Leverage the UDP-based QUIC transport with WorkSpaces Streaming Protocol (WSP)

UDP transport is particularly well-suited for transmitting RTC applications. To maximize efficiency, ensure that your network is set up to utilize QUIC transport for WSP. Note that UDP-based transport is available with native clients only.

Configure UC application for WorkSpaces

For enhanced video processing capabilities, such as background blur, virtual backgrounds, reactions, or hosting live events, opting for a GPU-enabled WorkSpace is essential to achieve optimal performance.

Most of the UC applications provide guidance to disable advanced video processing to reduce CPU utilization on non-GPU WorkSpaces.

For more information, refer to the following resources.

- Microsoft Teams: Teams for Virtualized Desktop Infrastructure
- Zoom Meetings: Managing the user experience for incompatible VDI plugins
- Webex: Deployment guide for Webex App for Virtual Desktop Infrastructure (VDI) - Manage and troubleshoot Webex App for VDI [Webex App]
- Google Meet: Using VDI

Enable bi-directional audio and webcam redirection

Amazon WorkSpaces inherently support audio-in, audio-out, and camera redirection through video-in by default. However, if these features have been disabled for any specific reasons, you can follow the provided guidance to re-enable redirection. For more information, refer to Enable or disable video-in redirection for WSP in the *Amazon WorkSpaces Administration Guide*. Users need to select the camera they want to use in session after connecting. For more information, users should refer to Webcams and other video devices in the *Amazon WorkSpaces User Guide*.

Limit maximum webcam resolution

For users employing Power or PowerPro WorkSpaces for video conferencing, it is strongly recommended to restrict the maximum resolution of redirected webcams. In the case of PowerPro, the recommended maximum resolution is 640 pixels in width by 480 pixels in height. For Power, the recommended maximum resolution is 320 pixels in width by 240 pixels in height.

Complete the following steps to configure the maximum webcam resolution.

1. Open the Windows Registry Editor.
2. Navigate to the following registry path:

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/webcam
```

3. Create a string value named `max-resolution` and set it to the desired resolution in the `(X,Y)` format, where `X` represents the horizontal pixel count (width) and `Y` represents the vertical pixel count (height). For example, specify `(640,480)`) to represent a resolution that is 640 pixels in width and 480 pixel in height.

Enable voice-optimized audio configuration

By default, WorkSpaces are set to deliver 7.1 high-fidelity audio from WorkSpaces to the client, ensuring superior music playback quality. However, if your primary use case involves audio or video conferencing, modifying the audio codec profile to a voice-optimized setting can conserve CPU and network resources.

Complete the following steps to set the audio profile to voice optimized.

1. Open the Windows Registry Editor.
2. Navigate to the following registry path:

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/audio
```

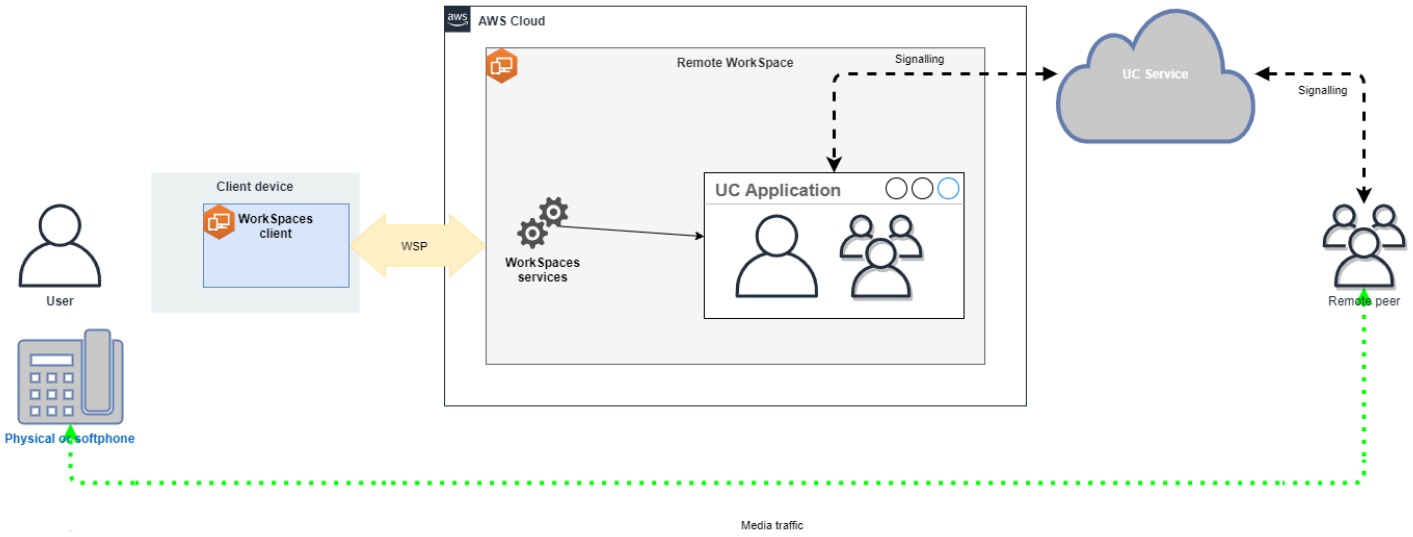
3. Create a string value name `default-profile` and set it to `voice`.

Use good quality headsets for audio and video calls

To enhance the audio experience and prevent echo, it's crucial to utilize high-quality headsets. Utilizing desktop speakers can lead to echo issues on the remote end of the call.

Configure Direct RTC

The configuration of Direct RTC mode depends on the specific Unified Communication (UC) application and does not necessitate any changes in the WorkSpaces configuration. The following list offers a non-exhaustive compilation of optimizations for various UC applications.



- Microsoft Teams:
  - Plan for SIP Gateway
  - Audio Conferencing in Microsoft 365
  - Plan your Teams voice solution
- Zoom Meetings:
  - Enabling or disabling toll call dial-in numbers
  - Using desk phone call control
  - Desk phone companion mode
- Webex:
  - Webex App | Make calls with your desk phone
  - Webex App | Supported calling options
- BlueJeans:
  - Dialing into a Meeting from a Desk Telephone
- Genesys:
  - Genesys Cloud WebRTC media helper
- Amazon Connect:
  - Amazon Connect Optimization for Amazon WorkSpaces
- Google Meet:
  - Use a phone for audio in a video meeting

Manage the running mode in WorkSpaces Personal

The *running mode* of a WorkSpace determines its immediate availability and how you pay for it (monthly or hourly). You can choose between the following running modes when you create the WorkSpace:

- **AlwaysOn** — Use when paying a fixed monthly fee for unlimited usage of your WorkSpaces. This mode is best for users who use their WorkSpace full time as their primary desktop.
- **AutoStop** — Use when paying for your WorkSpaces by the hour. With this mode, your WorkSpaces stop after a specified period of disconnection, and the state of apps and data is saved.

For more information, see WorkSpaces Pricing.

AutoStop WorkSpaces

To set the automatic stop time, select the WorkSpace in the Amazon WorkSpaces console, choose **Actions**, **Modify Running Mode Properties**, and then set **AutoStop Time (hours)**. By default, **AutoStop Time (hours)** is set to 1 hour, which means that the WorkSpace stops automatically an hour after the WorkSpace is disconnected.

After a WorkSpace is disconnected and the AutoStop Time period has expired, it might take several additional minutes for the WorkSpace to automatically stop. However, billing stops as soon as the AutoStop Time period expires, and you aren't charged for that additional time.

When possible, the state of the desktop is saved to the root volume of the WorkSpace. The WorkSpace resumes when a user logs in, and all open documents and running programs return to their saved state.

AutoStop Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro WorkSpaces do not preserve the state of data and programs when they stop. For these Autostop WorkSpaces, we recommend saving your work when you’re done using them each time.

For Bring Your Own License (BYOL) AutoStop WorkSpaces, a large number of concurrent logins could result in significantly increased time for WorkSpaces to be available. If you expect many users to log into your BYOL AutoStop WorkSpaces at the same time, please consult your account manager for advice.

> **Important**
>
> AutoStop WorkSpaces stop automatically only if the WorkSpaces are disconnected.

A WorkSpace is disconnected only in the following circumstances:

- If the user manually disconnects from the WorkSpace or quits the Amazon WorkSpaces client application.
- If the client device is shut down.
- If there's no connection between the client device and the WorkSpace for more than 20 minutes.

As a best practice, AutoStop WorkSpace users should manually disconnect from their WorkSpaces when they're done using them each day. To manually disconnect, choose **Disconnect WorkSpace** or **Quit Amazon WorkSpaces** from the **Amazon WorkSpaces** menu in the WorkSpaces client applications for Linux, macOS, or Windows. For Android or iPad, choose **Disconnect** from the sidebar menu.

AutoStop WorkSpaces may not stop automatically in the following situations:

- If the client device is only locked, sleeping, or otherwise inactive (for example, the laptop lid is closed) instead of shut down, the WorkSpaces application might still be running in the background. As long as the WorkSpaces application is still running, the WorkSpace might not be disconnected, and therefore the WorkSpace might not automatically stop.
- WorkSpaces can detect disconnection only when users are using WorkSpaces clients. If users are using third-party clients, WorkSpaces might not be able to detect disconnection, and therefore the WorkSpaces might not automatically stop and billing might not be suspended.

Modify the running mode

You can switch between running modes at any time.

To modify the running mode of a WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpace to modify and choose **Actions**, **Modify running mode**.

4. Select the new running mode, **AlwaysOn** or **AutoStop**, and then choose **Save**.

To modify the running mode of a WorkSpace using the AWS CLI

Use the modify-workspace-properties command.

Stop and start an AutoStop WorkSpace

When your AutoStop WorkSpaces are disconnected, they stop automatically after a specified period of disconnection, and hourly billing is suspended. To further optimize costs, you can manually suspend the hourly charges associated with AutoStop WorkSpaces. The WorkSpace stops and all apps and data are saved for the next time a user logs in to the WorkSpace.

When a user reconnects to a stopped WorkSpace, it resumes from where it left off, typically in under 90 seconds.

You can reboot (restart) AutoStop WorkSpaces that are available or in an error state.

To stop an AutoStop WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpace to stop and choose **Actions**, **Stop WorkSpaces**.
4. When prompted for confirmation, choose **Stop WorkSpace**.

To start an AutoStop WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpaces to start and choose **Actions**, **Start WorkSpaces**.
4. When prompted for confirmation, choose **Start WorkSpace**.

To remove the fixed infrastructure costs that are associated with AutoStop WorkSpaces, remove the WorkSpace from your account. For more information, see Delete a WorkSpace in WorkSpaces Personal.

To stop and start an AutoStop WorkSpace using the AWS CLI

Use the stop-WorkSpaces and start-WorkSpaces commands.

Manage applications in WorkSpaces Personal

After you launch a WorkSpace, you can see the list of all of the application bundles that are associated with your WorkSpace on the WorkSpaces console.

To see the list of all the application bundles associated to your WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. From the left navigation pane, choose **WorkSpaces**.
3. Select the WorkSpace and choose **View Details**.
4. Under **Applications**, find the list of applications that are associated with this WorkSpace, along with their installation status.

You can update the application bundles on your WorkSpace in the following ways:

- Install application bundles on your WorkSpace
- Uninstall application bundles from your WorkSpace
- Install application bundles and uninstall a different set of application bundles on your WorkSpace

> **Note**
>
> - To update application bundles, the WorkSpace must have a status of `AVAILABLE` or `STOPPED`.
> - Manage applications is only available for Windows WorkSpaces.
> - Manage applications is only available for application bundles that are subscribed through AWS.

Supported bundles for Manage applications

Manage applications allows you install and uninstall the following applications on your WorkSpaces. For Microsoft Office 2016 bundle and Microsoft Office 2019, you can only uninstall.

- Microsoft Office LTSC Professional Plus 2021
- Microsoft Visio LTSC Professional 2021
- Microsoft Project Professional 2021
- Microsoft Office LTSC Standard 2021
- Microsoft Visio LTSC Standard 2021
- Microsoft Project Standard 2021
- Microsoft Visual Studio Professional 2022
- Microsoft Visual Studio Enterprise 2022

The following table shows the list of supported and unsupported application and operating system combinations:

	Microsoft Office Professional Plus 2016 (32-bit)	**Microsoft Office Professional Plus 2019 (64-bit)**	**Microsoft LTSC Office Professional Plus / Standard 2021 (64-bit)**	**Microsoft Project Professional / Standard 2021 (64-bit)**	**Microsoft LTSC Visio Professional / Standard 2021 (64-bit)**	**Microsoft Visual Studio Professional / Enterprise 2022**
Windows Server 2016	Uninstall	Not supported	Not supported	Not supported	Not supported	Not supported
Windows Server 2019	Not supported	Uninstall	Install/uninstall	Install/uninstall	Install/uninstall	Not supported
Windows Server 2022	Not supported	Uninstall	Install/uninstall	Install/uninstall	Install/uninstall	Install/uninstall

	Microsoft Office Professional Plus 2016 (32-bit)	Microsoft Office Professional Plus 2019 (64-bit)	Microsoft LTSC Office Professional Plus / Standard 2021 (64-bit)	Microsoft Project Professional / Standard 2021 (64-bit)	Microsoft LTSC Visio Professional / Standard 2021 (64-bit)	Microsoft Visual Studio Professional / Enterprise 2022
Windows 10	Uninstall	Uninstall	Install/uninstall	Install/uninstall	Install/uninstall	Install/uninstall
Windows 11	Uninstall	Uninstall	Install/uninstall	Install/uninstall	Install/uninstall	Install/uninstall

Important

- Microsoft Office/Visio/Project must follow the same editions. For example, you cannot mix Standard applications with Professional applications.
- Microsoft Office/Visio/Project must follow the same versions. For example, you cannot mix 2019 applications with 2021 applications.
- Microsoft Office/Visio/Project 2021 Standard/Professional are not supported for Value, Graphics, and GraphicsPro WorkSpaces bundles.
- Value, Standard, Graphics, and GraphicsPro WorkSpaces bundles are not supported for Microsoft Visual Studio 2022 Enterprise/Professional. Performance bundles can be used for Visual Studio workloads that are less resource intensive. However, for best results, we recommended using Visual Studio with quad-core or higher bundle types. The bundle types Power, PowerPro, Graphics.g4dn, and GraphicsPro.g4dn meet this requirement. For more information, see Visual Studio 2022 Product Family System Requirements.
- When you uninstall **Plus applications bundle for Microsoft Office 2016** from your WorkSpaces, you will lose access to any Trend Micro solutions that were included as part of that Amazon WorkSpaces bundle. If you want to continue using Trend Micro solutions with your Amazon WorkSpaces, you can purchase them separately on the AWS marketplace.

- In order to install/uninstall Microsoft 365 apps, you need to bring in your own tools and installers, Manage application workflow cannot install/uninstall Microsoft 365 apps.
- You can create a custom image of WorkSpaces with applications installed/uninstalled through Manage applications.
- For opt-in Regions, such as Africa (Cape Town), WorkSpaces internet connection must be enabled at the directory level.

Update application bundles on a WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpace and choose **Actions**, **Manage applications**.
4. Under **Current applications** you will see a list of application bundles that are already installed on this WorkSpace and under **Choose applications** you have a list of application bundles that are available to install on this WorkSpace.
5. To install application bundles on this WorkSpace:
   a. Select an application bundle that you want to install on this WorkSpace, and choose **Associate**.
   b. Repeat the previous step to install other application bundles.
   c. While the application bundles are installing, you will see them under **Current applications** with the `Pending install deployment` status.
6. To uninstall application bundles from this WorkSpace:
   a. Under **Choose applications**, select an application bundle that you want to uninstall and choose **Disassociate**.
   b. Repeat the previous step to uninstall other application bundles.
   c. While the application bundles are uninstalling, you will see them under **Current applications** with the `Pending uninstall deployment` status.
7. To revert the bundles installation or installation state, do one of the following.
   - If you want to revert the bundles from the `Pending uninstall deployment` state, select the application you want to revert, then choose **Associate**.

- If you want to revert the bundles from the `Pending install deployment` state, select the application you want to revert, then choose **Disassociate**.

8. After the application bundles you chose to install or uninstall are in pending states, choose **Deploy applications**.

> **Important**
>
> After you select **Deploy applications**, the end user session will terminate and WorkSpaces will not be accessible while the applications are being installed or uninstalled.

9. To confirm your actions, type **confirm**. Choose **force** to install or uninstall applications bundles that are in an **Error** state.
10. To monitor the progress of your application bundles:

    a. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.

    b. In the navigation pane, choose **WorkSpaces**. You can see the status under **Status** including the following.

    - **UPDATING** - The application bundle update is still ongoing.
    - **AVAILABLE / STOPPED** - The application bundle update is complete and the WorkSpace is back to its original state.

    c. To monitor the installation or uninstallation status of your application bundles, select the WorkSpace and choose **View Details**. Under **Applications**, you can see the status under **Status**, including `Pending install`, `Pending uninstall`, and `Installed`.

> **Note**
>
> If your users observe that their newly installed application bundles through Managed Applications are not license activated, you can perform a manual WorkSpace reboot. Your users can begin using those applications following a reboot. For additional support, contact AWS Support.

Update Microsoft Visual Studio 2022 workloads on a WorkSpace

By default Microsoft Visual Studio 2022 is installed with the following workloads and requires 18 GB of hard disk space:

- Visual Studio core editor
- Azure development
- Data storage and processing
- .NET desktop development
- NET Multi-platform App UI development
- ASP.NET and web development
- Node.js development

Users have the flexibility to add or remove workloads and individual components, allowing them to tailor the application to their specific requirements. It's important to note that installing additional workloads requires more disk space. To learn more about workload configurations, see Modify Visual Studio workloads, components, and language packs.

Managing WorkSpaces modified using Manage applications

After installing or uninstalling application bundles on your WorkSpaces, the following actions can impact existing configurations.

- **Restore a WorkSpace** - Restoring a WorkSpace recreates both the root volume and user volume, based on the most recent snapshots of these volumes that were created when the WorkSpace was healthy. Full WorkSpace snapshots are taken every 12 hours. For more information, see Restore a WorkSpace. Ensure you wait for at least 12 hours before restoring your WorkSpaces that were modified using Manage applications. Restoring your WorkSpaces before the next full snapshot, which were modified using Manage applications, will result in the following:
  - The application bundles that were installed on your WorkSpaces using the Manage applications workflow will be removed from your WorkSpaces but the license will still be activated and your WorkSpaces will be billed for those applications. To get those application bundles back on your WorkSpaces you need to run the Manage application workflow again, uninstall the application to start fresh, and then install again.
  - The application bundles that were removed from your WorkSpaces using the Manage applications workflow will be back on your WorkSpaces. However, those application bundles

won't work properly because the license activation will be missing. In order to get rid of those application bundles, run a manual uninstall of those application bundles from your WorkSpaces.

- **Rebuild a WorkSpace** - Rebuilding a WorkSpace recreates the root volume. For more information, see Rebuild a WorkSpace. Rebuilding your WorkSpaces that were modified using Manage applications will result in the following:
  - The application bundles that were installed on your WorkSpaces using the Manage applications workflow will be removed and deactivated from your WorkSpaces. In order to get those applications back on your WorkSpaces you need to run the Manage applications workflow again.
  - The application bundles that were removed from your WorkSpaces via Manage applications workflow will be installed and activated on your WorkSpaces. In order to remove those application bundles from your WorkSpaces, you need to run the Manage applications workflow again.
- **Migrate a WorkSpace** - The migration process recreates the WorkSpace by using a new root volume from the target bundle image and the user volume from the last available snapshot of the original WorkSpace. A new WorkSpace with a new WorkSpace ID is created. For more information, see Migrate a WorkSpace Migrating your WorkSpaces that were modified using Manage applications will result in the following:
  - All the application bundle from the source WorkSpaces will be removed and deactivated. The new destination WorkSpaces will inherit applications from the destination WorkSpaces bundle. Source WorkSpaces application bundles will be billed for the full month but application bundles on destination bundle will have a pro-rated bill.

Modify a WorkSpace in WorkSpaces Personal

After you launch a WorkSpace, you can modify its configuration in three ways:

- You can change the size of its root volume (for Windows, drive C; for Linux, /) and its user volume (for Windows, drive D; for Linux /home).
- You can change its compute type to select a new bundle.
- You can modify the streaming protocol using the AWS CLI or Amazon WorkSpaces API if your WorkSpace was created with PCoIP bundles.

To see the current modification state of a WorkSpace, select the arrow to show more details about that WorkSpace. The possible values for **State** are **Modifying Compute**, **Modifying Storage,** and **None**.

If you want to modify a WorkSpace, it must have a status of `AVAILABLE` or `STOPPED`. You can't change the volume size and the compute type at the same time.

Changing the volume size or compute type of a WorkSpace will change the billing rate for the WorkSpace.

To allow your users to modify their volumes and compute types themselves, see Enable self-service WorkSpaces management capabilities for your users in WorkSpaces Personal.

Modify volume sizes

You can increase the size of the root and user volumes for a WorkSpace, up to 2000 GB each. WorkSpace root and user volumes come in set groups that can't be changed. The available groups are:

[Root (GB), User (GB)]
[80, 10]
[80, 50]
[80, 100]
[175 to 2000, 100 to 2000]

You can expand the root and user volumes whether they are encrypted or unencrypted, and you can expand both volumes once in a 6-hour period. However, you can't increase the size of the root and user volumes at the same time. For more information, see Limitations for Increasing Volumes.

> **Note**
>
> When you expand a volume for a WorkSpace, WorkSpaces automatically extends the volume's partition within Windows or Linux. When the process is finished, you must reboot the WorkSpace for the changes to take effect.

To ensure that your data is preserved, you cannot decrease the size of the root or user volumes after you launch a WorkSpace. Instead, make sure that you specify the minimum sizes for these volumes when launching a WorkSpace. You can launch a Value, Standard, Performance, Power, or PowerPro WorkSpace with a minimum of 80 GB for the root volume and 10 GB for the user volume. You can launch a Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro WorkSpace with a minimum of 100 GB for the root volume and 100 GB for the user volume.

While a WorkSpace disk size increase is in progress, users can perform most tasks on their WorkSpace. However, they can't change their WorkSpace compute type, switch the WorkSpace running mode, rebuild their WorkSpace, or reboot (restart) their WorkSpace.

> **Note**
>
> If you want your users to be able to use their WorkSpaces while the disk size increase is in progress, make sure the WorkSpaces have a status of `AVAILABLE` instead of `STOPPED` before you resize the volumes of the WorkSpaces. If the WorkSpaces are `STOPPED`, they can't be started while the disk size increase is in progress.

In most cases, the disk size increase process might take up to two hours. However, if you're modifying the volume sizes for a large number of WorkSpaces, the process can take significantly longer. If you have a large number of WorkSpaces to modify, we recommend contacting AWS Support for assistance.

Limitations for increasing volumes

- You can resize only SSD volumes.
- When you launch a WorkSpace, you must wait 6 hours before you can modify the sizes of its volumes.
- You cannot increase the size of the root and user volumes at the same time. To increase the root volume, you must first change the user volume to 100 GB. After that change is made, you can then update the root volume to any value between 175 and 2000 GB. After the root volume has been changed to any value between 175 and 2000 GB, you can then update the user volume further, to any value between 100 and 2000 GB.

> **Note**
>
> If you want to increase both volumes, you must wait 20-30 minutes for the first operation to finish before you can start the second operation.

- Unless the WorkSpace is a Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro WorkSpace, the root volume cannot be less than 175 GB when the user volume is 100 GB. Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro WorkSpaces can have the root and user volumes both set to 100 GB minimum.
- If the user volume is 50 GB, you cannot update the root volume to anything other than 80 GB. If the root volume is 80 GB, the user volume can only be 10, 50, or 100 GB.

To modify the root volume of a WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpace and choose **Actions**, **Modify root volume.**.
4. Under **Root volume sizes**, choose a volume size or choose **Custom** to enter a custom volume size.
5. Choose **Save changes**.
6. When the disk size increase is finished, you must reboot the WorkSpace for the changes to take effect. To avoid data loss, make sure the user saves any open files before you reboot the WorkSpace.

To modify the user volume of a WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpace and choose **Actions**, **Modify user volume.**.
4. Under **User volume sizes**, choose a volume size or choose **Custom** to enter a custom volume size.
5. Choose **Save changes**.

6. When the disk size increase is finished, you must reboot the WorkSpace for the changes to take effect. To avoid data loss, make sure the user saves any open files before you reboot the WorkSpace.

To change the volume sizes of a WorkSpace

Use the modify-workspace-properties command with the `RootVolumeSizeGib` or `UserVolumeSizeGib` property.

Modify compute type

You can switch a WorkSpace between the Standard, Power, Performance, and PowerPro compute types. For more information about these compute types, see Amazon WorkSpaces Bundles.

Note

- You can change the compute type from Graphics.g4dn to GraphicsPro.g4dn, or from GraphicsPro.g4dn to Graphics.g4dn. You cannot change the compute type of Graphics.g4dn and GraphicsPro.g4dn to any other value.
- Graphics bundle is no longer supported after November 30, 2023. We recommend migrating your WorkSpaces to Graphics.g4dn bundle. For more information, see Migrate a WorkSpace in WorkSpaces Personal.
- You cannot change the compute type of Graphics and GraphicsPro to any other value.

When you request a compute change, WorkSpaces reboots the WorkSpace using the new compute type. WorkSpaces preserves the operating system, applications, data, and storage settings for the WorkSpace.

You can request a larger compute type once in a 6-hour period or a smaller compute type once every 30 days. For a newly launched WorkSpace, you must wait 6 hours before requesting a larger compute type.

When a WorkSpace compute type change is in progress, users are disconnected from their WorkSpace, and they can't use or change the WorkSpace. The WorkSpace is automatically rebooted during the compute type change process.

> **Important**
>
> To avoid data loss, make sure users save any open documents and other application files before you change the WorkSpace compute type.

The compute type change process might take up to an hour.

To change the compute type of a WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpace and choose **Actions**, **Modify compute type**.
4. Under **Compute type**, choose a compute type.
5. Choose **Save changes**.

To change the compute type of a WorkSpace

Use the modify-workspace-properties command with the `ComputeTypeName` property.

Modify protocols

If your WorkSpace is created with PCoIP bundles, you can modify their streaming protocol using the AWS CLI or the Amazon WorkSpaces API. This allows you to migrate the protocol using your existing WorkSpace without using the WorkSpace migration feature. This also allows you to use the WorkSpaces Streaming Protocol (WSP) and maintain your root volume without re-creating existing PCoIP WorkSpaces during the migration process.

- You can only modify your protocol if your WorkSpace was created with PCoIP bundles and is not a GPU-enabled WorkSpace.
- Before you modify the protocol to WSP, ensure that your WorkSpace meets the following requirements for a WSP WorkSpace.
  - Your WorkSpaces client supports WSP
  - The region where your WorkSpace is deployed supports WSP
  - The IP address and port requirements for WSP are open. For more information, see IP address and port requirements for WorkSpaces.

- Ensure your current bundle is available with WSP.
- For the best experience with video conferencing we recommend using Power or PowerPro bundles only.

Note

- We highly recommend testing with your non-production WorkSpaces before you start changing the protocol.
- If you modify the protocol from PCoIP to WSP, and then modify the protocol back to PCoIP, you won't be able to connect to WorkSpaces through Web Access.

To change the protocol of a WorkSpace

1. [Optional] Reboot your WorkSpace and wait until it's in the `AVAILABLE` state before modifying the protocol.
2. [Optional] Use the `describe-workspaces` command to list the WorkSpace properties. Ensure that it's in the `AVAILABLE` state and its current `Protocol` is accurate.
3. Use the `modify-workspace-properties` command and modify the `Protocols` property from `PCOIP` to `WSP`, or the other way around.

```
aws workspaces modify-workspace-properties
--workspace-id <value>
--workspace-properties "Protocols=[WSP]"
```

Important

The `Protocols` property is case-sensitive. Ensure that you use `PCOIP` or `WSP`.

4. After you run the command, it can take up to 20 minutes for the WorkSpace to reboot and complete the necessary configurations.
5. Use the `describe-workspaces` command again to list the WorkSpace properties and verify that it's in an `AVAILABLE` state and the current `Protocols` property has been changed to the correct protocol.

> **Note**
>
> - Modifying the WorkSpace's protocol will not update the bundle description in the console. The **Launch Bundle** description will not change.
> - If the WorkSpace remains in an UNHEALTHY state after 20 min, reboot the WorkSpace in the console.

6. You can now connect to your WorkSpace.

Customize branding in WorkSpaces Personal

Amazon WorkSpaces allows you to create a familiar WorkSpaces experience for your users by using APIs to customize the appearance of your WorkSpace's login page with your own branding logo, IT support information, forgot password link, and login message. Your branding will be displayed to your users in their WorkSpace login page rather than the default WorkSpaces branding.

The following clients are supported:

- Windows
- Linux
- Android
- MacOS
- iOS
- Web Access

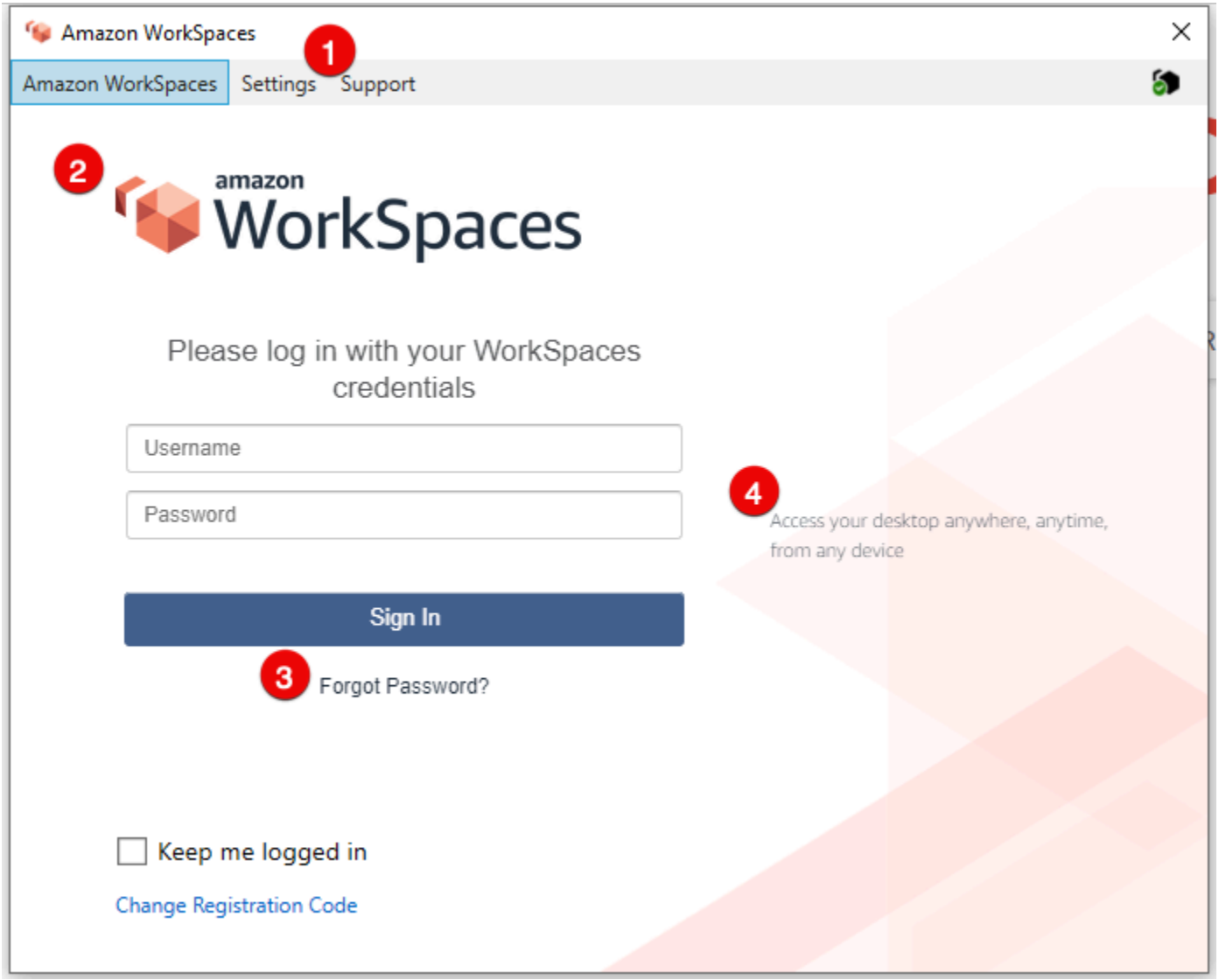
> **Note**
>
> To modify branding elements using the ClientBranding APIs in the AWS GovCloud (US) Region, use a WorkSpaces client version that is 5.10.0.

Import custom branding

To import your client branding customization, use the action `ImportClientBranding`, which includes the following elements. See ImportClientBranding API reference for more information.

Important

Client branding attributes are public facing. Ensure that you don't include sensitive information.



1. Support link
2. Logo
3. Forgot password link
4. Login message

Custom branding elements

Branding element	Description	Requirements and recommendations
Support link	Allows you to specify a support email link for users to contact for help with their WorkSpaces. You can use the `SupportEmail` attribute or provide a link to your support page using the `SupportLink` attribute.	• For each platform type, the `SupportEmail` and `SupportLink` parameters are mutually exclusive. You can specify a single parameter for each platform type, but not both. • The default email is `workspaces-feedback@amazon.com` . • Length constraints: Minimum length of 1. Maximum length of 200.

Logo	Allows you to customize your organization's logo using the Logo attribute.	• The only image format accepted is a binary data object that is converted from a `.png` file.
		• Recommended resolutions:
		  • Android: 978 x 190
		  • Desktop: 319 x 55
		  • iOS@2x: 110 x 200
		  • iOS@3x: 1650 x 300

Forgot password link	Allows you to add a web address using the ForgotPasswordLink attribute that users can go to if they forget their password to their WorkSpace.	Length Constraints: Minimum length of 1. Maximum length of 200.

Branding element	Description	Requirements and recommendations
Login message	Allows you to customize a message using the `LoginMessage` attribute on the sign in screen.	• Length Constraints: Minimum length of 0. Maximum length of 2000 characters for integrati on with HTML tags and different font size. For default cases without HTML tags, it is recommended to keep the login message under 600 characters. • HTML tags supported: `a, b, blockquote, br, cite, code, dd, dl, dt, div, em, i, li, ol, p, pre, q, small, span, strike, strong, sub, sup, u, ul`

The following are sample code snippets for using ImportClientBranding.

AWS CLI Version 2

> **Warning**
>
> Importing custom branding overwrites the attributes, within that platform, that you specify with your custom data. It also overwrites the attributes that you don't specify with default custom branding attribute values. You must include the data for any attribute that you don't want to overwrite.

```
aws workspaces import-client-branding \
--cli-input-json file://~/Downloads/import-input.json \
```

```
--region us-west-2
```

The import JSON file should look like the following sample code:

```
{
    "ResourceId": "<directory-id>",
    "DeviceTypeOsx": {
        "Logo":
 "iVBORw0KGgoAAAANSUhEUgAAAAIAAAACCAYAAABytg0kAAAAC0lEQVR42mNgQAcAABIAAeRVjecAAAAASUVORK5CYII="
        "ForgotPasswordLink": "https://amazon.com/",
        "SupportLink": "https://amazon.com/",
        "LoginMessage": {
            "en_US": "Hello!!"
        }
    }
}
```

The following sample Java code snippet converts the logo image into a base64-encoded string:

```
// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

//convert byte[] to base64 format and print it
String bytesBase64 = Base64.encodeBase64String(bytes);
System.out.println(bytesBase64);
```

The following sample Python code snippet converts the logo image into a base64-encoded string:

```
# Read logo into base64-encoded string
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    base64_string = base64.b64encode(f)
    print(base64_string)
```

Java

> **Warning**
>
> Importing custom branding overwrites the attributes, within that platform, that you specify with your custom data. It also overwrites the attributes that you don't specify with default custom branding attribute values. You must include the data for any attribute that you don't want to overwrite.

```
// Create WS Client
WorkSpacesClient client = WorkSpacesClient.builder().build();

// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

// Create import attributes for the plateform
DefaultImportClientBrandingAttributes attributes =
        DefaultImportClientBrandingAttributes.builder()
                .logo(SdkBytes.fromByteArray(bytes))
                .forgotPasswordLink("https://aws.amazon.com/")
                .supportLink("https://aws.amazon.com/")
                .build();

// Create import request
ImportClientBrandingRequest request =
        ImportClientBrandingRequest.builder()
                .resourceId("<directory-id>")
                .deviceTypeOsx(attributes)
                .build();

// Call ImportClientBranding API
ImportClientBrandingResponse response = client.importClientBranding(request);
```

Python

> **Warning**
>
> Importing custom branding overwrites the attributes, within that platform, that you specify with your custom data. It also overwrites the attributes that you don't specify with default custom branding attribute values. You must include the data for any attribute that you don't want to overwrite.

```
import boto3

# Read logo into bytearray
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    bytes = bytearray(f)

# Create WorkSpaces client
client = boto3.client('workspaces')

# Call import API
response = client.import_client_branding(
    ResourceId='<directory-id>',
    DeviceTypeOsx={
        'Logo': bytes,
        'SupportLink': 'https://aws.amazon.com/',
        'ForgotPasswordLink': 'https://aws.amazon.com/',
        'LoginMessage': {
            'en_US': 'Hello!!'
        }
    }
)
```

PowerShell

```
#Requires -Modules @{ ModuleName="AWS.Tools.WorkSpaces"; ModuleVersion="4.1.56"}

# Specify Image Path
$imagePath = "~/Downloads/logo.png"

# Create Byte Array from image file
```

```
$imageByte = ([System.IO.File]::ReadAllBytes($imagePath))

# Call import API
Import-WKSClientBranding -ResourceId <directory-id> `
    -DeviceTypeLinux_LoginMessage @{en_US="Hello!!"} `
    -DeviceTypeLinux_Logo $imageByte `
    -DeviceTypeLinux_ForgotPasswordLink "https://aws.amazon.com/" `
    -DeviceTypeLinux_SupportLink "https://aws.amazon.com/"
```

To preview the login page, launch the WorkSpaces application or web login page.

> **Note**
>
> Changes may take up to 1 minute to appear.

Describe custom branding

To see the details of the client branding customization you currently have, use the action `DescribeCustomBranding`. The following is the sample script for using DescribeClientBranding. See DescribeClientBranding API reference for more information.

```
aws workspaces describe-client-branding \
--resource-id <directory-id> \
--region us-west-2
```

Delete custom branding

To delete your client branding customization, use the action `DeleteCustomBranding`. The following is the sample script for using DeleteClientBranding. See DeleteClientBranding API reference for more information.

```
aws workspaces delete-client-branding \
--resource-id <directory-id> \
--platforms DeviceTypeAndroid DeviceTypeIos \
--region us-west-2
```

> **Note**
>
> Changes may take up to 1 minute to appear.

Tag resources in WorkSpaces Personal

You can organize and manage the resources for your WorkSpaces by assigning your own metadata to each resource in the form of *tags*. You specify a *key* and a *value* for each tag. A key can be a general category, such as "project," "owner," or "environment," with specific associated values. Using tags is a simple yet powerful way to manage AWS resources and to organize data, including billing data.

When you add tags to an existing resource, those tags don't appear in your cost allocation report until the first day of the following month. For example, if you add tags to an existing WorkSpace on July 15, the tags won't appear in your cost allocation report until August 1. For more information, see Using Cost Allocation Tags in the *AWS Billing User Guide*.

> **Note**
>
> To view your WorkSpaces resource tags in the Cost Explorer, you must activate the tags that you have applied to your WorkSpaces resources by following the instructions in Activating User-Defined Cost Allocation Tags in the *AWS Billing User Guide*.
> Although tags appear 24 hours after activation, it can take 4 to 5 days for values associated with those tags to appear in the Cost Explorer. Additionally, to appear and provide cost data in Cost Explorer, WorkSpaces resources that have been tagged must incur charges during that time. Cost Explorer only shows cost data from the time when the tags were activated and onward. No historical data is available at this time.

Resources that you can tag

- You can add tags to the following resources when you create them—WorkSpaces, imported images, and IP access control groups.
- You can add tags to existing resources of the following types—WorkSpaces, registered directories, custom bundles, images, and IP access control groups.

Tag restrictions

- Maximum number of tags per resource—50
- Maximum key length—127 Unicode characters
- Maximum value length—255 Unicode characters

- Tag keys and values are case-sensitive. Allowed characters are letters, spaces, and numbers representable in UTF-8, plus the following special characters: + - = . _ : / @. Do not use leading or trailing spaces.
- Do not use the `aws:` or `aws:workspaces:` prefixes in your tag names or values because they are reserved for AWS use. You can't edit or delete tag names or values with these prefixes.

To update the tags for an existing resource using the console (directories, WorkSpaces, or IP access control groups)

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose one of the following resource types: **Directories**, **WorkSpaces**, or **IP Access Controls**.
3. Select the resource to open its details page.
4. Do one or more of the following:
   - To update a tag, edit the values of **Key** and **Value**.
   - To add a tag, choose **Add Tag** and then edit the values of **Key** and **Value**.
   - To delete a tag, choose the delete icon (X) next to the tag.
5. When you are finished updating tags, choose **Save**.

To update the tags for an existing resource using the console (images or bundles)

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose one of the following resource types: **Bundles** or **Images**.
3. Choose the resource to open its details page.
4. Under **Tags**, choose **Manage tags**.
5. Do one or more of the following:
   - To update a tag, edit the values of **Key** and **Value**.
   - To add a tag, choose **Add new tag** and then edit the values of **Key** and **Value**.
   - To delete a tag, choose **Remove** next to the tag.
6. When you are finished updating tags, choose **Save changes**.

To update the tags for an existing resource using the AWS CLI

Use the create-tags and delete-tags commands.

Maintenance in WorkSpaces Personal

We recommend that you maintain your WorkSpaces on a regular basis. WorkSpaces schedules default maintenance windows for your WorkSpaces. During the maintenance window, the WorkSpace installs important updates from Amazon WorkSpaces and reboots as necessary. If available, operating system updates are also installed from the OS update server that the WorkSpace is configured to use. During maintenance, your WorkSpaces might be unavailable.

By default, your Windows WorkSpaces are configured to receive updates from Windows Update. To configure your own automatic update mechanisms for Windows, see the documentation for Windows Server Update Services (WSUS) and Configuration Manager.

Requirement

Your WorkSpaces must have access to the internet so that you can install updates to the operating system and deploy applications. For more information, see the section called “Internet access”.

Maintenance windows for AlwaysOn WorkSpaces

For AlwaysOn WorkSpaces, the maintenance window is determined by operating system settings. The default is a four-hour period from 00h00 to 04h00, in the time zone of the WorkSpace, each Sunday morning. By default, the time zone of an AlwaysOn WorkSpace is the time zone of the AWS Region for the WorkSpace. However, if you connect from another Region and time zone redirection is enabled, and then you disconnect, the time zone of the WorkSpace is updated to the time zone of the Region that you connected from.

You can disable time zone redirection for Windows WorkSpaces using Group Policy. You can disable time zone redirection for Linux WorkSpaces by using the PCoIP Agent conf.

For Windows WorkSpaces, you can configure the maintenance window using Group Policy; see Configure Group Policy Settings for Automatic Updates. You cannot configure the maintenance window for Linux WorkSpaces.

Maintenance windows for AutoStop WorkSpaces

AutoStop WorkSpaces are started automatically once a month in order to install important updates. Beginning on the third Monday of the month, and for up to two weeks, the maintenance

window is open each day from about 00h00 to 05h00, in the time zone of the AWS Region for the WorkSpace. The WorkSpace can be maintained on any one day in the maintenance window. During this window, only WorkSpaces older than 7 days are maintained.

During the time period when the WorkSpace is undergoing maintenance, the state of the WorkSpace is set to `MAINTENANCE`.

Although you cannot modify the time zone that is used for maintaining AutoStop WorkSpaces, you can disable the maintenance window for your AutoStop WorkSpaces as follows. If you disable maintenance mode, your WorkSpaces are not rebooted and do not enter the `MAINTENANCE` state.

To disable maintenance mode

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory, and choose **Actions**, **Update Details**.
4. Expand **Maintenance Mode**.
5. To enable automatic updates, choose **Enabled**. If you prefer to manage updates manually, choose **Disabled**.
6. Choose **Update and Exit**.

Manual maintenance

If you prefer, you can maintain your WorkSpaces on your own schedule. When you perform maintenance tasks, we recommend that you change the state of the WorkSpace to **Maintenance**. When you are finished, change the state of the WorkSpace to **Available**.

When a WorkSpace is in **Maintenance** state, the following behaviors occur:

- The WorkSpace does not respond to requests to reboot, stop, start, or rebuild.
- Users cannot log in to the WorkSpace.
- An AutoStop WorkSpace is not hibernated.

To change the state of the WorkSpace using the console

> **Note**
>
> To change the state of a WorkSpace, the WorkSpace must be in the **Available** state. The **Modify state** setting is not available when a WorkSpace is not in the **Available** state.

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select your WorkSpace, and choose **Actions**, **Modify state**.
4. Under **Modify state**, choose **Available** or **Maintenance**.
5. Choose **Save**.

To change the state of the WorkSpace using the AWS CLI

Use the modify-workspace-state command.

Encrypted WorkSpaces in WorkSpaces Personal

WorkSpaces is integrated with the AWS Key Management Service (AWS KMS). This enables you to encrypt storage volumes of WorkSpaces using AWS KMS Key. When you launch a WorkSpace, you can encrypt the root volume (for Microsoft Windows, the C drive; for Linux, /) and the user volume (for Windows, the D drive; for Linux, /home). Doing so ensures that the data stored at rest, disk I/O to the volume, and snapshots created from the volumes are all encrypted.

> **Note**
>
> - In addition to encrypting your WorkSpaces, you can also use FIPS endpoint encryption in certain AWS US Regions. For more information, see Configure FedRAMP authorization or DoD SRG compliance for WorkSpaces Personal.
> - BitLocker encryption is not supported for Amazon WorkSpaces.

Contents

- Limits
- Overview of WorkSpaces encryption using AWS KMS
- WorkSpaces encryption context
- Grant WorkSpaces permission to use a KMS Key on your behalf
- Encrypt a WorkSpace
- View encrypted WorkSpaces

Prerequisites

You need an AWS KMS Key before you can begin the encryption process. This KMS Key can be either the AWS managed KMS Key for Amazon WorkSpaces (**aws/workspaces**) or a symmetric customer managed KMS Key.

- **AWS managed KMS Keys** – The first time that you launch an unencrypted WorkSpace from the WorkSpaces console in a Region, Amazon WorkSpaces automatically creates an AWS managed KMS Key (**aws/workspaces**) in your account. You can select this AWS managed KMS Key to encrypt the user and root volumes of your WorkSpace. For details, see Overview of WorkSpaces encryption using AWS KMS.

  You can view this AWS managed KMS Key, including its policies and grants, and can track its use in AWS CloudTrail logs, but you cannot use or manage this KMS Key. Amazon WorkSpaces creates and manages this KMS Key. Only Amazon WorkSpaces can use this KMS Key, and WorkSpaces can use it only to encrypt WorkSpaces resources in your account.

  AWS managed KMS Key, including the one that Amazon WorkSpaces supports, are rotated every three years. For details, see Rotating AWS KMS Key in the *AWS Key Management Service Developer Guide*.
- **Customer managed KMS Key** – Alternatively, you can select a symmetric customer managed KMS Key that you created using AWS KMS. You can view, use, and manage this KMS Key, including setting its policies. For more information about creating KMS Keys, see Creating Keys in the *AWS Key Management Service Developer Guide*. For more information about creating KMS Keys using the AWS KMS API, see Working with Keys in the *AWS Key Management Service Developer Guide*.

  Customer managed KMS Keys are not automatically rotated unless you decide to enable automatic key rotation. For details, see Rotating AWS KMS Keys in the *AWS Key Management Service Developer Guide*.

> **Important**
>
> When you manually rotate KMS Keys, you must keep both the original KMS Key and the new KMS Key enabled so that AWS KMS can decrypt the WorkSpaces that the original KMS Key encrypted. If you don't want to keep the original KMS Key enabled, you must recreate your WorkSpaces and encrypt them using the new KMS Key.

You must meet the following requirements to use an AWS KMS Key to encrypt your WorkSpaces:

- **The KMS Key must be symmetric.** Amazon WorkSpaces does not support asymmetric KMS Keys. For information about distinguishing between symmetric and asymmetric KMS Keys, see Identifying Symmetric and Asymmetric KMS Keys in the *AWS Key Management Service Developer Guide*.
- **The KMS Key must be enabled.** To determine whether a KMS Key is enabled, see Displaying KMS Key Details in the *AWS Key Management Service Developer Guide*.
- **You must have the correct permissions and policies associated with the KMS Key.** For more information, see Part 2: Grant WorkSpaces administrators additional permissions using an IAM policy.

Limits

- You can't encrypt an existing WorkSpace. You must encrypt a WorkSpace when you launch it.
- Creating a custom image from an encrypted WorkSpace is not supported.
- Disabling encryption for an encrypted WorkSpace is not currently supported.
- WorkSpaces launched with root volume encryption enabled might take up to an hour to provision.
- To reboot or rebuild an encrypted WorkSpace, first make sure that the AWS KMS Key is enabled; otherwise, the WorkSpace becomes unusable. To determine whether a KMS Key is enabled, see Displaying KMS Key Details in the *AWS Key Management Service Developer Guide*.

Overview of WorkSpaces encryption using AWS KMS

When you create WorkSpaces with encrypted volumes, WorkSpaces uses Amazon Elastic Block Store (Amazon EBS) to create and manage those volumes. Amazon EBS encrypts your volumes

with a data key using the industry-standard AES-256 algorithm. Both Amazon EBS and Amazon WorkSpaces use your KMS Key to work with the encrypted volumes. For more information about EBS volume encryption, see Amazon EBS Encryption in the *Amazon EC2 User Guide*.

When you launch WorkSpaces with encrypted volumes, the end-to-end process works like this:

1. You specify the KMS Key to use for encryption as well as the user and directory for the WorkSpace. This action creates a grant that allows WorkSpaces to use your KMS Key only for this WorkSpace—that is, only for the WorkSpace associated with the specified user and directory.
2. WorkSpaces creates an encrypted EBS volume for the WorkSpace and specifies the KMS Key to use as well as the volume's user and directory. This action creates a grant that allows Amazon EBS to use your KMS Key only for this WorkSpace and volume—that is, only for the WorkSpace associated with the specified user and directory, and only for the specified volume.
3. Amazon EBS requests a volume data key that is encrypted under your KMS Key and specifies the WorkSpace user's Active Directory security identifier (SID) and AWS Directory Service directory ID as well as the Amazon EBS volume ID as the encryption context.
4. AWS KMS creates a new data key, encrypts it under your KMS Key, and then sends the encrypted data key to Amazon EBS.
5. WorkSpaces uses Amazon EBS to attach the encrypted volume to your WorkSpace. Amazon EBS sends the encrypted data key to AWS KMS with a `Decrypt` request and specifies the WorkSpace user's SID, the directory ID, and the volume ID, which is used as the encryption context.
6. AWS KMS uses your KMS Key to decrypt the data key, and then sends the plain text data key to Amazon EBS.
7. Amazon EBS uses the plain text data key to encrypt all data going to and from the encrypted volume. Amazon EBS keeps the plain text data key in memory for as long as the volume is attached to the WorkSpace.
8. Amazon EBS stores the encrypted data key (received at Step 4) with the volume metadata for future use in case you reboot or rebuild the WorkSpace.
9. When you use the AWS Management Console to remove a WorkSpace (or use the `TerminateWorkspaces` action in the WorkSpaces API), WorkSpaces and Amazon EBS retire the grants that allowed them to use your KMS Key for that WorkSpace.

WorkSpaces encryption context

WorkSpaces doesn't use your KMS Key directly for cryptographic operations (such as `Encrypt`, `Decrypt`, `GenerateDataKey`, etc.), which means WorkSpaces doesn't send requests to AWS KMS that include an encryption context. However, when Amazon EBS requests an encrypted data key for the encrypted volumes of your WorkSpaces (Step 3 in the Overview of WorkSpaces encryption using AWS KMS) and when it requests a plain text copy of that data key (Step 5), it includes encryption context in the request.

The encryption context provides additional authenticated data (AAD) that AWS KMS uses to ensure data integrity. The encryption context is also written to your AWS CloudTrail log files, which can help you understand why a given KMS Key was used. Amazon EBS uses the following for the encryption context:

- The security identifier (SID) of the Active Directory user that is associated with the WorkSpace
- The directory ID of the AWS Directory Service directory that is associated with the WorkSpace
- The Amazon EBS volume ID of the encrypted volume

The following example shows a JSON representation of the encryption context that Amazon EBS uses:

```
{
  "aws:workspaces:sid-directoryid":
 "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

Grant WorkSpaces permission to use a KMS Key on your behalf

You can protect your WorkSpace data under the AWS managed KMS Key for WorkSpaces (**aws/workspaces**) or a customer managed KMS Key. If you use a customer managed KMS Key, you need to grant WorkSpaces permission to use the KMS Key on behalf of the WorkSpaces administrators in your account. The AWS managed KMS Key for WorkSpaces has the required permissions by default.

To prepare your customer managed KMS Key for use with WorkSpaces, use the following procedure.

1. Add your WorkSpaces administrators to the list of key users in the KMS Key's key policy

2. Give your WorkSpaces administrators additional permissions with an IAM policy

Your WorkSpaces administrators also need permission to use WorkSpaces. For more information about these permissions, go to Identity and access management for WorkSpaces.

Part 1: Add WorkSpaces administrators to as key users

To give WorkSpaces administrators the permissions that they require, you can use the AWS Management Console or the AWS KMS API.

To add WorkSpaces administrators as key users for a KMS Key (console)

1. Sign in to the AWS Management Console and open the AWS Key Management Service (AWS KMS) console at https://console.aws.amazon.com/kms.
2. To change the AWS Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.
4. Choose the key ID or alias of your preferred customer managed KMS Key.
5. Choose the **Key policy** tab. Under **Key users**, choose **Add**.
6. In the list of IAM users and roles, select the users and roles that correspond to your WorkSpaces administrators, and then choose **Add**.

To add WorkSpaces administrators as key users for a KMS Key (API)

1. Use the GetKeyPolicy operation to get the existing key policy, and then save the policy document to a file.
2. Open the policy document in your preferred text editor. Add the IAM users and roles that correspond to your WorkSpaces administrators to the policy statements that give permission to key users. Then save the file.
3. Use the PutKeyPolicy operation to apply the key policy to the KMS Key.

Part 2: Grant WorkSpaces administrators additional permissions using an IAM policy

If you select a customer managed KMS Key to use for encryption, you must establish IAM policies that allow Amazon WorkSpaces to use the KMS Key on behalf of an IAM user in your account who launches encrypted WorkSpaces. That user also needs permission to use Amazon WorkSpaces. For more information about creating and editing IAM user policies, see Managing IAM Policies in the *IAM User Guide* and Identity and access management for WorkSpaces.

WorkSpaces encryption requires limited access to the KMS Key. The following is a sample key policy that you can use. This policy separates the principals who can manage the AWS KMS Key from those who can use it. Before you use this sample key policy, replace the example account ID and IAM user name with actual values from your account.

The first statement matches the default AWS KMS key policy. It gives your account permission to use IAM policies to control access to the KMS Key. The second and third statements define which AWS principals can manage and use the key, respectively. The fourth statement enables AWS services that are integrated with AWS KMS to use the key on behalf of the specified principal. This statement enables AWS services to create and manage grants. The statement uses a condition element that limits grants on the KMS Key to those made by AWS services on behalf of users in your account.

Note

If your WorkSpaces administrators use the AWS Management Console to create WorkSpaces with encrypted volumes, the administrators need permission to list aliases and list keys (the `"kms:ListAliases"` and `"kms:ListKeys"` permissions). If your WorkSpaces administrators use only the Amazon WorkSpaces API (not the console), you can omit the `"kms:ListAliases"` and `"kms:ListKeys"` permissions.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms:List*",
        "kms:Put*",
```

```
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms:Delete*"
       ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
    }
  ]
}
```

The IAM policy for a user or role that is encrypting a WorkSpace must include usage permissions on the customer managed KMS Key, as well as access to WorkSpaces. To give an IAM user or role WorkSpaces permissions, you can attach the following sample policy to the IAM user or role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "ds:*",
                "ds:DescribeDirectories",
                "workspaces:*",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:CreateWorkspaces",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

The following IAM policy is required by the user for using AWS KMS. It gives the user read-only access to the KMS Key along with the ability to create grants.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Describe*",
                "kms:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

If you want to specify the KMS Key in your policy, use an IAM policy similar to the following. Replace the example KMS Key ARN with a valid one.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Encrypt a WorkSpace

To encrypt a WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose **Launch WorkSpaces** and complete the first three steps.
3. For the **WorkSpaces Configuration** step, do the following:
   a. Select the volumes to encrypt: **Root Volume**, **User Volume**, or both volumes.
   b. For **Encryption Key**, select an AWS KMS Key, either the AWS managed KMS Key created by Amazon WorkSpaces or a KMS Key that you created. The KMS Key that you select must be symmetric. Amazon WorkSpaces does not support asymmetric KMS Keys.
   c. Choose **Next Step**.
4. Choose **Launch WorkSpaces**.

View encrypted WorkSpaces

To see which WorkSpaces and volumes have been encrypted from the WorkSpaces console, choose **WorkSpaces** from the navigation bar on the left. The **Volume Encryption** column shows whether each WorkSpace has encryption enabled or disabled. To see which specific volumes have been encrypted, expand the WorkSpace entry to see the **Encrypted Volumes** field.

Reboot a WorkSpace in WorkSpaces Personal

Occasionally, you might need to reboot (restart) a WorkSpace manually. Rebooting a WorkSpace disconnects the user and then performs a shutdown and reboot of the WorkSpace. To avoid data loss, make sure the user saves any open documents and other application files before you reboot the WorkSpace. The user data, operating system, and system settings are not affected.

> **Warning**
>
> To reboot an encrypted WorkSpace, first make sure that the AWS KMS Key is enabled; otherwise, the WorkSpace becomes unusable. To determine whether a KMS Key is enabled, see Displaying KMS Key Details in the *AWS Key Management Service Developer Guide*.

To reboot a WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpaces to reboot and choose **Actions**, **Reboot WorkSpaces**.
4. When prompted for confirmation, choose **Reboot WorkSpaces**.

To reboot a WorkSpace using the AWS CLI

Use the reboot-workspaces command.

To bulk reboot WorkSpaces

Use the amazon-workspaces-admin-module.

Rebuild a WorkSpace in WorkSpaces Personal

Rebuilding a WorkSpace recreates the root volume of the most recent image of the bundle that the WorkSpace was launched from, its user volume, and its primary elastic network interface. Rebuilding a WorkSpace deletes more data than restoring a WorkSpace, but it only requires you to have a snapshot of the user volume. To restore a WorkSpace, see Restore a WorkSpace in WorkSpaces Personal.

Rebuilding a WorkSpace causes the following to occur:

- The root volume (for Microsoft Windows, drive C; for Linux, /) is refreshed with the most recent image of the bundle that the WorkSpace was created from. Any applications that were installed, or system settings that were changed after the WorkSpace was created, are lost.
- The user volume (for Microsoft Windows, the D drive; for Linux, /home) is recreated from the most recent snapshot. The current contents of the user volume are overwritten.

  Automatic snapshots for use when rebuilding a WorkSpace are scheduled every 12 hours. These snapshots of the user volume are taken regardless of the health of the WorkSpace. When you choose **Actions**, **Rebuild / Restore WorkSpace**, the date and time of the most recent snapshot is shown.

  When you rebuild a WorkSpace, new snapshots are also taken soon after the rebuild is finished (often within 30 minutes).
- The primary elastic network interface is recreated. The WorkSpace receives a new private IP address.

> **Important**
>
> After January 14, 2020, WorkSpaces created from a public Windows 7 bundle can no longer be rebuilt. You might want to consider migrating your Windows 7 WorkSpaces to Windows 10. For more information, see Migrate a WorkSpace in WorkSpaces Personal.

You can rebuild a WorkSpace only if the following conditions are met:

- The WorkSpace must have a state of `AVAILABLE`, `ERROR`, `UNHEALTHY`, `STOPPED`, or `REBOOTING`. To rebuild a WorkSpace in the `REBOOTING` state, you must use the RebuildWorkspaces API operation or the rebuild-workspaces AWS CLI command.
- A snapshot of the user volume must exist.

To rebuild a WorkSpace

> **Warning**
>
> To rebuild an encrypted WorkSpace, first make sure that the AWS KMS Key is enabled; otherwise, the WorkSpace becomes unusable. To determine whether a KMS Key is enabled, see Displaying KMS Key Details in the *AWS Key Management Service Developer Guide*.

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpace to rebuild and choose **Actions**, **Rebuild / Restore WorkSpace**.
4. Under **Snapshot**, select the snapshot's time stamp.
5. Choose **Rebuild**.

To rebuild a WorkSpace using the AWS CLI

Use the rebuild-workspaces command.

Troubleshooting

If you rebuild a WorkSpace after changing the user's **sAMAccountName** user naming attribute in Active Directory, you might receive the following error message:

```
"ErrorCode": "InvalidUserConfiguration.Workspace"
"ErrorMessage": "The user was either not found or is misconfigured."
```

To work around this issue, either revert to the original user naming attribute and then re-initiate the rebuild, or create a new WorkSpace for that user.

Rebuild Microsoft Entra ID-joined WorkSpaces

When a user logs in to their WorkSpace for the first time after rebuilding, they need to go through the out-of-box experience (OOBE) again, similar to when they were assigned a new WorkSpace. As a result, a new user profile folder is created on the WorkSpace, overriding the original user profile folder. Hence, during the rebuild of an Entra joined WorkSpace, the content from the original user profile folder is saved under `D:\Users\<USERNAME%MMddyyTHHmmss`

%.NotMigrated> on the rebuilt WorkSpace. The user needs to copy the original profile content from D:\Users\<USERNAME%MMddyyTHHmmss%.NotMigrated> to the user's profile folder at D:\Users\<USERNAME> to restore all user profile data including desktop icons, shortcuts, and data files.

> **Note**
>
> For Microsoft Entra ID-joined WorkSpaces, we recommend to always use Restore WorkSpaces, when possible, instead of Rebuild WorkSpaces.

Restore a WorkSpace in WorkSpaces Personal

Restoring a WorkSpace recreates both the root volume and user volume using a snapshot of each volume that was taken when the WorkSpace was health. Restoring a WorkSpace rolls back the data on both the root and user volumes to the point in time when the snapshots were created. Rebuilding a WorkSpace only rolls back the data on the user volume. This means that restoring requires you to have snapshots of both the root volume and user volume, while rebuilding a WorkSpace only requires a snapshot of the user volume. To rebuild a WorkSpace, see Rebuild a WorkSpace in WorkSpaces Personal.

Restoring a WorkSpace causes the following to occur:

- The root volume (for Microsoft Windows, drive C; for Linux, /) is restored to the date and time specified using a snapshot. Any applications that were installed, or system settings that were changed after the snapshot was created, are lost.
- The user volume (for Microsoft Windows, the D drive; for Linux, /home) is recreated to the date and time specified using a snapshot. The current contents of the user volume are overwritten.

The restore point

When you choose **Actions** and **Rebuild / Restore WorkSpace**, the date and time of the snapshots used for the operation are shown. To verify the date and time of the snapshots used for the operation using the AWS CLI, use the describe-workspace-snapshots command.

When snapshots are taken

Snapshots of the root and user volume are taken on the following basis.

- **After a WorkSpace is first created** — Typically, the initial snapshots of the root and user volumes are taken soon after a WorkSpace is created (often within 30 minutes). In some AWS Regions, it might take several hours to take the initial snapshots after a WorkSpace is created.

  If a WorkSpace becomes unhealthy before the initial snapshots are taken, the WorkSpace can't be restored. In that case, you can try rebuilding the WorkSpace or contact AWS Support for assistance.
- **During regular use** — Automatic snapshots for use when restoring a WorkSpace are scheduled every 12 hours. If the WorkSpace is healthy, snapshots of both the root volume and user volume are created around the same time. If the WorkSpace is unhealthy, snapshots are created only for the user volume.
- **After a WorkSpace has been restored** — When you restore a WorkSpace, new snapshots are taken soon after the restore is finished (often within 30 minutes). In some AWS Regions, it might take several hours to take these snapshots after a WorkSpace is restored.

  After a WorkSpace has been restored, if the WorkSpace becomes unhealthy before new snapshots can be taken, the WorkSpace can't be restored again. In that case, you can try rebuilding the WorkSpace or contact AWS Support for assistance.

You can restore a WorkSpace only if the following conditions are met:

- The WorkSpace must have a state of `AVAILABLE`, `ERROR`, `UNHEALTHY`, or `STOPPED`.
- Snapshots of the root and user volumes must exist.

To restore a WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpace to restore and choose **Actions**, **Rebuild / Restore WorkSpace**.
4. Under **Snapshot**, select the snapshot's time stamp.
5. Choose **Restore**.

To restore a WorkSpace using the AWS CLI

Use the restore-workspace command.

Microsoft 365 Bring Your Own License (BYOL) in WorkSpaces Personal

Amazon WorkSpaces allows you to bring your own Microsoft 365 licenses if they meet Microsoft's licensing requirements. These licenses allow you to install and activate Microsoft 365 Apps for enterprise software on WorkSpaces that are powered by the following operating systems:

- Windows 10 (Bring Your Own License)
- Windows 11 (Bring Your Own License)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

To use Microsoft 365 Apps for enterprise on WorkSpaces, you must have subscription to Microsoft 365 E3/E5, Microsoft 365 A3/A5, Microsoft 365 G3/G5, or Microsoft 365 Business Premium.

On your Amazon WorkSpaces you can use your Microsoft 365 licenses to install and activate Microsoft 365 Apps for enterprise, including the following:

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Outlook
- Microsoft OneDrive

For more information, see the full list of Microsoft 365 Apps for enterprise.

You can also install Microsoft applications not included with Microsoft 365, such as Microsoft Project, Microsoft Visio, and Microsoft Power Automate on WorkSpaces but you need to bring in your own additional licenses.

You can install and use Microsoft 365 and other Microsoft applications on primary WorkSpaces and failover WorkSpaces using Multi-Region Resilience.

Contents

- Update your Microsoft 365 Apps for enterprise on WorkSpaces

Create WorkSpaces with Microsoft 365 Apps for enterprise

To create WorkSpaces with Microsoft 365 Apps for enterprise, you must create a custom image with the applications installed, and use it to create a custom bundle. You can use the bundle to launch new WorkSpaces that have the applications installed. WorkSpaces does not provide public bundles with Microsoft 365 Apps for enterprise.

To create WorkSpaces with Microsoft 365 Apps for enterprise:

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Launch a WorkSpace that you want to use as the image for other Microsoft application WorkSpaces. This is where you will install your Microsoft applications. For more information about launching a WorkSpace, see Launch a virtual desktop using WorkSpaces.
3. Start the client application at https://clients.amazonworkspaces.com/, enter the registration code from your invitation email, and choose **Register**.
4. When prompted to sign in, enter the user's sign-in credentials, and then choose **Sign In**.
5. Install and configure your Microsoft 365 Apps for enterprise.
6. Create a custom image from the WorkSpace, and use it to create a custom bundle. For more information about creating custom images and bundles, see Create a custom WorkSpaces image and bundle.
7. Launch WorkSpaces using the custom bundle that you created. These WorkSpaces have Microsoft 365 Apps for enterprise installed.

Migrate your existing WorkSpaces to use Microsoft 365 Apps for enterprise

If your WorkSpaces don't have a Microsoft Office license through AWS, you can install and configure Microsoft 365 Apps for enterprise on your WorkSpaces.

If your WorkSpaces do have a Microsoft Office license through AWS, you must first deregister your Microsoft Office license before installing Microsoft 365 Apps for enterprise.

Important

Uninstalling Microsoft Office applications from your WorkSpaces doesn't deregister the licenses. To avoid being charged for Microsoft Office licenses, deregister your WorkSpaces from Microsoft Office applications through AWS by doing either of the following:

- **Manage applications** (recommended) – You can uninstall Microsoft Office 2016 and 2019 from your WorkSpaces. For more information, see Manage applications. After you uninstall, you can install Microsoft 365 Apps for enterprise on your WorkSpaces.
- **Migrate a WorkSpace** – You can migrate a WorkSpace from one bundle to another while retaining the data on the user volume.
  - Migrate your WorkSpaces to a bundle with an image that doesn't have a Microsoft Office subscription. After the migration is complete, you can install Microsoft 365 Apps for enterprise on your WorkSpaces.
  - Or, create a custom WorkSpaces image and bundle that already has Microsoft 365 Apps for enterprise installed on the image, and then migrate your WorkSpaces to this new custom bundle. After migration is complete, your WorkSpaces users can start using Microsoft 365 Apps for enterprise.
  - For more information on how to migrate WorkSpaces, see Migrate a WorkSpace.

Update your Microsoft 365 Apps for enterprise on WorkSpaces

By default, your WorkSpaces running on the Microsoft Windows Operating System are configured to receive updates from Windows Update. However, updates for Microsoft 365 Apps for enterprise aren't available using Windows Update. Set up updates to run automatically from the Office CDN, or use Windows Server Update Services (WSUS) in conjunction with Microsoft Configuration Manager to update Microsoft 365 Apps for enterprise. For more information, see Manage updates to Microsoft 365 Apps with Microsoft Configuration Manager. To set the frequency of Microsoft 365 application updates, specify an update channel and set it to Current or Monthly Enterprise to comply with the Microsoft 365 on WorkSpaces licensing policy.

Upgrade Windows BYOL WorkSpaces in WorkSpaces Personal

On your Windows Bring Your Own License (BYOL) WorkSpaces, you can upgrade to a newer version of Windows using the in-place upgrade process. Follow the instructions in this topic to do so.

The in-place upgrade process applies only to Windows 10 and 11 BYOL WorkSpaces.

Important

Do not run Sysprep on an upgraded WorkSpace. If you do so, an error that prevents Sysprep from finishing might occur. If you plan to run Sysprep, do so only on a WorkSpace that hasn't been upgraded.

Note

You can use this process to upgrade your Windows 10 and 11 WorkSpaces to a newer version. However, this process cannot be used to upgrade your Windows 10 WorkSpaces to Windows 11.

Contents

Prerequisites

- If you have deferred or paused Windows 10 and 11 upgrades by using Group Policy or System Center Configuration Manager (SCCM), enable operating system upgrades for your Windows 10 and 11 WorkSpaces.
- If the WorkSpace is an AutoStop WorkSpace, change it to an AlwaysOn WorkSpace before the in-place upgrade process so that it won't stop automatically while updates are being applied. For more information, see Modify the running mode. If you prefer to keep the WorkSpace set to AutoStop, change the AutoStop time to three hours or more while the upgrade takes place.
- The in-place upgrade process recreates the user profile by making a copy of a special profile named Default User (`C:\Users\Default`). Do not use this default user profile to make

customizations. We recommend making any customizations to the user profile through Group Policy Objects (GPOs) instead. Customizations made through GPOs can be easily modified or rolled back and are less prone to error.

- The in-place upgrade process can back up and recreate only one user profile. If you have multiple user profiles on drive D, delete all the profiles except for the one that you need.

Considerations

The in-place upgrade process uses two registry scripts (`enable-inplace-upgrade.ps1` and `update-pvdrivers.ps1`) to make the necessary changes to your WorkSpaces that enable the Windows Update process to run. These changes involve creating a (temporary) user profile on drive C instead of drive D. If a user profile already exists on drive D, the data in that original user profile remains on drive D.

By default, WorkSpaces creates the user profile in `D:\Users\%USERNAME%`. The `enable-inplace-upgrade.ps1` script configures Windows to create a new user profile in `C:\Users\%USERNAME%` and redirects the user shell folders to `D:\Users\%USERNAME%`. This new user profile is created when a user logs on the first time.

After the in-place upgrade, you have the choice of leaving your user profiles on drive C to allow your users to use the Windows Update process to upgrade their machines in the future. However, be aware that WorkSpaces with profiles stored on drive C can't be rebuilt or migrated without losing all of the data in the user's profile unless you back up and restore that data yourself. If you decide to leave the profiles on drive C, you can use the **UserShellFoldersRedirection** registry key to redirect the user shell folders to drive D, as explained later in this topic.

To ensure that you can rebuild or migrate your WorkSpaces and to avoid any potential problems with user shell folder redirection, we recommend that you choose to restore your user profiles to drive D after the in-place upgrade. You can do so by using the **PostUpgradeRestoreProfileOnD** registry key, as explained later in this topic.

Known limitations

- The user profile location change from drive D to drive C does not happen during WorkSpace rebuilds or migrations. If you perform an in-place upgrade on a Windows 10 or 11 BYOL WorkSpace and then rebuild or migrate it, the new WorkSpace will have the user profile on drive D.

> **Warning**
>
> If you leave the user profile on drive C after the in-place upgrade, the user profile data stored on drive C will be lost during rebuilds or migrations unless you manually back up the user profile data prior to rebuilding or migrating, and then manually restore the user profile data after running the rebuild or migration process.

- If your default BYOL bundle contains an image that is based on an earlier release of Windows 10 and 11, you must perform the in-place upgrade again after the WorkSpace is rebuilt or migrated.

Summary of registry key settings

To enable the in-place upgrade process and to specify where you would like the user profile to be after the upgrade, you must set a number of registry keys.

Registry path: HKLM:\Software\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1

Registry key	Type	Values
Enabled	DWORD	**0** – (Default) Disables in-place upgrade **1** – Enables in-place upgrade
PostUpgradeRestoreProfileOnD	DWORD	**0** – (Default) Does not attempt to restore the user profile path after the in-place upgrade **1** – Restores the user profile path (**ProfileImagePath**) after the in-place upgrade
UserShellFoldersRedirection	DWORD	**0** – Does not enable redirecti on of user shell folders **1** – (Default) Enables redirecti on of user shell folders to `D:\Users\%USERNAME`

Registry key	Type	Values
		`%` after the user profile is regenerated on `C:\Users\%USERNAME%`
NoReboot	DWORD	**0** – (Default) Allows you to control when a reboot occurs after modifying the registry for the user profile **1** – Does not allow the script to reboot the WorkSpace after modifying the registry for the user profile

Registry path: HKLM:\Software\Amazon\WorkSpacesConfig\update-pvdrivers.ps1

Registry key	Type	Values
Enabled	DWORD	**0** – (Default) Disables AWS PV drivers update **1** – Enables AWS PV drivers update

Perform an in-place upgrade

To enable in-place Windows upgrades on your BYOL WorkSpaces, you must set certain registry keys, as described in the following procedure. You must also set certain registry keys to indicate the drive (C or D) where you want the user profiles to be after the in-place upgrades are finished.

You can make these registry changes manually. If you have multiple WorkSpaces to update, you can use Group Policy or SCCM to push a PowerShell script. For a sample PowerShell script, see Update your WorkSpace registry using a PowerShell script.

To perform an in-place upgrade of Windows 10 and 11

1. Make note of which version of Windows is currently running on the Windows 10 and 11 BYOL WorkSpaces that you are updating, and then reboot them.
2. Update the following Windows system registry keys to change the value data for **Enabled** from **0** to **1**. These registry changes enable in-place upgrades for the WorkSpace.

   - **HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1**
   - **HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\update-pvdrivers.ps1**

   > **Note**
   >
   > If these keys do not exist, reboot the WorkSpace. The keys should be added when the system is rebooted.

   (Optional) If you are using a managed workflow such as SCCM Task Sequences to perform the upgrade, set the following key value to **1** to prevent the computer from rebooting:

   HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1\NoReboot
3. Decide which drive you want user profiles to be on after the in-place upgrade process (for more information, see Considerations), and set the registry keys as follows:

   - Settings if you want the user profile on drive C after the upgrade:

     HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1

     Key name: **PostUpgradeRestoreProfileOnD**

     Key value: **0**

     Key name: **UserShellFoldersRedirection**

     Key value: **1**

- Settings if you want the user profile on drive D after the upgrade:

  HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1

  Key name: **PostUpgradeRestoreProfileOnD**

  Key value: **1**

  Key name: **UserShellFoldersRedirection**

  Key value: **0**

4. After saving the changes to the registry, reboot the WorkSpace again so that the changes are applied.

   > **Note**
   >
   > - After the reboot, logging in to the WorkSpace creates a new user profile. You might see placeholder icons in the **Start** menu. This behavior is automatically resolved after the in-place upgrade is complete.
   > - Allow 10 minutes to ensure that the WorkSpace is unblocked.

   (Optional) Confirm that the following key value is set to **1**, which unblocks the WorkSpace for updating:

   HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1\profileImagePathDeleted

5. Perform the in-place upgrade. You can use whichever method you like, such as SCCM, ISO, or Windows Update (WU). Depending on your original Windows 10 and 11 version and how many apps were installed, this process can take from 40 to 120 minutes.

   > **Note**
   >
   > The in-place upgrade process may take at least an hour. The WorkSpace instance status may appear as `UNHEALTHY` during the upgrade.

6. After the update process is finished, confirm that the Windows version has been updated.

   > **Note**
   >
   > If the in-place upgrade fails, Windows automatically rolls back to use the Windows 10 and 11 version that was in place before you started the upgrade. For more information about troubleshooting, see the Microsoft documentation.

   (Optional) To confirm that the update scripts have been run successfully, verify that the following key value is set to **1**:

   HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1\scriptExecutionComplete

7. If you modified the running mode of the WorkSpace by setting it to AlwaysOn or by changing the AutoStop time period so that the in-place upgrade process could run without interruption, set the running mode back to your original settings. For more information, see Modify the running mode.

If you haven't set the **PostUpgradeRestoreProfileOnD** registry key to **1**, the user profile is regenerated by Windows and placed in `C:\Users\%USERNAME%` after the in-place upgrade, so that you do not have to go through the above steps again for future Windows 10 and 11 in-place upgrades. By default, the `enable-inplace-upgrade.ps1` script redirects the following shell folders to drive D:

- `D:\Users\%USERNAME%\Downloads`
- `D:\Users\%USERNAME%\Desktop`
- `D:\Users\%USERNAME%\Favorites`
- `D:\Users\%USERNAME%\Music`
- `D:\Users\%USERNAME%\Pictures`
- `D:\Users\%USERNAME%\Videos`
- `D:\Users\%USERNAME%\Documents`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Network Shortcuts`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Printer Shortcuts`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs`

- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\SendTo`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates`

If you redirect the shell folders to other locations on your WorkSpaces, perform the necessary operations on the WorkSpaces after the in-place upgrades.

Troubleshooting

If you encounter any issues with the update, you can check the following items to assist with troubleshooting:

- Windows Logs, which are located, by default, in the following locations:

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\`

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\TRANSMITTED`
- Windows Event Viewer

  Windows Logs > Application > Source: Amazon WorkSpaces

> **Tip**
>
> During the in-place upgrade process, if you see that some icon shortcuts on the desktop no longer work, it's because WorkSpaces moves any user profiles located on drive D to drive C to prepare for the upgrade. After the upgrade is completed, the shortcuts will work as expected.

Update your WorkSpace registry using a PowerShell script

You can use the following sample PowerShell script to update the registry on your WorkSpaces to enable in-place upgrades. Follow the Perform an in-place upgrade, but use this script to update the registry on each WorkSpace.

```
# AWS WorkSpaces 1.28.20
# Enable In-Place Update Sample Scripts
# These registry keys and values will enable scripts to run on the next reboot of the
 WorkSpace.

$scriptlist = ("update-pvdrivers.ps1","enable-inplace-upgrade.ps1")
$wsConfigRegistryRoot="HKLM:\Software\Amazon\WorkSpacesConfig"
$Enabled = 1
$script:ErrorActionPreference = "Stop"

foreach ($scriptName in $scriptlist)
{
    $scriptRegKey = "$wsConfigRegistryRoot\$scriptName"

    try
    {
        if (-not(Test-Path $scriptRegKey))
        {
            Write-Host "Registry key not found. Creating registry key '$scriptRegKey'
 with 'Update' enabled."
            New-Item -Path $wsConfigRegistryRoot -Name $scriptName | Out-Null
            New-ItemProperty -Path $scriptRegKey -Name Enabled -PropertyType DWord -
Value $Enabled | Out-Null
            Write-Host "Value created. '$scriptRegKey' Enabled='$((Get-ItemProperty -
Path $scriptRegKey).Enabled)'"
        }
        else
        {
            Write-Host "Registry key is already present with value '$scriptRegKey'
 Enabled='$((Get-ItemProperty -Path $scriptRegKey).Enabled)'"
            if((Get-ItemProperty -Path $scriptRegKey).Enabled -ne $Enabled)
            {
                Set-ItemProperty -Path $scriptRegKey -Name Enabled -Value $Enabled
                Write-Host "Value updated. '$scriptRegKey' Enabled='$((Get-ItemProperty
 -Path $scriptRegKey).Enabled)'"
            }
        }
    }
    catch
    {
        write-host "Stopping script, the following error was encountered:" `r`n$_ -
ForegroundColor Red
        break
```

```
    }
}
```

Migrate a WorkSpace in WorkSpaces Personal

> **Note**
>
> If you want to unsubscribe from or uninstall Microsoft Office version licenses through AWS from your WorkSpace, we recommend using Manage applications.

You can migrate a WorkSpace from one bundle to another, while retaining the data on the user volume. The following are example scenarios:

- You can migrate WorkSpaces from the Windows 7 desktop experience to the Windows 10 desktop experience.
- You can migrate WorkSpaces from the PCoIP protocol to the WorkSpaces Streaming Protocol (WSP).
- You can migrate WorkSpaces from the 32-bit Microsoft Office on Windows Server 2016-powered WorkSpaces bundle to the 64-bit Microsoft Office on Windows Server 2019 and Windows Server 2022-powered WorkSpaces bundles.
- You can migrate WorkSpaces from one public or custom bundle to another. For example, you can migrate from GPU-enabled (Graphics.g4dn. GraphicsPro.g4dn, Graphics, and GraphicsPro) bundles to non-GPU-enabled bundles, as well as in the other direction.
- You can migrate WorkSpaces from the Windows 10 BYOL to the Windows 11 BYOL but migration from Windows 11 to Windows 10 is not supported.
- Value bundles are not supported on Windows 11. To migrate your Windows 7 or 10 value bundle WorkSpaces to Windows 11, you need to switch your Value WorkSpaces to a bigger bundle offering first.
- Before migrating WorkSpaces from Windows 7 to Windows 11, you need to migrate it to Windows 10. Log in to Windows 10 WorkSpace at least once before migrating it to Windows 11. Migrating from Windows 7 WorkSpaces directly to Windows 11 is not supported.
- You can migrate Windows WorkSpaces that use Microsoft Office through AWS to a custom WorkSpaces bundle with Microsoft 365 applications. After the migration, your WorkSpaces are unsubscribed from Microsoft Office.

- You can migrate Windows WorkSpaces that use Microsoft Office through AWS to a WorkSpaces bundle with no Office 2016/2019 subscription. After the migration, your WorkSpaces are unsubscribed from Microsoft Office.
- You can migrate BYOL BYOP WorkSpaces from Windows 10 to Windows 11, and license-included BYOP WorkSpaces from Windows Server 2019 to Windows Server 2022.

For more information about Amazon WorkSpaces bundles, see Bundles and images for WorkSpaces Personal.

The migration process recreates the WorkSpace by using a new root volume from the target bundle image and the user volume from the last available snapshot of the original WorkSpace. A new user profile is generated during migration for better compatibility. The old user profile is renamed, and then certain files in the old user profile are moved to the new user profile. (For details about what gets moved, see What happens during migration.)

The migration process takes up to one hour per WorkSpace. When you initiate the migration process, a new WorkSpace is created. If an error occurs that prevents successful migration, the original WorkSpace is recovered and returned to its original state, and the new WorkSpace is terminated.

Contents

Migration limits

- You cannot migrate to a public or custom Windows 7 desktop experience bundle. You also cannot migrate to Bring Your Own License (BYOL) Windows 7 bundles.

- You can migrate BYOL WorkSpaces only to other BYOL bundles. To migrate a BYOL WorkSpace from PCoIP to WSP, you must first create a BYOL bundle with the WSP protocol. You can then migrate your PCoIP BYOL WorkSpaces to that WSP BYOL bundle.
- You cannot migrate a WorkSpace created from public or custom bundles to a BYOL bundle.
- Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro bundles are available for only the PCoIP protocol at this time, so Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro WorkSpaces can't be migrated to WSP yet.
- Migrating Linux WorkSpaces is not currently supported.
- In AWS Regions that support more than one language, you can migrate WorkSpaces between language bundles.
- The source and target bundles must be different. (However, in Regions that support more than one language, you can migrate to the same Windows 10 bundle as long as the languages differ.) If you want to refresh your WorkSpace using the same bundle, rebuild the WorkSpace instead.
- You cannot migrate WorkSpaces across Regions.
- In some cases, if migration is unable to finish successfully, you might not receive an error message, and it might appear that the migration process did not start. If the WorkSpace bundle remains the same one hour after attempting migration, the migration is unsuccessful. Contact the AWS Support Center for assistance.
- You cannot migrate BYOP WorkSpaces to PCoIP or WSP WorkSpaces.

Migration scenarios

The following table shows which migration scenarios are available:

Source OS	Target OS	Available?
Public or custom bundle Windows 7	Public or custom bundle Windows 10	Yes
Custom bundle Windows 7	Public bundle Windows 7	No
Custom bundle Windows 7	Custom bundle Windows 7	No
Public bundle Windows 7	Custom bundle Windows 7	No

Source OS	Target OS	Available?
Public or custom bundle Windows 10	Public or custom bundle Windows 7	No
Public or custom bundle Windows 10	Custom bundle Windows 10	Yes
Windows 7 BYOL bundle	Windows 7 BYOL bundle	No
Windows 7 BYOL bundle	Windows 10 BYOL bundle	Yes
Windows 10 BYOL bundle	Windows 7 BYOL bundle	No
Windows 10 BYOL bundle	Windows 10 BYOL bundle	Yes
Windows Server 2016-powered Public Windows 10 bundle	Windows Server 2019-powered Public Windows 10 bundle 	Yes
Windows Server 2019-powered Public Windows 10 bundle 	Windows Server 2016-powered Public Windows 10 bundle	Yes
Windows 10 BYOL bundle	Windows 11 BYOL bundle	Yes
Windows 11 BYOL bundle	Windows 10 BYOL bundle	No
Windows Server 2016-powered custom Windows 10 bundle	Windows Server 2019-powered Public Windows 10 bundle	Yes

Source OS	Target OS	Available?
Windows Server 2016-powered custom Windows 10 bundle	Windows Server 2022-powered Public Windows 10 bundle	Yes
Windows Server 2019-powered custom Windows 10 bundle	Windows Server 2022-powered Public Windows 10 bundle	Yes
Windows 10 BYOP BYOL	Windows 11 BYOP BYOL	Yes
Windows 11 BYOP BYOL	Windows 10 BYOP BYOL	No
Windows Server 2019-powered Public BYOP	Windows Server 2022-powered Public BYOP	Yes
Windows Server 2022-powered Public BYOP	Windows Server 2019-powered Public BYOP	No

Note

Web access is not available for the Windows Server 2019-powered Public Windows 10 bundle PCoIP branch.

Important

The Windows Server 2016-powered Public Windows 10 plus bundle includes Microsoft Office 2016 and Trend Micro Worry-Free Business Security Services. The Windows Server 2019-powered Public Windows 10 plus bundle includes Microsoft Office 2019 only, and does not include Trend Micro Services.

What happens during migration

During migration, the data on the user volume (drive D) is preserved, but all of the data on the root volume (drive C) is lost. This means that none of the installed applications, settings, and changes

to the registry are preserved. The old user profile folder is renamed with the `.NotMigrated` suffix, and a new user profile is created.

The migration process recreates drive D based on the last snapshot of the original user volume. During the first boot of the new WorkSpace, the migration process moves the original `D:\Users\%USERNAME%` folder to a folder named `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`. A new `D:\Users\%USERNAME%\` folder is generated by the new OS.

After the new user profile is created, the files in the following user shell folders are moved from the old `.NotMigrated` profile to the new profile:

- `D:\Users\%USERNAME%\Desktop`
- `D:\Users\%USERNAME%\Documents`
- `D:\Users\%USERNAME%\Downloads`
- `D:\Users\%USERNAME%\Favorites`
- `D:\Users\%USERNAME%\Music`
- `D:\Users\%USERNAME%\Pictures`
- `D:\Users\%USERNAME%\Videos`

Important

The migration process attempts to move the files from the old user profile to the new profile. Any files that weren't moved during migration remain in the `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated` folder. If the migration is successful, you can see which files got moved in `C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs`. You can manually move any files that didn't get moved automatically.

By default, the public bundles have local search indexing disabled. If you were to enable it, the default is to search `C:\Users` and not `D:\Users`, so you need to adjust that as well. If you've set local search indexing specifically to `D:\Users\`*`username`* and not to `D:\Users`, then local search indexing might not work post-migration for any user files that are in the `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated` folder.

Any tags assigned to the original WorkSpace are carried over during migration, and the running mode of the WorkSpace is preserved. However, the new WorkSpace gets a new WorkSpace ID, computer name, and IP address.

Best practices

Before you migrate a WorkSpace, do the following:

- Back up any important data on drive C to another location. All data on drive C is erased during migration.
- Make sure that the WorkSpace being migrated is at least 12 hours old, to ensure that a snapshot of the user volume has been created. On the **Migrate WorkSpaces** page in the Amazon WorkSpaces console, you can see the time of the last snapshot. Any data created after the last snapshot is lost during migration.
- To avoid potential data loss, make sure that your users log out of their WorkSpaces and don't log back in until after the migration process is finished. Note that WorkSpaces cannot be migrated when they are in `ADMIN_MAINTENANCE` mode.
- Make sure that the WorkSpaces you want to migrate have a status of `AVAILABLE`, `STOPPED`, or `ERROR`.
- Make sure that you have enough IP addresses for the WorkSpaces you are migrating. During migration, new IP addresses will be allocated for the WorkSpaces.
- If you are using scripts to migrate WorkSpaces, migrate them in batches of no more than 25 WorkSpaces at a time.

Troubleshooting

- If your users report missing files after migration, check to see if their user profile files did not get moved during the migration process. You can see which files got moved in `C:\Program Files \Amazon\WorkspacesConfig\Logs\MigrationLogs`. The files that didn't get moved will be located in the `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated` folder. You can manually move any files that didn't get moved automatically.
- If you are using the API to migrate WorkSpaces and the migration does not succeed, the target WorkSpace ID returned by the API will not be used, and the WorkSpace will still have the original WorkSpace ID.
- If a migration does not successfully finish, check the Active Directory to see if it was cleaned up accordingly. You might need to manually remove WorkSpaces that you no longer need.

How billing is affected

During the month in which migration occurs, you are charged prorated amounts for both the new and the original WorkSpaces. For example, if you migrate WorkSpace A to WorkSpace B on May 10, you will be charged for WorkSpace A from May 1 to May 10, and you will be charged for WorkSpace B from May 11 to May 30.

> **Note**
>
> If you are migrating a WorkSpace to a different bundle type (for example, from Performance to Power, or Value to Standard), the size of the root volume (drive C) and the user volume (drive D) might increase during the migration process. If necessary, the root volume increases to match the default root volume size for the new bundle. However, if you had already specified a different size (higher or lower) for the user volume than the default for the original bundle, that same user volume size is retained during the migration process. Otherwise, the migration process uses the larger of the source WorkSpace user volume size and the default user volume size for the new bundle.

Migrating a WorkSpace

You can migrate WorkSpaces through the Amazon WorkSpaces console, the AWS CLI or the Amazon WorkSpaces API.

To migrate a WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select your WorkSpace and choose **Actions**, **Migrate WorkSpaces**.
4. Under **Bundles**, select the bundle that you'd like to migrate your WorkSpace to.

   > **Note**
   >
   > To migrate a BYOL WorkSpace from PCoIP to WSP, you must first create a BYOL bundle with the WSP protocol. You can then migrate your PCoIP BYOL WorkSpaces to that WSP BYOL bundle.

5. Choose **Migrate WorkSpaces**.

A new WorkSpace with a status of `PENDING` appears in the Amazon WorkSpaces console. When the migration is finished, the original WorkSpace is terminated, and the status of the new WorkSpace is set to `AVAILABLE`.

6. (Optional) To delete any custom bundles and images that you no longer need, see Delete a custom bundle or image in WorkSpaces Personal.

To migrate WorkSpaces through the AWS CLI, use the migrate-workspace command. To migrate WorkSpaces through the Amazon WorkSpaces API, see MigrateWorkSpace in the *Amazon WorkSpaces API Reference*.

Delete a WorkSpace in WorkSpaces Personal

When you are finished with a WorkSpace, you can delete it. You can also delete related resources.

Warning

Deleting a WorkSpace is a permanent action and cannot be undone. The WorkSpace user's data does not persist and is destroyed. For help with backing up user data, contact AWS Support.

Note

Simple AD and AD Connector are available to you free of charge to use with WorkSpaces. If there are no WorkSpaces being used with your Simple AD or AD Connector directory for 30 consecutive days, this directory will be automatically deregistered for use with Amazon WorkSpaces, and you will be charged for this directory as per the AWS Directory Service pricing terms.

To delete empty directories, see Delete a directory for WorkSpaces Personal. If you delete your Simple AD or AD Connector directory, you can always create a new one when you want to start using WorkSpaces again.

To delete a WorkSpace

You can delete a WorkSpace that is in any state except **Suspended**.

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select your WorkSpace and choose **Delete**.
4. When prompted for confirmation, choose **Delete WorkSpace**. It takes approximately 5 minutes to delete a WorkSpace. During deletion, the status of the WorkSpace is set to **Terminating**. When the deletion is complete, the WorkSpace disappears from the console.
5. (Optional) To delete any custom bundles and images that you are finished with, see Delete a custom bundle or image in WorkSpaces Personal.
6. (Optional) After you delete all WorkSpaces in a directory, you can delete the directory. For more information, see Delete a directory for WorkSpaces Personal.
7. (Optional) After you delete all resources in the virtual private cloud (VPC) for your directory, you can delete the VPC and release the Elastic IP address used for the NAT gateway. For more information, see Deleting your VPC and Working with Elastic IP addresses in the *Amazon VPC User Guide*.

To delete a WorkSpace using the AWS CLI

Use the terminate-workspaces command.

Bundles and images for WorkSpaces Personal

A *WorkSpace bundle* is a combination of an operating system, and storage, compute, and software resources. When you launch a WorkSpace, you select the bundle that meets your needs. The default bundles available for WorkSpaces are called *public bundles*. For more information about the various public bundles available for WorkSpaces, see Amazon WorkSpaces Bundles.

If you've launched a Windows or Linux WorkSpace and have customized it, you can create a custom image from that WorkSpace.

A *custom image* contains only the OS, software, and settings for the WorkSpace. A *custom bundle* is a combination of both that custom image and the hardware from which a WorkSpace can be launched.

After you create a custom image, you can build a custom bundle that combines the custom WorkSpace image and the underlying compute and storage configuration that you select. You can then specify this custom bundle when you launch new WorkSpaces to ensure that the new WorkSpaces have the same consistent configuration (hardware and software).

If you need to perform software updates or to install additional software on your WorkSpaces, you can update your custom bundle and use it to rebuild your WorkSpaces.

WorkSpaces supports several different operating systems (OS), streaming protocols, and bundles. The following table provides information about the licensing, streaming protocols, and bundles that are supported by each OS.

Operating System	Licenses	Streaming protocols	Supported bundles	Lifecycle policy / retirement date
Windows Server 2016	Included	WSP, PCoIP	Value, Standard, Performance, Power, PowerPro, Graphics (deprecated), GraphicsPro, Graphics.g4dn, GraphicsPro.g4dn	January 12, 2027
Windows Server 2019	Included	WSP, PCoIP	Value, Standard, Performance, Power, PowerPro, Graphics (deprecated), GraphicsPro, Graphics.g4dn, GraphicsPro.g4dn	January 9, 2029
Windows Server 2022	Included	WSP, PCoIP	Standard, Performance, Power, PowerPro, Graphics (deprecated), GraphicsPro, Graphics.g4dn, GraphicsPro.g4dn	October 14, 2031
Windows 10	Bring Your Own License (BYOL)	WSP, PCoIP	Value, Standard, Performance, Power, PowerPro, Graphics (deprecated), GraphicsPro, Graphics.g4dn, GraphicsPro.g4dn	In support
Windows 11	Bring Your Own License (BYOL)	WSP	Standard, Performance, Power, PowerPro	In support

Operating System	Licenses	Streaming protocols	Supported bundles	Lifecycle policy / retirement date
Amazon Linux 2	Included	WSP, PCoIP	Value, Standard, Performance, Power, PowerPro	June 30, 2025
Ubuntu 22.04 LTS	Included	WSP	Value, Standard, Performance, Power, PowerPro, Graphics.g4dn, GraphicsPro.g4dn	June, 2032
Red Hat Enterprise Linux 8	Included	WSP	Value, Standard, Performance, Power, PowerPro	May 31, 2029

Note

- Operating system versions that are no longer supported by the vender are not guaranteed to work and are not supported by AWS support.
- For WorkSpaces running on Windows operating system, Graphics bundles only supports PCoIP streaming protocol.

Contents

Bundle options for WorkSpaces Personal

Before selecting a bundle, ensure the bundle you want to select is compatible with your WorkSpaces' protocol, operating system, network, and compute type. For more information about protocols, see Protocols for Amazon WorkSpaces. For more information about networks, see Amazon WorkSpaces client network requirements.

Note

- We recommend not exceeding a 250 ms maximum network latency for PCoIP WorkSpaces. To get the best PCoIP WorkSpaces user experience, we recommend keeping the network latency under 100 ms. When the round-trip time (RTT) exceeds 375 ms, the WorkSpaces client connection will shut down. For the best WorkSpaces Streaming Protocol (WSP) user experience, we recommend keeping the RTT under 250 ms. If the RTT is between 250 ms and 400 ms, the user can access the WorkSpace, but performance will decrease significantly.
- We recommend testing the performance of bundles you want to choose in a test environment by running and using applications that replicate your users' daily tasks.

Important

- The Graphics bundle will no longer be supported after November 30, 2023. We recommend switching to the Graphics.g4dn bundle for WorkSpaces using the Graphics bundle.
- Graphics and GraphicsPro bundles aren't currently available in the Asia Pacific (Mumbai) Region.

The following are the bundles that WorkSpaces offers. For information about bundles in WorkSpaces, see Amazon WorkSpaces Bundles.

Value bundle

This bundle is well-suited for the following:

- Basic text editing and data entry

- Web browsing with light usage
- Instant messaging

This bundle is not recommended for word processing, audio and video conferencing, screen sharing, software development tool, business intelligence applications, and graphics applications.

Standard bundle

This bundle is well-suited for the following:

- Basic text editing and data entry
- Web browsing
- Instant messaging
- Email

This bundle is not recommended for audio and video conferencing, screen sharing, word processing, software development tool, business intelligence applications, and graphics applications

Performance bundle

This bundle is well-suited for the following:

- Web browsing
- Word processing
- Instant messaging
- Email
- Spreadsheets
- Audio processing
- Courseware

This bundle is not recommended for video conferencing, screen sharing, software development tool, business intelligence applications, and graphics applications

Power bundle

This bundle is well-suited for the following:

- Web browsing
- Word processing
- Email
- Instant messaging
- Spreadsheets
- Audio processing
- Software development (Integrated Development Environment (IDE))
- Entry to mid-level data processing
- Audio and video conferencing

This bundle is not recommended for screen sharing, software development tool, business intelligence applications, and graphics applications.

PowerPro bundle

This bundle is well-suited for the following:

- Web browsing
- Word processing
- Email
- Instant messaging
- Spreadsheets
- Audio processing
- Software development (Integrated Development Environment (IDE))
- Data warehousing
- Business intelligence applications
- Audio and video conferencing

This bundle is not recommended for machine learning model training, and graphics applications

GraphicsPro bundle

This bundle offers a baseline level of graphics performance, and high level of CPU performance and memory for your WorkSpaces. It is well-suited for the following:

- Web browsing
- Word processing
- Email
- Instant messaging
- Spreadsheets
- Audio conferencing
- Software development (Integrated Development Environment (IDE))
- Data warehousing
- Business intelligence applications
- Graphic design
- Image processing

This bundle is not recommended for audio and video conferencing, 3D rendering, and photo-realistic design

Graphics.g4dn bundle

This bundle offers a high level of graphics performance, and moderate level of CPU performance and memory for your WorkSpaces and is well-suited for the following:

- Web browsing
- Word processing
- Email
- Spreadsheets
- Instant messaging
- Audio conferencing
- Software development (Integrated Development Environment (IDE))
- Entry to mid-level data processing
- Data warehousing
- Business intelligence applications
- Graphic design
- CAD/CAM (computer-aided design/computer-aided manufacturing)

This bundle is not recommended for audio and video conferencing, 3D rendering, photo-realistic design, and machine learning model training

GraphicsPro.g4dn

GraphicsPro.g4dn bundle

This bundle offers a high level of graphics performance, CPU performance, and memory for your WorkSpaces and is well-suited for the following:

- Web browsing
- Word processing
- Email
- Spreadsheets
- Instant messaging
- Audio conferencing
- Software development (Integrated Development Environment (IDE))
- Entry to mid-level data processing
- Data warehousing
- Business intelligence applications
- Graphic design
- CAD/CAM (computer-aided design/computer-aided manufacturing)
- Video transcoding
- 3D rendering
- Photo-realistic design
- Game streaming
- ML (machine learning) model training and ML inference

This bundle is not recommended for audio and video conferencing.

Create a custom WorkSpaces image and bundle for WorkSpaces Personal

If you've launched a Windows or Linux WorkSpace and have customized it, you can create a custom image and custom bundles from that WorkSpace.

A *custom image* contains only the OS, software, and settings for the WorkSpace. A *custom bundle* is a combination of both that custom image and the hardware from which a WorkSpace can be launched.

> **Note**
>
> Ensure you wait at least 2 hours after deleting a bundle before creating a new bundle with the same name.

After you create a custom image, you can build a custom bundle that combines the custom image and the underlying compute and storage configuration that you select. You can then specify this custom bundle when you launch new WorkSpaces to ensure that the new WorkSpaces have the same consistent configuration (hardware and software).

You can use the same custom image to create various custom bundles by selecting different compute and storage options for each bundle.

> **Important**
>
> - If you plan to create an image from a Windows 10 WorkSpace, note that image creation is not supported on Windows 10 systems that have been upgraded from one version of Windows 10 to a newer version of Windows 10 (a Windows feature/version upgrade). However, Windows cumulative or security updates are supported by the WorkSpaces image-creation process.
> - After January 14, 2020, images cannot be created from public Windows 7 bundles. You might want to consider migrating your Windows 7 WorkSpaces to Windows 10. For more information, see Migrate a WorkSpace in WorkSpaces Personal.
> - Graphics bundle is no longer supported after November 30, 2023. We recommend migrating your WorkSpaces to Graphics.g4dn bundle. For more information, see Migrate a WorkSpace in WorkSpaces Personal.
> - Graphics and GraphicsPro bundles aren't currently available in the Asia Pacific (Mumbai) Region.
> - Custom bundle storage volumes can't be smaller than image storage volumes.

Custom bundles cost the same as the public bundles they are created from. For more information about pricing, see Amazon WorkSpaces Pricing.

Contents

Requirements to create Windows custom images

> **Note**
>
> Windows currently defines 1 GB as 1,073,741,824 bytes. Customers will need to ensure they have greater than 12,884,901,888 bytes (or 12 GiB) free on C drive and the user profile is less than 10,737,418,240 bytes (or 10 GiB) to create an image of a WorkSpace.

- The status of the WorkSpace must be **Available** and its modification state must be **None**.
- All applications and user profiles on WorkSpaces images must be compatible with Microsoft Sysprep.
- All applications to include in the image must be installed on the C drive.
- For Windows 7 WorkSpaces, and its total size (files and data) must be less than 10 GB.
- For Windows 7 WorkSpaces, the C drive must have at least 12 GB of available space.
- All application services running on the WorkSpace must use a local system account instead of domain user credentials. For example, you cannot have a Microsoft SQL Server Express installation running with a domain user's credentials.
- The WorkSpace must not be encrypted. Image creation from an encrypted WorkSpace is not currently supported.

- The following components are required in an image. Without these components, the WorkSpaces that you launch from the image will not function correctly. For more information, see the section called “Required configuration”.
  - Windows PowerShell version 3.0 or later
  - Remote Desktop Services
  - AWS PV drivers
  - Windows Remote Management (WinRM)
  - Teradici PCoIP agents and drivers
  - STXHD agents and drivers
  - AWS and WorkSpaces certificates
  - Skylight agent

Requirements to create Linux custom images

- The status of the WorkSpace must be **Available** and its modification state must be **None**.
- All applications to include in the image must be installed outside of the user volume (the `/home` directory).
- The root volume (/) should be less than 97% full.
- The WorkSpace must not be encrypted. Image creation from an encrypted WorkSpace is not currently supported.
- The following components are required in an image. Without these components, the WorkSpaces that you launch from the image will not function correctly:
  - Cloud-init
  - Teradici PCoIP or WSP agents and drivers
  - Skylight agent

Best practices

Before you create an image from a WorkSpace, do the following:

- Use a separate VPC that is not connected to your production environment.
- Deploy the WorkSpace in a private subnet and use a NAT instance for outbound traffic.
- Use a small Simple AD directory.

- Use the smallest volume size for the source WorkSpace, and then adjust the volume size as needed when creating the custom bundle.
- Install all operating system updates (except Windows feature/version updates) and all application updates on the WorkSpace. For more information, see the Important note at the start of this topic.
- Delete cached data from the WorkSpace that shouldn't be included in the bundle (for example, browser history, cached files, and browser cookies).
- Delete configuration settings from the WorkSpace that shouldn't be included in the bundle (for example, email profiles).
- Switch to dynamic IP address settings using DHCP.
- Make sure that you haven't exceeded your quota for WorkSpace images allowed in a Region. By default, you're allowed 40 WorkSpace images per Region. If you've reached this quota, new attempts to create an image will fail. To request a quota increase, use the WorkSpaces Limits form.
- Make sure that you aren't trying to create an image from an encrypted WorkSpace. Image creation from an encrypted WorkSpace is not currently supported.
- If you're running any antivirus software on the WorkSpace, disable it while you're attempting to create an image.
- If you have a firewall enabled on your WorkSpace, make sure that it isn't blocking any necessary ports. For more information, see IP address and port requirements for WorkSpaces Personal.
- For Windows WorkSpaces, don't configure any Group Policy Objects (GPOs) before image creation.
- For Windows WorkSpaces, do not customize the default user profile (`C:\Users\Default`) before creating an image. We recommend making any customizations to the user profile through GPOs, and applying them after image creation. GPOs can be easily modified or rolled back, and are therefore less prone to error than customizations made to the default user profile.
- For Linux WorkSpaces, see also the "Best Practices to Prepare Your Amazon WorkSpaces for Linux Images" whitepaper.
- If you want to use smart cards on Linux WorkSpaces with WorkSpaces Streaming Protocol (WSP) enabled, see Use smart cards for authentication in WorkSpaces Personal for the customizations that you must make to your Linux WorkSpace before creating your image.
- Ensure you update networking dependency drivers like ENA, NVMe, and PV drivers on your WorkSpaces. You should do this at least once every 6 months. For more information, see Install

or upgrade Elastic Network Adapter (ENA) driver , AWS NVMe drivers for Windows instances, and Upgrade PV drivers on Windows instances.

- Ensure you update the EC2Config, EC2Launch, and EC2Launch V2 agents to the latest versions periodically. You should do this at least once every 6 months. For more information, see Update EC2Config and EC2Launch.

(Optional) Step 1: Specify a custom computer name format for your image

For the WorkSpaces launched from your custom or Bring Your Own License (BYOL) images, you can specify a custom prefix for the computer name format instead of using the default computer name format. To specify a custom prefix, follow the appropriate procedure for your image type.

To specify a custom computer name format for custom images

> **Note**
>
> By default, the format of the computer name for Windows 10 WorkSpaces is `DESKTOP-XXXXX` and for Windows 11 WorkSpaces, `WORKSPA-XXXXX`.

1. On the WorkSpace that you're using to create your custom image, open `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml` in Notepad or another text editor. For more information about working with the `Unattend.xml` file, see Answer files (unattend.xml) in the Microsoft documentation.

   > **Note**
   >
   > To access the C: drive from the Windows File Explorer on your WorkSpace, enter **`C:\`** in the address bar.

2. In the `<settings pass="specialize">` section, make sure that `<ComputerName>` is set to an asterisk (*). If `<ComputerName>` is set to any other value, your custom computer name settings will be ignored. For more information about the `<ComputerName>` setting, see ComputerName in the Microsoft documentation.
3. In the `<settings pass="specialize">` section, set `<RegisteredOrganization>` and `<RegisteredOwner>` to your preferred values.

During Sysprep, the values that you specify for <RegisteredOwner> and <RegisteredOrganization> are concatenated together, and the first 7 characters of the combined string are used to create the computer name. For example, if you specify **Amazon.com** for <RegisteredOrganization> and **EC2** for <RegisteredOwner>. For Windows 10-based images, the computer names for the WorkSpaces using custom bundles will start with EC2AMAZ-*xxxxxxx*. For Windows 11 based images, the computer names for the WorkSpaces using custom bundles will start with WORKSPA-*xxxxxxx*.

> **Note**
>
> The <RegisteredOrganization> and <RegisteredOwner> values in the <settings pass="oobeSystem"> section are ignored by Sysprep.

4. Save your changes to the Unattend.xml file.

To specify a custom computer name format for BYOL images

1. If you are using Windows 10, open C:\Program Files\Amazon\Ec2ConfigService\Sysprep2008.xml in Notepad or another text editor. If you are using Windows 11, open C:\ProgramData\Amazon\EC2Launch\sysprep\OOBE_unattend.xml.
2. In the <settings pass="specialize"> section, uncomment <ComputerName>*</ComputerName>, and make sure that <ComputerName> is set to an asterisk (*). If <ComputerName> is set to any other value, your custom computer name settings will be ignored. For more information about the <ComputerName> setting, see ComputerName in the Microsoft documentation.
3. In the <settings pass="specialize"> section, set <RegisteredOrganization> and <RegisteredOwner> to your preferred values.

   During Sysprep, the values that you specify for <RegisteredOwner> and <RegisteredOrganization> are concatenated together, and the first 7 characters of the combined string are used to create the computer name. For example, if you specify **Amazon.com** for <RegisteredOrganization> and **EC2** for <RegisteredOwner>, the computer names for the WorkSpaces created from your custom bundle will start with EC2AMAZ-*xxxxxxx*.

> **Note**
>
> The `<RegisteredOrganization>` and `<RegisteredOwner>` values in the `<settings pass="oobeSystem">` section are ignored by Sysprep.

4. If you are using Windows 10, save your changes to the `Sysprep2008.xml` file. If you are using Windows 11, save your changes to `OOBE_unattend.xml`

Step 2: Run the Image Checker

> **Note**
>
> The Image Checker is available only for Windows WorkSpaces. If you are creating an image from a Linux WorkSpace, skip to Step 3: Create a custom image and custom bundle.

To confirm that your Windows WorkSpace meets the requirements for image creation, we recommend running the Image Checker. The Image Checker performs a series of tests on the WorkSpace that you want to use to create your image, and provides guidance on how to resolve any issues it finds.

> **Important**
>
> - The WorkSpace must pass all of the tests run by the Image Checker before you can use it for image creation.
> - Before you run the Image Checker, verify that the latest Windows security and cumulative updates are installed on your WorkSpace.

To get the Image Checker, do one of the following:

- Reboot your WorkSpace. The Image Checker is downloaded automatically during the reboot and installed at `C:\Program Files\Amazon\ImageChecker.exe`.
- Download the Amazon WorkSpaces Image Checker from https://tools.amazonworkspaces.com/ImageChecker.zip and extract the `ImageChecker.exe` file. Copy this file to `C:\Program Files\Amazon\`.

To run the Image Checker

1. Open the `C:\Program Files\Amazon\ImageChecker.exe` file.
2. In the **Amazon WorkSpaces Image Checker** dialog box, choose **Run**.
3. After each test is completed, you can view the status of the test.

   For any test with a status of **FAILED**, choose **Info** to display information about how to resolve the issue that caused the failure. For more information about how to resolve these issues, see Tips for resolving issues detected by the Image Checker.

   If any tests display a status of **WARNING**, choose the **Fix All Warnings** button.

   The tool generates an output log file in the same directory where the Image Checker is located. By default, this file is located at `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`.

   > **Tip**
   >
   > Do not delete this log file. If an issue occurs, this log file might be helpful in troubleshooting.

4. If applicable, resolve any issues that cause test failures and warnings, and repeat the process of running the Image Checker until the WorkSpace passes all tests. All failures and warnings must be resolved before you can create an image.
5. After your WorkSpace passes all tests, you see a **Validation Successful** message. You are now ready to create a custom bundle.

Tips for resolving issues detected by the Image Checker

In addition to consulting the following tips for resolving issues that are detected by the Image Checker, be sure to review the Image Checker log file at `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`.

PowerShell version 3.0 or later must be installed

Install the latest version of Microsoft Windows PowerShell.

> **Important**
>
> The PowerShell execution policy for a WorkSpace must be set to allow **RemoteSigned** scripts. To check the execution policy, run the **Get-ExecutionPolicy** PowerShell command. If the execution policy is not set to **Unrestricted** or **RemoteSigned**, run the **Set-ExecutionPolicy –ExecutionPolicy RemoteSigned** command to change the value of the execution policy. The **RemoteSigned** setting allows the execution of scripts on Amazon WorkSpaces, which is required to create an image.

Only the C and D drives can be present

Only the `C` and `D` drives can be present on a WorkSpace that's used for imaging. Remove all other drives, including virtual drives.

No pending reboot due to Windows Updates can be detected

- The Create Image process can't run until Windows is rebooted to finish installing security or cumulative updates. Reboot Windows to apply these updates, and make sure that no other pending Windows security or cumulative updates need to be installed.
- Image creation is not supported on Windows 10 systems that have been upgraded from one version of Windows 10 to a newer version of Windows 10 (a Windows feature/version upgrade). However, Windows cumulative or security updates are supported by the WorkSpaces image-creation process.

The Sysprep file must exist and can't be blank

If there are problems with your Sysprep file, contact the AWS Support Center to get your EC2Config or EC2Launch repaired.

The user profile size must be less than 10 GB

For Windows 7 WorkSpaces, the user profile (`D:\Users\`*`username`*) must be less than 10 GB total. Remove files as needed to reduce the size of the user profile.

Drive C must have enough free space

For Windows 7 WorkSpaces, you must have at least 12 GB of free space on drive `C`. Remove files as needed to free up space on drive `C`. For Windows 10 WorkSpaces, ignore if you receive a `FAILED` message and the disk space is above 2GB.

No services can be running under a domain account

To run the Create Image process, no services on the WorkSpace can be running under a domain account. All services must be running under a local account.

To run services under a local account

1. Open `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log` and find the list of services that are running under a domain account.
2. In the Windows search box, enter **`services.msc`** to open the Windows Services Manager.
3. Under **Log On As**, look for the services that are running under domain accounts. (Services running as **Local System**, **Local Service**, or **Network Service** do not interfere with image creation.)
4. Select a service that is running under a domain account, and then choose **Action**, **Properties**.
5. Open the **Log On** tab. Under **Log on as**, choose **Local System account**.
6. Choose **OK**.

The WorkSpace must be configured to use DHCP

You must configure all network adapters on the WorkSpace to use DHCP instead of static IP addresses.

To set all network adapters to use DHCP

1. In the Windows search box, enter **`control panel`** to open the Control Panel.
2. Choose **Network and Internet**.
3. Choose **Network and Sharing Center**.
4. Choose **Change adapter settings**, and select an adapter.
5. Choose **Change settings of this connection**.
6. On the **Networking** tab, select **Internet Protocol Version 4 (TCP/IPv4)**, and then choose **Properties**.
7. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select **Obtain an IP address automatically**.
8. Choose **OK**.
9. Repeat this process for all network adapters on the WorkSpace.

Remote Desktop Services must be enabled

The Create Image process requires Remote Desktop Services to be enabled.

To enable Remote Desktop Services

1. In the Windows search box, enter **`services.msc`** to open the Windows Services Manager.
2. In the **Name** column, find **Remote Desktop Services**.
3. Select **Remote Desktop Services**, and then choose **Action**, **Properties**.
4. On the **General** tab, for **Startup type**, choose **Manual** or **Automatic**.
5. Choose **OK**.

A user profile must exist

The WorkSpace that you're using to create images must have a user profile (`D:\Users\`*`username`*). If this test fails, contact the AWS Support Center for assistance.

The environment variable path must be properly configured

The environment variable path for the local machine is missing entries for System32 and for Windows PowerShell. These entries are required for Create Image to run.

To configure your environment variable path

1. In the Windows search box, enter **`environment variables`** and then choose **Edit the system environment variables**.
2. In the **System Properties** dialog box, open the **Advanced** tab, and choose **Environment Variables**.
3. In the **Environment Variables** dialog box, under **System variables**, select the **Path** entry and then choose **Edit**.
4. Choose **New**, and add the following path:

   ```
   C:\Windows\System32
   ```
5. Choose **New** again, and add the following path:

   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\
   ```
6. Choose **OK**.
7. Restart the WorkSpace.

> **Tip**
>
> The order in which items appear in the environment variable path matters. To determine the correct order, you might want to compare the environment variable path of your WorkSpace with one from a newly created WorkSpace or a new Windows instance.

Windows Modules Installer must be enabled

The Create Image process requires the Windows Modules Installer service to be enabled.

To enable the Windows Modules Installer service

1. In the Windows search box, enter **`services.msc`** to open the Windows Services Manager.
2. In the **Name** column, find **Windows Modules Installer**.
3. Select **Windows Modules Installer**, and then choose **Action**, **Properties**.
4. On the **General** tab, for **Startup type**, choose **Manual** or **Automatic**.
5. Choose **OK**.

Amazon SSM Agent must be disabled

The Create Image process requires the Amazon SSM Agent service to be disabled.

To disable the Amazon SSM Agent service

1. In the Windows search box, enter **`services.msc`** to open the Windows Services Manager.
2. In the **Name** column, find **Amazon SSM Agent**.
3. Select **Amazon SSM Agent**, and then choose **Action**, **Properties**.
4. On the **General** tab, for **Startup type**, choose **Disabled**.
5. Choose **OK**.

SSL3 and TLS version 1.2 must be enabled

To configure SSL/TLS for Windows, see How to Enable TLS 1.2 in the Microsoft Windows documentation.

Only one user profile can exist on the WorkSpace

There can be only one WorkSpaces user profile (`D:\Users\`*`username`*) on the WorkSpace that you're using to create images. Delete any user profiles that don't belong to the intended user of the WorkSpace.

For image creation to work, your WorkSpace can have only three user profiles on it:

- The user profile of the intended user of the WorkSpace (`D:\Users\`*`username`*)
- The default user profile (also known as Default Profile)
- The Administrator user profile

If there are additional user profiles, you can delete them through the advanced system properties in the Windows Control Panel.

To delete a user profile

1. To access the advanced system properties, do one of the following:
   - Press the **Windows key+Pause Break**, and then choose **Advanced system settings** in the left pane of the **Control Panel** > **System and Security** > **System** dialog box.
   - In the Windows search box, enter **`control panel`**. In the Control Panel, choose **System and Security**, then choose System, and then choose **Advanced system settings** in the left pane of the **Control Panel** > **System and Security** > **System** dialog box.
2. In the **System Properties** dialog box, on the **Advanced** tab, choose **Settings** under **User Profiles**.
3. If any profile is listed other than the Administrator profile, the Default Profile, and the profile of the intended WorkSpaces user, select that additional profile and choose **Delete**.
4. When asked if you want to delete the profile, choose **Yes**.
5. If necessary, repeat Steps 3 and 4 to remove any other profiles that don't belong on the WorkSpace.
6. Choose **OK** twice and close the Control Panel.
7. Restart the WorkSpace.

No AppX packages can be in a staged state

One or more AppX packages are in a staged state. This might cause a Sysprep error during image creation.

To remove all staged AppX packages

1. In the Windows search box, enter **`powershell`**. Choose **Run as Administrator**.
2. When asked "Do you want to allow this app to make changes to your device?", choose **Yes**.
3. In the Windows PowerShell window, enter the following commands to list all staged AppX packages, and press Enter after each one.

```
$workSpaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages |    Where-Object { `
                                 (($_.PackageUserInformation -like "*S-1-5-18*" -
and !($_.PackageUserInformation -like "*$workSpaceUserName*")) -and `
                                 ($_.PackageUserInformation -like "*Staged*" -or
 $_.PackageUserInformation -like "*Installed*")) -or `
                                 ((!($_.PackageUserInformation -like "*S-1-5-18*") -
and $_.PackageUserInformation -like "*$workSpaceUserName*") -and `
                                 $_.PackageUserInformation -like "*Staged*")
                                 }
```

4. Enter the following command to remove all staged AppX packages, and press Enter.

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. Run the Image Checker again. If this test still fails, enter the following commands to remove all AppX packages, and press Enter after each one.

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

Windows must not have been upgraded from a previous version

Image creation is not supported on Windows systems that have been upgraded from one version of Windows 10 to a newer version of Windows 10 (a Windows feature/version upgrade).

To create images, use a WorkSpace that has not undergone a Windows feature/version upgrade.

The Windows rearm count must not be 0

The rearm feature allows you to extend the activation period for the trial version of Windows. The Create Image process requires that the rearm count be a value other than 0.

To check the Windows rearm count

1. On the Windows **Start** menu, choose **Windows System**, then choose **Command Prompt**.
2. In the Command Prompt window, enter the following command, and then press Enter.

   ```
   cscript C:\Windows\System32\slmgr.vbs /dlv
   ```

To reset the rearm count to a value other than 0, see Sysprep (Generalize) a Windows installation in the Microsoft Windows documentation.

Other troubleshooting tips

If your WorkSpace passes all of the tests run by the Image Checker, but you are still unable to create an image from the WorkSpace, check for the following issues:

- Make sure that the WorkSpace isn't assigned to a user within a **Domain Guests** group. To check if there are any domain accounts, run the following PowerShell command.

  ```
  Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*
  $env:USERDOMAIN*" }
  ```

- For Windows 7 WorkSpaces only: If problems occur while the user profile is being copied during image creation, check for the following issues:
  - Long profile paths can cause image creation errors. Make sure that the paths of all folders within the user profile are less than 261 characters.
  - Make sure to grant full permissions on the profile folder to the system and all application packages.

  - If any files in the user profile are locked by a process or are in use during image creation, copying the profile might fail.
- Some Group Policy Objects (GPOs) restrict access to the RDP certificate thumbprint when it is requested by the EC2Config service or the EC2Launch scripts during Windows instance configuration. Before you try to create an image, move the WorkSpace to a new organizational unit (OU) with blocked inheritance and no GPOs applied.
- Make sure that the Windows Remote Management (WinRM) service is configured to start automatically. Do the following:
  1. In the Windows search box, enter **`services.msc`** to open the Windows Services Manager.
  2. In the **Name** column, find **Windows Remote Management (WS-Management)**.
  3. Select **Windows Remote Management (WS-Management)**, and then choose **Action**, **Properties**.
  4. On the **General** tab, for **Startup type**, choose **Automatic**.
  5. Choose **OK**.

Step 3: Create a custom image and custom bundle

After you have validated your WorkSpace image, you can proceed with creating your custom image and custom bundle.

To create a custom image and custom bundle

1. If you are still connected to the WorkSpace, disconnect by choosing **Amazon WorkSpaces** and **Disconnect** in the WorkSpaces client application.
2. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
3. In the navigation pane, choose **WorkSpaces**.
4. Select the WorkSpace to open its details page and choose **Create image**. If the status of the WorkSpace is **Stopped**, you must start it first (choose **Actions**, **Start WorkSpaces**) before you can choose **Actions**, **Create Image**.

   > **Note**
   >
   > To create an image programmatically, use the CreateWorkspaceImage API action. For more information, see CreateWorkspaceImage in the *Amazon WorkSpaces API Reference*.

5. A message displays, prompting you to reboot (restart) your WorkSpace before continuing. Rebooting your WorkSpace updates your Amazon WorkSpaces software to the latest version.

   Reboot your WorkSpace by closing the message and following the steps in Reboot a WorkSpace in WorkSpaces Personal. When you're done, repeat Step 4 of this procedure, but this time choose **Next** when the reboot message appears. To create an image, the status of the WorkSpace must be **Available** and its modification state must be **None**.

6. Enter an image name and a description that will help you identify the image, and then choose **Create Image**. While the image is being created, the status of the WorkSpace is **Suspended** and the WorkSpace is unavailable.

   > **Note**
   >
   > When entering an image description, make sure you don't use the special character "-" or you will get an error.

7. In the navigation pane, choose **Images**. The image is complete when the status of the WorkSpace changes to **Available** (this can take up to 45 minutes).

8. Select the image and choose **Actions**, **Create bundle**.

   > **Note**
   >
   > To create a bundle programmatically, use the **CreateWorkspaceBundle** API action. For more information, see CreateWorkspaceBundle in the *Amazon WorkSpaces API Reference*.

9. Enter a bundle name and a description, and then do the following:

   - For **Bundle hardware type**, choose the hardware to use when launching WorkSpaces from this custom bundle.
   - For **Storage settings**, select one of the default combinations for the root volume and user volume size, or select **Custom**, and then enter values (up to 2000 GB) for **Root volume size** and **User volume size**.

     The default available size combinations for the root volume (for Microsoft Windows, the C drive, for Linux, /) and the user volume (for Windows, the D drive; for Linux, /home) are as follows:

     - Root: 80 GB, User: 10 GB, 50 GB, or 100 GB

- Root: 175 GB, User: 100 GB
- For Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro WorkSpaces only: Root: 100 GB, User: 100 GB

Alternatively, you can expand the root and user volumes up to 2000 GB each.

> **Note**
>
> To ensure that your data is preserved, you cannot decrease the size of the root or user volumes after you launch a WorkSpace. Instead, make sure that you specify the minimum sizes for these volumes when launching a WorkSpace. You can launch a Value, Standard, Performance, Power, or PowerPro WorkSpace with a minimum of 80 GB for the root volume and 10 GB for the user volume. You can launch a Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro WorkSpace with a minimum of 100 GB for the root volume and 100 GB for the user volume.

10. Choose **Create bundle**.
11. To confirm that your bundle has been created, choose **Bundles** and verify that the bundle is listed.

What's included with Windows WorkSpaces custom images

When you create an image from a Windows 7, Windows 10, or Windows 11 WorkSpace, the entire contents of the C drive are included.

For Windows 10 or 11 WorkSpaces, the user profile in `D:\Users\`*`username`* is not included in the custom image.

For Windows 7 WorkSpaces, the entire contents of the user profile in `D:\Users\`*`username`* are included, except for the following:

- Contacts
- Downloads
- Music
- Pictures
- Saved games

- Videos
- Podcasts
- Virtual machines
- .virtualbox
- Tracing
- appdata\local\temp
- appdata\roaming\apple computer\mobilesync\
- appdata\roaming\apple computer\logs\
- appdata\roaming\apple computer\itunes\iphone software updates\
- appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\
- appdata\roaming\macromedia\flash player\#sharedobjects\
- appdata\roaming\adobe\flash player\assetcache\
- appdata\roaming\microsoft\windows\recent\
- appdata\roaming\microsoft\office\recent\
- appdata\roaming\microsoft office\live meeting
- appdata\roaming\microsoft shared\livemeeting shared\
- appdata\roaming\mozilla\firefox\crash reports\
- appdata\roaming\mcafee\common framework\
- appdata\local\microsoft\feeds cache
- appdata\local\microsoft\windows\temporary internet files\
- appdata\local\microsoft\windows\history\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\locallow\microsoft\internet explorer\iconcache\
- appdata\locallow\microsoft\internet explorer\domstore\
- appdata\locallow\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\recovery\
- appdata\local\mozilla\firefox\profiles\

What's included with Linux WorkSpace custom images

When you create an image from an Amazon Linux WorkSpace, the entire contents of the user volume (/home) are removed. The contents of the root volume (/) are included, except the following applicable folders and keys, which are removed:

- /tmp
- /var/spool/mail
- /var/tmp
- /var/lib/dhcp
- /var/lib/cloud
- /var/cache
- /var/backups
- /etc/sudoers.d
- /etc/udev/rules.d/70-persistent-net.rules
- /etc/network/interfaces.d/50-cloud-init.cfg
- /var/log/amazon/ssm
- /var/log/pcoip-agent
- /var/log/skylight
- /var/lock/.skylight.domain-join.lock
- /var/lib/skylight/domain-join-status
- /var/lib/skylight/configuration-data
- /var/lib/skylight/config-data.json
- /home
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan/zz-workspaces-domain.yaml
- /etc/netplan/yy-workspaces-base.yaml
- /var/lib/AccountsService/users

The following keys are shredded during custom image creation:

- /etc/ssh/ssh_host_*_key

- /etc/ssh/ssh_host_*_key.pub
- /var/lib/skylight/tls.*
- /var/lib/skylight/private.key
- /var/lib/skylight/public.key

Update a custom bundle for WorkSpaces Personal

You can update an existing custom WorkSpaces bundle by modifying a WorkSpace that is based on the bundle, creating an image from the WorkSpace, and updating the bundle with the new image. You can then launch new WorkSpaces using the updated bundle.

> **Important**
>
> Existing WorkSpaces aren't automatically updated when you update the bundle that they're based on. To update existing WorkSpaces that are based on a bundle that you've updated, you must either rebuild the WorkSpaces or delete and recreate them.

To update a bundle using the console

1. Connect to a WorkSpace that is based on the bundle and make the changes that you want. For example, you can apply the latest operating system and application patches and install additional applications.

   Alternatively, you can create a new WorkSpace with the same base software package (Plus or Standard) as the image used to create the bundle, and make changes.
2. If you are still connected to the WorkSpace, disconnect by choosing **Amazon WorkSpaces** and **Disconnect** in the WorkSpaces client application.
3. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
4. In the navigation pane, choose **WorkSpaces**.
5. Select the WorkSpace and choose **Actions**, **Create Image**. If the status of the WorkSpace is STOPPED, you must start it first (choose **Actions**, **Start WorkSpaces**) before you can choose **Actions**, **Create Image**.
6. Enter an image name and a description, and then choose **Create Image**. The WorkSpace is unavailable while the image is being created. For detailed information about the image creation process, see Create a custom WorkSpaces image and bundle for WorkSpaces Personal.

7. In the navigation pane, choose **Bundles**.
8. Choose the bundle to open its details page, and then under **Source image**, choose **Edit**.
9. On the **Update source image** page, select the image that you created and choose **Update bundle**.
10. As needed, update any existing WorkSpaces that are based on the bundle by rebuilding the WorkSpaces or deleting and recreating them. For more information, see Rebuild a WorkSpace in WorkSpaces Personal.

To update a bundle programmatically

To update a bundle programmatically, use the **UpdateWorkspaceBundle** API action. For more information, see UpdateWorkspaceBundle in the *Amazon WorkSpaces API Reference*.

Copy a custom image in WorkSpaces Personal

You can copy a custom WorkSpaces image within or across AWS Regions. Copying an image results in the creation of an identical image with its own unique identifier.

You can copy a Bring Your Own License (BYOL) image to another Region as long as the destination Region is enabled for BYOL. Ensure that BYOL is enabled for all accounts and Regions involved.

> **Note**
>
> In the China (Ningxia) Region, you can copy images only within the same Region.
> In the AWS GovCloud (US) Regions, to copy images to and from other AWS Regions, contact AWS Support.
> In Opt-in Regions, to copy images to other Regions, contact AWS Support. For more information about Opt-in Regions, see Available Regions.

You can also copy an image that has been shared with you by another AWS account. For more information about shared images, see Share or unshare a custom image in WorkSpaces Personal.

There are no additional charges for copying an image within or across Regions. However, the quota for the number of images in the destination Region applies. For more information about Amazon WorkSpaces quotas, see Amazon WorkSpaces quotas.

IAM Permissions to copy an image

If you use an IAM user to copy an image, the user must have permissions for `workspaces:DescribeWorkspaceImages` and `workspaces:CopyWorkspaceImage`.

The following example policy allows the user to copy the specified image to the specified account in the specified Region.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

Important

If you are creating an IAM policy for copying shared images for accounts that don't own the images, you cannot specify an account ID in the ARN. Instead, you must use * for the account ID, as shown in the following example policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
```

```
}
```

You can specify an account ID in the ARN only when that account owns the images to be copied.

For more information about working with IAM, see Identity and access management for WorkSpaces.

Bulk copy images

You can copy images one by one using the console. To bulk copy images, use the **CopyWorkspaceImage** API operation or the **copy-workspace-image** command in the AWS Command Line Interface (AWS CLI). For more information, see CopyWorkspaceImage in the *Amazon WorkSpaces API Reference* or see copy-workspace-image in the *AWS CLI Command Reference*.

Important

Before copying a shared image, be sure to verify that it has been shared from the correct AWS account. To determine if an image has been shared and to see the AWS account ID that owns an image, use the DescribeWorkSpaceImages and DescribeWorkspaceImagePermissions API operations or the describe-workspace-images and describe-workspace-image-permissions commands in the AWS CLI.

To copy an image using the console

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Images**.
3. Select the image and choose **Actions**, **Copy image**.
4. For **Select destination**, select the AWS Region that you want to copy the image to.
5. For **Name of the copy**, enter the new name for the copied image, and for **Description**, enter a description for the copied image.
6. (Optional) Under **Tags**, enter tags for the copied image. For more information, see Tag resources in WorkSpaces Personal.
7. Choose **Copy image**.

Share or unshare a custom image in WorkSpaces Personal

You can share custom WorkSpaces images across AWS accounts within the same AWS Region. After an image has been shared, the recipient account can copy the image to other AWS Regions as needed. For more information about copying images, see Copy a custom image in WorkSpaces Personal.

> **Note**
>
> In the China (Ningxia) Region, you can copy images only within the same Region.
> In the AWS GovCloud (US) Regions, to copy images to and from other AWS Regions, contact AWS Support.

There are no additional charges for sharing an image. However, the quota for the number of images in the AWS Region applies. A shared image doesn't count against the recipient account's quota until the recipient copies the image. For more information about Amazon WorkSpaces quotas, see Amazon WorkSpaces quotas.

To delete a shared image, you must unshare the image before you can delete it.

Share Bring Your Own License images

You can share Bring Your Own License (BYOL) images only with AWS accounts that are enabled for BYOL. The AWS account that you want to share BYOL images with must also be part of your organization (under the same payer account).

> **Note**
>
> Sharing BYOL images across AWS accounts isn't supported at this time in the AWS GovCloud (US-West) and AWS GovCloud (US-East) Regions. To share BYOL images across accounts in the AWS GovCloud (US-West) and AWS GovCloud (US-East) Regions, contact AWS Support.

Images shared with you

If images are shared with you, you can copy them. You can then use your copies of the shared images to create bundles for launching new WorkSpaces.

Important

Before copying a shared image, be sure to verify that it has been shared from the correct AWS account. To programmatically determine if an image has been shared, use the DescribeWorkSpaceImages and DescribeWorkspaceImagePermissions API operations or the describe-workspace-images and describe-workspace-image-permissions commands in the AWS command line interface (CLI).

The creation date shown for an image that has been shared with you is the date that the image was originally created, not the date that the image was shared with you.

If an image has been shared with you, you can't further share that image with other accounts.

To share an image

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Images**.
3. Choose the image to open its details page.
4. On the image detail page, in the **Shared accounts** section, choose **Add account**.
5. On the **Add account** page, under **Add account to share with**, enter the account ID of the account that you want to share the image with.

   Important

   Before sharing the image, confirm that you are sharing to the correct AWS account ID.

6. Choose **Share image**.

   Note

   To use the shared image, the recipient account must first copy the image. The recipient account can then use its copy of the shared image to create bundles for launching new WorkSpaces.

To stop sharing an image

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Images**.
3. Choose the image to open its details page.
4. On the image detail page, in the **Shared accounts** section, select the AWS account that you want to stop sharing with, and then choose **Unshare**.
5. When prompted to confirm unsharing the image, choose **Unshare**.

> **Note**
>
> If you want to delete the image after unsharing it, you must first unshare it from all of the accounts that it has been shared with.

After you stop sharing an image, the recipient account can no longer make copies of the image. However, any copies of shared images that are already in the recipient account remain in that account, and new WorkSpaces can be launched from those copies.

To share or unshare images programmatically

To share or unshare images programmatically, use the UpdateWorkspaceImagePermission API operation or the update-workspace-image-permission AWS Command Line Interface (AWS CLI) command. To determine if an image has been shared, use the DescribeWorkspaceImagePermissions API operation or the describe-workspace-image-permissions CLI command.

Delete a custom bundle or image in WorkSpaces Personal

You can delete unused custom bundles or custom images as needed.

Delete a bundle

To delete a bundle, you must first delete all of the WorkSpaces that are based on the bundle.

To delete a bundle using the console

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Bundles**.
3. Select the bundle and choose **Delete**.

4. When prompted for confirmation, choose **Delete**.

To delete a bundle programmatically

To delete a bundle programmatically, use the **DeleteWorkspaceBundle** API action. For more information, see DeleteWorkspaceBundle in the *Amazon WorkSpaces API Reference*.

> **Note**
>
> Ensure you wait at least 2 hours after deleting a bundle before creating a new bundle with the same name.

Delete an image

After you delete a custom bundle, you can delete the image that you used to create or update the bundle.

To delete an image, you must first either delete any bundles that are associated with the image, or you must update those bundles to use another source image. You must also unshare the image if it is shared with other accounts. The image also can't be in the **Pending** or **Validating** state.

To delete an image using the console

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Images**.
3. Select the image and choose **Delete**.
4. When prompted for confirmation, choose **Delete**.

To delete an image programmatically

To delete an image programmatically, use the **DeleteWorkspaceImage** API action. For more information, see DeleteWorkspaceImage in the *Amazon WorkSpaces API Reference*.

Monitor WorkSpaces Personal

You can use the following features to monitor your WorkSpaces.

CloudWatch metrics

Amazon WorkSpaces publishes data points to Amazon CloudWatch about your WorkSpaces. CloudWatch enables you to retrieve statistics about those data points as an ordered set of time-series data, known as *metrics*. You can use these metrics to verify that your WorkSpaces are performing as expected. For more information, see Monitor your WorkSpaces using CloudWatch metrics.

CloudWatch Events

Amazon WorkSpaces can submit events to Amazon CloudWatch Events when users log in to your WorkSpace. This enables you to respond when the event occurs. For more information, see Monitor your WorkSpaces using Amazon EventBridge.

CloudTrail logs

AWS CloudTrail provides a record of actions taken by a user, role, or an AWS service in WorkSpaces. Using the information collected by CloudTrail, you can determine the request that was made to WorkSpaces, the IP address from which the request was made, who made the request, when it was made, and additional details. For more information, see Logging WorkSpaces API Calls by Using CloudTrail. AWS CloudTrail logs successful and unsuccessful sign-in events for smart card users. For more information, see Understanding AWS sign-in events for smart card users.

CloudWatch Internet Monitor

Amazon CloudWatch Internet Monitor provides visibility into how internet issues impact the performance and availability between your applications hosted on AWS and your end users. You can also use CloudWatch Internet Monitor to:

- Create monitors for one or more WorkSpace directories.
- Monitor internet performance.
- Get alarms for issues between your end users' city-network, including its location and ASN, which is typically the Internet Service Provider (ISP), and their WorkSpace Regions.

Internet Monitor uses the connectivity data that AWS captures from its global networking footprint to calculate a baseline of performance and availability for internet-facing traffic. Internet Monitor currently can't provide internet performance for individual end user but it can at city and ISP level.

Amazon S3 Access Logs

If your users have application settings data or home folders data stored in Amazon S3 buckets, consider viewing Amazon S3 server access logs to monitor access. These logs provide detailed records about requests that are made to a bucket. Server access logs are useful for many applications. For example, access log information can be useful in security and access audits. For more information, see Amazon S3 Server Access Logging in the *Amazon Simple Storage Service User Guide*.

Monitor your WorkSpaces health using the CloudWatch automatic dashboard

You can monitor WorkSpaces using CloudWatch automatic dashboard, which collects raw data and processes it into readable, near real-time metrics. The metrics are kept for 15 months to access historical information and to monitor the performance of your web application or service. You can also set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see the Amazon CloudWatch User Guide.

The CloudWatch dashboard is automatically created when you use your AWS account to configure your WorkSpaces. The dashboard allows you to monitor your WorkSpaces metrics, such as their health and performance, across Regions. You can also use the dashboard for the following purposes:

- Identify unhealthy WorkSpace instances.
- Identify running modes, protocols, and operating systems that have unhealthy WorkSpace instances.
- View critical resource utilization over time.
- Identify anomalies to help with troubleshooting.

WorkSpaces CloudWatch automatic dashboards are available in all AWS commercial Regions.

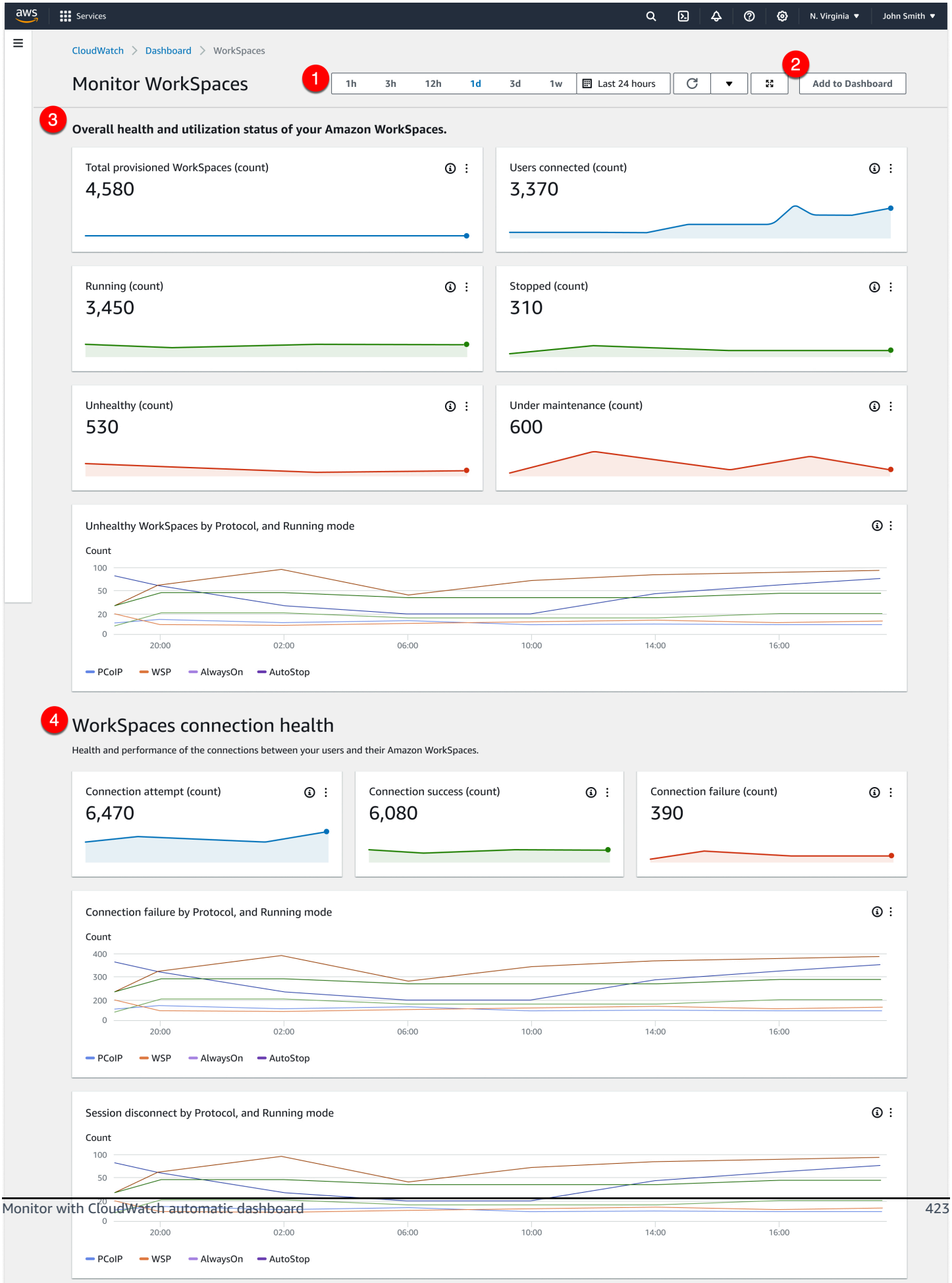
To use the WorkSpaces CloudWatch automatic dashboard

1. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
2. In the navigation pane, choose **Dashboards**.
3. Choose the **Automatic dashboards** tab.

4. Choose **WorkSpaces**.

Understanding your WorkSpaces CloudWatch automatic dashboard

The CloudWatch automatic dashboard allows you to gain insight into the performance of your WorkSpaces resources and helps you identify performance issues.


aws
Services
N. Virginia
John Smith
CloudWatch
Dashboard
WorkSpaces
Monitor WorkSpaces
1
1h
3h
12h
1d
3d
1w
Last 24 hours
2
Add to Dashboard
3
Overall health and utilization status of your Amazon WorkSpaces.
Total provisioned WorkSpaces (count)
4,580
Users connected (count)
3,370
Running (count)
3,450
Stopped (count)
310
Unhealthy (count)
530
Under maintenance (count)
600
Unhealthy WorkSpaces by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
4
WorkSpaces connection health
Health and performance of the connections between your users and their Amazon WorkSpaces.
Connection attempt (count)
6,470
Connection success (count)
6,080
Connection failure (count)
390
Connection failure by Protocol, and Running mode
Count
400
300
200
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
Session disconnect by Protocol, and Running mode
Count
100
50
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop

The dashboard consists of the following features:

1. View historical data using time and date range controls.
2. Add customized dashboard view to the CloudWatch custom dashboards.
3. Monitor the overall health and utilization status of your WorkSpaces by doing the following:
    a. View the total number of provisioned WorkSpaces, number of users connected, number of unhealthy and healthy WorkSpace instances.
    b. View unhealthy WorkSpaces and their different variables, such as protocol and compute mode.
    c. Hover over the line chart to view the number of healthy or unhealthy WorkSpace instances for a specific protocol and running mode over a period of time.
    d. Choose the ellipsis menu, then choose **View in metrics** to view the metrics on a time scale chart.
4. View your connection metrics and their different variables, such as number of connection attempts, successful connections, and failed connections in your WorkSpaces environment at any given time.
5. View InSession latencies that impact your user's experience, such as round trip time (RTT), to determine connection health and packet loss to monitor network health.
6. View host performance and resource utilization to identify and troubleshoot potential performance issues.

Monitor your WorkSpaces using CloudWatch metrics

WorkSpaces and Amazon CloudWatch are integrated, so you can gather and analyze performance metrics. You can monitor these metrics using the CloudWatch console, the CloudWatch command line interface, or programmatically using the CloudWatch API. CloudWatch also allows you to set alarms when you reach a specified threshold for a metric.

For more information about using CloudWatch and alarms, see the Amazon CloudWatch User Guide.

Prerequisites

To get CloudWatch metrics, enable access on port 443 on the `AMAZON` subset in the `us-east-1` Region. For more information, see IP address and port requirements for WorkSpaces Personal.

Contents

WorkSpaces metrics

The AWS/WorkSpaces namespace includes the following metrics.

Metric	Description	Dimensions	Statistics	Units
Available [1]	The number of WorkSpaces that returned a healthy status.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Sum, Maximum, Minimum, Data Samples	Count
Unhealthy [1]	The number of WorkSpaces that returned an unhealthy status.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Sum, Maximum, Minimum, Data Samples	Count

Metric	Description	Dimensions	Statistics	Units
ConnectionAttempt [2]	The number of connection attempts.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Sum, Maximum, Minimum, Data Samples	Count
ConnectionSuccess [2]	The number of successful connections.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Sum, Maximum, Minimum, Data Samples	Count

Metric	Description	Dimensions	Statistics	Units
ConnectionFailure [2]	The number of failed connections.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Sum, Maximum, Minimum, Data Samples	Count
SessionLaunchTime [2,6]	The amount of time it takes to initiate a WorkSpaces session.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Sum, Maximum, Minimum, Data Samples	Second (time)

Metric	Description	Dimensions	Statistics	Units
InSessionLatency [2,6]	The round trip time between the WorkSpaces client and the WorkSpace.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Sum, Maximum, Minimum, Data Samples	Millisecond (time)
SessionDisconnect [2,6]	The number of connections that were closed, including user-initiated and failed connections.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Sum, Maximum, Minimum, Data Samples	Count

Metric	Description	Dimensions	Statistics	Units
UserConnected [3]	The number of WorkSpaces that have a user connected.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Sum, Maximum, Minimum, Data Samples	Count
Stopped	The number of WorkSpaces that are stopped.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Sum, Maximum, Minimum, Data Samples	Count

Metric	Description	Dimensions	Statistics	Units
Maintenance [4]	The number of WorkSpaces that are under maintenance.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Sum, Maximum, Minimum, Data Samples	Count
TrustedDeviceValidationAttempt [5,6]	The number of device authentication signature validation attempts.	DirectoryId	Average, Sum, Maximum, Minimum, Data Samples	Count
TrustedDeviceValidationSuccess [5,6]	The number of successful device authentication signature validations.	DirectoryId	Average, Sum, Maximum, Minimum, Data Samples	Count
TrustedDeviceValidationFailure [5,6]	The number of failed device authentication signature validations.	DirectoryId	Average, Sum, Maximum, Minimum, Data Samples	Count

Metric	Description	Dimensions	Statistics	Units
TrustedDeviceCertificateDaysBeforeExpiration [6]	Days left before the root certificate associated with the directory is expired.	CertificateId	Average, Sum, Maximum, Minimum, Data Samples	Count
CPUUsage	The percentage of the CPU resource used.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Maximum, Minimum	Percentage
MemoryUsage	The percentage of the machine memory used.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Maximum, Minimum	Percentage

Metric	Description	Dimensions	Statistics	Units
RootVolumeDiskUsage	The percentage of the root disk volume used.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Maximum, Minimum	Percentage
UserVolumeDiskUsage	The percentage of the user disk volume used.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Maximum, Minimum	Percentage

Metric	Description	Dimensions	Statistics	Units
UDPPacketLossRate [7]	The percentage of packets dropped between the client and the gateway.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Maximum, Minimum, Data Samples	Percentage
UpTime	The time since the last reboot of a WorkSpace.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average, Maximum, Minimum, Data Samples	Seconds

[1] WorkSpaces periodically sends status requests to a WorkSpace. A WorkSpace is marked `Available` when it responds to these requests, and `Unhealthy` when it fails to respond to these requests. These metrics are available at a per-WorkSpace level of granularity, and also aggregated for all WorkSpaces in an organization.

[2] WorkSpaces records metrics on connections made to each WorkSpace. These metrics are emitted after a user has successfully authenticated via the WorkSpaces client and the client then initiates a session. The metrics are available at a per-WorkSpace level of granularity, and also aggregated for all WorkSpaces in a directory.

[3] WorkSpaces periodically sends connection status requests to a WorkSpace. Users are reported as connected when they are actively using their sessions. This metric is available at a per-WorkSpace level of granularity, and is also aggregated for all WorkSpaces in an organization.

[4] This metric applies to WorkSpaces that are configured with an AutoStop running mode. If you have maintenance enabled for your WorkSpaces, this metric captures the number of WorkSpaces that are currently under maintenance. This metric is available at a per-WorkSpace level of granularity, which describes when a WorkSpace went into maintenance and when it was removed.

[5] If the trusted devices feature is enabled for the directory, Amazon WorkSpaces uses certificate-based authentication to determine whether a device is trusted. When users attempt to access their WorkSpaces, these metrics are emitted to indicate successful or failed trusted device authentication. These metrics are available at a per-directory level of granularity, and only for the Amazon WorkSpaces Windows and macOS client applications.

[6] Not available on WorkSpaces Web Access.

[7] This metric measures average packet loss.

- **On PCoIP**: Measures average UDP packet loss from client to gateway.

  > **Note**
  >
  > This is measured at the gateway.

- **On WSP**: Measures UDP packet loss from gateway to client.

  > **Note**
  >
  > This is measured at the gateway.

Dimensions for WorkSpaces metrics

To filter the metric data, use the following dimensions.

Dimension	Description
`DirectoryId`	Filters the metric data to the WorkSpaces in the specified directory. The form of the directory ID is `d-XXXXXXXXXX` .
`WorkspaceId`	Filters the metric data to the specified WorkSpace. The form of the WorkSpace ID is `ws-XXXXXXXXXX` .
`CertificateId`	Filters the metric data to the specified root certificate associated with the directory. The form of the certificate ID is `wsc-XXXXXXXXX` .
`RunningMode`	Filters the metric data to the WorkSpaces by their running mode. The form of the running mode is AutoStop or AlwaysOn.
`BundleId`	Filters the metric data to the WorkSpaces by the protocol. The form of the bundle is `wsb-XXXXXXXXXX` .
`ComputeType`	Filters the metric data to the WorkSpaces by the compute type.
`Protocol`	Filters the metric data to the WorkSpaces by the protocol type.
`UserName`	Filters the metric data to the WorkSpaces by the user's name. **Note** The `UserName` cannot consist of non-ASCII characters, such as the following: • Accented letters: é, à, ö, ñ, etc. • Non-Latin alphabets

Dimension	Description
	• Symbols: ©#, ®#, €, £, µ, ¥, etc.

Monitoring example

The following example demonstrates how you can use the AWS CLI to respond to a CloudWatch alarm and determine which WorkSpaces in a directory have experienced connection failures.

To respond to a CloudWatch alarm

1. Determine which directory the alarm applies to using the describe-alarms command.

```
aws cloudwatch describe-alarms --state-value "ALARM"

{
  "MetricAlarms": [
    {
      ...
      "Dimensions": [
        {
          "Name": "DirectoryId",
          "Value": "directory_id"
        }
      ],
      ...
    }
  ]
}
```

2. Get the list of WorkSpaces in the specified directory using the describe-workspaces command.

```
aws workspaces describe-workspaces --directory-id directory_id

{
  "Workspaces": [
    {
      ...
      "WorkspaceId": "workspace1_id",
      ...
    },
```

```
    {
      ...
      "WorkspaceId": "workspace2_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace3_id",
      ...
    }
  ]
}
```

3. Get the CloudWatch metrics for each WorkSpace in the directory using the get-metric-statistics command.

```
aws cloudwatch get-metric-statistics \
--namespace AWS/WorkSpaces \
--metric-name ConnectionFailure \
--start-time 2015-04-27T00:00:00Z \
--end-time 2015-04-28T00:00:00Z \
--period 3600 \
--statistics Sum \
--dimensions "Name=WorkspaceId,Value=workspace_id"

{
  "Datapoints" : [
    {
      "Timestamp": "2015-04-27T00:18:00Z",
      "Sum": 1.0,
      "Unit": "Count"
    },
    {
      "Timestamp": "2014-04-27T01:18:00Z",
      "Sum": 0.0,
      "Unit": "Count"
    }
  ],
  "Label" : "ConnectionFailure"
}
```

Monitor your WorkSpaces using Amazon EventBridge

You can use events from Amazon WorkSpaces to view, search, download, archive, analyze, and respond to successful logins to your WorkSpaces. For example, you can use events for the following purposes:

- Store or archive WorkSpaces login events as logs for future reference, analyze the logs to look for patterns, and take action based on those patterns.
- Use the WAN IP address to determine where users are logged in from, and then use policies to allow users access only to files or data from WorkSpaces that meet the access criteria found in the event type of `WorkSpaces Access`.
- Analyze login data and perform automated actions using AWS Lambda.
- Use policy controls to block access to files and applications from unauthorized IP addresses.
- Find out the WorkSpaces client version used to connect to WorkSpaces.

Amazon WorkSpaces emits these events on a best-effort basis. Events are delivered to EventBridge in near real time. With EventBridge, you can create rules that trigger programmatic actions in response to an event. For example, you can configure a rule that invokes an SNS topic to send an email notification or invokes a Lambda function to take some action. For more information, see the Amazon EventBridge User Guide.

WorkSpaces Access events

WorkSpaces client applications send `WorkSpaces Access` events when a user successfully logs in to a WorkSpace. All WorkSpaces clients send these events.

Events emitted for WorkSpaces using the WorkSpaces Streaming Protocol (WSP) require the WorkSpaces client application version 4.0.1 or later.

Events are represented as JSON objects. The following is example data for a `WorkSpaces Access` event.

```
{
    "version": "0",
    "id": "64ca0eda-9751-dc55-c41a-1bd50b4fc9b7",
    "detail-type": "WorkSpaces Access",
    "source": "aws.workspaces",
    "account": "123456789012",
```

```
    "time": "2023-04-05T16:13:59Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "clientIpAddress": "192.0.2.3",
        "actionType": "successfulLogin",
        "workspacesClientProductName": "WorkSpacesWebClient",
        "loginTime": "2023-04-05T16:13:37.603Z",
        "clientPlatform": "Windows",
        "directoryId": "domain/d-123456789",
        "clientVersion": "5.7.0.3472",
        "workspaceId": "ws-xyskdga"
    }
}
```

Event-specific fields

`clientIpAddress`

The WAN IP address of the client application. For PCoIP zero clients, this is the IP address of the Teradici auth client.

`actionType`

This value is always `successfulLogin`.

`workspacesClientProductName`

The following values are case-sensitive.

- `WorkSpaces Desktop client` — Windows, macOS, and Linux clients
- `Amazon WorkSpaces Mobile client` — iOS client
- `WorkSpaces Mobile Client` — Android clients
- `WorkSpaces Chrome Client` — Chromebook client
- `WorkSpacesWebClient` — Web Access client
- `AmazonWorkSpacesThinClient` — Amazon WorkSpaces Thin Client device
- `Teradici PCoIP Zero Client, Teradici PCoIP Desktop Client, or Dell Wyse PCoIP Client` — Zero Client

`loginTime`

The time at which the user logged in to the WorkSpace.

`clientPlatform`

- `Android`
- `Chrome`
- `iOS`
- `Linux`
- `OSX`
- `Windows`
- `Teradici PCoIP Zero Client and Tera2`
- `Web`

`directoryId`

The identifier of the directory for the WorkSpace. You must prepend the directory identifier with `domain/`. For example, `"domain/d-123456789"`.

`clientVersion`

The client version used to connect to WorkSpaces.

`workspaceId`

The identifier of the WorkSpace.

Create a rule to handle WorkSpaces events

Use the following procedure to create a rule to handle the WorkSpaces events.

Prerequisite

To receive email notifications, create an Amazon Simple Notification Service topic.

1. Open the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
2. In the navigation pane, choose **Topics**.
3. Choose **Create topic**.
4. For **Type**, choose **Standard**.
5. For **Name**, enter a name for your topic.

6. Choose **Create topic**.
7. Choose **Create subscription**.
8. For **Protocol**, choose **Email**.
9. For **Endpoint**, enter the email address that receives the notifications.
10. Choose **Create subscription**.
11. You'll receive an email message with the following subject line: AWS Notification - Subscription Confirmation. Follow the directions to confirm your subscription.

To create a rule to handle WorkSpaces events

1. Open the Amazon EventBridge console at https://console.aws.amazon.com/events/.
2. Choose **Create rule**.
3. For **Name**, enter a name for your rule.
4. For **Rule type**, choose **Rule with an event pattern**.
5. Choose **Next**.
6. For **Event pattern**, do the following:
    a. For **Event source**, choose **AWS services**.
    b. For **AWS service**, choose **WorkSpaces**.
    c. For **Event type**, choose **WorkSpaces Access**.
    d. By default, we send notifications for every event. If you prefer, you can create an event pattern that filters events for specific clients or workspaces.
7. Choose **Next**.
8. Specify a target as follows:
    a. For **Target types**, choose **AWS service**.
    b. For **Select a target**, choose **SNS topic**.
    c. For **Topic**, choose the SNS topic that you created for notifications.
9. Choose **Next**.
10. (Optional) Add tags to your rule.
11. Choose **Next**.
12. Choose **Create rule**.

Understanding AWS sign-in events for smart card users

AWS CloudTrail logs successful and unsuccessful sign-in events for smart card users. This includes sign-in events that are captured each time a user is prompted to solve a specific credential challenge or factor, as well as the status of that particular credential verification request. A user is signed in only after completing all required credential challenges, which results in a `UserAuthentication` event being logged.

The following table captures each of the sign-in CloudTrail event names and their purposes.

Event name	Event purpose
`CredentialChallenge`	Notifies that AWS sign-in has requested that the user solve a specific credential challenge and specifies the `CredentialType` that is required (for example, SMARTCARD).
`CredentialVerification`	Notifies that the user has attempted to solve a specific `CredentialChallenge` request, and specifies whether that credential has succeeded or failed.
`UserAuthentication`	Notifies that all authentication requirements that the user was challenged with have been successfully completed and that the user was successfully signed in. When users fail to successfully complete the required credential challenges, no `UserAuthentication` event is logged.

The following table captures additional useful event data fields contained within specific sign-in CloudTrail events.

Event name	Event purpose	Sign-in event applicability	Example values
`AuthWorkflowID`	Correlates all events emitted across an entire sign-in sequence. For each user sign-in,	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	"AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83"

Event name	Event purpose	Sign-in event applicability	Example values
	multiple events can be emitted by AWS sign-in.		
`CredentialType`	Notifies that the user has attempted to solve a specific `CredentialChallenge` request and specifies whether that credential has succeeded or failed.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	CredentialType": "SMARTCARD" (possible values today: SMARTCARD)
`LoginTo`	Notifies that all authentication requirements that the user was challenged with have been successfully completed and that the user was successfully signed in. When users fail to successfully complete the required credential challenges, no `UserAuthentication` event is logged.	`UserAuthentication`	"LoginTo": "https://skylight.local“

Example events for AWS sign-in scenarios

The following examples show the expected sequence of CloudTrail events for different sign-in scenarios.

Contents

Successful sign-in when authenticating with smart card

The following sequence of events captures an example of a successful smart card sign-in.

CredentialChallenge


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:29Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "65551a6d-654a-4be8-90b5-bbfef7187d3a",
    "eventID": "fb603838-f119-4304-9fdc-c0f947a82116",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```

Successful CredentialVerification


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "84c0a2ff-413f-4d0f-9108-f72c90a41b6c",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Success"
    }
}
```


Successful UserAuthentication


```
{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "UserAuthentication",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "LoginTo": "https://skylight.local",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "acc0dba8-8e8b-414b-a52d-6b7cd51d38f6",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        UserAuthentication": "Success"
    }
}
```


Failed sign-in when authenticating with only a smart card

The following sequence of events captures an example of failed smart card sign-in.

CredentialChallenge


```
{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:06Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awaRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "73eb499d-91a8-4c18-9c5d-281fd45ab50a",
    "eventID": "f30a50ec-71cf-415a-a5ab-e287edc800da",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```


Failed CredentialVerification


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
```

```
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:13Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "051ca316-0b0d-4d38-940b-5fe5794fda03",
    "eventID": "4e6fbfc7-0479-48da-b7dc-e875155a8177",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Failure"
    }
}
```


Create custom CloudWatch dashboards using AWS CloudFormation templates

AWS provides AWS CloudFormation templates that you can use to create custom CloudWatch dashboards for WorkSpaces. Choose from the following AWS CloudFormation template options to create custom dashboards for your WorkSpaces in the AWS CloudFormation console.

Considerations before getting started

Consider the following before you get started with custom CloudWatch dashboards:

- Create your dashboards in the same AWS Region as the deployed WorkSpaces you want to monitor.

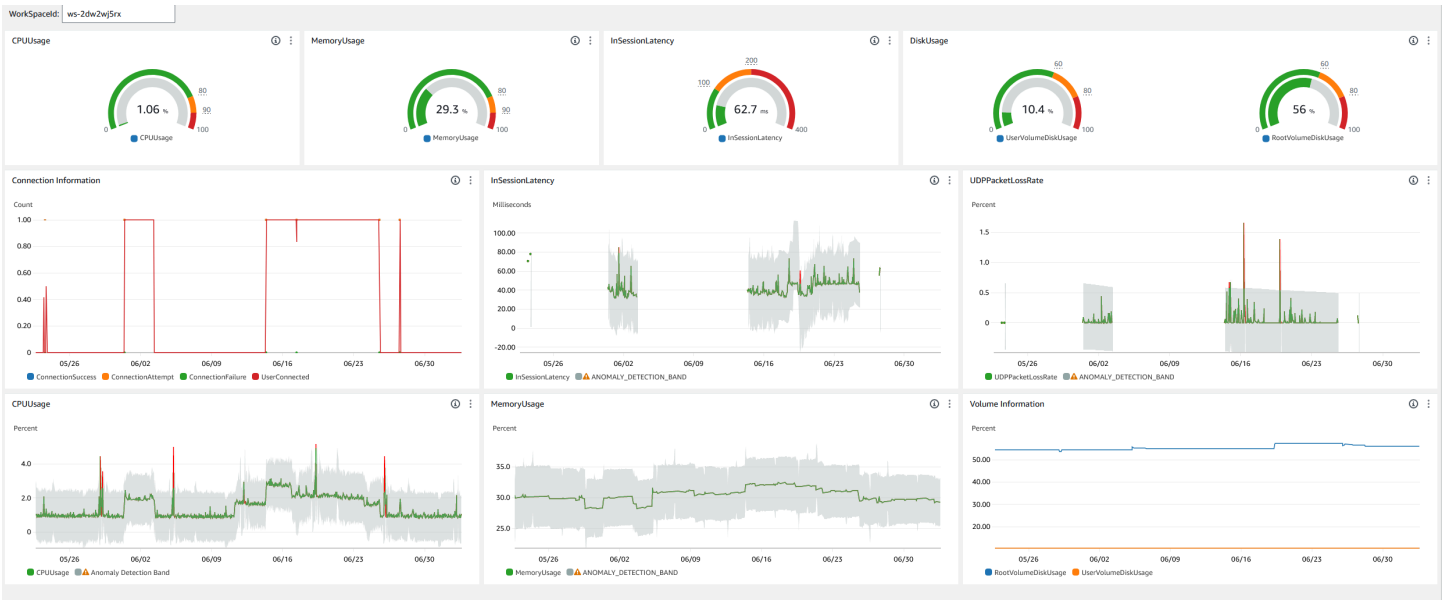
- You can also create custom dashboards using the CloudWatch console.
- A cost might be associated with custom CloudWatch dashboards. For information about pricing, see Amazon CloudWatch Pricing

Help Desk dashboard

The Help Desk dashboard displays the following metrics for a specific WorkSpace:

- CPU usage
- Memory usage
- In-session latency
- Root volume
- User volume
- Packet loss
- Disk usage

Following is an example of the Help Desk dashboard.



Complete the following procedure to create a custom dashboard in CloudWatch using AWS CloudFormation.

1. Open the Create Stack page in the AWS CloudFormation console. This link opens the page with the Amazon S3 bucket location of the Help Desk custom CloudWatch dashboard template pre-populated.
2. Review the default selections on the **Create Stack** page. Note that the **Amazon S3 URL** field is pre-populated with the Amazon S3 bucket location of the AWS CloudFormation template.
3. Choose **Next**.
4. In the **Stack name** text box, enter the name of the stack.

   The stack name is an identifier that helps you find a particular stack from a list of stacks. A stack name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 128 characters.
5. In the **DashboardName** text box, enter the name you want to give your dashboard.

   The dashboard name can contain only alphanumerics, dash (–), and underscore (_).
6. Choose **Next**.
7. Review the default selections on the **Configure stack options** page, and choose **Next**.
8. Scroll down to **Transforms might require access capabilities** and check the boxes for acknowledgement. Then choose **Submit** to create the stack and the custom CloudWatch dashboard.

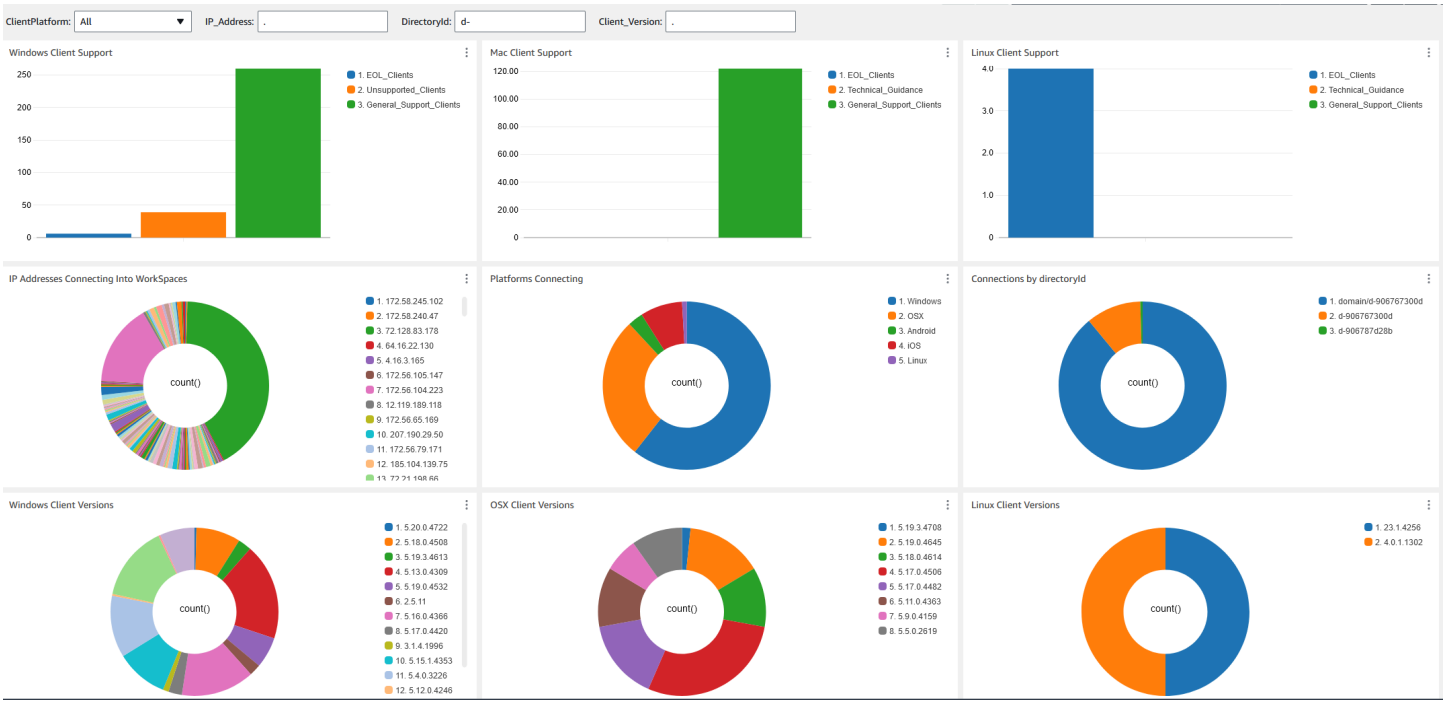
   > **Important**
   >
   > A cost might be associated with custom CloudWatch dashboards. For information about pricing, see Amazon CloudWatch Pricing
9. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
10. In the left navigation bar, choose **Dashboards**.
11. Under **Custom Dashboards**, choose the dashboard with the dashboard name you entered earlier in this procedure.
12. Using the Help Desk sample template, enter the WorkSpaceId to monitor its data.

Connection Insights dashboard

The Connection Insights dashboard displays the client versions, platforms, and IP addresses that are connected to your WorkSpaces. This dashboard allows you to better understand how your users

are connecting so that you can proactively notify your users using an outdated client. The dynamic variables allows you to monitor the details of IP addresses or specific directories.

Following is an example of the Connection Insights dashboard.



Complete the following procedure to create a custom dashboard in CloudWatch using AWS CloudFormation.

1. Open the Create Stack page in the AWS CloudFormation console. This link opens the page with the Amazon S3 bucket location of the Connection Insights custom CloudWatch dashboard template pre-populated.
2. Review the default selections on the **Create Stack** page. Note that the **Amazon S3 URL** field is pre-populated with the Amazon S3 bucket location of the AWS CloudFormation template.
3. Choose **Next**.
4. In the **Stack name** text box, enter the name of the stack.

   The stack name is an identifier that helps you find a particular stack from a list of stacks. A stack name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 128 characters.
5. In the **DashboardName** text box, enter the name you want to give your dashboard. Enter other relevant CloudWatch access group setup information.

   The dashboard name can contain only alphanumerics, dash (–), and underscore (_).

6. Under **LogRetention**, enter the number of days you want to retain your LogGroup for.
7. Under **SetupEventBridge**, choose whether you want to deploy the EventBridge rule to get WorkSpaces access logs.
8. Under **WorkSpaceAccessLogsName**, enter the name of the CloudWatch LogGroup that has the WorkSpaces access logs.
9. Choose **Next**.
10. Review the default selections on the **Configure stack options** page, and choose **Next**.
11. Scroll down to **Transforms might require access capabilities** and check the boxes for acknowledgement. Then choose **Submit** to create the stack and the custom CloudWatch dashboard.

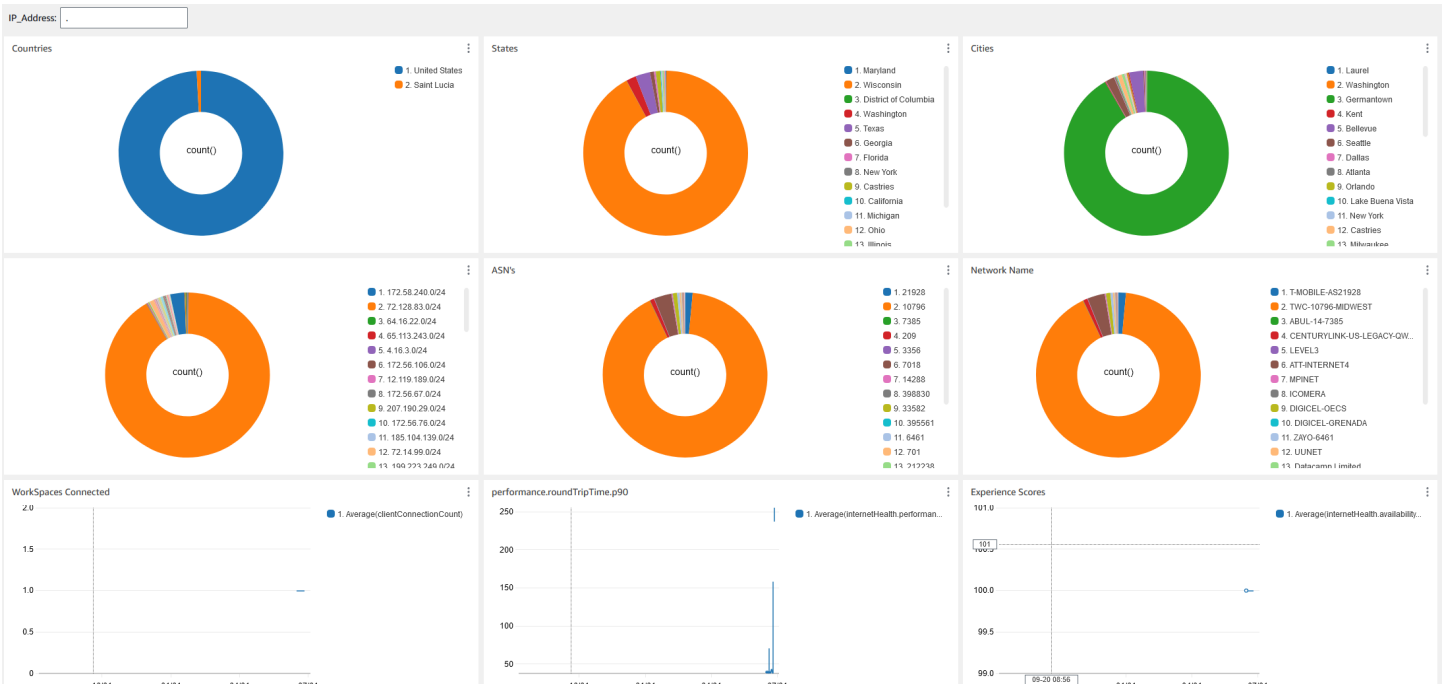
> **Important**
>
> A cost might be associated with custom CloudWatch dashboards. For information about pricing, see Amazon CloudWatch Pricing

12. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
13. In the left navigation bar, choose **Dashboards**.
14. Under **Custom Dashboards**, choose the dashboard with the dashboard name you entered earlier in this procedure.
15. You can now monitor you WorkSpace's data using the Connection Insights dashboard.

Internet Monitoring dashboard

The Internet Monitoring dashboard displays details about the Internet Service Provider (ISP) that your users are using to join their WorkSpaces instances. It provides details on the city, state, ASN, network name, number of connected WorkSpaces, performance, and experience scores. You can also use specific IP addresses to get the details of your users connecting from a specific location. Deploy CloudWatch internet monitor to get ISP data information. For more information, see Using Amazon CloudWatch Internet Monitor.

Following is an example of the Internet Monitoring dashboard.



To create a custom dashboard in CloudWatch using AWS CloudFormation

> **Note**
>
> Before creating a custom dashboard, make sure you create an Internet Monitor with CloudWatch Internet Monitor. For more information, see Creating a monitor in Amazon CloudWatch Internet Monitor using the console

1. Open the Create Stack page in the AWS CloudFormation console. This link opens the page with the Amazon S3 bucket location of the Internet Monitoring custom CloudWatch dashboard template pre-populated.
2. Review the default selections on the **Create Stack** page. Note that the **Amazon S3 URL** field is pre-populated with the Amazon S3 bucket location of the AWS CloudFormation template.
3. Choose **Next**.
4. In the **Stack name** text box, enter the name of the stack.

   The stack name is an identifier that helps you find a particular stack from a list of stacks. A stack name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 128 characters.

5. In the **DashboardName** text box, enter the name you want to give your dashboard. Enter other relevant CloudWatch access group setup information.

   The dashboard name can contain only alphanumerics, dash (–), and underscore (_).
6. Under **ResourcesToMonitor**, enter the directory ID of the directory that you've enabled internet monitoring for.
7. Under **MonitorName**, enter the name of the internet monitor you want to use.
8. Choose **Next**.
9. Review the default selections on the **Configure stack options** page, and choose **Next**.
10. Scroll down to **Transforms might require access capabilities** and check the boxes for acknowledgement. Then choose **Submit** to create the stack and the custom CloudWatch dashboard.

    > **Important**
    >
    > A cost might be associated with custom CloudWatch dashboards. For information about pricing, see Amazon CloudWatch Pricing
11. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
12. In the left navigation bar, choose **Dashboards**.
13. Under **Custom Dashboards**, choose the dashboard with the dashboard name you entered earlier in this procedure.
14. You can now monitor you WorkSpace's data using the Internet Monitoring dashboard.

Business continuity for WorkSpaces Personal

Amazon WorkSpaces is built on the AWS global infrastructure, which is organized into AWS Regions and Availability Zones. These Regions and Availability Zones provide resiliency in terms of both physical isolation and data redundancy. For more information, see Resilience in Amazon WorkSpaces.

Amazon WorkSpaces also provides cross-Region redirection, a feature that works with your Domain Name System (DNS) routing policies to redirect your WorkSpaces users to alternative WorkSpaces when their primary WorkSpaces aren't available. For example, by using DNS failover routing policies, you can connect your users to WorkSpaces in your specified failover Region when they can't access their WorkSpaces in the primary Region.

You can use cross-Region redirection to achieve regional resiliency and high availability. You can also use it for other purposes, such as traffic distribution or providing alternative WorkSpaces during maintenance periods. If you use Amazon Route 53 for your DNS configuration, you can take advantage of health checks that monitor Amazon CloudWatch alarms.

Amazon WorkSpaces Multi-Region Resilience provides automated, redundant virtual desktop infrastructure in a secondary WorkSpace Region and streamlines the process of redirecting users to the secondary Region when the primary Region is unreachable due to outages.

You can use WorkSpaces Multi-Region Resilience with cross-Region redirection to deploy redundant virtual desktop infrastructure in a secondary WorkSpace Region and design a cross-Region failover strategy in preparation for disruptive events. You can also use this solution for other purposes, such as traffic distribution or providing alternative WorkSpaces during maintenance periods. If you use Route 53 for your DNS configuration, you can take advantage of health checks that monitor CloudWatch alarms.

Contents

Cross-Region redirection for WorkSpaces Personal

With the cross-Region redirection feature in Amazon WorkSpaces, you can use a fully qualified domain name (FQDN) as the registration code for your WorkSpaces. Cross-Region redirection works with your Domain Name System (DNS) routing policies to redirect your WorkSpaces users to alternative WorkSpaces when their primary WorkSpaces aren't available. For example, by using DNS failover routing policies, you can connect your users to WorkSpaces in your specified failover AWS Region when they can't access their WorkSpaces in the primary Region.

You can use cross-Region redirection along with your DNS failover routing policies to achieve regional resiliency and high availability. You can also use this feature for other purposes, such as traffic distribution or providing alternative WorkSpaces during maintenance periods. If you use Amazon Route 53 for your DNS configuration, you can take advantage of health checks that monitor Amazon CloudWatch alarms.

To use this feature, you must set up WorkSpaces for your users in two (or more) AWS Regions. You must also create special FQDN-based registration codes called *connection aliases*. These connection

aliases replace Region-specific registration codes for your WorkSpaces users. (The Region-specific registration codes remain valid; however, for cross-Region redirection to work, your users must use the FQDN instead as their registration code.)

To create a connection alias, you specify a *connection string*, which is your FQDN, such as `www.example.com` or `desktop.example.com`. To use this domain for cross-Region redirection, you must register it with a domain registrar and configure the DNS service for your domain.

After you've created your connection aliases, you associate them with your WorkSpaces directories in different Regions to create *association pairs*. Each association pair has a primary Region and one or more failover Regions. If an outage occurs in the primary Region, your DNS failover routing policies redirect your WorkSpaces users to the WorkSpaces that you've set up for them in the failover Region.

To designate your primary and failover Regions, you define the Region priority (either primary or secondary) when configuring your DNS failover routing policies.

Contents

Prerequisites

- You must own and register the domain that you want to use as the FQDN in your connection aliases. If you're not already using another domain registrar, you can use Amazon Route 53 to register your domain. For more information, see Registering domain names using Amazon Route 53 in the *Amazon Route 53 Developer Guide*.

  > **Important**
  >
  > You must have all necessary rights to use any domain name that you use in conjunction with Amazon WorkSpaces. You agree that the domain name does not violate or infringe on the legal rights of any third party or otherwise violate applicable law.

  The total length of your domain name can't exceed 255 characters. For more information about domain names, see DNS domain name format in the *Amazon Route 53 Developer Guide*.

  Cross-Region redirection works with both public domain names and domain names in private DNS zones. If you're using a private DNS zone, you must provide a virtual private network (VPN) connection to the virtual private cloud (VPC) that contains your WorkSpaces. If your WorkSpaces users attempt to use a private FQDN from the public internet, the WorkSpaces client applications return the following error message:

  ```
  "We're unable to register the WorkSpace because of a DNS server issue. Contact your administrator for help."
  ```

- You must set up your DNS service and configure the necessary DNS routing policies. Cross-Region redirection works in conjunction with your DNS routing policies to redirect your WorkSpaces users as needed.
- In each primary and failover Region where you want to set up cross-Region redirection, create WorkSpaces for your users. Make sure that you use the same usernames in each WorkSpaces directory in each Region. To keep your Active Directory user data in sync, we recommend using AD Connector to point to the same Active Directory in each Region where you've set up WorkSpaces for your users. For more information about creating WorkSpaces, see Launch WorkSpaces.

> **Important**
>
> If you configure your AWS Managed Microsoft AD directory for multi-Region replication, only the directory in the primary Region can be registered for use with Amazon WorkSpaces. Attempts to register the directory in a replicated Region for use with Amazon WorkSpaces will fail. Multi-Region replication with AWS Managed Microsoft AD isn't supported for use with Amazon WorkSpaces within replicated Regions.

When you've finished setting up cross-Region redirection, you must make sure your WorkSpaces users are using the FQDN-based registration code instead of the Region-based registration code (for example, `WSpdx+ABC12D`) for their primary Region. To do this, you must send them an email with the FQDN connection string by using the procedure in Step 5: Send the connection string to your WorkSpaces users.

> **Note**
>
> If you create your users in the WorkSpaces console instead of creating them in Active Directory, WorkSpaces automatically sends an invitation email to your users with a Region-based registration code whenever you launch a new WorkSpace. This means that when you set up WorkSpaces for your users in the failover Region, your users will also automatically receive emails for these failover WorkSpaces. You will need to instruct your users to ignore emails with Region-based registration codes.

Limitations

- Cross-Region redirection doesn't automatically check whether connections to the primary Region have failed and then fails your WorkSpaces over to another Region. In other words, automatic failover doesn't occur.

  To implement an automatic failover scenario, you must use some other mechanism in conjunction with cross-Region redirection. For example, you can use an Amazon Route 53 failover DNS routing policy paired with a Route 53 health check that monitors a CloudWatch alarm in the primary Region. If the CloudWatch alarm in the primary Region is triggered, your DNS failover routing policy then redirects your WorkSpaces users to the WorkSpaces that you've set up for them in the failover Region.

- When you're using cross-Region redirection, user data isn't persisted between WorkSpaces in different Regions. To ensure that users can access their files from different Regions, we recommend that you set up Amazon WorkDocs for your WorkSpaces users, if Amazon WorkDocs is supported in your primary and failover Regions. For more information about Amazon WorkDocs, see Amazon WorkDocs Drive in the *Amazon WorkDocs Administration Guide*. For more information about enabling Amazon WorkDocs for your WorkSpace users, see Register an existing AWS Directory Service directory with WorkSpaces Personal and Enable Amazon WorkDocs for AWS Managed Microsoft AD. For information about how WorkSpaces users can set up Amazon WorkDocs on their WorkSpaces, see Integrate with WorkDocs in the *Amazon WorkSpaces User Guide*.
- Cross-Region redirection is supported only on version 3.0.9 or later of the Linux, macOS, and Windows WorkSpaces client applications. You can also use cross-Region redirection with Web Access.
- Cross-Region redirection is available in all AWS Regions where Amazon WorkSpaces is available, except for the AWS GovCloud (US) Regions and the China (Ningxia) Region.

Step 1: Create connection aliases

Using the same AWS account, create connection aliases in each primary and failover Region where you want to set up cross-Region redirection.

To create a connection alias

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the upper-right corner of the console, select the primary AWS Region for your WorkSpaces.
3. In the navigation pane, choose **Account Settings**.
4. Under **Cross-Region redirection**, choose **Create connection alias**.
5. For **Connection string**, enter an FQDN, such as `www.example.com` or `desktop.example.com`. A connection string can be a maximum of 255 characters. It can include only letters (A-Z and a-z), numbers (0-9), and the following characters: .-

> **Important**
>
> After you create a connection string, it is always associated with your AWS account. You cannot recreate the same connection string with a different account, even if you

delete all instances of it from the original account. The connection string is globally reserved for your account.

6. (Optional) Under **Tags**, specify any tags that you want to associate with your connection alias.
7. Choose **Create connection alias**.
8. Repeat these steps, but in Step 2, be sure to select the failover Region for your WorkSpaces. If you have more than one failover Region, repeat these steps for each failover Region. Be sure to use the same AWS account to create the connection alias in each failover Region.

(Optional) Step 2: Share a connection alias with another account

You can share a connection alias with one other AWS account in the same AWS Region. Sharing a connection alias with another account gives that account permission to associate or disassociate that alias with a directory owned by that account in the same Region only. Only the account that owns a connection alias can delete the alias.

Note

A connection alias can be associated with only one directory per AWS Region. If you share a connection alias with another AWS account, only one account (your account or the shared account) can associate the alias with a directory in that Region.

To share a connection alias with another AWS account

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the upper-right corner of the console, select the AWS Region where you want to share the connection alias with another AWS account.
3. In the navigation pane, choose **Account Settings**.
4. Under **Cross-Region redirection associations**, select the connection string, and then choose **Actions**, **Share/unshare connection alias**.

   You can also share an alias from the details page for your connection alias. To do so, under **Shared account**, choose **Share connection alias**.
5. On the **Share/unshare connection alias** page, under **Share with an account**, enter the AWS account ID that you want to share your connection alias with in this AWS Region.

6. Choose **Share**.

Step 3: Associate connection aliases with directories in each Region

Associating the same connection alias with a WorkSpaces directory in two or more Regions creates an association pair between the directories. Each association pair has a primary Region and one or more failover Regions.

For example, if your primary Region is the US West (Oregon) Region, you can pair your WorkSpaces directory in the US West (Oregon) Region with a WorkSpaces directory in the US East (N. Virginia) Region. If an outage occurs in the primary Region, cross-Region redirection works in conjunction with your DNS failover routing policies and any health checks that you've put in place on the US West (Oregon) Region to redirect your users to the WorkSpaces you've set up for them in the US East (N. Virginia) Region. For more information about the cross-Region redirection experience, see What happens during cross-Region redirection.

> **Note**
>
> If your WorkSpaces users are located a significant distance from the failover Region (for example, thousands of miles away), their WorkSpaces experience might be less responsive than usual. To check the round-trip time (RTT) to the various AWS Regions from your location, use the Amazon WorkSpaces Connection Health Check.

To associate a connection alias with a directory

You can associate a connection alias with only one directory per AWS Region. If you have shared a connection alias with another AWS account, only one account (your account or the shared account) can associate the alias with a directory in that Region.

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the upper-right corner of the console, select the primary AWS Region for your WorkSpaces.
3. In the navigation pane, choose **Account Settings**.
4. Under **Cross-Region redirection associations**, select the connection string, and then choose **Actions**, **Associate/disassociate**.

   You can also associate a connection alias with a directory from the details page for your connection alias. To do so, under **Associated directory**, choose **Associate directory**.

5. On the **Associate/disassociate** page, Under **Associate to a directory**, select the directory that you want to associate your connection alias with in this AWS Region.

   > **Note**
   >
   > If you configure your AWS Managed Microsoft AD directory for multi-Region replication, only the directory in the primary Region can be used with Amazon WorkSpaces. Attempts to use the directory in a replicated Region with Amazon WorkSpaces will fail. Multi-Region replication with AWS Managed Microsoft AD isn't supported for use with Amazon WorkSpaces within replicated Regions.

6. Choose **Associate**.
7. Repeat these steps, but in Step 2, be sure to select the failover Region for your WorkSpaces. If you have more than one failover Region, repeat these steps for each failover Region. Be sure to associate the same connection alias with a directory in each failover Region.

Step 4: Configure your DNS service and set up DNS routing policies

After you've created your connection aliases and your connection alias association pairs, you can then configure the DNS service for the domain that you've used in your connection strings. You can use any DNS service provider for this purpose. If you don't already have a preferred DNS service provider, you can use Amazon Route 53. For more information, see Configuring Amazon Route 53 as your DNS service in the *Amazon Route 53 Developer Guide*.

After you've configured the DNS service for your domain, you must set up the DNS routing policies that you want to use for cross-Region redirection. For example, you can use Amazon Route 53 health checks to determine whether your users can connect to their WorkSpaces in a particular Region. If your users can't connect, you can use a DNS failover policy to route your DNS traffic from one Region to another.

For more information about choosing your DNS routing policy, see Choosing a routing policy in the *Amazon Route 53 Developer Guide*. For more information about Amazon Route 53 health checks, see How Amazon Route 53 checks the health of your resources in the *Amazon Route 53 Developer Guide*.

When you're setting up your DNS routing policies, you will need the *connection identifier* for the association between the connection alias and the WorkSpaces directory in the primary Region. You

will also need the connection identifier for the association between the connection alias and the WorkSpaces directory in your failover Region or Regions.

> **Note**
>
> The connection identifier is **not** the same as the connection alias ID. The connection alias ID starts with `wsca-`.

To find the connection identifier for a connection alias association

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the upper-right corner of the console, select the primary AWS Region for your WorkSpaces.
3. In the navigation pane, choose **Account Settings**.
4. Under **Cross-Region redirection associations**, select the connection string text (the FQDN) to view the connection alias details page.
5. On the details page for your connection alias, under **Associated directory**, make note of the value that's displayed for **Connection identifier**.
6. Repeat these steps, but in Step 2, be sure to select the failover Region for your WorkSpaces. If you have more than one failover Region, repeat these steps to find the connection identifier for each failover Region.

Example: To set up a DNS failover routing policy using Route 53

The following example sets up a public hosted zone for your domain. However, you can set up a public or a private hosted zone. For more information about setting up a hosted zone, see Working with hosted zones in the *Amazon Route 53 Developer Guide*.

This example also uses a failover routing policy. You can use other routing policy types for your cross-Region redirection strategy. For more information about choosing your DNS routing policy, see Choosing a routing policy in the *Amazon Route 53 Developer Guide*.

When you're setting up a failover routing policy in Route 53, a health check is required for the primary Region. For more information about creating a health check in Route 53, see Creating Amazon Route 53 health checks and configuring DNS failover and Creating, updating, and deleting health checks in the *Amazon Route 53 Developer Guide*.

If you want to use an Amazon CloudWatch alarm with your Route 53 health check, you'll also need to set up a CloudWatch alarm to monitor the resources in your primary Region. For more information about CloudWatch, see What Is Amazon CloudWatch? in the *Amazon CloudWatch User Guide*. For more information about how Route 53 uses CloudWatch alarms in its health checks, see How Route 53 determines the status of health checks that monitor CloudWatch alarms and Monitoring a CloudWatch alarm in the *Amazon Route 53 Developer Guide*.

To set up a DNS failover routing policy in Route 53, you first need to create a hosted zone for your domain.

1. Open the Route 53 console at https://console.aws.amazon.com/route53/.
2. In the navigation pane, choose **Hosted zones**, and then choose **Create hosted zone**.
3. On the **Created hosted zone** page, enter your domain name (such as `example.com`) under **Domain name**.
4. Under **Type**, choose **Public hosted zone**.
5. Choose **Create hosted zone**.

Then create a health check for your primary Region.

1. Open the Route 53 console at https://console.aws.amazon.com/route53/.
2. In the navigation pane, choose **Health checks**, and then choose **Create health check**.
3. On the **Configure health check** page, enter a name for your health check.
4. For **What to monitor**, select either **Endpoint**, **Status of other health checks (calculated health check)**, or **State of CloudWatch alarm**.
5. Depending on what you've selected in the prior step, configure your health check, and then choose **Next**.
6. On the **Get notified when health check fails** page, for **Create alarm**, choose **Yes** or **No**.
7. Choose **Create health check**.

After you've created your health check, you can create the DNS failover records.

1. Open the Route 53 console at https://console.aws.amazon.com/route53/.
2. In the navigation pane, choose **Hosted zones**.
3. On the **Hosted zones** page, select your domain name.

4. On the details page for your domain name, choose **Create record**.
5. On the **Choose routing policy** page, select **Failover**, and then choose **Next**.
6. On the **Configure records** page, under **Basic configuration**, for **Record name**, enter your subdomain name. For example, if your FQDN is `desktop.example.com`, enter **`desktop`**.

   > **Note**
   >
   > If you want to use the root domain, leave **Record name** blank. However, we recommend using a subdomain, such as `desktop` or `workspaces`, unless you've set up the domain solely for use with your WorkSpaces.

7. For **Record type**, select **TXT – Used to verify email senders and for application-specific values**.
8. Leave the **TTL seconds** settings at the default.
9. Under **Failover records to add to *`your_domain_name`***, choose **Define failover record**.

Now you need to set up the failover records for your primary and failover Regions.

Example: To set up the failover record for your primary Region

1. In the **Define failover record** dialog box, for **Value/route traffic to**, select **IP address or another value depending on the record type**.
2. A box opens for you to enter your sample text entries. Enter the connection identifier for the connection alias association for your primary Region.
3. For **Failover record type**, choose **Primary**.
4. For **Health check**, select a health check that you've created for your primary Region.
5. For **Record ID**, enter a description to identify this record.
6. Choose **Define failover record**. Your new failover record appears under **Failover records to add to *`your_domain_name`***.

Example: To set up the failover record for your failover Region

1. Under **Failover records to add to *`your_domain_name`***, choose **Define failover record**.
2. In the **Define failover record** dialog box, for **Value/route traffic to**, select **IP address or another value depending on the record type**.

3. A box opens for you to enter your sample text entries. Enter the connection identifier for the connection alias association for your failover Region.
4. For **Failover record type**, choose **Secondary**.
5. (Optional) For **Health check**, enter a health check that you've created for your failover Region.
6. For **Record ID**, enter a description to identify this record.
7. Choose **Define failover record**. Your new failover record appears under **Failover records to add to *your_domain_name***.

If the health check that you've set up for your primary Region fails, your DNS failover routing policy redirects your WorkSpaces users to your failover Region. Route 53 continues to monitor the health check for your primary Region, and when the health check for your primary Region no longer fails, Route 53 automatically redirects your WorkSpaces users back to their WorkSpaces in the primary Region.

For more information about creating DNS records, see Creating records by using the Amazon Route 53 console in the *Amazon Route 53 Developer Guide*. For more information about configuring DNS TXT records, see TXT record type in the *Amazon Route 53 Developer Guide*.

Step 5: Send the connection string to your WorkSpaces users

To make sure your users' WorkSpaces will be redirected as needed during an outage, you must send the connection string (FQDN) to your users. If you've already issued Region-based registration codes (for example, `WSpdx+ABC12D`) to your WorkSpaces users, those codes remain valid. However, for cross-Region redirection to work, your WorkSpaces users must use the connection string as their registration code when registering their WorkSpaces in the WorkSpaces client application.

> **Important**
>
> If you create your users in the WorkSpaces console instead of creating them in Active Directory, WorkSpaces automatically sends an invitation email to your users with a Region-based registration code (for example, `WSpdx+ABC12D`) whenever you launch a new WorkSpace. Even if you've already set up cross-Region redirection, the invitation email that's automatically sent for new WorkSpaces contains this Region-based registration code instead of your connection string.

To make sure your WorkSpaces users are using the connection string instead of the Region-based registration code, you must send them another email with the connection string by using the procedure below.

To send the connection string to your WorkSpaces users

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the upper-right corner of the console, select the primary AWS Region for your WorkSpaces.
3. In the navigation pane, choose **WorkSpaces**.
4. On the **WorkSpaces** page, use the search box to search for a user that you want to send an invitation to, and then select the corresponding WorkSpace from the search results. You can select only one WorkSpace at a time.
5. Choose **Actions**, **Invite User**.
6. On the **Invite Users to Their WorkSpaces** page, you will see an email template to send to your users.
7. (Optional) If there is more than one connection alias associated with your WorkSpaces directory, select the connection string that you want your users to use from the **Connection alias string** list. The email template updates to display the string that you've chosen.
8. Copy the email template text and paste it into an email to the users using your own email application. In your email application, you can modify the text as needed. When the invitation email is ready, send it to your users.

Cross-Region Redirection architecture diagram

The following diagram describes the deployment process of cross-Region redirection.

Note

Cross-Region redirection only facilitates cross-Region failover and fallback. It doesn't facilitate creating and maintaining WorkSpaces in the secondary Region and doesn't allow cross-Region data replication. WorkSpaces in both the primary and secondary Regions should be managed separately.

Initiate cross-Region redirection

In the event of an outage, you can either update the DNS records manually or use automated routing policies based on health checks, which determine the failover Region. We recommend following the disaster recovery mechanisms outlined in Creating Disaster Recovery Mechanisms Using Amazon Route 53.

What happens during cross-Region redirection

During Region failover, your WorkSpaces users are disconnected from their WorkSpaces in the primary Region. When they attempt to reconnect, they receive the following error message:

```
We can't connect to your WorkSpace. Check your network connection, and then try again.
```

Your users are then prompted to log in again. If they're using the FQDN as their registration code, when they log in again, your DNS failover routing policies redirect them to the WorkSpaces that you've set up for them in the failover Region.

> **Note**
>
> In some cases, users might be unable to reconnect when they log in again. If this behavior occurs, they must close and restart the WorkSpaces client application, and then try to log in again.

Disassociate a connection alias from a directory

Only the account that owns a directory can disassociate a connection alias from the directory.

If you've shared a connection alias with another account and that account has associated the connection alias with a directory owned by that account, that account must be used to disassociate the connection alias from the directory.

To disassociate a connection alias from a directory

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the upper-right corner of the console, select the AWS Region that contains the connection alias that you want to disassociate.

3. In the navigation pane, choose **Account Settings**.
4. Under **Cross-Region redirection associations**, select the connection string, and then choose **Actions**, **Associate/disassociate**.

   You can also dissociate a connection alias from the connection alias details page. To do so, under **Associated directory**, choose **Disassociate**.
5. On the **Associate/disassociate** page, choose **Disassociate**.
6. In the dialog box that asks you to confirm the disassociation, choose **Disassociate**.

Unshare a connection alias

Only the owner of a connection alias can unshare the alias. If you unshare a connection alias with an account, that account can no longer associate the connection alias with a directory.

To unshare a connection alias

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the upper-right corner of the console, select the AWS Region that contains the connection alias that you want to unshare.
3. In the navigation pane, choose **Account Settings**.
4. Under **Cross-Region redirection associations**, select the connection string, and then choose **Actions**, **Share/unshare connection alias**.

   You can also unshare a connection alias from the connection alias details page. To do so, under **Shared account**, choose **Unshare**.
5. On the **Share/unshare connection alias** page, choose **Unshare**.
6. In the dialog box that asks you to confirm unsharing the connection alias, choose **Unshare**.

Delete a connection alias

You can delete a connection alias only if it is owned by your account and if it isn't associated with a directory.

If you've shared a connection alias with another account and that account has associated the connection alias with a directory owned by that account, that account must first disassociate the connection alias from the directory before you can delete the connection alias.

Important

After you create a connection string, it is always associated to your AWS account. You cannot recreate the same connection string with a different account, even if you delete all instances of it from the original account. The connection string is globally reserved for your account.

Warning

If you will no longer be using an FQDN as the registration code for your WorkSpaces users, you must take certain precautions to prevent potential security issues. For more information, see Security considerations if you stop using cross-Region redirection.

To delete a connection alias

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the upper-right corner of the console, select the AWS Region that contains the connection alias that you want to delete.
3. In the navigation pane, choose **Account Settings**.
4. Under **Cross-Region redirection associations**, select the connection string, and then choose **Delete**.

   You can also delete a connection alias from the connection alias details page. To do so, choose **Delete** in the upper-right corner of the page.

   Note

   If the **Delete** button is disabled, make sure that you are the owner of the alias, and make sure that the alias isn't associated with a directory.

5. In the dialog box that asks you to confirm deletion, choose **Delete**.

IAM permissions to associate and disassociate connection aliases

If you use an IAM user to associate or disassociate connection aliases, the user must have permissions for `workspaces:AssociateConnectionAlias` and `workspaces:DisassociateConnectionAlias`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

Important

If you are creating an IAM policy for associating or disassociating connection aliases for accounts that don't own the connection aliases, you cannot specify an account ID in the ARN. Instead, you must use * for the account ID, as shown in the following example policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
```

```
}
```

You can specify an account ID in the ARN only when that account owns the connection alias to be associated or disassociated.

For more information about working with IAM, see Identity and access management for WorkSpaces.

Security considerations if you stop using cross-Region redirection

If you will no longer be using an FQDN as the registration code for your WorkSpaces users, you must take the following precautions to prevent potential security issues:

- Be sure to issue your WorkSpaces users the Region-specific registration code (for example, `WSpdx+ABC12D`) for their WorkSpaces directory and instruct them to stop using the FQDN as their registration code.
- **If you still own this domain**, be sure to update your DNS TXT record to remove this domain so that it cannot be exploited in a phishing attack. If you remove this domain from your DNS TXT record and your WorkSpaces users attempt to use the FQDN as their registration code, their connection attempts will fail harmlessly.
- **If you no longer own this domain**, your WorkSpaces users **must** use their Region-specific registration code. If they continue trying to use the FQDN as their registration code, their connection attempts could be redirected to a malicious site.

Multi-Region Resilience for WorkSpaces Personal

Amazon WorkSpaces Multi-Region Resilience (MRR) enables you to redirect users to a secondary Region when your primary WorkSpaces Region is unreachable due to disruptive events, without requiring your users to switch registration codes when logging to their standby WorkSpaces. Standby WorkSpaces is a feature of Amazon WorkSpaces Multi-Region Resilience that streamlines the standby deployment creation and management. After setting up a user directory in your secondary Region, select the WorkSpace in your primary Region that you want to create a standby WorkSpace for. The system automatically mirrors the primary WorkSpace bundle images to the secondary Region. It then automatically provisions a new standby WorkSpace in your secondary Region

Amazon WorkSpaces Multi-Region Resilience is built upon cross-Region redirection that leverages DNS health check and failover capabilities. It allows you to use a fully qualified domain name (FQDN) as your WorkSpaces registration code. When your users log in to WorkSpaces, you can redirect them across supported WorkSpaces Regions based on your Domain Name System (DNS) policies for the FQDN. If you use Amazon Route 53, we recommend using health checks that monitor Amazon CloudWatch alarms when devising a cross-Region redirection strategy for WorkSpaces. For more information, see Creating Amazon Route 53 health checks and configuring DNS failover in the *Amazon Route 53 Developer Guide*.

Data replication is an add-on feature of standby WorkSpaces that replicates data one-way from the primary Region to the secondary Region. After enabling data replication, EBS snapshots of the system and user volumes are taken every 12 hours. Multi-Region Resilience regularly checks for fresh snapshots. When the snapshots are found, it initiates a copy to the secondary Region. As copies arrive in the secondary Region, they are used to update the secondary WorkSpace.

Contents

Prerequisites

- You must create WorkSpaces for your users in the primary Region before creating standby WorkSpaces. For more information about creating WorkSpaces, see Create a directory for WorkSpaces Personal.
- To enable data replication on standby WorkSpaces, you should have either a self- managed Active Directory or an AWS Managed Microsoft AD configured to replicate to your standby Regions. For more information, see Create your AWS Managed Microsoft AD directory and Add a replicated Region.

- Ensure you update networking dependency drivers like ENA, NVMe, and PV drivers on your primary WorkSpaces. You should do this at least once every 6 months. For more information, see Install or upgrade Elastic Network Adapter (ENA) driver , AWS NVMe drivers for Windows instances, and Upgrade PV drivers on Windows instances.
- Ensure you update the EC2Config, EC2Launch, and EC2Launch V2 agents to the latest versions periodically. You should do this at least once every 6 months. For more information, see Update EC2Config and EC2Launch.
- To ensure proper data replication, ensure the Active Directories in the primary and secondary regions are in sync for FQDN, OU, and user SID.
- The default quota (limit) for standby WorkSpaces is 0. You need to request a service quota increase before creating a standby WorkSpace. For more information, see Amazon WorkSpaces quotas.
- Ensure you are using customer managed keys to encrypt both your primary and standby WorkSpaces. You can either use single Region keys or multi-Region keys to encrypt your primary and standby WorkSpaces.

Limitations

- Standby WorkSpaces only copies the bundle image of your primary WorkSpaces but it doesn't copy the system volume (drive C) or user volume (drive D) from your primary WorkSpaces. To copy the system volume (drive C) or user volume (drive D) from your primary WorkSpaces to standby WorkSpaces, you have to enable data replication.
- You cannot directly modify, rebuild, restore, or migrate a standby WorkSpace.
- Failover for cross-Region redirection is controlled by your DNS settings. To implement an automatic failover scenario, you must use a different mechanism in conjunction with cross-Region redirection. For example, you can use an Amazon Route 53 failover DNS routing policy paired with a Route 53 health check that monitors a CloudWatch alarm in the primary Region. If the CloudWatch alarm in the primary Region is invoked, your DNS failover routing policy then redirects your WorkSpaces users to the WorkSpaces that you've set up for them in the failover Region.
- Data replication only goes one way, copying data from primary Region to secondary Region. During standby WorkSpaces failover, you can access the data and application between 12 and 24 hours. After an outage, manually back up any data that you created on the secondary WorkSpace and log out. We recommend saving your work to external drives, such as your network drive, so that you can access your data from the primary WorkSpace.

- Data replication does not support AWS Simple AD.
- When you enable data replication on standby WorkSpaces, EBS snapshots of the primary WorkSpaces (both root and system volumes) are taken every 12 hours. The initial snapshot for a particular data volume is full and subsequent snapshots are incremental. As a result, the first replication for a given WorkSpace will take longer than subsequent ones. Snapshots are initiated on a schedule that is internal to WorkSpaces and you cannot control the timing.
- If the primary WorkSpace and standby WorkSpace join using the same domain, we recommend that you only connect to either the primary WorkSpace or standby WorkSpace at a given point in time to avoid losing connection with the domain controller.
- If you configure your AWS Managed Microsoft AD for Multi-Region replication, only the directory in the primary Region can be registered for use with WorkSpaces. If you try to register the directory in a replicated Region for use with WorkSpaces, it will fail. Multi-Region replication with AWS Managed Microsoft AD isn't supported for use with WorkSpaces within replicated Regions.
- If you've already set up your cross-Region redirection and created WorkSpaces in both your primary and secondary Regions without using standby WorkSpaces, you cannot convert the existing WorkSpace in the secondary Region to a standby WorkSpace directly. Instead, you need to shut down the WorkSpace in your secondary Region, select the WorkSpace in your primary Region that you want to create a standby WorkSpace for, and use standby WorkSpaces to create the standby WorkSpace.
- After an outage, manually back up any data that you created on the secondary WorkSpace and log out. We recommend saving your work to external drives, such as your network drive, so that you can access your data from the primary WorkSpace.
- WorkSpaces Multi-Region Resilience is currently available in the following Regions:
  - US East (N. Virginia) Region
  - US West (Oregon) Region
  - Europe (Frankfurt) Region
  - Europe (Ireland) Region
- WorkSpaces Multi-Region Resilience is only supported on version 3.0.9 or later of the Linux, macOS, and Windows WorkSpaces client applications. You can also use Multi-Region Resilience with Web Access.
- WorkSpaces Multi-Region Resilience supports Windows and Bring Your Own License (BYOL) WorkSpaces. It doesn't support Amazon Linux 2, Ubuntu WorkSpaces, Red Hat Enterprise Linux, or GPU-enabled WorkSpaces (e.g. Graphics, GraphicsPro, Graphics.g4dn, or GraphicsPro.g4dn).
- After failover or failback completes, wait 15 to 30 minutes before connecting to your WorkSpace.

Configure your Multi-Region Resilience standby WorkSpace

To configure your Multi-Region Resilience standby WorkSpace

1. Set up user directories in both your primary and secondary Regions. Ensure that you use the same user names in each WorkSpaces directory in each Region.

   To keep your Active Directory user data in sync, we recommend using AD Connector to point to the same Active Directory in each Region where you've set up WorkSpaces for your users. For more information about creating a directory, see Register a directory with WorkSpaces.

   > **Important**
   >
   > If you configure your AWS Managed Microsoft AD directory for multi-Region replication, only the directory in the primary Region can be registered for use with WorkSpaces. Attempts to register the directory in a replicated Region for use with WorkSpaces will fail. Multi-Region replication with AWS Managed Microsoft AD isn't supported for use with WorkSpaces within replicated Regions.

2. Create WorkSpaces for your users in the primary Region. For more information about creating WorkSpaces, see Launch WorkSpaces.
3. Create a standby WorkSpace in the secondary Region. For more information about creating a standby WorkSpace, see Create a standby WorkSpace.
4. Create and associate connection strings (FQDN) with user directories in primary and secondary Regions.

   You must enable cross-Region redirection in your account because standby WorkSpaces is built upon cross-Region redirection. Follow step 1 - 3 of the instructions for Cross-Region redirection for Amazon WorkSpaces.
5. Configure DNS service and set up DNS routing policies.

   You must set up your DNS service and configure the necessary DNS routing policies. Cross-Region redirection works in conjunction with your DNS routing policies to redirect your WorkSpaces users as needed.
6. When you've finished setting up cross-Region redirection, you must send your users an email with a FQDN connection string. For more information see Step 5: Send the connection string to your WorkSpaces users. Ensure your WorkSpaces users are using the FQDN-based

registration code instead of the Region-based registration code (for example, WSpdx+ABC12D) for their primary Region.

> **Important**
>
> - If you create your users in the WorkSpaces console instead of creating them in Active Directory, WorkSpaces automatically sends an invitation email to your users with a Region-based registration code whenever you launch a new WorkSpace. This means that when you set up WorkSpaces for your users in the secondary Region, your users will also automatically receive emails for these secondary WorkSpaces. You will need to instruct your users to ignore emails with Region-based registration codes.
> - The Region-specific registration codes remain valid; however, for cross- Region redirection to work, your users must use the FQDN instead as their registration code.

Create a standby WorkSpace

Before you create a standby WorkSpace, ensure you have completed the prerequisites, including creating a user directory in both primary and secondary Regions, provisioning WorkSpaces for your users in your primary Region, configuring cross-Region redirection in your account, and requesting standby WorkSpaces limit increase through the service quota.

To create a standby WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the upper-right corner of the console, select the primary AWS Region for your WorkSpaces.
3. In the navigation pane, choose **WorkSpaces**.
4. Select a WorkSpace you want to create a standby WorkSpace for.
5. Choose **Actions** and then choose **Create standby WorkSpace**.
6. Select the secondary Region, where you will create your standby WorkSpace, and then choose **Next**.
7. Select the user directory in your secondary Region and then choose **Next**.
8. (Optional) Add encryption key, enable data encryption, and manage tags.
   - To add an encryption key, enter it under Input encryption key.

- To enable data replication, choose **Enable data replication**. Then, check the checkbox to confirm that you authorize additional monthly charge.
- To add a new tag, choose **Add new tag**.

Then, choose **Next**.

> **Note**
>
> - If the original WorkSpace is encrypted, this field is prepopulated. However, you can choose to replace it with your own encryption key.
> - It takes a few minutes to update the data replication status.
> - After the standby WorkSpace is successfully updated with the snapshots from the primary WorkSpace, you can find the times stamps of the snapshots under **Recovery Snapshot**.

9. Review the settings of your standby WorkSpaces and then choose **Create**.

> **Note**
>
> - To view information about your standby WorkSpaces, go to the primary WorkSpace detail page.
> - The standby WorkSpace only copies the bundle image of your primary WorkSpace but it does not copy the system volume (drive C) or user volume (drive D) from your primary WorkSpaces. By default, data replication is off. To copy the system volume (drive C) or user volume (drive D) from your primary WorkSpaces to standby WorkSpaces, you have to enable data replication.

Manage a standby WorkSpace

You cannot directly modify, rebuild, restore, or migrate a standby WorkSpace.

To enable data replication for your standby WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Go to your primary Region, select the primary WorkSpace ID.

3. Scroll down to the Standby WorkSpace section and choose **Edit Standby WorkSpace**.
4. Choose **Enable data replication**. Then, check the checkbox to confirm that you authorize additional monthly charge. Then, choose **Save**.

Note

- Standby WorkSpaces cannot hibernate. If you stop the standby WorkSpace, it does not preserve your unsaved work. We recommend users to always save their work before exiting their standby WorkSpaces.
- To enable data replication on standby WorkSpaces, you should have either a self-managed Active Directory or an AWS Managed Microsoft AD configured to replicate to your standby Regions. To set up your directories, follow steps 1 to 3 in the Walkthrough section of Building for business continuity with Amazon WorkSpaces and AWS Directory Services or see Using multi-Region AWS Managed Active Directory with Amazon WorkSpaces. Multi-Region replication is only supported for the Enterprise Edition of AWS Managed Microsoft AD.
- It takes a few minutes to update the data replication status.
- After the standby WorkSpace is successfully updated with the snapshots from the primary WorkSpace, you can find the times stamps of the snapshots under **Recovery Snapshot**.

Delete a standby WorkSpace

You can terminate a standby WorkSpace the same way you terminate a regular WorkSpace.

To delete a standby WorkSpace

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the upper-right corner of the console, select the primary AWS Region for your WorkSpaces.
3. In the navigation pane, choose **WorkSpaces**.
4. Select the standby WorkSpace and choose **Delete**. It takes approximately 5 minutes to delete a standby WorkSpace. During deletion, the status of the standby WorkSpace will be set to **Terminating**. When the deletion is complete, the standby WorkSpace disappears from the console.

> **Note**
>
> Deleting a standby WorkSpace is a permanent action and cannot be undone. The standby WorkSpace user's data does not persist and is destroyed. For help with backing up user data, contact AWS Support.

One-way data replication for standby WorkSpaces

Enabling data replication in Multi-Region Resilience allows you to replicate data from a primary Region to a secondary Region. During steady state, Multi-Region Resilience captures snapshots of the system (C drive) and data (D drive) of primary WorkSpaces every 12 hours. These snapshots are transferred to the secondary Region and used to update the standby WorkSpaces. By default, data replication is disabled for standby WorkSpaces.

After data replication is enabled for the standby WorkSpaces, the initial snapshot for a particular data volume is complete, while subsequent snapshots are incremental. As a consequence, the first replication for a given WorkSpace will take longer than subsequent ones. Snapshots are triggered at predetermined intervals within WorkSpaces and the timing cannot be controlled by users.

During failover, when users are redirected to the secondary Region, they can access their standby WorkSpaces with data and applications that are between 12 and 24 hours old. While users are using standby WorkSpaces, Multi-Region Resilience will not force them to log out of their standby WorkSpaces or update the standby WorkSpaces with the snapshots from the primary Region.

After an outage, users should manually back up any data they have created on their secondary WorkSpaces before logging out of their standby WorkSpaces. When they log in again, they will be directed to the primary Region and their primary WorkSpaces.

Plan to reserve Amazon EC2 capacity for recovery

Amazon Multi-Region Resilience(MRR) relies on Amazon EC2 On-Demand pools by default. If a specific Amazon EC2 instance type is unavailable to support your recovery, MRR will automatically attempt to scale up the instance repeatedly until an available instance type is found, but in extreme circumstances, instances may not always be available. To improve the availability of the required instance types you need for your most critical WorkSpaces, contact AWS Support and we will assist you on capacity planning.

Troubleshoot issues for WorkSpaces Personal

The following information can help you troubleshoot issues with your WorkSpaces.

Enabling advanced logging

To help troubleshoot issues that your users might experience, you can enable advanced logging on any Amazon WorkSpaces client.

Advanced logging generates log files that contain diagnostic information and debugging-level details, including verbose performance data. For the 1.0+ and 2.0+ clients, these advanced logging files are automatically uploaded to a database in AWS.

> **Note**
>
> To get AWS review of advanced logging files, and to receive technical support for issues with your WorkSpaces clients, contact AWS Support. For more information, see AWS Support Center.

To enable advanced logging for Web Access

To enable advanced logging for Web Access

1. Open your Amazon WorkSpaces Web Access client.
2. At the top of the WorkSpaces sign in page, choose **Diagnostic logging**.
3. In the pop-up dialog box, ensure that **Diagnostic logging** is enabled.
4. For **Log level**, choose **Advanced logging**.

To access log files in Google Chrome, Microsoft Edge, and Firefox

1. Open the context (right-click) menu on the browsers or press **Ctrl**+**Shift**+**I** (or for Mac, **command**+**option**+**I**) on your keyboard to open the developer tools panel.
2. In the developer tools panel, choose the **Console** tab to find the log files.

To access log files in Safari

1. Choose **Safari**, **Settings**.

2. In the **Settings** window, choose the **Advanced** tab.
3. Choose **Show Develop menu in menu bar**.
4. From the **Develop** tab in the menu bar, choose **Develop** > **Show Web Inspector**.
5. In the Safari Web Inspector panel, choose the **Console** tab to find the log files.

To enable advanced logging for 4.0+ clients

The Windows client logs are stored in the following location:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

To enable advanced logging for Windows clients

1. Close the Amazon WorkSpaces client.
2. Open the Command Prompt app.
3. Launch the WorkSpaces client with the `-l3` flag.

```
c:

cd "C:\Program Files\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

> **Note**
>
> If WorkSpaces is installed for one user and not all users, use the following commands:
> ```
> c:
> cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
> workspaces.exe -l3
> ```

The macOS client logs are stored in the following location:

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
```

To enable advanced logging for macOS clients

1. Close the Amazon WorkSpaces client.
2. Open Terminal.
3. Run the following command.

```
open -a workspaces --args -l3
```

To enable advanced logging for Android clients

1. Close the Amazon WorkSpaces client.
2. Open the Android client menu.
3. Select **Support**.
4. Select **Logging settings**.
5. Select **Enable advanced logging**.

To retrieve logs for Android clients after enabling advanced logging:

- Select **Extract log** to save zipped logs locally.

The Linux client logs are stored in the following location:

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

To enable advanced logging for Linux clients

1. Close the Amazon WorkSpaces client.
2. Open Terminal.
3. Run the following command.

```
/opt/workspacesclient/workspacesclient -l3
```

To enable advanced logging for 3.0 clients

The Windows client logs are stored in the following location:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

To enable advanced logging for Windows clients

1. Close the Amazon WorkSpaces client.
2. Open the Command Prompt app.
3. Launch the WorkSpaces client with the `-l3` flag.

```
c:

cd "C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

> **Note**
>
> If WorkSpaces is installed for one user and not all users, use the following commands:
> ```
> c:
> cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
> workspaces.exe -l3
> ```

The macOS client logs are stored in the following location:

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
```

To enable advanced logging for macOS clients

1. Close the Amazon WorkSpaces client.
2. Open Terminal.
3. Run the following command.

```
open -a workspaces --args -l3
```

To enable advanced logging for Android clients

1. Close the Amazon WorkSpaces client.
2. Open the Android client menu.

3. Select **Support**.
4. Select **Logging settings**.
5. Select **Enable advanced logging**.

To retrieve logs for Android clients after enabling advanced logging:

- Select **Extract log** to save zipped logs locally.

The Linux client logs are stored in the following location:

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

To enable advanced logging for Linux clients

1. Close the Amazon WorkSpaces client.
2. Open Terminal.
3. Run the following command.

   ```
   /opt/workspacesclient/workspacesclient -l3
   ```

To enable advanced logging for 1.0+ and 2.0+ clients

1. Open the WorkSpaces client.
2. Choose the gear icon in the upper-right corner of the client application.
3. Choose **Advanced Settings**.
4. Select the **Enable Advanced Logging** check box.
5. Choose **Save**.

The Windows client logs are stored in the following location:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\1.0\Logs
```

The macOS client logs are stored in the following location:

```
~/Library/Logs/Amazon Web Services/Amazon WorkSpaces/1.0
```

Troubleshoot specific issues

The following information can help you troubleshoot specific issues with your WorkSpaces.

Issues

- I can't create an Amazon Linux WorkSpace because there are non-valid characters in the user name
- I changed the shell for my Amazon Linux WorkSpace and now I can't provision a PCoIP session
- My Amazon Linux WorkSpaces won't start
- Launching WorkSpaces in my connected directory often fails
- Launching WorkSpaces fails with an internal error
- When I try to register a directory, the registration fails and leaves the directory in an ERROR state
- My users can't connect to a Windows WorkSpace with an interactive logon banner
- My users can't connect to a Windows WorkSpace
- My users are having issues when they try to log on to WorkSpaces from WorkSpaces Web Access
- The Amazon WorkSpaces client displays a gray "Loading..." screen for a while before returning to the login screen. No other error message appears.
- My users receive the message "WorkSpace Status: Unhealthy. We were unable to connect you to your WorkSpace. Please try again in a few minutes."
- My users receive the message "This device is not authorized to access the WorkSpace. Please contact your administrator for assistance."
- My users receive the message "No network. Network connection lost. Check your network connection or contact your administrator for help." when trying to connect to a WSP WorkSpace
- The WorkSpaces client gives my users a network error, but they are able to use other network-enabled apps on their devices
- My WorkSpace users see the following error message: "Device can't connect to the registration service. Check your network settings."
- My PCoIP zero client users are receiving the error "The supplied certificate is invalid due to timestamp"
- USB printers and other USB peripherals aren't working for PCoIP zero clients
- My users skipped updating their Windows or macOS client applications and aren't getting prompted to install the latest version

- My users are unable to install the Android client application on their Chromebooks
- My users aren't receiving invitation emails or password reset emails
- My users don't see the Forgot password? option on the client login screen
- I receive the message "The system administrator has set policies to prevent this installation" when I try to install applications on a Windows WorkSpace
- No WorkSpaces in my directory can connect to the internet
- My WorkSpace has lost its internet access
- I receive a "DNS unavailable" error when I try to connect to my on-premises directory
- I receive a "Connectivity issues detected" error when I try to connect to my on-premises directory
- I receive an "SRV record" error when I try to connect to my on-premises directory
- My Windows WorkSpace goes to sleep when it's left idle
- One of my WorkSpaces has a state of UNHEALTHY
- My WorkSpace is unexpectedly crashing or rebooting
- The same username has more than one WorkSpace, but the user can log in to only one of the WorkSpaces
- I'm having trouble using Docker with Amazon WorkSpaces
- I receive ThrottlingException errors to some of my API calls
- My WorkSpace keeps disconnecting when I let it run in the background
- SAML 2.0 federation isn't working. My users are not authorized to stream their WorkSpaces desktop.
- My users are getting disconnected from their WorkSpaces session every 60 minutes.
- My users get a redirect URI error when they federate using the SAML 2.0 identity provider (IdP)-initiated flow, or an additional instance of the WorkSpaces client application starts every time my users attempt to sign in from the client after federating to the IdP.
- My users receive the message, "Something went wrong: An error occurred while launching your WorkSpace" when they attempt to sign in to the WorkSpaces client application after federating to the IdP.
- My users receive the message, "Unable to validate tags” when they attempt to sign in to the WorkSpaces client application after federating to the IdP.
- My users receive the message, "The client and the server cannot communicate, because they do not possess a common algorithm".

- My microphone or web cam is not working on Windows WorkSpaces.
- My users cannot log in using certificate-based authentication and are prompted for the password either at the WorkSpaces client or the Windows sign-on screen when they connect to their desktop session.
- I am trying to do something that requires Windows installation media but WorkSpaces does not provide it.
- I want to launch WorkSpaces with an existing AWS Managed Directory created in an unsupported WorkSpaces Region.
- I want to update Firefox on Amazon Linux 2.
- My user is able to reset their password using the WorkSpaces client, ignoring the Fine Grained Password Policy (FFGP) setting that is configured on AWS Managed Microsoft AD.
- My users receive the error message "This OS/platform is not authorized to access your WorkSpace" when trying to access the Windows/Linux WorkSpace using Web Access

I can't create an Amazon Linux WorkSpace because there are non-valid characters in the user name

For Amazon Linux WorkSpaces, user names:

- Can contain a maximum of 20 characters
- Can contain letters, spaces, and numbers that are representable in UTF-8
- Can include the following special characters: _.-#
- Cannot begin with a dash symbol (-) as the first character of the user name

> **Note**
>
> These limitations do not apply to Windows WorkSpaces. Windows WorkSpaces support the @ and - symbols for all characters in the user name.

I changed the shell for my Amazon Linux WorkSpace and now I can't provision a PCoIP session

To override the default shell for Linux WorkSpaces, see Override the default shell for Amazon Linux WorkSpaces.

My Amazon Linux WorkSpaces won't start

Starting July 20, 2020, Amazon Linux WorkSpaces will be using new license certificates. These new certificates are compatible only with versions 2.14.1.1, 2.14.7, 2.14.9, and 20.10.6 or later of the PCoIP agent.

If you're using an unsupported version of the PCoIP agent, you must upgrade it to the latest version (20.10.6), which has the latest fixes and performance improvements that are compatible with the new certificates. If you don't make these upgrades by July 20, session provisioning for your Linux WorkSpaces will fail and your end users won't be able to connect to their WorkSpaces.

To upgrade your PCoIP agent to the latest version

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select your Linux WorkSpace, and reboot it by choosing **Actions**, **Reboot WorkSpaces**. If the WorkSpace status is `STOPPED`, you must choose **Actions**, **Start WorkSpaces** first and wait until its status is `AVAILABLE` before you can reboot it.
4. After your WorkSpace has rebooted and its status is `AVAILABLE`, we recommend that you change the status of the WorkSpace to `ADMIN_MAINTENANCE` while you are performing this upgrade. When you are finished, change the status of the WorkSpace to `AVAILABLE`. For more information about `ADMIN_MAINTENANCE` mode, see Manual Maintenance.

   To change the status of a WorkSpace to `ADMIN_MAINTENANCE`, do the following:

   a. Select the WorkSpace and choose **Actions**, **Modify WorkSpace**.
   b. Choose **Modify State**.
   c. For **Intended State**, select **ADMIN_MAINTENANCE**.
   d. Choose **Modify**.
5. Connect to your Linux WorkSpace through SSH. For more information, see Enable SSH connections for your Linux WorkSpaces in WorkSpaces Personal.
6. To update the PCoIP agent, run the following command:

   ```
   sudo yum --enablerepo=pcoip-stable install pcoip-agent-standard-20.10.6
   ```
7. To verify the agent version and to confirm that the update succeeded, run the following command:

```
rpm -q pcoip-agent-standard
```

The verification command should produce following result:

```
pcoip-agent-standard-20.10.6-1.el7.x86_64
```

8. Disconnect from the WorkSpace and reboot it again.
9. If you set the status of the WorkSpace to `ADMIN_MAINTENANCE` in Step 4, repeat Step 4 and set **Intended State** to `AVAILABLE`.

If your Linux WorkSpace still fails to start after you upgrade the PCoIP agent, contact AWS Support.

Launching WorkSpaces in my connected directory often fails

Verify that the two DNS servers or domain controllers in your on-premises directory are accessible from each of the subnets that you specified when you connected to your directory. You can verify this connectivity by launching an Amazon EC2 instance in each subnet and joining the instance to your directory using the IP addresses of the two DNS servers.

Launching WorkSpaces fails with an internal error

Check whether your subnets are configured to automatically assign IPv6 addresses to instances launched in the subnet. To check this setting, open the Amazon VPC console, select your subnet, and choose **Subnet Actions**, **Modify auto-assign IP settings**. If this setting is enabled, you cannot launch WorkSpaces using the Performance or Graphics bundles. Instead, disable this setting and specify IPv6 addresses manually when you launch your instances.

When I try to register a directory, the registration fails and leaves the directory in an ERROR state

This problem can occur if you're trying to register an AWS Managed Microsoft AD directory that has been configured for multi-Region replication. Although the directory in the primary Region can be successfully registered for use with Amazon WorkSpaces, attempting to register the directory in a replicated Region fails. Multi-Region replication with AWS Managed Microsoft AD isn't supported for use with Amazon WorkSpaces within replicated Regions.

My users can't connect to a Windows WorkSpace with an interactive logon banner

If an interactive logon message has been implemented to display a logon banner, this prevents users from being able to access their Windows WorkSpaces. The interactive logon message Group Policy setting is not currently supported by PCoIP WorkSpaces. Move the WorkSpaces to an organizational unit (OU) where the **Interactive logon: Message text for users attempting to log on** Group Policy isn't applied. The logon message is supported on WSP WorkSpaces, and users have to login again after accepting the logon banner.

My users can't connect to a Windows WorkSpace

My users receive the following error when they try to connect to their Windows WorkSpaces:

```
"An error occurred while launching your WorkSpace. Please try again."
```

This error often occurs when the WorkSpace can't load the Windows desktop using PCoIP. Check the following:

- This message appears if the PCoIP Standard Agent for Windows service is not running. Connect using RDP to verify that the service is running, that it's set to start automatically, and that it can communicate over the management interface (eth0).

- If the PCoIP agent was uninstalled, reboot the WorkSpace through the Amazon WorkSpaces console to reinstall it automatically.

- You might also receive this error on the Amazon WorkSpaces client after a long delay if the WorkSpaces security group was modified to restrict outbound traffic. Restricting outbound traffic prevents Windows from communicating with your directory controllers for login. Verify that your security groups allow your WorkSpaces to communicate with your directory controllers on all required ports over the primary network interface.

Another cause of this error is related to the User Rights Assignment Group Policy. If the following group policy is incorrectly configured, it prevents users from being able to access their Windows WorkSpaces:

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

- **Incorrect policy:**

  Policy: **Access this computer from the network**

  Setting: *Domain name*\Domain Computers

  Winning GPO: Allow File Access

- **Correct policy:**

  Policy: **Access this computer from the network**

  Setting: *Domain name*\Domain Users

  Winning GPO: Allow File Access

> **Note**
>
> This policy setting should be applied to **Domain Users** instead of **Domain Computers**.

For more information, see Access this computer from the network - security policy setting and Configure security policy settings in the Microsoft Windows documentation.

My users are having issues when they try to log on to WorkSpaces from WorkSpaces Web Access

Amazon WorkSpaces relies on a specific logon screen configuration to enable users to successfully log on from their Web Access client.

To enable Web Access users to log on to their WorkSpaces, you must configure a Group Policy setting and three Security Policy settings. If these settings are not correctly configured, users might experience long logon times or black screens when they try to log on to their WorkSpaces. To configure these settings, see Enable and configure WorkSpaces Web Access for WorkSpaces Personal.

Important

Beginning October 1, 2020, customers will no longer be able to use the Amazon WorkSpaces Web Access client to connect to Windows 7 custom WorkSpaces or to Windows 7 Bring Your Own License (BYOL) WorkSpaces.

The Amazon WorkSpaces client displays a gray "Loading..." screen for a while before returning to the login screen. No other error message appears.

This behavior usually indicates that the WorkSpaces client can authenticate over port 443, but can't establish a streaming connection over port 4172 (PCoIP) or port 4195 (WSP). This situation can occur when network prerequisites aren't met. Issues on the client side often cause the network check in the client to fail. To see which health checks are failing, choose the network check icon (typically a red triangle with an exclamation point in the bottom-right corner of the login screen for 2.0+ clients or the network icon 
in the upper-right corner of the 3.0+ clients).

Note

The most common cause of this problem is a client-side firewall or proxy preventing access over port 4172 or 4195 (TCP and UDP). If this health check fails, check your local firewall settings.

If the network check passes, there might be a problem with the network configuration of the WorkSpace. For example, a Windows Firewall rule might block port UDP 4172 or 4195 on the management interface. Connect to the WorkSpace using a Remote Desktop Protocol (RDP) client to verify that the WorkSpace meets the necessary port requirements.

My users receive the message "WorkSpace Status: Unhealthy. We were unable to connect you to your WorkSpace. Please try again in a few minutes."

This error usually indicates the SkyLightWorkSpacesConfigService service isn't responding to health checks.

If you just rebooted or started your WorkSpace, wait a few minutes, and then try again.

If the WorkSpace has been running for some time and you still see this error, connect using RDP to verify that the SkyLightWorkSpacesConfigService service:

- Is running.
- Is set to start automatically.
- Can communicate over the management interface (eth0).
- Isn't blocked by any third-party antivirus software.

My users receive the message "This device is not authorized to access the WorkSpace. Please contact your administrator for assistance."

This error indicates that one of the following might be occurring:

- IP access control groups are configured on the WorkSpace directory, but the client IP address isn't allowlisted.

  Check the settings on your directory. Confirm that the public IP address the user is connecting from allows access to the WorkSpace.
- Under access control, your device's operating system isn't allowed as a trusted device or your device doesn't have the proper certificates installed when using the **Trusted devices** option. Add your device type as a trusted device by doing the following:

  1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
  2. In the navigation pane, choose **Directories**.
  3. Choose the directory you're using.
  4. Scroll down to **Access control options** and choose **Edit**.
  5. Under **Trusted devices**, for the device types you want to allow access to, choose **Allow all** in the drop-down. If you want to restrict the devices to ones that have client certificates installed, choose **Trusted devices**.
  6. If you chose **Trusted devices** in the previous step, ensure you have imported at least one root certificate and that the client certificate that has been issued by the root certification authority (CA) has been installed on the client. For more information about creating,

deploying, and importing root certificates, see Restrict access to trusted devices for WorkSpaces Personal.

7. Choose **Save**.

- Your device types are not granted access to WorkSpaces. Grant access to your device type by doing the following:

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Choose the directory you're using.
4. Scroll down to **Other platforms** and choose **Edit**.
5. Check from one of the following device types you want to grant WorkSpaces access.
   - ChromeOS
   - iOS
   - Linux
   - Web Access
   - Zero Clients
6. Choose **Save**.

My users receive the message "No network. Network connection lost. Check your network connection or contact your administrator for help." when trying to connect to a WSP WorkSpace

If this error occurs and your users don't have connectivity issues, make sure that port 4195 is open on your network's firewalls. For WorkSpaces using the WorkSpaces Streaming Protocol (WSP), the port used to stream the client session was changed from 4172 to 4195.

The WorkSpaces client gives my users a network error, but they are able to use other network-enabled apps on their devices

The WorkSpaces client applications rely on access to resources in the AWS Cloud, and require a connection that provides at least 1 Mbps download bandwidth. If a device has an intermittent connection to the network, the WorkSpaces client application might report an issue with the network.

WorkSpaces enforces the use of digital certificates issued by Amazon Trust Services, as of May 2018. Amazon Trust Services is already a trusted Root CA on the operating systems that are supported by WorkSpaces. If the Root CA list for the operating system is not up to date, the device cannot connect to WorkSpaces and the client gives a network error.

To recognize connection issues due to certificate failures

- PCoIP zero clients — The following error message is displayed.

```
Failed to connect. The server provided a certificate that is invalid. See below for
 details:
- The supplied certificate is invalid due to timestamp
- The supplied certificate is not rooted in the devices local certificate store
```

- Other clients — The health checks fail with a red warning triangle for **Internet**.

To resolve certificate failures

- Windows client application
- PCoIP zero clients
- Other client applications

Windows client application

Use one of the following solutions for certificate failures.

Solution 1: Update the client application

Download and install the latest Windows client application from https://clients.amazonworkspaces.com/ . During installation, the client application ensures that your operating system trusts certificates issued by Amazon Trust Services.

Solution 2: Add Amazon Trust Services to the local Root CA list

1. Open https://www.amazontrust.com/repository/.
2. Download the Starfield certificate in DER format (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92).
3. Open the Microsoft Management Console. (From the Command Prompt, run **mmc**.)
4. Choose **File**, **Add/Remove Snap-in**, **Certificates**, **Add**.

5. On the **Certificates snap-in** page, select **Computer account** and choose **Next**. Keep the default, **Local computer**. Choose **Finish**. Choose **OK**.
6. Expand **Certificates (Local Computer)** and select **Trusted Root Certification Authorities**. Choose **Action**, **All Tasks**, **Import**.
7. Follow the wizard to import the certificate that you downloaded.
8. Exit and restart the WorkSpaces client application.

Solution 3: Deploy Amazon Trust Services as a trusted CA using Group Policy

Add the Starfield certificate to the trusted Root CAs for the domain using Group Policy. For more information, see Use Policy to Distribute Certificates.

PCoIP zero clients

To connect directly to a WorkSpace using firmware version 6.0 or later, download and install the certificate issued by Amazon Trust Services.

To add Amazon Trust Services as a trusted Root CA

1. Open https://certs.secureserver.net/repository/.
2. Download the certificate under **Starfield Certificate Chain** with the thumbprint 14 65 FA 20 53 97 B8 76 FA A6 F0 A9 95 8E 55 90 E4 0F CC 7F AA 4F B7 C2 C8 67 75 21 FB 5F B6 58.
3. Upload the certificate to the zero client. For more information, see Uploading Certificates in the Teradici documentation.

Other client applications

Add the Starfield certificate (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92) from Amazon Trust Services. For more information about how to add a Root CA, see the following documentation:

- Android: Add & remove certificates
- Chrome OS: Manage client certificates on Chrome devices
- macOS and iOS: Installing a CA's Root Certificate on Your Test Device

My WorkSpace users see the following error message: "Device can't connect to the registration service. Check your network settings."

When a registration service failure occurs, your WorkSpace users might see the following error message on the **Connection Health Check** page: "Your device is not able to connect to the WorkSpaces Registration service. You will not be able to register your device with WorkSpaces. Please check your network settings."

This error occurs when the WorkSpaces client application can't reach the registration service. Typically, this happens when the WorkSpaces directory has been deleted. To resolve this error, make sure that the registration code is valid and corresponds to a running directory in the AWS Cloud.

My PCoIP zero client users are receiving the error "The supplied certificate is invalid due to timestamp"

If Network Time Protocol (NTP) isn't enabled in Teradici, your PCoIP zero client users might receive certificate failure errors. To set up NTP, see Set up PCoIP zero clients for WorkSpaces Personal.

USB printers and other USB peripherals aren't working for PCoIP zero clients

Starting with version 20.10.4 of the PCoIP agent, Amazon WorkSpaces disables USB redirection by default through the Windows registry. This registry setting affects the behavior of USB peripherals when your users are using PCoIP zero client devices to connect to their WorkSpaces.

If your WorkSpaces are using version 20.10.4 or later of the PCoIP agent, USB peripheral devices won't work with PCoIP zero client devices until you've enabled USB redirection.

> **Note**
>
> If you're using 32-bit virtual printer drivers, you must also update those drivers to their 64-bit versions.

To enable USB redirection for PCoIP zero client devices

We recommend that you push out these registry changes to your WorkSpaces through Group Policy. For more information, see Configuring the agent and Configurable settings in the Teradici documentation.

1. Set the following registry key value to 1 (enabled):

   KeyPath = **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP\pcoip_admin**

   KeyName = **pcoip.enable_usb**

   KeyType = **DWORD**

   KeyValue = **1**
2. Set the following registry key value to 1 (enabled):

   KeyPath = **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP \pcoip_admin_defaults**

   KeyName = **pcoip.enable_usb**

   KeyType = **DWORD**

   KeyValue = **1**
3. If you haven't already done so, log out of the WorkSpace, and then log back in. Your USB devices should now work.

My users skipped updating their Windows or macOS client applications and aren't getting prompted to install the latest version

When users skip updates to the Amazon WorkSpaces Windows client application, the **SkipThisVersion** registry key gets set, and they are no longer prompted to update their clients when a new version of the client is released. To update to the latest version, you can edit the registry as described in Update the WorkSpaces Windows Client Application to a Newer Version in the *Amazon WorkSpaces User Guide*. You can also run the following PowerShell command:

```
Remove-ItemProperty -Path "HKCU:\Software\Amazon Web Services. LLC\Amazon WorkSpaces
\WinSparkle" -Name "SkipThisVersion"
```

When users skip updates to the Amazon WorkSpaces macOS client application, the `SUSkippedVersion` preference gets set, and they are no longer prompted to update their clients when a new version of the client is released. To update to the latest version, you can reset this preference as described in Update the WorkSpaces macOS Client Application to a Newer Version in the *Amazon WorkSpaces User Guide*.

My users are unable to install the Android client application on their Chromebooks

Version 2.4.13 is the final release of the Amazon WorkSpaces Chromebook client application. Because Google is phasing out support for Chrome Apps, there will be no further updates to the WorkSpaces Chromebook client application, and its use is unsupported.

For Chromebooks that support installing Android applications, we recommend using the WorkSpaces Android client application instead.

In some cases, you might need to enable your users' Chromebooks to install Android applications. For more information, see Set up Android for Chromebooks for WorkSpaces Personal.

My users aren't receiving invitation emails or password reset emails

Users do not automatically receive welcome or password reset emails for WorkSpaces that were created using AD Connector or a trusted domain. Invitation emails also aren't sent automatically if the user already exists in Active Directory.

To manually send welcome emails to these users, see Send an invitation email.

To reset user passwords, see Set up Active Directory Administration Tools for WorkSpaces Personal.

My users don't see the Forgot password? option on the client login screen

If you're using AD Connector or a trusted domain, your users won't be able to reset their own passwords. (The **Forgot password?** option on the WorkSpaces client application login screen won't be available.) For information about how to reset user passwords, see Set up Active Directory Administration Tools for WorkSpaces Personal.

I receive the message "The system administrator has set policies to prevent this installation" when I try to install applications on a Windows WorkSpace

You can address this issue by modifying the Windows Installer Group Policy setting. To deploy this policy to multiple WorkSpaces in your directory, apply this setting to a Group Policy object that is linked to the WorkSpaces organizational unit (OU) from a domain-joined EC2 instance. If you are using AD Connector, you can make these changes from a domain controller. For more information about using the Active Directory administration tools to work with Group Policy objects, see Installing the Active Directory Administration Tools in the *AWS Directory Service Administration Guide*.

The following procedure shows how to configure the Windows Installer setting for the WorkSpaces Group Policy object.

1. Make sure that the most recent WorkSpaces Group Policy administrative template is installed in your domain.
2. Open the Group Policy Management tool on your Windows WorkSpace client and navigate to and select the WorkSpaces Group Policy object for your WorkSpaces machine accounts. From the main menu, choose **Action**, **Edit**.
3. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Classic Administrative Templates**, **Windows Components**, **Windows Installer**.
4. Open the **Turn Off Windows Installer** setting.
5. In the **Turn Off Windows Installer** dialog box, change **Not Configured** to **Enabled**, and then set **Disable Windows Installer** to **Never**.
6. Choose **OK**.
7. To apply the group policy changes, do one of the following:
   - Reboot the WorkSpace (in the WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - From an administrative command prompt, enter **gpupdate /force**.

No WorkSpaces in my directory can connect to the internet

WorkSpaces cannot communicate with the internet by default. You must explicitly provide internet access. For more information, see Provide internet access for WorkSpaces Personal.

My WorkSpace has lost its internet access

If your WorkSpace has lost access to the internet and you can't connect to the WorkSpace by using RDP, this issue is probably caused by the loss of the public IP address for the WorkSpace. If you have enabled automatic assignment of Elastic IP addresses at the directory level, an Elastic IP address (from the Amazon-provided pool) is assigned to your WorkSpace when it is launched. However, if you associate an Elastic IP address that you own to a WorkSpace, and then you later disassociate that Elastic IP address from the WorkSpace, the WorkSpace loses its public IP address, and it doesn't automatically get a new one from the Amazon-provided pool.

To associate a new public IP address from the Amazon-provided pool with the WorkSpace, you must rebuild the WorkSpace. If you don't want to rebuild the WorkSpace, you must associate another Elastic IP address that you own to the WorkSpace.

We recommend that you not modify the elastic network interface of a WorkSpace after the WorkSpace is launched. After an Elastic IP address has been assigned to a WorkSpace, the WorkSpace retains the same public IP address (unless the WorkSpace is rebuilt, in which case it gets a new public IP address).

I receive a "DNS unavailable" error when I try to connect to my on-premises directory

You receive an error message similar to the following when connecting to your on-premises directory.

```
DNS unavailable (TCP port 53) for IP: dns-ip-address
```

AD Connector must be able to communicate with your on-premises DNS servers via TCP and UDP over port 53. Verify that your security groups and on-premises firewalls allow TCP and UDP communication over this port.

I receive a "Connectivity issues detected" error when I try to connect to my on-premises directory

You receive an error message similar to the following when connecting to your on-premises directory.

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: ip-address
Kerberos/authentication unavailable (TCP port 88) for IP: ip-address
Please ensure that the listed ports are available and retry the operation.
```

AD Connector must be able to communicate with your on-premises domain controllers via TCP and UDP over the following ports. Verify that your security groups and on-premises firewalls allow TCP and UDP communication over these ports:

- 88 (Kerberos)
- 389 (LDAP)

I receive an "SRV record" error when I try to connect to my on-premises directory

You receive an error message similar to one or more of the following when connecting to your on-premises directory.

```
SRV record for LDAP does not exist for IP: dns-ip-address

SRV record for Kerberos does not exist for IP: dns-ip-address
```

AD Connector needs to obtain the `_ldap._tcp.`*`dns-domain-name`* and `_kerberos._tcp.`*`dns-domain-name`* SRV records when connecting to your directory. You get this error if the service cannot obtain these records from the DNS servers that you specified when connecting to your directory. Make sure that your DNS servers contain these SRV records. For more information, see SRV Resource Records on Microsoft TechNet.

My Windows WorkSpace goes to sleep when it's left idle

To resolve this issue, connect to the WorkSpace and change the power plan to **High performance** by using the following procedure:

1. From the WorkSpace, open **Control Panel**, then choose **Hardware** or choose **Hardware and Sound** (the name might differ, depending on your version of Windows).
2. Under **Power Options**, choose **Choose a power plan**.
3. In the **Choose or customize a power plan** pane, choose the **High performance** power plan, and then choose **Change plan settings**.
   - If the option to choose the **High performance** power plan is disabled, choose **Change settings that are currently unavailable**, and then choose the **High performance** power plan.
   - If the **High performance** plan isn't visible, choose the arrow to the right of **Show additional plans** to display it, or choose **Create a power plan** in the left navigation, choose **High performance**, give the power plan a name, and then choose **Next**.
4. On the **Change settings for the plan: High performance** page, make sure **Turn off the display** and (if available) **Put the computer to sleep** are set to **Never**.
5. If you made any changes to the high performance plan, choose **Save changes** (or choose **Create** if you're creating a new plan).

If the preceding steps do not solve the issue, do the following:

1. From the WorkSpace, open **Control Panel**, then choose **Hardware** or choose **Hardware and Sound** (the name might differ, depending on your version of Windows).
2. Under **Power Options**, choose **Choose a power plan**.
3. In the **Choose or customize a power plan** pane, choose the **Change plan settings** link to the right of the **High performance** power plan, then choose the **Change advanced power settings** link.
4. In the **Power Options** dialog box, in the list of settings, choose the plus sign to the left of **Hard disk** to display the relevant settings.
5. Verify that the **Turn off hard disk after** value for **Plugged in** is greater than the value for **On battery** (the default value is 20 minutes).
6. Choose the plus sign to the left of **PCI Express**, and do the same for **Link State Power Management**.
7. Verify that the **Link State Power Management** settings are **Off**.
8. Choose **OK** (or **Apply** if you changed any settings) to close the dialog box.
9. In the **Change settings for the plan** pane, if you changed any settings, choose **Save changes**.

One of my WorkSpaces has a state of `UNHEALTHY`

The WorkSpaces service periodically sends status requests to a WorkSpace. A WorkSpace is marked `UNHEALTHY` when it fails to respond to these requests. Common causes for this problem are:

- An application on the WorkSpace is blocking network ports, which prevents the WorkSpace from responding to the status request.
- High CPU utilization is preventing the WorkSpace from responding to the status request in a timely manner.
- The computer name of the WorkSpace has been changed. This prevents a secure channel from being established between WorkSpaces and the WorkSpace.

You can attempt to correct the situation using the following methods:

- Reboot the WorkSpace from the WorkSpaces console.
- Connect to the unhealthy WorkSpace using the following procedure, which should be used only for troubleshooting purposes:

  1. Connect to an operational WorkSpace in the same directory as the unhealthy WorkSpace.

2. From the operational WorkSpace, use Remote Desktop Protocol (RDP) to connect to the unhealthy WorkSpace using the IP address of the unhealthy WorkSpace. Depending on the extent of the problem, you might not be able to connect to the unhealthy WorkSpace.
3. On the unhealthy WorkSpace, confirm that the minimum port requirements are met.

- Make sure the SkyLightWorkSpacesConfigService service can respond to health checks. To troubleshoot this issue, see My users receive the message "WorkSpace Status: Unhealthy. We were unable to connect you to your WorkSpace. Please try again in a few minutes.".
- Rebuild the WorkSpace from the WorkSpaces console. Because rebuilding a WorkSpace can potentially cause a loss of data, this option should be used only if all other attempts to correct the problem have been unsuccessful.

My WorkSpace is unexpectedly crashing or rebooting

If your WorkSpace configured for PCoIP is repeatedly crashing or rebooting and your error logs or crash dumps are pointing to problems with `spacedeskHookKmode.sys` or `spacedeskHookUmode.dll`, or if you're receiving the following error messages, you might need to disable Web Access to the WorkSpace:

```
The kernel power manager has initiated a shutdown transition.
Shutdown reason: Kernel API
```

```
The computer has rebooted from a bugcheck.
```

Note

- These troubleshooting steps are not applicable to WorkSpaces that are configured for WorkSpaces Streaming Protocol (WSP). They are applicable only to WorkSpaces that are configured for PCoIP.
- You should disable Web Access only if you aren't allowing your users to use Web Access.

To disable Web Access to the WorkSpace, you must disable Web Access in the WorkSpaces directory and reboot the WorkSpace.

The same username has more than one WorkSpace, but the user can log in to only one of the WorkSpaces

If you delete a user in Active Directory (AD) without first deleting their WorkSpace and then you add the user back to Active Directory and create a new WorkSpace for that user, the same username will now have two WorkSpaces in the same directory. However, if the user tries to connect to their original WorkSpace, they will receive the following error:

```
"Unrecognized user. No WorkSpace found under your username. Contact your administrator
 to request one."
```

Additionally, searches for the username in the Amazon WorkSpaces console return only the new WorkSpace, even though both WorkSpaces still exist. (You can find the original WorkSpace by searching for the WorkSpace ID instead of the username.)

This behavior can also occur if you rename a user in Active Directory without first deleting their WorkSpace. If you then change their username back to the original username and create a new WorkSpace for the user, the same username will have two WorkSpaces in the directory.

This problem occurs because Active Directory uses the user's security identifier (SID), rather than the username, to uniquely identify the user. When a user is deleted and recreated in Active Directory, the user is assigned a new SID, even if their username remains the same. During searches for a username, the Amazon WorkSpaces console uses the SID to search Active Directory for matches. The Amazon WorkSpaces clients also use the SID to identify users when they are connecting to WorkSpaces.

To resolve this problem, do one of the following:

- If this problem occurred because the user was deleted and recreated in Active Directory, you might be able to restore the original deleted user object if you have enabled the Recycle Bin feature in Active Directory. If you're able to restore the original user object, make sure the user can connect to their original WorkSpace. If they can, you can delete the new WorkSpace after manually backing up and transferring any user data from the new WorkSpace to the original WorkSpace (if needed).
- If you can't restore the original user object, delete the user's original WorkSpace. The user should be able to connect to and use their new WorkSpace instead. Be sure to manually back up and transfer any user data from the original WorkSpace to the new WorkSpace.

> **Warning**
>
> Deleting a WorkSpace is a permanent action and cannot be undone. The WorkSpace user's data does not persist and is destroyed. For help with backing up user data, contact AWS Support.

I'm having trouble using Docker with Amazon WorkSpaces

Windows WorkSpaces

Nested virtualization (including the use of Docker) is not supported on Windows WorkSpaces. For more information, see the Docker documentation.

Linux WorkSpaces

To use Docker on Linux WorkSpaces, make sure that the CIDR blocks used by Docker don't overlap with the CIDR blocks used in the two elastic network interfaces (ENIs) associated with the WorkSpace. If you encounter problems with using Docker on Linux WorkSpaces, contact Docker for assistance.

I receive ThrottlingException errors to some of my API calls

The default allowed rate for WorkSpaces API calls is a constant rate of two API calls per second, with a maximum allowed "burst" rate of five API calls per second. The following table shows how the burst rate limit works for API requests.

Second	Number of requests sent	Net requests allowed	Details
1	0	5	During the first second (second 1), five requests are allowed, up to the burst rate maximum of five calls per second.
2	2	5	Because two or fewer calls were issued in second 1, the full burst capacity of five calls is still available.

Second	Number of requests sent	Net requests allowed	Details
3	5	5	Because only two calls were issued in second 2, the full burst capacity of five calls is still available.
4	2	2	Because the full burst capacity was used in second 3, only the constant rate of two calls per second is available.
5	3	2	Because there is no remaining burst capacity, only two calls are allowed at this time. This means that one of the three API calls is throttled. The one throttled call will respond after a short delay.
6	0	1	Because one of the calls from second 5 is being retried in second 6, there is capacity for only one additional call in second 6 because of the constant rate limit of two calls per second.
7	0	3	Now that there are no longer any throttled API calls in the queue, the rate limit continues to increase, up to the burst rate limit of five calls.
8	0	5	Because no calls were issued in second 7, the maximum number of requests is allowed.
9	0	5	Even though no calls were issued in second 8, the rate limit does not increase above five.

My WorkSpace keeps disconnecting when I let it run in the background

For Mac users, check to see if the Power Nap feature is on. If it is on, turn it off. To turn Power Nap off, open your terminal and run the following command:

```
defaults write com.amazon.workspaces NSAppSleepDisabled -bool YES
```

SAML 2.0 federation isn't working. My users are not authorized to stream their WorkSpaces desktop.

This might happen because the inline policy that is embedded for the SAML 2.0 federation IAM role does not include permissions to stream from the directory Amazon Resource Name (ARN). The IAM role is assumed by the federated user who is accessing a WorkSpaces directory. Edit the role permissions to include the directory ARN and ensure that the user has a WorkSpace in the directory. For more information, see SAML 2.0 Authentication and Troubleshooting SAML 2.0 Federation with AWS.

My users are getting disconnected from their WorkSpaces session every 60 minutes.

If you have configured SAML 2.0 authentication to WorkSpaces, depending on your identity provider (IdP), you might need to configure the information that the IdP passes as SAML attributes to AWS as part of the authentication response. This includes configuring the **Attribute** element with the `SessionDuration` attribute set to `https://aws.amazon.com/SAML/Attributes/SessionDuration`.

`SessionDuration` specifies the maximum amount of time that a federated streaming session can remain active for a user before reauthentication is required. Although `SessionDuration` is an optional attribute, we recommend that you include it in the SAML authentication response. If you don't specify this attribute, the session duration defaults to 60 minutes.

To resolve this issue, configure your IdP to include the `SessionDuration` value in the SAML authentication response and set the value as required. For more information, see Step 5: Create assertions for the SAML authentication response.

My users get a redirect URI error when they federate using the SAML 2.0 identity provider (IdP)-initiated flow, or an additional instance of the WorkSpaces client application starts every time my users attempt to sign in from the client after federating to the IdP.

This error occurs due to a relay state URL that's not valid. Make sure that the relay state in your IdP federation setup is correct, and that the user access URL and relay state parameter name are configured correctly for your IdP federation in the WorkSpaces directory properties. If they are valid and the problem still persists, contact AWS Support. For more information, see Setting Up SAML.

My users receive the message, "Something went wrong: An error occurred while launching your WorkSpace" when they attempt to sign in to the WorkSpaces client application after federating to the IdP.

Review the SAML 2.0 assertions for your federation. The **SAML Subject NameID** value must match the WorkSpaces user name, and is typically the same as the **sAMAccountName** attribute for the Active Directory user. In addition, the **Attribute** element that has the `PrincipalTag:Email` attribute set to `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email` must match the WorkSpaces user's email address as defined in the WorkSpaces directory. For more information, see Setting Up SAML.

My users receive the message, "Unable to validate tags" when they attempt to sign in to the WorkSpaces client application after federating to the IdP.

Review the `PrincipalTag` attribute values in the SAML 2.0 assertions for your federation, such as `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`. Tag values may include combinations of the characters `_ . : / = + - @`, letters, numbers, and spaces.. For more information, see Rules for tagging in IAM and AWS STS.

My users receive the message, "The client and the server cannot communicate, because they do not possess a common algorithm".

This problem can occur if you do not enable TLS 1.2.

My microphone or web cam is not working on Windows WorkSpaces.

Check your privacy setting by opening the Start menu

- **Start** > **Settings** > **Privacy** > **Camera**
- **Start** > **Settings** > **Privacy** > **Microphone**

If they are turned off turn them on.

Alternatively, WorkSpaces administrators can create a Group Policy Object (GPO) to enable microphone and or webcam as needed.

My users cannot log in using certificate-based authentication and are prompted for the password either at the WorkSpaces client or the Windows sign-on screen when they connect to their desktop session.

Certificate-based authentication was unsuccessful for the session. If the problem continues, certificate-based authentication failure can be the result of one of the following issues:

- The WorkSpaces or the client is not supported. Certificate-based authentication is supported with Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) bundles using the latest WorkSpaces Windows client application.
- The WorkSpaces needs to be rebooted after enabling certificate-based authentication on the WorkSpaces Directory.
- WorkSpaces could not communicate with AWS Private CA, or AWS Private CA did not issue the certificate. Check AWS CloudTrail to determine if a certificate was issued. For more information, see Manage certificate-based authentication.
- The domain controller has no domain controller certificate for smart card logon, or it is expired. For more information, see step 7, "*Configure domain controllers with a domain controller certificate to authenticate smart card users*" in Prerequisites.
- The certificate is not trusted. For more information, see step 7, "*Publish the CA to Active Directory*" in Prerequisites. Run `certutil -viewstore -enterprise NTAuth` on domain controllers to confirm that the CA is published.
- There is a certificate in cache, but attributes have changed for the user that have invalidated the certificate. Contact AWS Support to clear the cache before certificate expiry (24 hours). For more information, see AWS Support Center.
- The userPrincipalName format for the `UserPrincipalName` SAML attribute is not formatted properly or does not resolve to the actual domain for the user. For more information, see step 1 in in Prerequisites.
- The (optional) `ObjectSid` attribute in your SAML assertion does not match the Active Directory security identifier (SID) for user specified in the SAML_Subject `NameID`. Confirm that attribute mapping is correct in your SAML federation and that your SAML identity provider is synchronizing the SID attribute for the Active Directory user.
- There are Group Policy settings that are modifying the default Active Directory settings for smart card logon or taking action if a smart card is removed from a smart card reader. These settings may cause additional unexpected behavior than the errors listed above. Certificate-based authentication presents a virtual smart card to the instance operating system and removes

it after logon is complete. Check the Primary Group Policy settings for smart cards and the Additional smart card Group Policy settings and registry keys, including Smart card removal behavior.

- The CRL distribution point for the private CA is not online nor accessible from either the WorkSpaces or the domain controller. For more information, see step 5 in Prerequisites.
- To check if there are any stale CAs in the domain or forest, run `PKIVIEW.msc` on the CA to verify. If there are stale CAs, use the `PKIVIEW.msc` mmc to manually delete them.
- To check if Active Directory replication is working and that there are no stale domain controllers in the domain, run `repadmin /replsum`.

Additional troubleshooting steps involve reviewing the WorkSpaces instance Windows event logs. A common event to review for logon failure is Event 4625: An account failed to logon in the Windows Security log.

If the problem persists, contact AWS Support. For more information, see AWS Support Center.

I am trying to do something that requires Windows installation media but WorkSpaces does not provide it.

If you are using an AWS-provided public bundle, you can use the Windows Server OS installation media EBS snapshots provided by Amazon EC2 when needed.

Create an EBS volume from these snapshots, attach it to Amazon EC2, and transfer the files to the WorkSpace where the files as needed. If you are using Windows 10 on BYOL on WorkSpaces and need an installation media, you will need to prepare your own installation media. For more information, see Add Windows components using installation media. Since you can't directly attach an EBS volume to a WorkSpace, you'll need to attach it to an Amazon EC2 instance and copy the files.

I want to launch WorkSpaces with an existing AWS Managed Directory created in an unsupported WorkSpaces Region.

To launch Amazon WorkSpaces using a directory in a Region that is not currently supported by WorkSpaces, follow the steps below.

> **Note**
>
> If you receive errors when running AWS Command Line Interface commands, ensure you're using the most recent AWS CLI version. For more information, see Confirm that you're running a recent version of the AWS CLI.

Step 1: Create virtual private cloud (VPC) peering with another VPC in your account

1. Create the VPC peering connection with a VPC in a different Region. For more information, see Create with VPCs in the same account and different Regions.
2. Accept the VPC peering connection. For more information, see Accept a VPC peering connection.
3. After you activate the VPC peering connection, you can view your VPC peering connections using the Amazon VPC console, the AWS CLI, or an API.

Step 2: Update route tables for VPC peering in both Regions

Update your route tables to turn on communication with the peer VPC over IPv4 or IPv6. For more information, see Update your route tables for a VPC peering connection.

Step 3: Create an AD Connector and register Amazon WorkSpaces

1. To review the AD Connector prerequisites, see AD Connector prerequisites.
2. Connect your existing directory with AD Connector. For more information, see Create an AD Connector.
3. When the AD Connector status changes to **Active**, open the AWS Directory Service console, then choose the hyperlink for your **Directory ID**.
4. For AWS apps and services, choose **Amazon WorkSpaces** to turn on access for WorkSpaces on this directory.
5. Register the directory with WorkSpaces. For more information, see Register a directory with WorkSpaces.

I want to update Firefox on Amazon Linux 2.

Step 1: Verify auto-update is enabled

To verify that autoupdate is enabled, run the command `systemctl status *os-update-mgmt.timer | grep enabled` on your WorkSpace. In the output, there should be two lines with the word `enabled` on them.

Step 2: Initiate an update

Firefox usually updates automatically in Amazon Linux 2 WorkSpaces along with all other software packages in the system during the maintenance window. However, this depends on the type of WorkSpaces you are using.

- For AlwaysOn WorkSpaces, the weekly maintenance window is on Sunday 00h00 to 04h00, in the time zone of the WorkSpace.
- For AutoStop WorkSpaces. beginning on the third Monday of the month, and for up to two weeks, the maintenance window is open each day from about 00h00 to 05h00, in the time zone of the AWS Region for the WorkSpace.

For more information about maintenance windows, see WorkSpace maintenance.

You can also initiate an immediate update cycle by rebooting your WorkSpace and reconnecting after 15 minutes. You can also initiate updates by entering `sudo yum update`. To initiate an update for Firefox only, enter `sudo yum install firefox`.

If you are not able to configure access for Amazon Linux 2 repositories and prefer to install Firefox using binaries built by Mozilla, see Install Firefox from Mozilla builds on Mozilla support. We recommend uninstalling the RPM-packaged version of Firefox altogether to make sure you don't run an outdated version by mistake. You can uninstall it by running command `sudo yum remove firefox`.

You can also download the necessary RPM packages from Amazon Linux 2 repositories by running the command `yumdownloader firefox` on a different machine. Then, side-load the repositories onto WorkSpaces, where you can install them with a standard YUM command like `sudo yum install firefox-102.11.0-2.amzn2.0.1.x86_64.rpm`.

> **Note**
>
> The exact file name will change based on the package version.

Step 3: Verify Firefox repository is used

Amazon Linux Extras automatically provides Firefox updates for Amazon Linux 2 WorkSpaces. Amazon Linux 2 WorkSpaces created after July 31, 2023 will already have the Firefox Extra repository activated. To verify that your WorkSpace is using the Firefox Extra repository, run the following command.

```
yum repolist | grep amzn2extra-firefox
```

The command output should look something like `amzn2extra-firefox/2/x86_64 Amazon Extras repo for firefox 10` if Firefox Extra repository is used. It will be empty if the Firefox Extra repository is not used. If Firefox Extra repository is not used, you can attempt to enable it manually with the following command:

```
sudo amazon-linux-extras install firefox
```

If the Firefox Extra repository activation still fails, check your internet access and ensure that your VPC endpoints are unconfigured. To continue receiving Firefox updates for Amazon Linux 2 WorkSpaces via YUM repositories, ensure that your WorkSpaces are able to reach Amazon Linux 2 repositories. For more information on accessing Amazon Linux 2 repositories without internet access, see this knowledge center article.

My user is able to reset their password using the WorkSpaces client, ignoring the Fine Grained Password Policy (FFGP) setting that is configured on AWS Managed Microsoft AD.

If your user's WorkSpaces client is associated with AWS Managed Microsoft AD, they will have to reset their password using the default complexity setting.

The default complexity password is case-sensitive and must be between 8 and 64 characters in length, inclusive. It must contain at least one character from each of the following categories:

- Lowercase characters (a-z)

- Uppercase characters (A-Z)
- Numbers (0-9)
- Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Make sure the password doesn't include non-printable unicode characters, such as white spaces, carriage reture tabs, line breaks, and null characters.

If your organization requires you to enforce FFGP for WorkSpaces, contact your Active Directory administrator to reset your user's password directly from the Active Directory instead of the WorkSpaces client.

My users receive the error message "This OS/platform is not authorized to access your WorkSpace" when trying to access the Windows/Linux WorkSpace using Web Access

The operating system version your user is trying to use isn't compatible with WorkSpaces Web Access. Make sure you enable Web Access under the WorkSpace directory's **Other Platform** setting. For more information on enabling your WorkSpace's Web Access, see Enable and configure WorkSpaces Web Access for WorkSpaces Personal.

Client application end of life policy for WorkSpaces Personal

The Amazon WorkSpaces end of life (EOL) policy is applicable to specific major versions (and all of their minor versions) of WorkSpaces that no longer receive support and are no longer tested for compatibility with newer versions.

The lifecycle of a WorkSpaces client version has three phases—general support, technical guidance, and end of life(EOL). The general support phase begins on the date of initial public release of a WorkSpaces client and lasts for a fixed duration. During the general support phase, the WorkSpaces support team provides full support for configuration issues. Defect resolutions and feature requests are implemented for that major version and the associated minor versions of the WorkSpaces client.

Technical guidance is provided from the end of the general support phase until the EOL date. During the technical guidance phase, you receive support and guidance for supported configurations only. Defect resolutions and feature requests are implemented for the most recent versions of the WorkSpaces client only. They are not implemented for older versions. During the

technical guidance phase, if a fix is required, AWS will schedule that fix for the upcoming publicly available version release, and you will have the option to upgrade to the latest WorkSpaces version to receive support related to the fix.

EOL for a major version occurs when both general support and technical guidance have ended. After the EOL date, no further support or maintenance is provided. AWS stops testing for compatibility issues. For continued support, you must upgrade to the latest WorkSpaces client version.

Refer to this table for more information about support for specific versions.

Windows client	General support	Technical guidance	EOL
2.x	2018	March 31, 2023	August 31, 2023

Linux client	General support	Technical guidance	EOL
4.x for Ubuntu 18.04	August 12, 2021	March 31, 2023	August 31, 2023
3.x for Ubuntu 18.04	November 25, 2019	March 31, 2023	August 31, 2023

macOS client	General support	Technical guidance	EOL
2.x	2019	March 31, 2023	August 31, 2023
1.x	2018	March 31, 2023	August 31, 2023

iPad client	General support	Technical guidance	EOL
1.x	2018	March 31, 2023	August 31, 2023

Android client	General support	Technical guidance	EOL
2.x	2019	March 31, 2023	August 31, 2023

Android client	General support	Technical guidance	EOL
1.x	2018	March 31, 2023	August 31, 2023

Web access	General support
Google Chrome	Current version, plus two most recent major versions
Firefox	Current version, plus two most recent major versions
Microsoft Edge	Current version, plus two most recent major versions

Unsupported clients

The following WorkSpaces clients are not supported.

Operating system	Client version	General support	Technical guidance	EOL	Notes
Windows	5.11	July 3, 2023	October 1, 2023	October 1, 2023	Not supported due to quality issues
Windows	5.10	June 19, 2023	October 1, 2023	October 1, 2023	Not supported due to quality issues

Operating system	Client version	General support	Technical guidance	EOL	Notes
Windows	5.9	May 9, 2023	October 1, 2023	October 1, 2023	Not supported due to quality issues

EOL FAQs

I'm using a version of a WorkSpaces client that has reached its EOL. What should I do to upgrade to a supported version?

Go to the WorkSpaces client download page to download and install a fully supported version of WorkSpaces.

Can I use a version of the WorkSpaces client that has reached its EOL with a supported WorkSpace?

We strongly recommend upgrading your clients to the latest version as previous resolutions and features are no longer applied to clients versions that have reached their EOL. If you are using a client version that has reached its EOL, contact the AWS support team for more information.

I'm using a version of a WorkSpaces client that has reached its EOL. Can I still report issues for it?

You must first upgrade to a supported version and try to reproduce the issue. If the issue persists in the supported version, open a support case with the AWS support team.

I'm using a supported WorkSpaces client version on an operating system that has reached its EOL. Can I still report issues for it?

Technical assistance and software updates are no longer available for operating systems that have reached EOL and AWS doesn't provide support to WorkSpaces clients that use operating systems that have reached its EOL. Use a supported operating system to ensure you have support for your WorkSpaces clients.

Manage WorkSpaces Pools

WorkSpaces Pools offers non-persistent virtual desktops, tailored for users who need access to highly-curated desktop environments hosted on ephemeral infrastructure.

Topics

AWS Regions and Availability Zones for WorkSpaces Pools

WorkSpaces Pools is available in the following AWS Regions.

> **Note**
>
> For the AWS Regions that apply to WorkSpaces Personal, see Amazon WorkSpaces endpoints and quotas in the *AWS General Reference Reference guide*.

Region Name	Region	Endpoint	Protocol	Availability Zones	
US East (N.	us-east-1	workspaces.us-east-1.amazonaws.com	HTTPS	use1-az2,	

Region Name	Region	Endpoint	Protocol	Availability Zones	
Virginia)		workspaces-fips.us-east-1.amazonaws.com	HTTPS	use1-az4, use1-az6	
US West (Oregon)	us-west-2	workspaces.us-west-2.amazonaws.com workspaces-fips.us-west-2.amazonaws.com	HTTPS HTTPS	usw2-az1, usw2-az2, usw2-az3	
Asia Pacific (Mumbai)	ap-south-1	workspaces.ap-south-1.amazonaws.com	HTTPS	aps1-az1, aps1-az3	
Asia Pacific (Seoul)	ap-northeast-2	workspaces.ap-northeast-2.amazonaws.com	HTTPS	apne2-az1, apne2-az3	
Asia Pacific (Singapore)	ap-southeast-1	workspaces.ap-southeast-1.amazonaws.com	HTTPS	apse1-az1, apse1-az2	
Asia Pacific (Sydney)	ap-southeast-2	workspaces.ap-southeast-2.amazonaws.com	HTTPS	apse2-az1, apse2-az3	

Region Name	Region	Endpoint	Protocol	Availability Zones	
Asia Pacific (Tokyo)	ap-northeast-1	workspaces.ap-northeast-1.amazonaws.com	HTTPS	apne1-az1, apne1-az4	
Canada (Central)	ca-central-1	workspaces.ca-central-1.amazonaws.com	HTTPS	cac1-az1, cac1-az2	
Europe (Frankfurt)	eu-central-1	workspaces.eu-central-1.amazonaws.com	HTTPS	euc1-az2, euc1-az3	
Europe (Ireland)	eu-west-1	workspaces.eu-west-1.amazonaws.com	HTTPS	euw1-az1, euw1-az2, euw1-az3	
Europe (London)	eu-west-2	workspaces.eu-west-2.amazonaws.com	HTTPS	euw2-az2, euw2-az3	
South America (São Paulo)	sa-east-1	workspaces.sa-east-1.amazonaws.com	HTTPS	sae1-az1, sae1-az3	

Region Name	Region	Endpoint	Protocol	Availability Zones	
AWS GovCloud (US-East)	us-gov-east-1	workspaces.us-gov-east-1.amazonaws.com workspaces-fips.us-gov-east-1.amazonaws.com	HTTPS HTTPS	usgw1-az1, usgw1-az2, usgw1-az3	
AWS GovCloud (US-West)	us-gov-west-1	workspaces.us-gov-west-1.amazonaws.com workspaces-fips.us-gov-west-1.amazonaws.com	HTTPS HTTPS	usge1-az1, usge1-az2, usge1-az3	

Manage directories for WorkSpaces Pools

WorkSpaces Pools uses a directory to store and manage information for your WorkSpaces and users. In this section, we show you how to create and manage directories for WorkSpaces Pools.

Contents

Configure SAML 2.0 and create a WorkSpaces Pools directory

You can enable WorkSpaces client application registration and signing in to WorkSpaces in a WorkSpaces Pool by setting up identity federation using SAML 2.0. To do this, you use an AWS Identity and Access Management (IAM) role and a relay state URL to configure your SAML 2.0 identity provider (IdP) and enable it for AWS. This grants your federated users access to a WorkSpace Pool directory. The relay state is the WorkSpaces directory endpoint to which users are forwarded after successfully signing in to AWS.

Topics

Step 1: Consider the requirements

The following requirements apply when setting up SAML for a WorkSpaces Pools directory.

- The workspaces_DefaultRole IAM role must exist in your AWS account. This role is automatically created when you use the WorkSpaces Quick Setup or if you previously launched a WorkSpace using the AWS Management Console. It grants Amazon WorkSpaces permission to access specific AWS resources on your behalf. If the role already exists, you might need to attach the AmazonWorkSpacesPoolServiceAccess managed policy to it, which Amazon WorkSpaces uses to access required resources in the AWS account for WorkSpaces Pools. For more information, see Create the workspaces_DefaultRole Role and AWS managed policy: AmazonWorkSpacesPoolServiceAccess.
- You can configure SAML 2.0 authentication for WorkSpaces Pools in the AWS Regions that support the feature. For more information, see AWS Regions and Availability Zones for WorkSpaces Pools.
- To use SAML 2.0 authentication with WorkSpaces, the IdP must support unsolicited IdP-initiated SSO with a deep link target resource or relay state endpoint URL. Examples of IdPs that support this include ADFS, Azure AD, Duo Single Sign-On, Okta, PingFederate, and PingOne. Consult your IdP documentation for more information.
- SAML 2.0 authentication is supported only on the following WorkSpaces clients. For the latest WorkSpaces clients, see the Amazon WorkSpaces Client Download page.
  - Windows client application version 5.20.0 or later

- macOS client version 5.20.0 or later
- Web Access

Step 2: Complete the prerequisites

Complete the following prerequisites before configuring your SAML 2.0 IdP connection to a WorkSpaces Pool directory.

- Configure your IdP to establish a trust relationship with AWS.
- See Integrating third-party SAML solution providers with AWS for more information on configuring AWS federation. Relevant examples include IdP integration with IAM to access the AWS Management Console.
- Use your IdP to generate and download a federation metadata document that describes your organization as an IdP. This signed XML document is used to establish the relying party trust. Save this file to a location that you can access from the IAM console later.
- Create a WorkSpaces Pool directory by using the WorkSpaces console. For more information, see Using Active Directory with WorkSpaces Pools.
- Create a WorkSpaces Pool for users who can sign in to the IdP using a supported directory type. For more information, see Create a WorkSpaces Pool.

Step 3: Create a SAML identity provider in IAM

To get started, you must create a SAML IdP in IAM. This IdP defines your organization's IdP-to-AWS trust relationship using the metadata document generated by the IdP software in your organization. For more information, see Creating and managing a SAML identity provider in the *AWS Identity and Access Management User Guide*. For information about working with SAML IdPs in AWS GovCloud (US) Regions, see AWS Identity and Access Management in the *AWS GovCloud (US) User Guide*.

Step 4: Create WorkSpace Pool directory

Complete the following procedure to create a WorkSpaces Pool directory.

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose **Directories** in the navigation pane.
3. Choose **Create directory**.

4. For **WorkSpace type**, choose **Pool**.
5. In the **User identity source** section of the page:
   a. Enter a placeholder value into the **User access URL** text box. For example, enter `placeholder` into the text box. You will edit this later after setting up the application entitlement in your IdP.
   b. Leave the **Relay state parameter name** text box blank. You will edit this later after setting up the application entitlement in your IdP.
6. In the **Directory information** section of the page, enter a name and a description for the directory. The directory name and description must be less than 128 characters, can contain alphanumeric characters and the following special characters: `_ @ # % * + = : ? . / ! \ -`. The directory name and description cannot start with a special character.
7. In the **Networking and security** section of the page:
   a. Choose a VPC and 2 subnets that have access to the network resources that your application needs. For increased fault tolerance, you should choose two subnets in different Availability Zones.
   b. Choose a security group that allows WorkSpaces to create network links in your VPC. Security groups control what network traffic is allowed to flow from WorkSpaces to your VPC. For example, if your security group restricts all inbound HTTPS connections, users accessing your web portal won't be able to load HTTPS websites from the WorkSpaces.
8. The **Active Directory Config** section is optional. However, you should specify your Active Directory (AD) details during the creation of your WorkSpaces Pools directory if you plan to use an AD with your WorkSpaces Pools. You can't edit the **Active Directory Config** for your WorkSpaces Pools directory after you create it. For more information about specifying your AD details for your WorkSpaces Pool directory, see Specify Active Directory details for your WorkSpaces Pools directory. After you complete the process outlined in that topic, you should return to this topic to finish creating your WorkSpaces Pools directory.

   You can skip the **Active Directory Config** section if you don't plan on using an AD with your WorkSpaces Pools.
9. In the **Streaming properties** section of the page:
   - Choose the clipboard permissions behavior, and enter a copy to local character limit (optional), and paste to remote session character limit (optional).
   - Choose to allow or not allow print to local device.

- Choose to allow or not allow diagnostic logging.
- Choose to allow or not allow smart card sign in. This feature applies only if you enabled AD configuration earlier in this procedure.

10. In the **Storage** section of the page, you can choose to enable home folders.
11. In the **IAM role section** of the page, choose an IAM role to be available to all desktop streaming instances. To create a new one, choose **Create new IAM role**.

    When you apply an IAM role from your account to a WorkSpace Pool directory, you can make AWS API requests from a WorkSpace in the WorkSpace Pool without manually managing AWS credentials. For more information, see Creating a role to delegate permissions to an IAM user in *AWS Identity and Access Management User Guide*.
12. Choose **Create directory**.

Step 5: Create a SAML 2.0 federation IAM role

Complete the following procedure to create a SAML 2.0 federation IAM role in the IAM console.

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. Choose **Roles** in the navigation pane.
3. Choose Create role.
4. Choose **SAML 2.0 federation** for the trusted entity type.
5. For SAML 2.0-based provider, choose the identity provider you created in IAM. For more information, see Create a SAML identity provider in IAM.
6. Choose **Allow programmatic access only** for the access to be allowed.
7. Choose **SAML:aud** for the attribute.
8. For **Value**, enter `https://signin.aws.amazon.com/saml`. This value restricts role access to SAML user streaming requests that include a SAML subject type assertion with a value of `persistent`. If the SAML:sub_type is persistent, your IdP sends the same unique value for the `NameID` element in all SAML requests from a particular user. For more information, see Uniquely identifying users in SAML-based federation in *AWS Identity and Access Management User Guide*.
9. Choose **Next** to continue.
10. Don't make changes or selections in the **Add permissions** page. Choose **Next** to continue.
11. Enter a name and a description for the role.

12. Choose **Create role**.
13. In the **Roles** page, choose the role you must created.
14. Choose the **Trust relationships** tab.
15. Choose **Edit trust policy**.
16. In the **Edit trust policy** JSON text box, add the **sts:TagSession** action to the trust policy. For more information, see Passing session tags in AWS STS in *AWS Identity and Access Management User Guide*.

    The result should look like the following example.

17. Choose **Update policy**.
18. Choose the **Permissions** tab.
19. In the **Permissions policies** section of the page choose **Add permissions** and then choose **Create inline policy**.
20. In the **Policy editor** section of the page, choose **JSON**.
21. In the **Policy editor** JSON text box, enter the following policy. Be sure to replace:

    - *<region-code>* with the code of the AWS Region in which you created your WorkSpace Pool directory.
    - *<account-id>* with the AWS account ID.
    - *<directory-id>* with the ID of the directory you created earlier. You can get this in the WorkSpaces console.

For resources in AWS GovCloud (US) Regions, use the following format for the ARN: `arn:aws-us-gov:workspaces:<region-code>:<account-id>:directory/<directory-id>`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:<region-code>:<account-
id>:directory/<directory-id>",
            "Condition": {
                "StringEquals": {"workspaces:userId": "${saml:sub}"}
            }
        }
    ]
}
```

22. Choose Next.
23. Enter a name for the policy, and then choose **Create policy**.

Step 6: Configure your SAML 2.0 identity provider

Depending on your SAML 2.0 IdP, you might need to manually update your IdP to trust AWS as a service provider. You do this by downloading the `saml-metadata.xml` file found at https://signin.aws.amazon.com/static/saml-metadata.xml, and then uploading it to your IdP. This updates your IdP's metadata.

For some IdPs, the update might already be configured. You can skip this step if it's already configured. If the update isn't already configured in your IdP, review the documentation provided by your IdP for information about how to update the metadata. Some providers give you the option to type the URL of the XML file into their dashboard, and the IdP obtains and installs the file for you. Others require you to download the file from the URL and then upload it to their dashboard.

> **Important**
>
> At this time, you can also authorize users in your IdP to access the WorkSpaces application you have configured in your IdP. Users who are authorized to access the WorkSpaces

application for your directory don't automatically have a WorkSpace created for them. Likewise, users that have a WorkSpace created for them are not automatically authorized to access the WorkSpaces application. To successfully connect to a WorkSpace using SAML 2.0 authentication, a user must be authorized by the IdP and must have a WorkSpace created.

Step 7: Create assertions for the SAML authentication response

Configure the information that your IdP sends to AWS as SAML attributes in its authentication response. Depending on your IdP, this is might already be configured. You can skip this step if it's already configured. If it's not already configured, provide the following:

- **SAML Subject NameID** — The unique identifier for the user who is signing in. Don't change the format/value of this field. Otherwise, the home folder feature will not work as expected because the user will be treated as different user.

  Note

  For domain-joined WorkSpaces Pools, the `NameID` value for the user must be provided in the `domain\username` format using the `sAMAccountName`, or in the `username@domain.com` format using `userPrincipalName`, or just `userName`. If you are using the `sAMAccountName` format, you can specify the domain by using either the NetBIOS name or the fully qualified domain name (FQDN). The `sAMAccountName` format is required for Active Directory one-way trust scenarios. For more information, see Using Active Directory with WorkSpaces Pools. if just `userName` is provided, the user will be logged in to the primary-domain

- **SAML Subject Type (with a value set to `persistent`)** — Setting the value to `persistent` ensures that your IdP sends the same unique value for the `NameID` element in all SAML requests from a particular user. Make sure that your IAM policy includes a condition to only allow SAML requests with a SAML `sub_type` set to `persistent`, as described in the Step 5: Create a SAML 2.0 federation IAM role section.
- **`Attribute` element with the `Name` attribute set to https://aws.amazon.com/SAML/Attributes/Role** — This element contains one or more `AttributeValue` elements that list the IAM role and SAML IdP to which the user is mapped by your IdP. The role and IdP are specified as a comma-delimited pair of ARNs. An example of the expected value is

`arn:aws:iam::<account-id>:role/<role-name>,arn:aws:iam::<account-id>:saml-provider/<provider-name>`.

- **`Attribute` element with the `Name` attribute set to https://aws.amazon.com/SAML/Attributes/RoleSessionName** — This element contains one `AttributeValue` element that provides an identifier for the AWS temporary credentials that are issued for SSO. The value in the `AttributeValue` element must be between 2 and 64 characters long, can contain alphanumeric characters and the following special characters: `_ . : / = + - @`. It can't contain spaces. The value is typically an email address or a user principal name (UPN). It shouldn't be a value that includes a space, such as a user's display name.
- **`Attribute` element with the `Name` attribute set to https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email** — This element contains one `AttributeValue` element that provides the email address of the user. The value must match the WorkSpaces user email address as defined in the WorkSpaces directory. Tag values may include combinations of letters, numbers, spaces, and `_ . : / = + - @` characters. For more information, see Rules for tagging in IAM and AWS STS in the *AWS Identity and Access Management User Guide*.
- (Optional) **`Attribute` element with the `Name` attribute set to https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName** — This element contains one `AttributeValue` element that provides the Active Directory `userPrincipalName` for the user who is signing in. The value must be provided in the `username@domain.com` format. This parameter is used with certificate-based authentication as the Subject Alternative Name in the end user certificate. For more information, see Certificate-based authentication.
- (Optional) **`Attribute` element with the `Name` attribute set to https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid (optional)** — This element contains one `AttributeValue` element that provides the Active Directory security identifier (SID) for the user who is signing in. This parameter is used with certificate-based authentication to enable strong mapping to the Active Directory user. For more information, see Certificate-based authentication.
- (Optional) **`Attribute` element with the `Name` attribute set to https://aws.amazon.com/SAML/Attributes/PrincipalTag:Domain** — This element contains one `AttributeValue` element that provides the Active Directory DNS fully qualified domain name (FQDN) for users signing in. This parameter is used with certificate-based authentication when the Active Directory `userPrincipalName` for the user contains an alternative suffix. The value must be provided in the `domain.com` format, and must include any subdomains.
- (Optional) **`Attribute` element with the `Name` attribute set to https://aws.amazon.com/SAML/Attributes/SessionDuration** — This element contains one `AttributeValue` element

that specifies the maximum amount of time that a federated streaming session for a user can remain active before re-authentication is required. The default value is `3600` seconds (60 minutes). For more information, see the SAML SessionDurationAttribute in the *AWS Identity and Access Management User Guide*.

> **Note**
>
> Although `SessionDuration` is an optional attribute, we recommend that you include it in the SAML response. If you don't specify this attribute, the session duration is set to a default value of `3600` seconds (60 minutes). WorkSpaces desktop sessions are disconnected after their session duration expires.

For more information about how to configure these elements, see Configuring SAML assertions for the authentication response in the *AWS Identity and Access Management User Guide*. For information about specific configuration requirements for your IdP, see your IdP's documentation.

Step 8: Configure the relay state of your federation

Use your IdP to configure the relay state of your federation to point to the WorkSpaces Pool directory relay state URL. After successful authentication by AWS, the user is directed to the WorkSpaces Pool directory endpoint, defined as the relay state in the SAML authentication response.

The following is the relay state URL format:

```
https://relay-state-region-endpoint/sso-idp?registrationCode=registration-code
```

The following table lists the relay state endpoints for the AWS Regions where WorkSpaces SAML 2.0 authentication is available. AWS Regions in which the WorkSpaces Pools feature is not available have been removed.

Region	Relay state endpoint
US East (N. Virginia) Region	workspaces.euc-sso.us-east-1.amazon.com

Region	Relay state endpoint
US West (Oregon) Region	workspaces.euc-sso.us-west-2.aws.amazon.com
Asia Pacific (Mumbai) Region	workspaces.euc-sso.ap-south-1.aws.amazon.com
Asia Pacific (Seoul) Region	workspaces.euc-sso.ap-northeast-2.aws.amazon.com
Asia Pacific (Singapore) Region	workspaces.euc-sso.ap-southeast-1.aws.amazon.com
Asia Pacific (Sydney) Region	workspaces.euc-sso.ap-southeast-2.aws.amazon.com
Asia Pacific (Tokyo) Region	workspaces.euc-sso.ap-northeast-1.aws.amazon.com
Canada (Central) Region	workspaces.euc-sso.ca-central-1.aws.amazon.com
Europe (Frankfurt) Region	workspaces.euc-sso.eu-central-1.aws.amazon.com
Europe (Ireland) Region	workspaces.euc-sso.eu-west-1.aws.amazon.com
Europe (London) Region	workspaces.euc-sso.eu-west-2.aws.amazon.com
South America (São Paulo) Region	workspaces.euc-sso.sa-east-1.aws.amazon.com

Region	Relay state endpoint
AWS GovCloud (US-West)	workspaces.euc-sso.us-gov-west-1.amazonaws-us-gov.com **Note** For information about working with SAML IdPs in AWS GovCloud (US) Regions, see Amazon WorkSpaces in the *AWS GovCloud (US) User Guide*.
AWS GovCloud (US-East)	workspaces.euc-sso.us-gov-east-1.amazonaws-us-gov.com **Note** For information about working with SAML IdPs in AWS GovCloud (US) Regions, see Amazon WorkSpaces in the *AWS GovCloud (US) User Guide*.

Step 9: Enable integration with SAML 2.0 on your WorkSpace Pool directory

Complete the following procedure to enable SAML 2.0 authentication for the WorkSpaces Pool directory.

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose **Directories** in the navigation pane.
3. Choose the **Pools directories** tab.
4. Choose the ID of the directory you want to edit.
5. Choose **Edit** in the **Authentication** section of the page.
6. Choose **Edit SAML 2.0 Identity Provider**.
7. For the **User Access URL**, which is sometimes know as the "SSO URL", replace the placeholder value with the SSO URL provided to you by your IdP.

8. For the **IdP deep link parameter name**, enter the parameter that is applicable to your IdP and the application you have configured. The default value is `RelayState` if you omit the parameter name.

   The following table lists the user access URLs and deep link parameter names that are unique to various identity providers for applications.

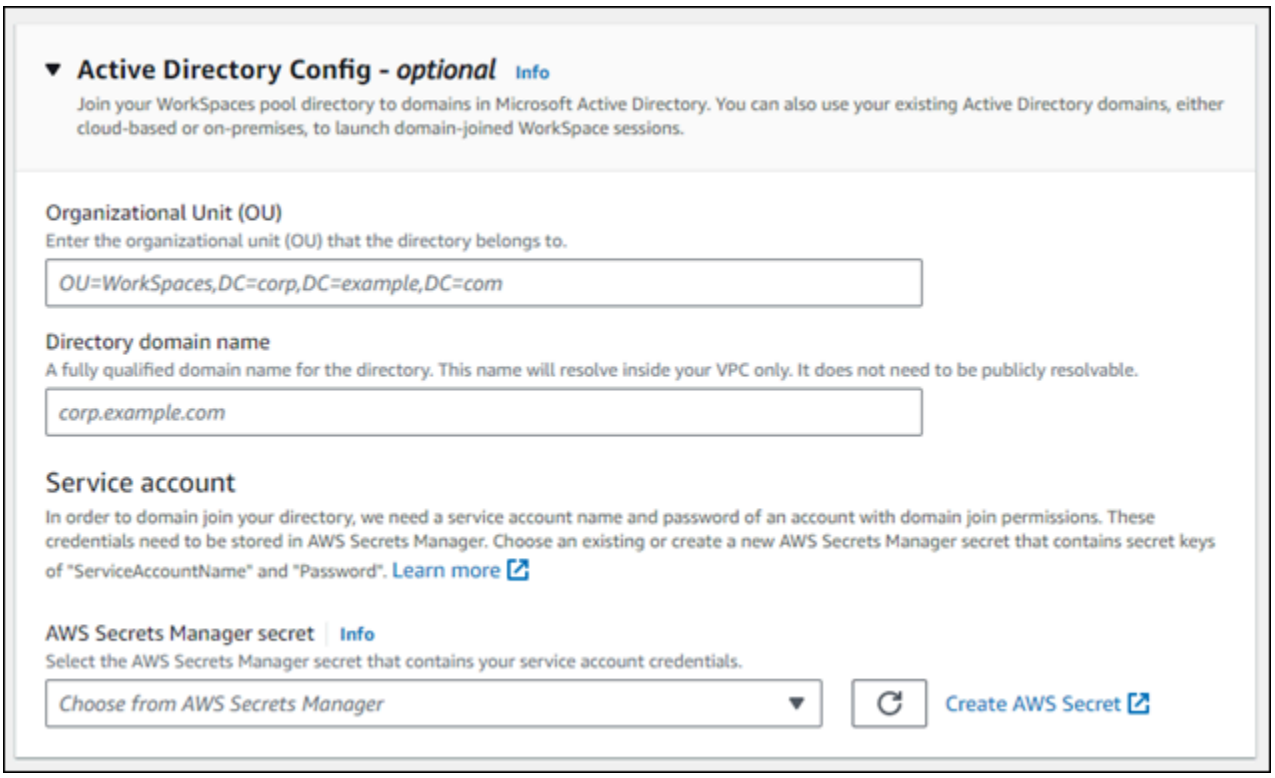
Identity provider	Parameter	User access URL
ADFS	`RelayState`	`https://<host>/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID= <relaying-party-uri>`
Azure AD	`RelayState`	`https://myapps.microsoft.com/signin/ <app-id>?tenantId = <tenant-id>`
Duo Single Sign-On	`RelayState`	`https://<sub-domain> .sso.duosecurity.com/saml2/sp/ <app-id>/sso`
Okta	`RelayState`	`https://<sub-domain> .okta.com/app/<app-name> /<app-id>/sso/saml`
OneLogin	`RelayState`	`https://<sub-domain> .onelogin.com/trust/saml2/http-post/sso/ <app-id>`

Identity provider	Parameter	User access URL
JumpCloud	RelayState	https://sso.jumpcloud.com/saml2/ *<app-id>*
Auth0	RelayState	https://*<default-tenant-name>* .us.auth0.com/samlp/ *<client-id>*
PingFederate	TargetResource	https://*<host>*/idp/startSSO.ping?PartnerSpId= *<sp-id>*
PingOne for Enterprise	TargetResource	https://sso.connect.pingidentity.com/sso/sp/initsso?saasid= *<app-id>*&idpid=*<idp-id>*

9. Choose **Save**.

Specify Active Directory details for your WorkSpaces Pools directory

In this topic, we show you how to specify your Active Directory (AD) details within the **Create WorkSpaces Pool directory** page of the WorkSpaces console. As you create your WorkSpaces Pool directory, you should specify your AD details if you plan to use an AD with your WorkSpaces Pools. You cannot edit the **Active Directory Config** for your WorkSpaces Pools directory after you create it. Following is an example of the **Active Directory Config** section of the **Create WorkSpaces Pool directory** page.



Note

The full process for creating a WorkSpaces Pool directory is outlined in the Configure SAML 2.0 and create a WorkSpaces Pools directory topic. The procedures outlined on this page represent only a subset of steps of the full process to create a WorkSpaces Pool directory.

Topics

- Specify the organization unit and directory domain name for your AD
- Specify the service account for your AD

Specify the organization unit and directory domain name for your AD

Complete the following procedure to specify an organizational unit (OU) and a directory domain name for your AD in the **Create a WorkSpaces Pool directory** page.

1. For **Organization Unit**, enter the OU that the pool belongs to. WorkSpace machine accounts are placed in the organizational unit (OU) that you specify for the WorkSpaces Pool directory.

> **Note**
>
> The OU name can't contain spaces. If you specify an OU name that contains spaces, when it attempts to rejoin the Active Directory domain, WorkSpaces cannot cycle the computer objects correctly and the domain rejoin doesn't work.

2. For **Directory domain name**, enter the fully qualified domain name (FQDN) of the Active Directory domain (for example, `corp.example.com`). Each AWS Region can have only one directory config value with a specific directory name.

   - You can join your WorkSpaces Pool directories to domains in Microsoft Active Directory. You can also use your existing Active Directory domains, either cloud-based or on-premises, to launch domain-joined WorkSpaces.
   - You can also use AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, to create an Active Directory domain. Then, you can use that domain to support your WorkSpaces resources.
   - By joining WorkSpaces to your Active Directory domain, you can:
     - Allow your users and applications to access Active Directory resources, such as printers and file shares from streaming sessions.
     - Use Group Policy settings that are available in the Group Policy Management Console (GPMC) to define the end user experience.
     - Stream applications that require users to be authenticated using their Active Directory login credentials.
     - Apply your enterprise compliance and security policies to your WorkSpaces streaming instances.

3. For **Service account**, continue to the Specify the service account for your AD next section of this page.

Specify the service account for your AD

When you configure Active Directory (AD) for your WorkSpaces Pools as part of the directory creation process, you must specify the AD service account to be used for managing the AD. This requires that you provide the service account credentials, which must be stored in AWS Secrets Manager and encrypted using a AWS Key Management Service (AWS KMS) customer managed key.

In this section, we show you how to create the AWS KMS customer managed key and the Secrets Manager secret to store your AD service account credentials.

Step 1: Create an AWS KMS customer managed key

Complete the following procedure to create an AWS KMS customer managed key

1. Open the AWS KMS console at https://console.aws.amazon.com/kms.
2. To change the AWS Region, use the Region selector in the upper-right corner of the page.
3. Choose **Create a key**, and then choose **Next**.
4. Choose **Symetric** for the key type, and **Encrypt and decrypt** for the key usage, and then choose **Next**.
5. Enter an alias for the key, such as `WorkSpacesPoolDomainSecretKey`, and then choose **Next**.
6. Don't choose a key administrator. Choose **Next** to continue.
7. Don't define key usage permissions. Choose **Next** to continue.
8. In the Key policy section of the page, add the following:

```
{
    "Sid": "Allow access for Workspaces SP",
    "Effect": "Allow",
    "Principal": {
        "Service": "workspaces.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*"
}
```

The result should appear like the following example.

```
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::[redacted]:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow access for Workspaces SP",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "workspaces.amazonaws.com"
                ]
            },
            "Action": "kms:Decrypt",
            "Resource": "*"
        }
```

9. Choose **Finish**.

   Your AWS KMS customer managed key is now ready to be used with Secrets Manager. Continue to the Step 2: Create Secrets Manager secret to store your AD service account credentials section of this page.

Step 2: Create Secrets Manager secret to store your AD service account credentials

Complete the following procedure to create a Secrets Manager secret to store your AD service account credentials.

1. Open the AWS Secrets Manager console at https://console.aws.amazon.com/secretsmanager/.
2. Choose **Create a new secret**.
3. Choose **Other type of secret**.
4. For the first key/value pair, enter `Service Account Name` for the key, and the name of the service account for the value, such as `domain\username`.
5. For the second key/value pair, enter a `Service Account Password` for the key, and the password of the service account for the value.
6. For the encryption key, choose the AWS KMS customer managed key that you created earlier, and then choose **Next**.
7. Enter a name for the secret, such as `WorkSpacesPoolDomainSecretAD`.

8. Choose **Edit permissions** in the **Resource permissions** section of the page.
9. Enter the following permission policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "workspaces.amazonaws.com"
                ]
            },
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "*"
        }
    ]
}
```

10. Choose **Save** to save the permission policy.
11. Choose **Next** to continue.
12. Don't configure automatic rotation. Choose **Next** to continue.
13. Choose **Store** to finish storing your secret.

Your AD service account credentials are now stored in Secrets Manager. Continue to the Step 3: Select the Secrets Manager secret that contains your AD service account credentails section of this page.

Step 3: Select the Secrets Manager secret that contains your AD service account credentails

Complete the following procedure to select the Secrets Manager secret you created in the Active Directory config for your WorkSpaces Pool directory.

- For **Service account**, choose the AWS Secrets Manager secret that contains your service account credentials. Complete the following steps to create the secret if you haven't already done so. The secret must be encrypted using a AWS Key Management Service customer managed key.

Now that you've completed all of the fields within the **Active Directory Config** section of the **Create WorkSpaces Pool directory** page, you can continue to finish creating your WorkSpaces Pool directory. Go to Step 4: Create WorkSpace Pool directory and start on step 9 of the procedure.

Update directory details for your WorkSpaces Pools

You can complete the following directory management tasks using the WorkSpaces Pools console.

Authentication

You can configure additional authentication options for your WorkSpaces Pools. Pools requires SAML 2.0 authentication.

To enable and configure SAML 2.0 Identity Provider authentiation

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose **Directories** in the navigation pane.
3. Choose the directory you want to configure.
4. Go to authentication and choose **Edit**.
5. Choose **Edit SAML 2.0 Identity Provider**.
6. Check the **Enable SAML 2.0 authentication** checkbox.
7. Enter the **User Access URL** to direct the WorkSpaces Pools client during federated sign-in.
8. Enter the **IdP deep link parameter name** (optional).
9. Choose **Save**.

To enable and configure Certificate-Based Authentication

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose **Directories** in the navigation pane.
3. Choose the directory you want to configure.
4. Go to Authentication and choose **Edit**.
5. Choose **Edit Certificate-Based Authentication**.
6. Check the **Enable Certificate-Based Authentication** checkbox.
7. Choose from the dropdown the **AWS Certificate Manager (ACM) Private Certificate Authority (CA)**.

8. Choose **Save**.

Security group

Apply a security group to your WorkSpaces Pools in your directory.

To configure security group for your WorkSpaces Pools

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose **Directories** in the navigation pane.
3. Choose the directory you want to configure.
4. Go to Security group and choose **Edit**.
5. From the dropdown, choose a security group.

Active Directory Config

Configure your directory Active Directory Config with an Organization Unit (OU), directory domain name, and AWS Secrets Manager secret.

To configure your Active Directory

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose **Directories** in the navigation pane.
3. Choose the directory you want to configure.
4. Go to Active Directory Config and choose **Edit**.
5. To find an Organizational Unit (OU), you can start typing all or part of the OU name and choose the OU you want to use.

> **Note**
>
> (Optional) After choosing the OU, rebuild the existing WorkSpaces to update the OU. For more information, see Rebuild a WorkSpace in WorkSpaces Personal

6. Choose **Save**.

> **Note**
>
> The directory domain name and AWS Secrets Manager secret can't be edited after you've created your pool.

Streaming properties

Configure how your users can transfer data between their pooled WorkSpace and their local device.

To configure streaming properties

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose **Directories** in the navigation pane.
3. Choose the directory you want to configure.
4. Go to Streaming properties and choose **Edit**.
5. Configure the following streaming properties:
   - Clipboard permissions
     - From the drop down list, choose one of the following:
       - **Allow copy and paste** - Allows copying to local device and pasting to remote session.
       - **Allow paste to remote session** - Allows pasting to remote session.
       - **Allow copy to local device** - Allows copying to a local device.
       - Disabled
     - Choose to allow or not allow print to local device.
     - Choose to allow or not allow diagnostic logging.
     - Choose to allow or not allow smart card sign in.
     - To enable Home Folders storage, choose **Enable Home Folders**.
6. Choose **Save**.

IAM role

Select an IAM role for you WorkSpaces Pools.

To select an IAM role

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose **Directories** in the navigation pane.
3. Choose the directory you want to configure.
4. Go to IAM role and choose **Edit**.
5. Choose an IAM role from the drop down. To create a new IAM role, choose **Create new IAM role**.
6. Choose **Save**.

Tags

Add new tags to your WorkSpaces Pools

To add a new tag

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose **Directories** in the navigation pane.
3. Choose the directory you want to configure.
4. Go to Tags and choose **Manage tags**.
5. Choose **Add new tags** and enter the key pair value that you want to use. A key can be a general category, such as "project," "owner," or "environment," with specific associated values.
6. Choose **Save changes**.

Deregister a WorkSpaces Pools directory

Complete the following procedures to deregister a WorkSpaces Pools directory.

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose **Directories** in the navigation pane.
3. Select the directory.
4. Choose **Actions**, **Deregister**.
5. When prompted for confirmation, choose **Deregister**. After deregistration is complete, the value of **Registered** is No.

Networking and Access for WorkSpaces Pools

The following topics provide information about enabling users to connect to WorkSpaces Pools and enabling your WorkSpaces Pools to access network resources and the internet.

Contents

Internet Access for WorkSpaces Pools

If your WorkSpaces in WorkSpaces Pools require internet access, you can enable it in several ways. When you choose a method for enabling internet access, consider the number of users your deployment must support and your deployment goals. For example:

- If your deployment must support more than 100 concurrent users, configure a VPC with private subnets and a NAT gateway.
- If your deployment supports fewer than 100 concurrent users, you can configure a new or existing VPC with a public subnet.
- If your deployment supports fewer than 100 concurrent users and you are new to WorkSpaces Pools and want to get started using the service, you can use the default VPC, public subnet, and security group.

The following sections provide more information about each of these deployment options.

- Configure a VPC with Private Subnets and a NAT Gateway (recommended) — With this configuration, you launch your WorkSpaces Pools builders in a private subnet and configure a NAT gateway in a public subnet in your VPC. Your streaming instances are assigned a private IP address that is not directly accessible from the internet.

  In addition, unlike configurations that use the **Default Internet Access** option for enabling internet access, the NAT configuration is not limited to 100 WorkSpaces in WorkSpaces Pools. If your deployment must support more than 100 concurrent users, use this configuration.

You can create and configure a new VPC to use with a NAT gateway, or add a NAT gateway to an existing VPC.

- Configure a New or Existing VPC with a Public Subnet — With this configuration, you launch your WorkSpaces Pools in a public subnet. When you enable this option, WorkSpaces Pools uses the internet gateway in your Amazon VPC public subnet to provide the internet connection. Your streaming instances are assigned a public IP address that is directly accessible from the internet. You can create a new VPC or configure an existing one for this purpose.

  > **Note**
  >
  > When you configure a new or existing VPC with a public subnet, a maximum of 100 WorkSpaces are supported in WorkSpaces Pools. If your deployment must support more than 100 concurrent users, use the NAT gateway configuration instead.

- Use the Default VPC, Public Subnet, and Security Group — If you are new to WorkSpaces Pools and want to get started using the service, you can launch your WorkSpaces Pools in a default public subnet. When you enable this option, WorkSpaces Pools uses the internet gateway in your Amazon VPC public subnet to provide the internet connection. Your streaming instances are assigned a public IP address that is directly accessible from the internet.

  Default VPCs are available in Amazon Web Services accounts created after 2013-12-04.

  The default VPC includes a default public subnet in each Availability Zone and an internet gateway that is attached to your VPC. The VPC also includes a default security group.

  > **Note**
  >
  > When you use the default VPC, public subnet, and security group, a maximum of 100 WorkSpaces are supported in WorkSpaces Pools. If your deployment must support more than 100 concurrent users, use the NAT gateway configuration instead.

Configure a VPC for WorkSpaces Pools

When you set up WorkSpaces Pools, you must specify the virtual private cloud (VPC) and at least one subnet in which to launch your WorkSpaces. A VPC is a virtual network in your own logically

isolated area within the Amazon Web Services Cloud. A subnet is a range of IP addresses in your VPC.

When you configure your VPC for WorkSpaces Pools, you can specify either public or private subnets, or a mix of both types of subnets. A public subnet has direct access to the internet through an internet gateway. A private subnet, which doesn't have a route to an internet gateway, requires a Network Address Translation (NAT) gateway or NAT instance to provide access to the internet.

Contents

VPC Setup Recommendations for WorkSpaces Pools

When you create a WorkSpaces Pools, you specify the VPC and one or more subnets to use. You can provide additional access control to your VPC by specifying security groups.

The following recommendations can help you configure your VPC more effectively and securely. In addition, they can help you configure an environment that supports effective WorkSpaces Pools scaling. With effective WorkSpaces Pools scaling, you can meet current and anticipated WorkSpaces user demand, while avoiding unnecessary resource usage and associated costs.

Overall VPC Configuration

- Make sure that your VPC configuration can support your WorkSpaces Pools scaling needs.

  As you develop your plan for WorkSpaces Pools scaling, keep in mind that one user requires one WorkSpaces. Therefore, the size of your WorkSpaces Pools determines the number of users who can stream concurrently. For this reason, for each instance type that you plan to use, make sure that the number of WorkSpaces that your VPC can support is greater than the number of anticipated concurrent users for the same instance type.
- Make sure that your WorkSpaces Pools account quotas (also referred to as limits) are sufficient to support your anticipated demand. To request a quota increase, you can use the Service Quotas console at https://console.aws.amazon.com/servicequotas/. For information about default WorkSpaces Pools quotas, see Amazon WorkSpaces quotas.

- If you plan to provide your WorkSpaces in WorkSpaces Pools with access to the internet, we recommend that you configure a VPC with two private subnets for your streaming instances and a NAT gateway in a public subnet.

  The NAT gateway lets the WorkSpaces in your private subnets connect to the internet or other AWS services. However, it prevents the internet from initiating a connection with those WorkSpaces. In addition, unlike configurations that use the **Default Internet Access** option for enabling internet access, the NAT configuration supports more than 100 WorkSpaces. For more information, see Configure a VPC with Private Subnets and a NAT Gateway.

Elastic Network Interfaces

- WorkSpaces Pools creates as many elastic network interfaces (network interfaces) as the maximum desired capacity of your WorkSpaces Pools. By default, the limit for network interfaces per Region is 5000.

  When planning capacity for very large deployments, for example, thousands of WorkSpaces, consider the number of Amazon EC2 instances that are also used in the same Region.

Subnets

- If you are configuring more than one private subnet for your VPC, configure each in a different Availability Zone. Doing so increases fault tolerance and can help prevent insufficient capacity errors. If you use two subnets in the same AZ, you might run out of IP addresses, because WorkSpaces Pools will not use the second subnet.
- Make sure that the network resources required for your applications are accessible through both of your private subnets.
- Configure each of your private subnets with a subnet mask that allows for enough client IP addresses to account for the maximum number of expected concurrent users. In addition, allow for additional IP addresses to account for anticipated growth. For more information, see VPC and Subnet Sizing for IPv4.
- If you are using a VPC with NAT, configure at least one public subnet with a NAT Gateway for internet access, preferably two. Configure the public subnets in the same Availability Zones where your private subnets reside.

  To enhance fault tolerance and reduce the chance of insufficient capacity errors for large WorkSpaces Pools deployments, consider extending your VPC configuration into a third

Availability Zone. Include a private subnet, public subnet, and NAT gateway in this additional Availability Zone.

Security Groups

- Use security groups to provide additional access control to your VPC.

  Security groups that belong to your VPC let you control the network traffic between WorkSpaces Pools streaming instances and network resources required by applications. These resources may include other AWS services such as Amazon RDS or Amazon FSx, license servers, database servers, file servers, and application servers.
- Make sure that the security groups provide access to the network resources that your applications require.

  For general information about security groups, see Control traffic to your AWS resources using security groups in the *Amazon VPC User Guide*.

Configure a VPC with Private Subnets and a NAT Gateway

If you plan to provide your WorkSpaces in WorkSpaces Pools with access to the internet, we recommend that you configure a VPC with two private subnets for your WorkSpaces and a NAT gateway in a public subnet. You can create and configure a new VPC to use with a NAT gateway, or add a NAT gateway to an existing VPC. For additional VPC configuration recommendations, see VPC Setup Recommendations for WorkSpaces Pools.

The NAT gateway lets the WorkSpaces in your private subnets connect to the internet or other AWS services, but prevents the internet from initiating a connection with those WorkSpaces. In addition, unlike configurations that use the **Default Internet Access** option for enabling internet access for WorkSpaces, this configuration is not limited to 100 WorkSpaces.

For information about using NAT Gateways and this configuration, see NAT Gateways and VPC with Public and Private Subnets (NAT) in the *Amazon VPC User Guide*.

Contents

Create and Configure a New VPC

This topic describes how to use the VPC wizard to create a VPC with a public subnet and one private subnet. As part of this process, the wizard creates an internet gateway and a NAT gateway. It also creates a custom route table associated with the public subnet and updates the main route table associated with the private subnet. The NAT gateway is automatically created in the public subnet of your VPC.

After you use the wizard to create the initial VPC configuration, you'll add a second private subnet. For more information about this configuration, see VPC with Public and Private Subnets (NAT) in the *Amazon VPC User Guide*.

> **Note**
>
> If you already have a VPC, complete the steps in Add a NAT Gateway to an Existing VPC instead.

Contents

Step 1: Allocate an Elastic IP Address

Before you create your VPC, you must allocate an Elastic IP address in your WorkSpaces Region. You must first allocate an Elastic IP address for use in your VPC, and then associate it with your NAT gateway. For more information, see Elastic IP Addresses in the *Amazon VPC User Guide*.

> **Note**
>
> Charges may apply to Elastic IP addresses that you use. For more information, see Elastic IP Addresses on the Amazon EC2 pricing page.

Complete the following steps if you don't already have an Elastic IP address. If you want to use an existing Elastic IP address, verify that it's not currently associated with another instance or network interface.

To allocate an Elastic IP address

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, under **Network & Security**, choose **Elastic IPs**.
3. Choose **Allocate New Address**, and then choose **Allocate**.
4. Note the Elastic IP address.
5. In the upper right of the **Elastic IPs** pane, click the X icon to close the pane.

Step 2: Create a New VPC

Complete the following steps to create a new VPC with a public subnet and one private subnet.

To create a new VPC

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **VPC Dashboard**.
3. Choose **Launch VPC Wizard**.
4. In **Step 1: Select a VPC Configuration**, choose **VPC with Public and Private Subnets**, and then choose **Select**.
5. In **Step 2: VPC with Public and Private Subnets**, configure the VPC as follows:
   - For **IPv4 CIDR block**, specify an IPv4 CIDR block for the VPC.
   - For **IPv6 CIDR block**, keep the default value, **No IPv6 CIDR Block**.
   - For **VPC name**, type a unique name for the VPC.
6. Configure the public subnet as follows:
   - For **Public subnet's IPv4 CIDR**, specify the CIDR block for the subnet.
   - For **Availability Zone**, keep the default value, **No Preference**.
   - For **Public subnet name**, type a name for the subnet; for example, `WorkSpaces Public Subnet`.
7. Configure the first private subnet as follows:

- For **Private subnet's IPv4 CIDR**, specify the CIDR block for the subnet. Make a note of the value that you specify.
- For **Availability Zone**, select a specific zone and make a note of the zone that you select.
- For **Private subnet name**, type a name for the subnet; for example, `WorkSpaces Private Subnet1`.
- For the remaining fields, where applicable, keep the default values.

8. For **Elastic IP Allocation ID**, click in the text box and select the value that corresponds to the Elastic IP address that you created. This address is assigned to the NAT gateway. If you don't have an Elastic IP address, create one by using the Amazon VPC console at https://console.aws.amazon.com/vpc/.
9. For **Service endpoints**, if an Amazon S3 endpoint is required for your environment, specify one. An S3 endpoint is required to provide users with access to home folders or to enable application settings persistence for your users in a private network.

   To specify an Amazon S3 endpoint, do the following:

   a. Choose **Add Endpoint**.
   b. For **Service**, select the entry in the list that ends with "s3" (the `com.amazonaws.region.s3` entry that corresponds to the Region in which the VPC is being created).
   c. For **Subnet**, choose **Private subnet**.
   d. For **Policy**, keep the default value, **Full Access**.
10. For **Enable DNS hostnames**, keep the default value, **Yes**.
11. For **Hardware tenancy**, keep the default value, **Default**.
12. Choose **Create VPC**.
13. Note that it takes several minutes to set up your VPC. After the VPC is created, choose **OK**.

Step 3: Add a Second Private Subnet

In the previous step (Step 2: Create a New VPC), you created a VPC with one public subnet and one private subnet. Perform the following steps to add a second private subnet. We recommend that you add a second private subnet in a different Availability Zone than your first private subnet.

1. In the navigation pane, choose **Subnets**.

2. Select the first private subnet that you created in the previous step. On the **Description** tab, below the list of subnets, make a note of the Availability Zone for this subnet.
3. On the upper left of the subnets pane, choose **Create Subnet**.
4. For **Name tag**, type a name for the private subnet; for example, `WorkSpaces Private Subnet2`.
5. For **VPC**, select the VPC that you created in the previous step.
6. For **Availability Zone**, select an Availability Zone other than the one you are using for your first private subnet. Selecting a different Availability Zone increases fault tolerance and helps prevent insufficient capacity errors.
7. For **IPv4 CIDR block**, specify a unique CIDR block range for the new subnet. For example, if your first private subnet has an IPv4 CIDR block range of `10.0.1.0/24`, you could specify a CIDR block range of `10.0.2.0/24` for the new private subnet.
8. Choose **Create**.
9. After your subnet is created, choose **Close**.

Step 4: Verify and Name Your Subnet Route Tables

After you've created and configured your VPC, complete the following steps to specify a name for your route tables, and to verify that:

- The route table associated with the subnet in which your NAT gateway resides includes a route that points internet traffic to an internet gateway. This ensures that your NAT gateway can access the internet.
- The route tables associated with your private subnets are configured to point internet traffic to the NAT gateway. This enables the streaming instances in your private subnets to communicate with the internet.

1. In the navigation pane, choose **Subnets**, and select the public subnet that you created; for example, `WorkSpaces Public Subnet`.
    a. On the **Route Table** tab, choose the ID of the route table; for example, `rtb-12345678`.
    b. Select the route table. Under **Name**, choose the edit icon (the pencil), and type a name (for example, `workspaces-public-routetable`), and then select the check mark to save the name.

c. With the public route table still selected, on the **Routes** tab, verify that there is one route for local traffic and another route that sends all other traffic to the internet gateway for the VPC. The following table describes these two routes:

Destination	Target	Description
Public subnet IPv4 CIDR Block (for example, 10.0.0/20)	Local	All traffic from the resources destined for IPv4 addresses within the public subnet IPv4 CIDR block is routed locally within the VPC.
Traffic destined to all other IPv4 addresses (for example, 0.0.0.0/0	Outbound (`igw-`*ID*)	Traffic destined for all other IPv4 addresses is routed to the internet gateway (identified by `igw-`*ID*) that was created by the VPC Wizard.

2. In the navigation pane, choose **Subnets**, and select the first private subnet that you created (for example, `WorkSpaces Private Subnet1`).

   a. On the **Route Table** tab, choose the ID of the route table.

   b. Select the route table. Under **Name**, choose the edit icon (the pencil), and enter a name (for example, `workspaces-private-routetable`), and then choose the check mark to save the name.

   c. On the **Routes** tab, verify that the route table includes the following routes:

Destination	Target	Description
Public subnet IPv4 CIDR Block (for example, 10.0.0/20)	Local	All traffic from the resources destined for IPv4 addresses within the public subnet IPv4 CIDR block is routed locally within the VPC.
Traffic destined to all other IPv4 addresses (for example, 0.0.0.0/0	Outbound (`nat-`*ID*)	Traffic destined for all other IPv4 addresses is routed to the NAT gateway (identified by `nat-`*ID*).

Destination	Target	Description
Traffic destined for S3 buckets (applicable if you specified an S3 endpoint) [pl-*ID* (com.amazonaws. *region*.s3)]	Storage (vpce-*ID*)	Traffic destined for S3 buckets is routed to the S3 endpoint (identified by vpce-*ID*).

3. In the navigation pane, choose **Subnets**, and select the second private subnet that you created (for example, WorkSpaces Private Subnet2).
4. On the **Route Table** tab, verify that the route table is the private route table (for example, workspaces-private-routetable). If the route table is different, choose **Edit** and select this route table.

Next Steps

To enable your WorkSpaces in WorkSpaces Pools to access the internet, complete the steps in Enable Internet Access for WorkSpaces Pools.

Add a NAT Gateway to an Existing VPC

If you have already configured a VPC, complete the following steps to add a NAT gateway to your VPC. If you need to create a new VPC, see Create and Configure a New VPC.

To add a NAT gateway to an existing VPC

1. To create your NAT gateway, complete the steps in Creating a NAT Gateway in the *Amazon VPC User Guide*.
2. Verify that your VPC has at least one private subnet. We recommend that you specify two private subnets from different Availability Zones for high availability and fault tolerance. For information about how to create a second private subnet, see Step 3: Add a Second Private Subnet.
3. Update the route table associated with one or more of your private subnets to point internet-bound traffic to the NAT gateway. This enables the streaming instances in your private subnets to communicate with the internet. To do so, complete the steps in Updating Your Route Table in the *Amazon VPC User Guide*.

Next Steps

To enable your WorkSpaces in WorkSpaces Pools to access the internet, complete the steps in Enable Internet Access for WorkSpaces Pools.

Enable Internet Access for WorkSpaces Pools

After your NAT gateway is available on a VPC, you can enable internet access for your WorkSpaces Pools. You can enable internet access when you create the WorkSpaces Pool directory. Choose the VPC with a NAT gateway when you create the directory. Then select a private subnet for **Subnet 1** and, optionally, another private subnet for **Subnet 2**. If you don't already have a private subnet in your VPC, you may need to create a second private subnet.

You can test your internet connectivity by starting your WorkSpaces Pool, and then connecting to a WorkSpace in the pool and browsing to the internet.

Configure a New or Existing VPC with a Public Subnet

If you created your Amazon Web Services account after 2013-12-04, you have a default VPC in each AWS Region that includes default public subnets. However, you may want to create your own nondefault VPC or configure an existing VPC to use with your WorkSpaces Pool directory. This topic describes how to configure a nondefault VPC and public subnet to use with WorkSpaces Pools.

After you configure your VPC and public subnet, you can provide your WorkSpaces in WorkSpaces Pools with access to the internet by enabling the **Default Internet Access** option. When you enable this option, WorkSpaces Pools enables internet connectivity by associating an Elastic IP address to the network interface that is attached from the streaming instance to your public subnet. An Elastic IP address is a public IPv4 address that is reachable from the internet. For this reason, we recommend that you instead use a NAT gateway to provide internet access to your WorkSpaces in WorkSpaces Pools. In addition, when **Default Internet Access** is enabled, a maximum of 100 WorkSpaces are supported. If your deployment must support more than 100 concurrent users, use the NAT gateway configuration instead.

For more information, see the steps in Configure a VPC with Private Subnets and a NAT Gateway. For additional VPC configuration recommendations, see VPC Setup Recommendations for WorkSpaces Pools.

Contents

Step 1: Configure a VPC with a Public Subnet

You can configure your own non-default VPC with a public subnet by using either of the following methods:

- Create a New VPC with a Single Public Subnet
- Configure an Existing VPC

Create a New VPC with a Single Public Subnet

When you use the VPC wizard to create a new VPC, the wizard creates an internet gateway and a custom route table that is associated with the public subnet. The route table routes all traffic destined for an address outside the VPC to the internet gateway. For more information about this configuration, see VPC with a Single Public Subnet in the *Amazon VPC User Guide*.

1. Complete the steps in Step 1: Create the VPC in the *Amazon VPC User Guide* to create your VPC.
2. To enable your WorkSpaces to access the internet, complete the steps in Step 2: Enable Default Internet Access For Your WorkSpaces Pools.

Configure an Existing VPC

If you want to use an existing VPC that does not have a public subnet, you can add a new public subnet. In addition to a public subnet, you must also have an internet gateway attached to your VPC and a route table that routes all traffic destined for an address outside the VPC to the internet gateway. To configure these components, complete the following steps.

1. To add a public subnet, complete the steps in Creating a Subnet in Your VPC. Use the existing VPC that you plan to use with WorkSpaces Pools.

   If your VPC is configured to support IPv6 addressing, the **IPv6 CIDR block** list displays. Select **Don't assign Ipv6**.
2. To create and attach an internet gateway to your VPC, complete the steps in Creating and Attaching an Internet Gateway.
3. To configure your subnet to route internet traffic through the internet gateway, complete the steps in Creating a Custom Route Table. In step 5, for **Destination**, use IPv4 format (`0.0.0.0/0`).

4. To enable your WorkSpaces and image builders to access the internet, complete the steps in Step 2: Enable Default Internet Access For Your WorkSpaces Pools.

Step 2: Enable Default Internet Access For Your WorkSpaces Pools

You can enable internet access when you create the WorkSpaces Pool directory. Choose the VPC with a public subnet when you create the directory. Then select a public subnet for **Subnet 1** and, optionally, another public subnet for **Subnet 2**.

You can test your internet connectivity by starting your WorkSpaces Pool, and then connecting to a WorkSpace in the pool and browsing to the internet.

Use the Default VPC, Public Subnet, and Security Group

Your Amazon Web Services account, if it was created after 2013-12-04, has a default VPC in each AWS Region. The default VPC includes a default public subnet in each Availability Zone and an internet gateway that is attached to your VPC. The VPC also includes a default security group.
If you are new to WorkSpaces Pools and want to get started using the service, you can keep the default VPC and security group selected when you create a WorkSpaces Pool. Then, you can select at least one default subnet.

> **Note**
>
> If your Amazon Web Services account was created before 2013-12-04, you must create a new VPC or configure an existing one to use with WorkSpaces Pools. We recommend that you manually configure a VPC with two private subnets for your WorkSpaces Pools and a NAT gateway in a public subnet. For more information, see Configure a VPC with Private Subnets and a NAT Gateway. Alternatively, you can configure a non-default VPC with a public subnet. For more information, see Configure a New or Existing VPC with a Public Subnet.

You can enable internet access when you create the WorkSpaces Pool directory.

Choose the default VPC when you create the directory. The default VPC name uses the following format: `vpc-`*`vpc-id`* `(No_default_value_Name)`.

Then select a default public subnet for **Subnet 1** and, optionally, another default public subnet for **Subnet 2**. The default subnet names use the following format: `subnet-`*`subnet-id`* `| (`*`IPv4 CIDR block`*`) | Default in `*`availability-zone`*.

You can test your internet connectivity by starting your WorkSpaces Pool, and then connecting to a WorkSpace in the pool and browsing to the internet.

Using Amazon S3 VPC Endpoints for WorkSpaces Pools Features

When you enable Application Settings Persistence for a WorkSpaces Pool or Home folders for a WorkSpaces Pool directory, WorkSpaces uses the VPC you specify for your directory to provide access to Amazon Simple Storage Service (Amazon S3) buckets. To enable WorkSpaces Pools access to your private S3 endpoint, attach the following custom policy to your VPC endpoint for Amazon S3. For more information about private Amazon S3 endpoints, see VPC Endpoints and Endpoints for Amazon S3 in the *Amazon VPC User Guide*.

Commercial AWS Regions

Use the following policy for resources in the commercial AWS Regions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow-WorkSpaces-to-access-S3-buckets",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:sts::<account-id>:assumed-role/
workspaces_DefaultRole/WorkSpacesPoolSession"
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:GetObjectVersion",
                "s3:DeleteObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::wspool-logs-*",
                "arn:aws:s3:::wspool-app-settings-*",
                "arn:aws:s3:::wspool-home-folder-*"
```

```
            ]
        }
    ]
}
```

AWS GovCloud (US) Regions

Use the following policy for resources in the commercial AWS GovCloud (US) Regions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow-WorkSpaces-to-access-S3-buckets",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:sts::<account-id>:assumed-role/
workspaces_DefaultRole/WorkSpacesPoolSession"
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:GetObjectVersion",
                "s3:DeleteObjectVersion"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::wspool-logs-*",
                "arn:aws-us-gov:s3:::wspool-app-settings-*",
                "arn:aws-us-gov:s3:::wspool-home-folder-*"
            ],
        }
    ]
}
```

Connections to Your VPC for WorkSpaces Pools

To enable WorkSpaces Pools connectivity to network resources and the internet, configure your WorkSpaces as follows.

Network Interfaces

Each WorkSpaces in WorkSpaces Pools has the following network interfaces:

- The customer network interface provides connectivity to the resources within your VPC, as well as the internet, and is used to join the WorkSpaces to your directory.
- The management network interface is connected to a secure WorkSpaces Pools management network. It is used for interactive streaming of the WorkSpace to a user's device, and to allow WorkSpaces Pools to manage the WorkSpace.

WorkSpaces Pools selects the IP address for the management network interface from the following private IP address range: 198.19.0.0/16. Do not use this range for your VPC CIDR or peer your VPC with another VPC with this range, as this might create a conflict and cause WorkSpaces to be unreachable. Also, do not modify or delete any of the network interfaces attached to a WorkSpace, as this might also cause the WorkSpace to become unreachable.

Management Network Interface IP Address Range and Ports

The management network interface IP address range is 198.19.0.0/16. The following ports must be open on the management network interface of all WorkSpaces:

- Inbound TCP on port 8300. This is used for establishment of the streaming connection.
- Inbound TCP on ports 8000 and 8443. These are used for management of the WorkSpaces.
- Inbound UDP on port 8300. This is used for establishment of the streaming connection over UDP.

Limit the inbound range on the management network interface to 198.19.0.0/16.

Under normal circumstances, WorkSpaces Pools correctly configures these ports for your WorkSpaces. If any security or firewall software is installed on a WorkSpace that blocks any of these ports, the WorkSpaces might not function correctly or might be unreachable.

Do not disable IPv6. If you disable IPv6, WorkSpaces Pools will not function correctly. For information about configuring IPv6 for Windows, see Guidance for configuring IPv6 in Windows for advanced users.

Note

WorkSpaces Pools relies on the DNS servers within your VPC to return a non-existent domain (NXDOMAIN) response for local domain names that don't exist. This enables the WorkSpaces Pools-managed network interface to communicate with the management servers.
When you create a directory with Simple AD, AWS Directory Service creates two domain controllers that also function as DNS servers on your behalf. Because the domain controllers don't provide the NXDOMAIN response, they can't be used with WorkSpaces Pools.

Customer Network Interface Ports

- For internet connectivity, the following ports must be open to all destinations. If you are using a modified or custom security group, you need to add the required rules manually. For more information, see Security Group Rules in the *Amazon VPC User Guide*.
  - TCP 80 (HTTP)
  - TCP 443 (HTTPS)
  - UDP 4195
- If you join your WorkSpaces to a directory, the following ports must be open between your WorkSpaces Pools VPC and your directory controllers.
  - TCP/UDP 53 - DNS
  - TCP/UDP 88 - Kerberos authentication
  - UDP 123 - NTP
  - TCP 135 - RPC
  - UDP 137-138 - Netlogon
  - TCP 139 - Netlogon
  - TCP/UDP 389 - LDAP
  - TCP/UDP 445 - SMB
  - TCP 1024-65535 - Dynamic ports for RPC

  For a complete list of ports, see Active Directory and Active Directory Domain Services Port Requirements in the Microsoft documentation.

- All WorkSpaces require that port 80 (HTTP) be open to IP address `169.254.169.254` to allow access to the EC2 metadata service. The IP address range `169.254.0.0/16` is reserved for WorkSpaces Pools service usage for management traffic. Failure to exclude this range might result in streaming issues.

User connections to WorkSpaces Pools

Users can connect to WorkSpaces in WorkSpaces Pools through the default public internet endpoint.

By default, WorkSpaces Pools is configured to route streaming connections over the public internet. Internet connectivity is required to authenticate users and deliver the web assets that WorkSpaces Pools requires to function. To allow this traffic, you must allow the domains listed in Allowed Domains.

> **Note**
>
> For user authentication, WorkSpaces Pools supports Security Assertion Markup Language 2.0 (SAML 2.0). For more information, see Configure SAML 2.0 and create a WorkSpaces Pools directory.

The following topics provide information about how to enable user connections to WorkSpaces Pools.

Contents

Bandwidth Recommendations

To optimize the performance of WorkSpaces Pools, make sure that your network bandwidth and latency can sustain your users' needs.

WorkSpaces Pools uses NICE Desktop Cloud Visualization (DCV) to enable your users to securely access and stream your applications over varying network conditions. To help reduce bandwidth

consumption, NICE DCV uses H.264-based video compression and encoding. During streaming sessions, the visual output of applications is compressed and streamed to your users as an AES-256 encrypted pixel stream over HTTPS. After the stream is received, it is decrypted and output to your users' local screen. When your users interact with their streaming applications, the NICE DCV protocol captures their input and sends it back to their streaming applications over HTTPS.

Network conditions are constantly measured during this process and information is sent back to WorkSpaces Pools. WorkSpaces Pools dynamically responds to changing network conditions by changing the video and audio encoding in real time to produce a high-quality stream for a wide variety of applications and network conditions.

The recommended bandwidth and latency for WorkSpaces Pools streaming sessions depends on the workload. For example, a user who works with graphic-intensive applications to perform computer-aided design tasks will require more bandwidth and lower latency than a user who works with business productivity applications to write documents.

The following table provides guidance on the recommended network bandwidth and latency for WorkSpaces Pools streaming sessions based on common workloads.

For each workload, the bandwidth recommendation is based on what an individual user might require at a specific point in time. The recommendation does not reflect the bandwidth required for sustained throughput. When only a few pixels change on the screen during a streaming session, the sustained throughput is much lower. Although users who have less bandwidth available can still stream their applications, the frame rate or image quality may not be optimal.

Workload	Description	Bandwidth recommended per user	Recommend ed maximum roundtrip latency
Line of business applications	Document writing applications, database analysis utilities	2 Mbps	< 150 ms
Graphics applications	Computer-aided design and modeling applicati	5 Mbps	< 100 ms

Workload	Description	Bandwidth recommended per user	Recommended maximum roundtrip latency
	ons, photo and video editing		
High fidelity	High-fidelity datasets or maps across multiple monitors	10 Mbps	< 50 ms

IP Address and Port Requirements for WorkSpaces Pools User Devices

WorkSpaces Pools users' devices require outbound access on port 443 (TCP) and port 4195 (UDP) when using the internet endpoints, and if you are using DNS servers for domain name resolution, port 53 (UDP).

- Port 443 is used for HTTPS communication between WorkSpaces Pools users' devices and WorkSpaces when using the internet endpoints. Typically, when end users browse the web during streaming sessions, the web browser randomly selects a source port in the high range for streaming traffic. You must ensure that return traffic to this port is allowed.
- Port 4195 is used for UDP HTTPS communication between WorkSpaces Pools users' devices and WorkSpaces when using the internet endpoints. This is currently only supported in the Windows native client. UDP is not supported if you are using VPC endpoints.
- Port 53 is used for communication between WorkSpaces Pools users' devices and your DNS servers. The port must be open to the IP addresses for your DNS servers so that public domain names can be resolved. This port is optional if you are not using DNS servers for domain name resolution.

Allowed Domains

For WorkSpaces Pools users to access WorkSpaces, you must allow various domains on the network from which users initiate access to the WorkSpaces. For more information, see IP address and port requirements for WorkSpaces Personal. Note that the page specifies that it applies to WorkSpaces Personal but it also applies to WorkSpaces Pools.

> **Note**
>
> If your S3 bucket has a "." character in the name, the domain used is `https://s3.<aws-region>.amazonaws.com`. If your S3 bucket does not have a "." character in the name, the domain used is `https://<bucket-name>.s3.<aws-region>.amazonaws.com`.

Create a WorkSpaces Pool

Set up and create a pool from which user applications are launched and streamed.

> **Note**
>
> You should create a directory before you create a WorkSpaces Pool. For more information, see Configure SAML 2.0 and create a WorkSpaces Pools directory.

To set up and create a pool

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**, **Pool**.
3. Choose **Create WorkSpaces Pools**.
4. Under **Onboarding** (optional), you can choose **Recommend options to me based on my use case** to get recommendations on the type of WorkSpace you want to use. You can skip this step if you know that you want to use WorkSpaces Pools.
5. Under **Configure WorkSpaces**, enter the following details:
   - For **Name**, enter a unique name identifier for the pool. Special characters aren't allowed.
   - For **Description**, enter a description for the pool (maximum of 256 characters).
   - For **Bundle**, choose from the following the bundle type that you want to use for your WorkSpaces.
     - **Use a base WorkSpaces bundle** - Choose one of the bundles from the drop down. For more information about the bundle type you selected, choose **Bundle details**. To compare bundles offered for pools, choose **Compare all bundles**.

  - **Use your own custom bundle** - Choose a bundle that you previously created. To create a custom bundle, see Create a custom WorkSpaces image and bundle for WorkSpaces Personal.

- For **Maximum session duration in minutes**, choose the maximum amount of time that a streaming session can remain active. If users are still connected to a streaming instance five minutes before this limit is reached, they are prompted to save any open documents before being disconnected. After this time elapses, the instance is terminated and replaced by a new instance. The maximum session duration that you can set in the WorkSpaces Pools console is 5760 minutes (96 hours). The maximum session duration that you can set using the WorkSpaces Pools API and CLI is 432000 seconds (120 hours).
- For **Disconnect timeout in minutes**, choose the amount of time that a streaming session remains active after users disconnect. If users try to reconnect to the streaming session after a disconnection or network interruption within this time interval, they are connected to their previous session. Otherwise, they are connected to a new session with a new streaming instance.
- If a user ends the session by choosing **End Session** or **Logout** on the pools toolbar, the disconnect timeout doesn't apply. Instead, the user is prompted to save any open documents, and then immediately disconnected from the streaming instance. The instance the user was using is then terminated.
- For **Idle disconnect timeout in minutes**, choose the amount of time that users can be idle (inactive) before they are disconnected from their streaming session and the **Disconnect timeout in minutes** time interval begins. Users are notified before they are disconnected due to inactivity. If they try to reconnect to the streaming session before the time interval specified in **Disconnect timeout in minutes** has elapsed, they are connected to their previous session. Otherwise, they are connected to a new session with a new streaming instance. Setting this value to 0 disables it. When this value is disabled, users are not disconnected due to inactivity.

> **Note**
>
> Users are considered idle when they stop providing keyboard or mouse input during their streaming session. For domain-joined pools, the countdown for the idle disconnect timeout doesn't begin until users log in with their Active Directory domain password or with a smart card. File uploads and downloads, audio in, audio out, and pixels changing do not qualify as user activity. If users continue to be idle

after the time interval in **Idle disconnect timeout in minutes** elapses, they are disconnected.

- For **Scheduled capacity policies** (optional), choose **Add new schedule capacity**. Indicate the start and end date and time for when to provision the minimum and maximum number of instances for your pool based on the minimum number of expected concurrent users.
- For **Manual scaling policies** (optional), specify the scaling policies for pools to use to increase and decrease the capacity of your pool. Expand **Manual scaling policies** to add new scaling policies.

> **Note**
>
> The size of your pool is limited by the minimum and maximum capacity that you specified.

  - Choose **Add new scale out policies** and enter the values for adding specified instances if the specified capacity utilization is less or more than the specified threshold value.
  - Choose **Add new scale in policies** and enter the values for removing specified instances if the specified capacity utilization is less or more than the specified threshold value.
- For **Tags**, specify the key pair value that you want to use. A key can be a general category, such as "project," "owner," or "environment," with specific associated values.

6. On the **Select directory page**, choose the directory that you created. To create a directory, choose **Create directory**. For more information, see Manage directories for WorkSpaces Pools.
7. Choose **Create WorkSpace Pool**.

Administer WorkSpaces Pools

A WorkSpaces Pool consists of WorkSpaces that run the image that you specify.

Contents

- Auto scaling for WorkSpaces Pools

Running mode for WorkSpaces Pools

WorkSpaces run only when users are streaming applications and desktops. WorkSpaces not yet assigned to users are in a stopped state. WorkSpaces must be provisioned before a user is able to stream. The number of WorkSpaces provisioned is managed through auto scaling rules.

When your users choose their application or desktop, they will start streaming after a 1-2 minute wait. You are charged a lower stopped instance fee for WorkSpaces that are not yet assigned to users, and the running instance fee for WorkSpaces that are assigned to users.

WorkSpaces Pools Bundles

A *WorkSpace bundle* is a combination of an operating system, and storage, compute, and software resources. When you launch a WorkSpace, you select the bundle that meets your needs. The default bundles available for WorkSpaces are called *public bundles*. For more information about the various public bundles available for WorkSpaces, see Amazon WorkSpaces Bundles.

The following table provides information about the licensing, streaming protocols, and bundles that are supported by each OS.

Operating System	Licenses	Streaming protocols	Supported bundles
Windows Server 2019	Included	WSP	Value, Standard, Performance, Power, PowerPro
Windows Server 2022	Included	WSP	Standard, Performance, Power, PowerPro

Note

- Operating system versions that are no longer supported by the vender are not guaranteed to work and are not supported by AWS support.

Modify a pool

After creating a WorkSpaces Pool, you can modify the following:

- Directory ID (if the WorkSpaces Pool is stopped)
- Basic details
- Bundle and hardware
- Session disconnect settings
- Capacity and scaling
- Scaling activities
- Tags

To modify a WorkSpaces Pool

1. In the navigation pane, choose **WorkSpaces**, **Pools**.
2. Select the pool you want to modify.
3. Go to the section that you want to modify and choose **Edit**.
4. Make the modifications that you want to make and choose **Save**.

Delete a pool

You can delete pools to free up resources and to avoid unintended charges to your account. We recommend stopping any unused, running pools.

To delete a pool

1. In the navigation pane, choose **WorkSpaces**, **Pools**.
2. Select the pool that you want to stop, and then choose **Stop**. It takes about 5 minutes to stop a pool.
3. When the status of the pool is **Stopped**, choose **Delete**.

Auto scaling for WorkSpaces Pools

Auto Scaling lets you change the size of your pools automatically to match the supply of available instances to user demand. The size of your pool determines the number of users who can stream

concurrently. One instance is required for each user session. You can specify your pool capacity in terms of instances. Based on your pool configurations and auto scaling policies, the required number of instances will be made available. You can define scaling policies that adjust the size of your pool automatically based on a variety of utilization metrics, and optimize the number of available instances to match user demand. You can also choose to turn off automatic scaling and make the pool run at a fixed size.

Note

- As you develop your plan for WorkSpaces Pools scaling, make sure that your network configuration meets your requirements.
- When you use scaling, you work with the Application Auto Scaling API. For Auto Scaling to work correctly with WorkSpaces Pools, Application Auto Scaling requires permission to describe and update your pools and describe your Amazon CloudWatch alarms, and permissions to modify your pool capacity on your behalf.

The following topics provide information to help you understand and use Auto Scaling for WorkSpaces Pools.

Contents

Scaling concepts

WorkSpaces Pools scaling is provided by Application Auto Scaling. For more information, see the Application Auto Scaling API Reference.

To use Auto Scaling with WorkSpaces Pools effectively, you must understand the following terms and concepts.

Minimum capacity/minimum user sessions for the pool

The minimum number of instances. The number of instances can't be below this value, and scaling policies will not scale your pool below this value. For example, if you set the minimum capacity for a pool to 2, your pool will never have less than 2 instances.

Maximum capacity/maximum user sessions for the pool

The maximum number of instances. The number of instances can't be above this value, and scaling policies will not scale your pool above this value. For example, if you set the maximum capacity for a pool to 10, your pool will never have more than 10 instances.

Desired user session capacity

The total number of sessions that are either running or pending. This represents the total number of concurrent streaming sessions your pool can support in a steady state.

Scaling policy action

The action that scaling policies perform on your pool when the **Scaling Policy Condition** is met. You can choose an action based on **% capacity** or **number of instance(s)**. For example, if **Desired user session capacity** is 4 and **Scaling Policy Action** is set to "Add 25% capacity", **Desired user session capacity** is increased by 25% to 5 when **Scaling Policy Condition** is met.

Scaling policy condition

The condition that triggers the action set in **Scaling Policy Action**. This condition includes a scaling policy metric, a comparison operator, and a threshold. For example, to scale a pool if the utilization of the pool is greater than 50%, your scaling policy condition should be "If Capacity Utilization > 50%".

Scaling policy metric

Your scaling policy is based on this metric. The following metrics are available for scaling policies:

Capacity Utilization

The percentage of instances in a pool that are being used. You can use this metric to scale your pool based on usage of the pool. For example, **Scaling Policy Condition**: "If Capacity Utilization < 25%" perform **Scaling Policy Action**: "Remove 25 % capacity".

Available capacity

The number of instances in your pool that are available for users. You can use this metric to maintain a buffer in your capacity available for users to start streaming sessions. For

example, **Scaling Policy Condition**: "If Available Capacity < 5" perform **Scaling Policy Action**: "Add 5 instance(s)".

Insufficient capacity error

The number of session requests rejected due to lack of capacity. You can use this metric to provision new instances for users who can't start streaming sessions due to lack of capacity. For example, **Scaling Policy Condition**: "If Insufficient Capacity Error > 0" perform **Scaling Policy Action**: "Add 1 instance(s)".

Managing pool scaling using the console

You can set up and manage scaling by using the WorkSpaces console in either of the following two ways: During pool creation, or any time, by using the **Pools** tab. After you create pools, go to the **Scaling Policies** tab to add new scaling policies for your pool. For more information, see Create a WorkSpaces Pool.

For user environments that vary in number, define scaling policies to control how scaling responds to demand. If you expect a fixed number of users or have other reasons for disabling scaling, you can set your pool with a fixed number of instances for user sessions.

To do this, set the minimum capacity to your desired number of instances. Adjust the maximum capacity to be at least the value of the minimum capacity. This avoids validation errors, but the maximum capacity will ultimately be ignored since the pool will not be scaled. Then, delete all scaling policies for that pool.

To set a pool scaling policy using the console

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Pools**.
3. Select the pool.
4. On that pool's page, scroll down to capacity and scaling.
5. Choose **Edit**.
6. Edit existing policies and set the desired values in their field and choose **Save**. The policy changes go into effect within a few minutes.
7. You can also add new capacity and scaling policies by choosing **Add new schedule capacity**, **Add new scale out policy**, or **Add new scale in policy**.

The following is an example usage graph of scaling activity when five users connect to the pool and then disconnect. This example is from a pool using the following scaling policy values:

- Minimum capacity = 10
- Maximum capacity = 50
- Scale out = If my pool Capacity Utilization is Greater than 75% then add 5 instances
- Scale in = If my pool Capacity Utilization is Less than 25% then remove 6 instances

> **Note**
>
> During the session, 5 new instances will be launched during a scale out event. During a scale in event, 6 instances will be reclaimed, if there are enough instances without active user sessions, and the total number of instances does not drop below the minimum capacity of 10 instances. Instances with running user sessions will not be reclaimed. Only instances with no user sessions running will be reclaimed.

Managing pool scaling using the AWS CLI

You can set up and manage pool scaling by using the AWS Command Line Interface (AWS CLI). For more advanced features such as setting scale-in and scale-out cooldown times, use the AWS CLI. Before running scaling policy commands, you must register your pool as a scalable target. To do so, use the following register-scalable-target command:

```
aws application-autoscaling register-scalable-target
  --service-namespace workspaces \
  --resource-id workspacespool/PoolId \
  --scalable-dimension workspaces:workspacespool:DesiredUserSessions \
  --min-capacity 1 --max-capacity 5
```

Examples

- Example 1: Applying a scaling policy based on capacity utilization
- Example 2: Applying a scaling policy based on insufficient capacity errors
- Example 3: Applying a scaling policy based on low capacity utilization
- Example 4: Change the pool capacity based on a schedule
- Example 5: Applying a target tracking scaling policy

Example 1: Applying a scaling policy based on capacity utilization

This AWS CLI example sets up a scaling policy that scales out a pool by 25% if Utilization >= 75%.

The following put-scaling-policy command defines a utilization-based scaling policy:

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-out-
utilization.json
```

The contents of the file `scale-out-utilization.json` are as follows:

```
{
    "PolicyName": "policyname",
    "ServiceNamespace": "workspaces",
    "ResourceId": "workspacespool/PoolId",
    "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
    "PolicyType": "StepScaling",
    "StepScalingPolicyConfiguration": {
        "AdjustmentType": "PercentChangeInCapacity",
        "StepAdjustments": [
            {
                "MetricIntervalLowerBound": 0,
                "ScalingAdjustment": 25
            }
        ],
        "Cooldown": 120
    }
}
```

If the command is successful, the output is similar to the following, although some details are unique to your account and Region. In this example, the policy identifier is `e3425d21-16f0-d701-89fb-12f98dac64af`.

```
{"PolicyARN": "arn:aws:autoscaling:us-west-2:123456789012:scalingPolicy:e3425d21-16f0-
d701-89fb-12f98dac64af:resource/workspaces/workspacespool/PoolId:policyName/scale-out-
utilization-policy"}
```

Now, set up a CloudWatch alarm for this policy. Use the names, Region, account number, and policy identifier that apply to you. You can use the policy ARN returned by the previous command for the `-- alarm-actions` parameter.

```
aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when Available User Session Capacity exceeds 75 percent" \
--metric-name AvailableUserSessionCapacity \
--namespace AWS/WorkSpaces \
--statistic Average \
--period 300 \
--threshold 75 \
--comparison-operator GreaterThanOrEqualToThreshold \
--dimensions "Name=WorkSpaces pool ID,Value=PoolId" \
--evaluation-periods 1 --unit Percent \
--alarm-actions "arn:aws:autoscaling:your-region-code:account-
number-without-hyphens:scalingPolicy:policyid:resource/workspaces/
workspacespool/PoolId:policyName/policyname"
```

Example 2: Applying a scaling policy based on insufficient capacity errors

This AWS CLI example sets up a scaling policy that scales out the pool by 1 if the pool returns an `InsufficientCapacityError` error.

The following command defines a insufficient capacity-based scaling policy:

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-out-
capacity.json
```

The contents of the file `scale-out-capacity.json` are as follows:

```
{
    "PolicyName": "policyname",
    "ServiceNamespace": "workspaces",
    "ResourceId": "workspacespool/PoolId",
    "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
    "PolicyType": "StepScaling",
    "StepScalingPolicyConfiguration": {
        "AdjustmentType": "ChangeInCapacity",
        "StepAdjustments": [
            {
                "MetricIntervalLowerBound": 0,
                "ScalingAdjustment": 1
            }
        ],
        "Cooldown": 120
```

```
    }
}
```

If the command is successful, the output is similar to the following, although some details are unique to your account and Region. In this example, the policy identifier is `f4495f21-0650-470c-88e6-0f393adb64fc`.

```
{"PolicyARN": "arn:aws:autoscaling:us-
west-2:123456789012:scalingPolicy:f4495f21-0650-470c-88e6-0f393adb64fc:resource/
workspaces/workspacespool/PoolId:policyName/scale-out-insufficient-capacity-policy"}
```

Now, set up a CloudWatch alarm for this policy. Use the names, Region, account number, and policy identifier that apply to you. You can use the policy ARN returned by the previous command for the `--alarm-actions` parameter.

```
aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when out of capacity is > 0" \
--metric-name InsufficientCapacityError \
--namespace AWS/WorkSpaces \
--statistic Maximum \
--period 300 \
--threshold 0 \
--comparison-operator GreaterThanThreshold \
--dimensions "Name=Pool,Value=PoolId" \
--evaluation-periods 1 --unit Count \
--alarm-actions "arn:aws:autoscaling:your-region-code:account-
number-without-hyphens:scalingPolicy:policyid:resource/workspaces/
workspacespool/PoolId:policyName/policyname"
```

Example 3: Applying a scaling policy based on low capacity utilization

This AWS CLI example sets up a scaling policy that scales in the pool to reduce actual capacity when `UserSessionsCapacityUtilization` is low.

The following command defines an excess capacity-based scaling policy:

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-in-
capacity.json
```

The contents of the file `scale-in-capacity.json` are as follows:

```
{
    "PolicyName": "policyname",
    "ServiceNamespace": "workspaces",
    "ResourceId": "workspacespool/PoolId",
    "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
    "PolicyType": "StepScaling",
    "StepScalingPolicyConfiguration": {
        "AdjustmentType": "PercentChangeInCapacity",
        "StepAdjustments": [
            {
                "MetricIntervalUpperBound": 0,
                "ScalingAdjustment": -25
            }
        ],
        "Cooldown": 360
    }
}
```

If the command is successful, the output is similar to the following, although some details are unique to your account and Region. In this example, the policy identifier is `12ab3c4d-56789-0ef1-2345-6ghi7jk8lm90`.

```
{"PolicyARN": "arn:aws:autoscaling:us-
west-2:123456789012:scalingPolicy:12ab3c4d-56789-0ef1-2345-6ghi7jk8lm90:resource/
workspaces/workspacespool/PoolId:policyName/scale-in-utilization-policy"}
```

Now, set up a CloudWatch alarm for this policy. Use the names, Region, account number, and policy identifier that apply to you. You can use the policy ARN returned by the previous command for the `--alarm-actions` parameter.

```
aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when Capacity Utilization is less than or equal to 25
 percent" \
--metric-name UserSessionsCapacityUtilization \
--namespace AWS/WorkSpaces \
--statistic Average \
--period 120 \
--threshold 25 \
--comparison-operator LessThanOrEqualToThreshold \
--dimensions "Name=Pool,Value=PoolId" \
```

```
--evaluation-periods 10 --unit Percent \
--alarm-actions "arn:aws:autoscaling:your-region-code:account-
number-without-hyphens:scalingPolicy:policyid:resource/workspaces/
workspacespool/PoolId:policyName/policyname"
```

Example 4: Change the pool capacity based on a schedule

Changing your pool capacity based on a schedule lets you scale your pool capacity in response to predictable changes in demand. For example, at the start of a work day, you might expect a certain number of users to request streaming connections at one time. To change your pool capacity based on a schedule, you can use the Application Auto Scaling PutScheduledAction API action or the put-scheduled-action AWS CLI command.

Before changing your pool capacity, you can list your current pool capacity by using the WorkSpaces describe-workspaces-pools AWS CLI command.

```
aws workspaces describe-workspaces-pools --name PoolId
```

The current pool capacity will appear similar to the following output (shown in JSON format):

```
{
    "CapacityStatus": {
        "AvailableUserSessions": 1,
        "DesiredUserSessions": 1,
        "ActualUserSessions": 1,
        "ActiveUserSessions": 0
    },
}
```

Then, use the `put-scheduled-action` command to create a scheduled action to change your pool capacity. For example, the following command changes the minimum capacity to 3 and the maximum capacity to 5 every day at 9:00 AM UTC.

> **Note**
>
> For cron expressions, specify when to perform the action in UTC. For more information, see Cron Expressions.

```
aws application-autoscaling put-scheduled-action --service-namespace workspaces \
```

```
--resource-id workspacespool/PoolId \
--schedule="cron(0 9 * * ? *)" \
--scalable-target-action MinCapacity=3,MaxCapacity=5 \
--scheduled-action-name ExampleScheduledAction \
--scalable-dimension workspaces:workspacespool:DesiredUserSessions
```

To confirm that the scheduled action to change your pool capacity was successfully created, run the describe-scheduled-actions command.

```
aws application-autoscaling describe-scheduled-actions --service-namespace workspaces
 --resource-id workspacespool/PoolId
```

If the scheduled action was successfully created, the output appears similar to the following.

```
{
    "ScheduledActions": [
        {
            "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
            "Schedule": "cron(0 9 * * ? *)",
            "ResourceId": "workspacespool/ExamplePool",
            "CreationTime": 1518651232.886,
            "ScheduledActionARN": "<arn>",
            "ScalableTargetAction": {
                "MinCapacity": 3,
                "MaxCapacity": 5
            },
            "ScheduledActionName": "ExampleScheduledAction",
            "ServiceNamespace": "workspaces"
        }
    ]
}
```

For more information, see Scheduled Scaling in the *Application Auto Scaling User Guide*.

Example 5: Applying a target tracking scaling policy

With target tracking scaling, you can specify a capacity utilization level for your pool.

When you create a target tracking scaling policy, Application Auto Scaling automatically creates and manages CloudWatch alarms that trigger the scaling policy. The scaling policy adds or removes capacity as required to keep capacity utilization at, or close to, the specified target value. To ensure

application availability, your pool scales out proportionally to the metric as fast as it can but scales in more gradually.

The following put-scaling-policy command defines a target tracking scaling policy that attempts to maintain 75% capacity utilization for a WorkSpaces pool.

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://config.json
```

The contents of the file `config.json` are as follows:

```
{
  "PolicyName":"target-tracking-scaling-policy",
  "ServiceNamespace":"workspaces",
  "ResourceId":"workspacespool/PoolId",
  "ScalableDimension":"workspaces:workspacespool:DesiredUserSessions",
  "PolicyType":"TargetTrackingScaling",
  "TargetTrackingScalingPolicyConfiguration":{
    "TargetValue":75.0,
    "PredefinedMetricSpecification":{
      "PredefinedMetricType":"WorkSpacesAverageUserSessionsCapacityUtilization"
    },
    "ScaleOutCooldown":300,
    "ScaleInCooldown":300
  }
}
```

If the command is successful, the output is similar to the following, although some details are unique to your account and Region. In this example, the policy identifier is 6d8972f3-efc8-437c-92d1-6270f29a66e7.

```
{
    "PolicyARN": "arn:aws:autoscaling:us-west-2:123456789012:scalingPolicy:6d8972f3-
efc8-437c-92d1-6270f29a66e7:resource/workspaces/workspacespool/PoolId:policyName/
target-tracking-scaling-policy",
    "Alarms": [
        {
            "AlarmARN": "arn:aws:cloudwatch:us-
west-2:123456789012:alarm:TargetTracking-workspacespool/PoolId-AlarmHigh-d4f0770c-
b46e-434a-a60f-3b36d653feca",
            "AlarmName": "TargetTracking-workspacespool/PoolId-AlarmHigh-d4f0770c-
b46e-434a-a60f-3b36d653feca"
```

```
        },
        {
            "AlarmARN": "arn:aws:cloudwatch:us-
west-2:123456789012:alarm:TargetTracking-workspacespool/PoolId-AlarmLow-1b437334-
d19b-4a63-a812-6c67aaf2910d",
            "AlarmName": "TargetTracking-workspacespool/PoolId-AlarmLow-1b437334-
d19b-4a63-a812-6c67aaf2910d"
        }
    ]
}
```

For more information, see Target Tracking Scaling Policies in the *Application Auto Scaling User Guide*.

Additional resources

To learn more about using the Application Auto Scaling AWS CLI commands or API actions, see the following resources:

- application-autoscaling section of the *AWS CLI Command Reference*
- Application Auto Scaling API Reference
- Application Auto Scaling User Guide

Using Active Directory with WorkSpaces Pools

You can join your Windows WorkSpaces in WorkSpaces Pools to domains in Microsoft Active Directory and use your existing Active Directory domains, either cloud-based or on-premises, to launch domain-joined streaming instances. You can also use AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, to create an Active Directory domain and use that to support your WorkSpaces Pools resources. For more information about using AWS Managed Microsoft AD, see Microsoft Active Directory in the *AWS Directory Service Administration Guide*.

By joining WorkSpaces Pools to your Active Directory domain, you can:

- Allow your users and applications to access Active Directory resources such as printers and file shares from streaming sessions.
- Use Group Policy settings that are available in the Group Policy Management Console (GPMC) to define the end user experience.

- Stream applications that require users to be authenticated using their Active Directory login credentials.
- Apply your enterprise compliance and security policies to your WorkSpaces in WorkSpaces Pools.

Contents

Overview of Active Directory Domains

Using Active Directory domains with WorkSpaces Pools requires an understanding of how they work together and the configuration tasks that you'll need to complete. You'll need to complete the following tasks:

1. Configure Group Policy settings as needed to define the end user experience and security requirements for applications.
2. Create the domain-joined directory in WorkSpaces Pools.
3. Create the WorkSpaces Pools application in the SAML 2.0 identity provider and assign it to end users either directly or through Active Directory groups.

User Authentication Flow

1. The user browses to `https://applications.exampleco.com`. The sign-on page requests authentication for the user.
2. The federation service requests authentication from the organization's identity store.
3. The identity store authenticates the user and returns the authentication response to the federation service.
4. On successful authentication, the federation service posts the SAML assertion to the user's browser.
5. The user's browser posts the SAML assertion to the AWS Sign-In SAML endpoint (`https://signin.aws.amazon.com/saml`). AWS Sign-In receives the SAML request, processes the

request, authenticates the user, and forwards the authentication token to the WorkSpaces Pools service.

6. Using the authentication token from AWS, WorkSpaces Pools authorizes the user and presents applications to the browser.
7. The user chooses an application and, depending on the Windows login authentication method that is enabled on the WorkSpaces Pools directory, they're prompted to enter their Active Directory domain password or choose a smart card. If both authentication methods are enabled, the user can choose whether to enter their domain password or use their smart card. Certificate-based authentication can also be used to authenticate users, removing the prompt.
8. The domain controller is contacted for user authentication.
9. After being authenticated with the domain, the user's session starts with domain connectivity.

From the user's perspective, this process is transparent. The user starts by navigating to your organization's internal portal and is redirected to a WorkSpaces Pools portal, without having to enter AWS credentials. Only an Active Directory domain password or smart card credentials are required.

Before a user can initiate this process, you must configure Active Directory with the required entitlements and Group Policy settings and create a domain-joined WorkSpaces Pools directory.

Before You Begin Using Active Directory with WorkSpaces Pools

Before you use Microsoft Active Directory domains with WorkSpaces Pools, be aware of the following requirements and considerations.

Contents

Active Directory Domain Environment

- You must have a Microsoft Active Directory domain to which to join your WorkSpaces. If you don't have an Active Directory domain or you want to use your on-premises Active Directory

environment, see Active Directory Domain Services on the AWS Cloud: Quick Start Reference Deployment.

- You must have a domain service account with permissions to create and manage computer objects in the domain that you intend to use with WorkSpaces Pools. For information, see How to Create a Domain Account in Active Directory in the Microsoft documentation.

  When you associate this Active Directory domain with WorkSpaces Pools, provide the service account name and password. WorkSpaces Pools uses this account to create and manage computer objects in the directory. For more information, see Granting Permissions to Create and Manage Active Directory Computer Objects.
- When you register your Active Directory domain with WorkSpaces Pools, you must provide an organizational unit (OU) distinguished name. Create an OU for this purpose. The default Computers container is not an OU and cannot be used by WorkSpaces Pools. For more information, see Finding the Organizational Unit Distinguished Name.
- The directories that you plan to use with WorkSpaces Pools must be accessible through their fully qualified domain names (FQDNs) through the virtual private cloud (VPC) in which your WorkSpaces are launched. For more information, see Active Directory and Active Directory Domain Services Port Requirements in the Microsoft documentation.

Domain-Joined WorkSpaces in WorkSpaces Pools

SAML 2.0-based user federation is required for application streaming from domain-joined WorkSpaces. Also, you must use a Windows image that supports joining to an Active Directory domain. All public images published on or after July 24, 2017 support joining an Active Directory domain.

Group Policy Settings

Verify your configuration for the following Group Policy settings. If required, update the settings as described in this section so that they don't block WorkSpaces Pools from authenticating and logging in your domain users. Otherwise, when your users try to log in to WorkSpaces the login may not succeed. Instead, a message displays, notifying users that "An unknown error occurred."

- **Computer Configuration > Administrative Templates > Windows Components > Windows Logon Options > Disable or Enable software Secure Attention Sequence** — Set this to **Enabled** for **Services**.

- **Computer Configuration > Administrative Templates > System > Logon > Exclude credential providers** — Ensure that the following CLSID is *not* listed: `e7c1bab5-4b49-4e64-a966-8d99686f8c7c`
- **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Interactive Logon > Interactive Logon: Message text for users attempting to log on** — Set this to **Not defined**.
- **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Interactive Logon > Interactive Logon: Message title for users attempting to log on** — Set this to **Not defined**.

Smart Card Authentication

WorkSpaces Pools supports the use of Active Directory domain passwords or smart cards such as Common Access Card (CAC) and Personal Identity Verification (PIV) smart cards for Windows sign in to WorkSpaces in WorkSpaces Pools. For information about how to configure your Active Directory environment to enable smart card sign in by using third-party certification authorities (CAs), see Guidelines for enabling smart card logon with third-party certification authorities in the Microsoft documentation.

Certificate-Based Authentication

You can use certificate-based authentication with WorkSpaces Pools joined to Microsoft Active Directory. This removes the user prompt for the Active Directory domain password when a user logs in. By using certificate-based authentication with your Active Directory domain, you can:

- Rely on your SAML 2.0 identity provider to authenticate the user and provide SAML assertions to match the user in Active Directory.
- Create a single sign-on logon experience with fewer user prompts.
- Enable passwordless authentication flows using your SAML 2.0 identity provider.

Certificate-based authentication uses AWS Private Certificate Authority (AWS Private CA) resources in your AWS account. With AWS Private CA, you can create private certificate authority (CA) hierarchies, including root and subordinate CAs. You can also create your own CA hierarchy and issue certificates from it that authenticate internal users. For more information, see What is AWS Private CA.

When you use AWS Private CA for certificate-based authentication, WorkSpaces Pools requests certificates for your users automatically at session reservation for each WorkSpace in a WorkSpaces Pool. It authenticates users to Active Directory with a virtual smart card provisioned with the certificates.

Certificate-based authentication is supported on domain-joined WorkSpaces Pools that run Windows instances.

Contents

Prerequisites

Complete the following steps before you use certificate-based authentication.

1. Configure your WorkSpaces Pools directory with SAML 2.0 integration to use certificate-based authentication. For more information, see Configure SAML 2.0 and create a WorkSpaces Pools directory.

   > **Note**
   >
   > Don't enable **Smart card sign in** in your pool directory if you want to use certificate-based authentication.

2. Configure the `userPrincipalName` attribute in your SAML assertion. For more information, see Step 7: Create assertions for the SAML authentication response.
3. (Optional) Configure the `ObjectSid` attribute in your SAML assertion. You can use this attribute to perform strong mapping with the Active Directory user. Certificate-based authentication fails if the `ObjectSid` attribute doesn't match the Active Directory security identifier (SID) for the user specified in the SAML_Subject `NameID`. For more information, see Step 7: Create assertions for the SAML authentication response.
4. Add the `sts:TagSession` permission to the IAM role trust policy that you use with your SAML 2.0 configuration. For more information, see Passing session tags in AWS STS in the *AWS*

Identity and Access Management User Guide. This permission is required to use certificate-based authentication. For more information, see Step 5: Create a SAML 2.0 federation IAM role.

5. Create a private certificate authority (CA) using AWS Private CA, if you don't have one configured with your Active Directory. AWS Private CA is required to use certificate-based authentication. For more information, see Planning your AWS Private CA deployment in the *AWS Private Certificate Authority User Guide*. The following AWS Private CA settings are common for many certificate-based authentication use cases:
   - **CA type options**
     - **Short-lived certificate CA usage mode** – Recommended if the CA only issues end user certificates for certificate-based authentication.
     - **Single level hierarchy with a Root CA** – Choose a subordinate CA to integrate it with an existing CA hierarchy.
   - **Key algorithm options** – RSA 2048
   - **Subject distinguished name options** – Use the most appropriate options to identify this CA in your Active Directory Trusted Root Certification Authorities store.
   - **Certificate revocation options** – CRL distribution

   > **Note**
   >
   > Certificate-based authentication requires an online CRL distribution point accessible from both the WorkSpaces in WorkSpaces Pools and the domain controller. This requires unauthenticated access to the Amazon S3 bucket configured for AWS Private CA CRL entries, or a CloudFront distribution with access to the Amazon S3 bucket if it blocks public access. For more information about these options, see Planning a certificate revocation list (CRL) in the *AWS Private Certificate Authority User Guide*.

6. Tag your private CA with a key entitled `euc-private-ca` to designate the CA for use with WorkSpaces Pools certificate-based authentication. This key doesn't require a value. For more information, see Managing tags for your private CA in the *AWS Private Certificate Authority User Guide*..
7. Certificate-based authentication uses virtual smart cards to log on. For more information, see Guidelines for enabling smart card logon with third-party certification authorities. Follow these steps:
   a. Configure domain controllers with a domain controller certificate to authenticate smart card users. If you have an Active Directory Certificate Services enterprise CA configured in your

Active Directory, it automatically enrolls domain controllers with certificates that enable smart card logon. If you don't have Active Directory Certificate Services, see Requirements for domain controller certificates from a third-party CA. You can create a domain controller certificate with AWS Private CA. If you do this, don't use a private CA configured for short-lived certificates.

> **Note**
>
> If you use AWS Managed Microsoft AD, you can configure Certificate Services on an Amazon EC2 instance that satisfies the requirement for domain controller certificates. See Deploy Active Directory to a new Amazon Virtual Private Cloud for example deployments of AWS Managed Microsoft AD configured with Active Directory Certificate Services.
> With AWS Managed Microsoft AD and Active Directory Certificate Services, you must also create outbound rules from the controller's VPC security group to the Amazon EC2 instance running Certificate Services. You must provide the security group access to TCP port 135, and ports 49152 through 65535 to enable certificate auto-enrollment. The Amazon EC2 instance must also allow inbound access on these same ports from domain instances, including domain controllers. For more information on locating the security group for AWS Managed Microsoft AD, see Configure your VPC subnets and security groups.

b. On the AWS Private CA console, or with the SDK or CLI, export the private CA certificate. For more information, see Exporting a private certificate.

c. Publish the private CA to Active Directory. Log on to a domain controller or a domain-joined machine. Copy the private CA certificate to any *<path>**<file>* and run the following commands as a domain administrator. You can also use Group Policy and the Microsoft PKI Health Tool (PKIView) to publish the CA. For more information, see Configuration instructions.

```
certutil -dspublish -f <path>\<file> RootCA
```

```
certutil -dspublish -f <path>\<file> NTAuthCA
```

Make sure that the commands complete successfully, then remove the private CA certificate file. Depending on your Active Directory replication settings, it can take several minutes for the CA to publish to your domain controllers and WorkSpaces in WorkSpaces Pools.

> **Note**
>
> Active Directory must distribute the CA to the Trusted Root Certification Authorities and Enterprise NTAuth stores automatically for WorkSpaces in WorkSpaces Pools when they join the domain.

> **Note**
>
> Active Directory domain controllers must be in Compatibility mode for certificate strong enforcement to support certificate-based authentication. For more information, see KB5014754—Certificate-based authentication changes on Windows domain controllers in the Microsoft Support documentation. If you are using AWS Managed Microsoft AD, see Configure directory security settings for more information.

Enable Certificate-based Authentication

Complete the following steps to enable certificate-based authentication.

To enable certificate-based authentication

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose **Directories** in the navigation pane.
3. Choose the **Pools directories** tab.
4. Choose the directory you want to configure.
5. Choose **Edit** in the **Authentication** section of the page.
6. Choose **Edit Certificate-Based Authentication** in the **Certificate-Based Authentication** section of the page.
7. Choose **Enable Certificate-Based Authentication**.
8. Choose the certificate in the **AWS Certificate Manager (ACM) Private Certificate Authority (CA)** drop-down.

   To appear in the drop-down, you should store the private CA in the same AWS account and AWS Region. You must also tag the private CA with a key named `euc-private-ca`.

9. Configure directory log in fallback. With Fallback, users can log in with their AD domain password if certificate-based authentication is unsuccessful. This is recommended only in cases where users know their domain passwords. When fallback is turned off, a session can disconnect the user if a lock screen or Windows log off occurs. If fallback is turned on, the session prompts the user for their AD domain password.
10. Choose **Save**.

Certificate-based authentication is now enabled. When users authenticate with SAML 2.0 to an WorkSpaces Pools directory using the domain-joined WorkSpaces, they will no longer receive a prompt for the domain password. Users will see a **Connecting with certificate-based authentication** message when connecting to a session enabled for certificate-based authentication.

Manage Certificate-based Authentication

After you enable certificate-based authentication, review the following tasks.

Private CA Certificate

In a typical configuration, the private CA certificate has a validity period of 10 years. For more information about replacing a private CA with an expired certificate, or reissuing the private CA with a new validity period, see Managing the private CA lifecycle

End User Certificates

End user certificates issued by AWS Private Certificate Authority for WorkSpaces Pools certificate-based authentication don't require renewal or revocation. These certificates are short-lived. WorkSpaces Pools automatically issues a new certificate for each new session, or every 24 hours for sessions with a long duration. The WorkSpaces Pools session governs the use of these end user certificates. If you end a session, WorkSpaces Pools stops using that certificate. These end user certificates have a shorter validity period than a typical AWS Private Certificate Authority CRL distribution. As a result, end user certificates don't need to be revoked and won't appear in a CRL.

Audit Reports

You can create an audit report to list all of the certificates that your private CA has issued or revoked. For more information, see Using audit reports with your private CA.

Logging and Monitoring

You can use CloudTrail to record API calls to a private CA by WorkSpaces Pools. For more information see What Is AWS CloudTrail? in the *AWS CloudTrail User Guide*, and Using CloudTrail in the *AWS Private Certificate Authority User Guide*. In CloudTrail Event history you can view **GetCertificate** and **IssueCertificate** event names from **acm-pca.amazonaws.com** event source made by the WorkSpaces Pools **EcmAssumeRoleSession** user name. These events will be recorded for every WorkSpaces Pools certificate-based authentication request. For more information, see Viewing events with CloudTrail Event history in the *AWS CloudTrail User Guide*.

Enable Cross-account PCA Sharing

Private CA (PCA) cross-account sharing offers the ability to grant permissions for other accounts to use a centralized CA. The CA can generate and issue certificates by using AWS Resource Access Manager (RAM) to manage the permissions. This removes the need for a Private CA in every account. Private CA cross-account sharing can be used with AppStream 2.0 certificate-based Authentication (CBA) within the same AWS Region.

To use a shared Private CA resource with WorkSpaces Pools CBA, complete the following steps:

1. Configure the Private CA for CBA in a centralized AWS account. For more information, see the section called “Certificate-based authentication”.
2. Share the Private CA with the resource AWS accounts where WorkSpaces Pools resources utilize CBA. To do this, follow the steps in How to use AWS RAM to share your ACM Private CA cross-account. You do not need to complete step 3 to create a certificate. You can either share the Private CA with individual AWS accounts, or share through AWS Organizations. If you share with individual accounts, you need to accept the shared Private CA in your resource account by using the AWS Resource Access Manager console or APIs.

   When configuring the share, confirm that the AWS Resource Access Manager resource share for the Private CA in the resource account is using the `AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority` managed permission template. This template aligns with the PCA template used by the WorkSpaces Pools service role when issuing CBA certificates.
3. After the share is successful, view the shared Private CA by using the Private CA console in the resource account.

4. Use the API or CLI to associate the Private CA ARN with CBA in your WorkSpaces Pools directory. At this time, the WorkSpaces Pools console does not support selection of shared Private CA ARNs. For more information, see the Amazon WorkSpaces Service API Reference.

WorkSpaces Pools Active Directory Administration

Setting up and using Active Directory with WorkSpaces Pools involves the following administrative tasks.

Tasks

- Granting Permissions to Create and Manage Active Directory Computer Objects
- Finding the Organizational Unit Distinguished Name
- Granting Local Administrator Rights on custom images
- Locking the Streaming Session When the User is Idle
- Configuring WorkSpaces Pools to Use Domain Trusts

Granting Permissions to Create and Manage Active Directory Computer Objects

To allow WorkSpaces Pools to perform Active Directory computer object operations, you need an account with sufficient permissions. As a best practice, use an account that has only the minimum privileges necessary. The minimum Active Directory organizational unit (OU) permissions are as follows:

- Create Computer Object
- Change Password
- Reset Password
- Write Description

Before setting up permissions, you'll need to do the following first:

- Obtain access to a computer or an EC2 instance that is joined to your domain.
- Install the Active Directory User and Computers MMC snap-in. For more information, see Installing or Removing Remote Server Administration Tools for Windows 7 in the Microsoft documentation.
- Log in as a domain user with appropriate permissions to modify the OU security settings.

- Create or identify the user, service account, or group for which to delegate permissions.

To set up minimum permissions

1. Open **Active Directory Users and Computers** in your domain or on your domain controller.
2. In the left navigation pane, select the first OU on which to provide domain join privileges, open the context (right-click) menu , and then choose **Delegate Control**.
3. On the **Delegation of Control Wizard** page, choose **Next**, **Add**.
4. For **Select Users, Computers, or Groups**, select the pre-created user, service account, or group, and then choose **OK**.
5. On the **Tasks to Delegate** page, choose **Create a custom task to delegate**, and then choose **Next**.
6. Choose **Only the following objects in the folder**, **Computer objects**.
7. Choose **Create selected objects in this folder**, **Next**.
8. For **Permissions**, choose **Read**, **Write**, **Change Password**, **Reset Password**, **Next**.
9. On the **Completing the Delegation of Control Wizard** page, verify the information and choose **Finish**.
10. Repeat steps 2-9 for any additional OUs that require these permissions.

If you delegated permissions to a group, create a user or service account with a strong password and add that account to the group. This account will then have sufficient privileges to connect your WorkSpaces to the directory. Use this account when creating your WorkSpaces Pools directory configuration.

Finding the Organizational Unit Distinguished Name

When you register your Active Directory domain with WorkSpaces Pools, you must provide an organizational unit (OU) distinguished name. Create an OU for this purpose. The default Computers container is not an OU and cannot be used by WorkSpaces Pools. The following procedure shows how to obtain this name.

> **Note**
>
> The distinguished name must start with **OU=** or it cannot be used for computer objects.

Before you complete this procedure, you'll need to do the following first:

- Obtain access to a computer or an EC2 instance that is joined to your domain.
- Install the Active Directory User and Computers MMC snap-in. For more information, see Installing or Removing Remote Server Administration Tools for Windows 7 in the Microsoft documentation.
- Log in as a domain user with appropriate permissions to read the OU security properties.

To find the distinguished name of an OU

1. Open **Active Directory Users and Computers** in your domain or on your domain controller.
2. Under **View**, ensure that **Advanced Features** is enabled.
3. In the left navigation pane, select the first OU to use for WorkSpaces computer objects, open the context (right-click) menu, and then choose **Properties**.
4. Choose **Attribute Editor**.
5. Under **Attributes**, for **distinguishedName**, choose **View**.
6. For **Value**, select the distinguished name, open the context menu, and then choose **Copy**.

Granting Local Administrator Rights on custom images

By default, Active Directory domain users do not have local administrator rights on images. You can grant these rights by using Group Policy preferences in your directory, or manually, by using the local administrator account on an image. Granting local administrator rights to a domain user allows that user to install applications on and create custom images in WorkSpaces Pools.

Contents

Using Group Policy preferences

You can use Group Policy preferences to grant local administrator rights to Active Directory users or groups and to all computer objects in the specified OU. The Active Directory users or groups to which you want to grant local administrator permissions must already exist. To use Group Policy preferences, you'll need to do the following first:

- Obtain access to a computer or an EC2 instance that is joined to your domain.
- Install the Group Policy Management Console (GPMC) MMC snap-in. For more information, see Installing or Removing Remote Server Administration Tools for Windows 7 in the Microsoft documentation.
- Log in as a domain user with permissions to create Group Policy objects (GPOs). Link GPOs to the appropriate OUs.

To use Group Policy preferences to grant local administrator permissions

1. In your directory or on a domain controller, open the command prompt as an administrator, type `gpmc.msc`, and then press ENTER.
2. In the left console tree, select the OU where you will create a new GPO or use an existing GPO, and then do either of the following:
   - Create a new GPO by opening the context (right-click) menu and choosing **Create a GPO in this domain, Link it here**. For **Name**, provide a descriptive name for this GPO.
   - Select an existing GPO.
3. Open the context menu for the GPO, and choose **Edit**.
4. In the console tree, choose **Computer Configuration**, **Preferences**, **Windows Settings**, **Control Panel Settings**, and **Local Users and Groups**.
5. Select **Local Users and Groups** selected, open the context menu , and choose **New**, **Local Group**.
6. For **Action**, choose **Update**.
7. For **Group name**, choose **Administrators (built-in)**.
8. Under **Members**, choose **Add...** and specify the Active Directory users or groups to which to assign local administrator rights on the streaming instance. For **Action**, choose **Add to this group**, and choose **OK**.
9. To apply this GPO to other OUs, select the additional OU, open the context menu and choose **Link an Existing GPO**.
10. Using the new or existing GPO name that you specified in step 2, scroll to find the GPO, and then choose **OK**.
11. Repeat steps 9 and 10 for additional OUs that should have this preference.
12. Choose **OK** to close the **New Local Group Properties** dialog box.

13. Choose **OK** again to close the GPMC.

To apply the new preference to the GPO, you must stop and restart any running image builders or fleets. The Active Directory users and groups that you specified in step 8 are automatically granted local administrator rights on the image builders and fleets in the OU to which the GPO is linked.

Using the local Administrators group on the WorkSpace to create images

To grant Active Directory users or groups local administrator rights on an image, you can manually add these users or groups to the local Administrators group on the image.

The Active Directory users or groups to which to grant local administrator rights must already exist.

1. Connect to the WorkSpace you use to build images. The WorkSpace must be running and domain-joined.
2. Choose **Start**, **Administrative Tools**, and then double-click **Computer Management**.
3. In the left navigation pane, choose **Local Users and Groups** and open the **Groups** folder.
4. Open the **Administrators** group and choose **Add...**.
5. Select all Active Directory users or groups to which to assign local administrator rights and choose **OK**. Choose **OK** again to close the **Administrator Properties** dialog box.
6. Close Computer Management.
7. To log in as an Active Directory user and test whether that user has local administrator rights on the WorkSpaces, choose **Admin Commands**, **Switch user**, and then enter the credentials of the relevant user.

Locking the Streaming Session When the User is Idle

WorkSpaces Pools relies on a setting that you configure in the GPMC to lock the streaming session after your user is idle for specified amount of time. To use the GPMC, you'll need to do the following first:

- Obtain access to a computer or an EC2 instance that is joined to your domain.
- Install the GPMC. For more information, see Installing or Removing Remote Server Administration Tools for Windows 7 in the Microsoft documentation.
- Log in as a domain user with permissions to create GPOs. Link GPOs to the appropriate OUs.

To automatically lock the streaming instance when your user is idle

1. In your directory or on a domain controller, open the command prompt as an administrator, type `gpmc.msc`, and then press ENTER.
2. In the left console tree, select the OU where you will create a new GPO or use an existing GPO, and then do either of the following:
   - Create a new GPO by opening the context (right-click) menu and choosing **Create a GPO in this domain, Link it here**. For **Name**, provide a descriptive name for this GPO.
   - Select an existing GPO.
3. Open the context menu for the GPO, and choose **Edit**.
4. Under **User Configuration**, expand **Policies**, **Administrative Templates**, **Control Panel**, and then choose **Personalization**.
5. Double-click **Enable screen saver**.
6. In the **Enable screen saver** policy setting, choose **Enabled**.
7. Choose **Apply**, and then choose **OK**.
8. Double-click **Force specific screen saver**.
9. In the **Force specific screen saver** policy setting, choose **Enabled**.
10. Under **Screen saver executable name**, enter **`scrnsave.scr`**. When this setting is enabled, the system displays a black screen saver on the user's desktop.
11. Choose **Apply**, and then choose **OK**.
12. Double-click **Password protect the screen saver**.
13. In the **Password protect the screen saver** policy setting, choose **Enabled**.
14. Choose **Apply**, and then choose **OK**.
15. Double-click **Screen saver timeout**.
16. In the **Screen saver timeout** policy setting, choose **Enabled**.
17. For **Seconds**, specify the length of time that users must be idle before the screen saver is applied. To set the idle time to 10 minutes, specify 600 seconds.
18. Choose **Apply**, and then choose **OK**.
19. In the console tree, under **User Configuration**, expand **Policies**, **Administrative Templates**, **System**, and then choose **Ctrl+Alt+Del Options**.
20. Double-click **Remove Lock Computer**.

21. In the **Remove Lock Computer** policy setting, choose **Disabled**.
22. Choose **Apply**, and then choose **OK**.

Configuring WorkSpaces Pools to Use Domain Trusts

WorkSpaces Pools supports Active Directory domain environments where network resources such as file servers, applications, and computer objects reside in one domain, and the user objects reside in another. The domain service account used for computer object operations does not need to be in the same domain as the WorkSpaces Pools computer objects.

When creating the directory configuration, specify a service account that has the appropriate permissions to manage computer objects in the Active Directory domain where the file servers, applications, computer objects and other network resources reside.

Your end user Active Directory accounts must have the "Allowed to Authenticate" permissions for the following:

- WorkSpaces Pools computer objects
- Domain controllers for the domain

For more information, see Granting Permissions to Create and Manage Active Directory Computer Objects.

More Info

For more information related to this topic, see the following resources:

- Microsoft Active Directory—Information about using AWS Directory Service.

Bundles and images for WorkSpaces Pools

A *WorkSpace bundle* is a combination of an operating system, and storage, compute, and software resources. When you launch a WorkSpace, you select the bundle that meets your needs. The default bundles available for WorkSpaces are called *public bundles*. For more information about the various public bundles available for WorkSpaces, see Amazon WorkSpaces Bundles.

If you've launched a Windows WorkSpace and have customized it, you can create a custom image from that WorkSpace for use with WorkSpaces Pool. Linux are not supported in WorkSpaces Pool.

A *custom image* contains only the OS, software, and settings for the WorkSpace. A *custom bundle* is a combination of both that custom image and the hardware from which a WorkSpace can be launched.

After you create a custom image, you can build a custom bundle that combines the custom WorkSpace image and the underlying compute and storage configuration that you select. You can then specify this custom bundle when you create new WorkSpaces Pools to ensure that the new WorkSpaces in the pool have the same consistent configuration (hardware and software).

If you need to perform software updates or to install additional software on your WorkSpaces, you can update your custom bundle and use it to rebuild your WorkSpaces.

WorkSpaces Pools supports several different operating systems (OS), streaming protocols, and bundles. The following table provides information about the licensing, streaming protocols, and bundles that are supported by each OS.

Operating System	Licenses	Streaming protocols	Supported bundles	Lifecycle policy / retirement date
Windows Server 2019	Included	WSP	Value, Standard, Performance, Power, PowerPro	January 9, 2029
Windows Server 2022	Included	WSP	Standard, Performance, Power, PowerPro	October 14, 2031

Note

- Operating system versions that are no longer supported by the vender are not guaranteed to work and are not supported by AWS support.

Topics

- Bundle options for WorkSpaces Pools
- Create a custom image and bundle for WorkSpaces Pools
- Manage custom images and bundles for WorkSpaces Pools

- Use session scripts to manage your users' streaming experience

Bundle options for WorkSpaces Pools

Before selecting a bundle to use with WorkSpaces Pool, ensure the bundle you want to select is compatible with your WorkSpaces' protocol, operating system, network, and compute type. We recommend testing the performance of bundles you want to choose in a test environment by running and using applications that replicate your users' daily tasks. For more information about protocols, see Protocols for WorkSpaces Personal. For more information about networks, see Client network requirements for WorkSpaces Personal.

The following public bundles can be used with WorkSpaces Pool. For information about bundles in WorkSpaces, see Amazon WorkSpaces Bundles. Value, Standard, Performance, Power, PowerPro

Value bundle

This bundle is well-suited for the following:

- Basic text editing and data entry
- Web browsing with light usage
- Instant messaging

This bundle is not recommended for word processing, audio and video conferencing, screen sharing, software development tool, business intelligence applications, and graphics applications.

Standard bundle

This bundle is well-suited for the following:

- Basic text editing and data entry
- Web browsing
- Instant messaging
- Email

This bundle is not recommended for audio and video conferencing, screen sharing, word processing, software development tool, business intelligence applications, and graphics applications

Performance bundle

This bundle is well-suited for the following:

- Web browsing
- Word processing
- Instant messaging
- Email
- Spreadsheets
- Audio processing
- Courseware

This bundle is not recommended for video conferencing, screen sharing, software development tool, business intelligence applications, and graphics applications

Power bundle

This bundle is well-suited for the following:

- Web browsing
- Word processing
- Email
- Instant messaging
- Spreadsheets
- Audio processing
- Software development (Integrated Development Environment (IDE))
- Entry to mid-level data processing
- Audio and video conferencing

This bundle is not recommended for screen sharing, software development tool, business intelligence applications, and graphics applications.

PowerPro bundle

This bundle is well-suited for the following:

- Web browsing
- Word processing
- Email
- Instant messaging
- Spreadsheets
- Audio processing
- Software development (Integrated Development Environment (IDE))
- Data warehousing
- Business intelligence applications
- Audio and video conferencing

This bundle is not recommended for machine learning model training, and graphics applications

Create a custom image and bundle for WorkSpaces Pools

WorkSpaces Pool supports Windows images and bundles only. If you've launched a Windows or WorkSpace and have customized it, you can create a custom image and custom bundles from that WorkSpace.

A *custom image* contains only the OS, software, and settings for the WorkSpace. A *custom bundle* is a combination of both that custom image and the hardware from which a WorkSpace can be launched.

After you create a custom image, you can build a custom bundle that combines the custom image and the underlying compute and storage configuration that you select. You can then specify this custom bundle when you launch new WorkSpaces to ensure that the new WorkSpaces have the same consistent configuration (hardware and software).

You can use the same custom image to create various custom bundles by selecting different compute and storage options for each bundle.

Important

- Custom bundle storage volumes can't be smaller than image storage volumes.

Custom bundles cost the same as the public bundles they are created from. For more information about pricing, see Amazon WorkSpaces Pricing.

Contents

Requirements to create Windows custom images

> **Note**
>
> Windows currently defines 1 GB as 1,073,741,824 bytes. You must ensure they have greater than 12,884,901,888 bytes (or 12 GiB) free on C drive and the user profile is less than 10,737,418,240 bytes (or 10 GiB) to create an image of a WorkSpace.

- The status of the WorkSpace must be **Available** and its modification state must be **None**.
- All applications and user profiles on WorkSpaces images must be compatible with Microsoft Sysprep.
- All applications to include in the image must be installed on the C drive.
- All application services running on the WorkSpace must use a local system account instead of domain user credentials. For example, you cannot have a Microsoft SQL Server Express installation running with a domain user's credentials.
- The WorkSpace must not be encrypted. Image creation from an encrypted WorkSpace is not currently supported.
- The following components are required in an image. Without these components, the WorkSpaces that you launch from the image will not function correctly. For more information, see the section called “Required configuration”.
  - Windows PowerShell version 3.0 or later
  - Remote Desktop Services

- AWS PV drivers
- Windows Remote Management (WinRM)
- Teradici PCoIP agents and drivers
- STXHD agents and drivers
- AWS and WorkSpaces certificates
- Skylight agent

Best practices

Before you create an image from a WorkSpace, do the following:

- Use a separate VPC that is not connected to your production environment.
- Deploy the WorkSpace in a private subnet and use a NAT instance for outbound traffic.
- Use a small Simple AD directory.
- Use the smallest volume size for the source WorkSpace, and then adjust the volume size as needed when creating the custom bundle.
- Install all operating system updates (except Windows feature/version updates) and all application updates on the WorkSpace.
- Delete cached data from the WorkSpace that shouldn't be included in the bundle (for example, browser history, cached files, and browser cookies).
- Delete configuration settings from the WorkSpace that shouldn't be included in the bundle (for example, email profiles).
- Switch to dynamic IP address settings using DHCP.
- Make sure that you haven't exceeded your quota for WorkSpace images allowed in a Region. By default, you're allowed 40 WorkSpace images per Region. If you've reached this quota, new attempts to create an image will fail. To request a quota increase, use the WorkSpaces Limits form.
- Make sure that you aren't trying to create an image from an encrypted WorkSpace. Image creation from an encrypted WorkSpace is not currently supported.
- If you're running any antivirus software on the WorkSpace, disable it while you're attempting to create an image.
- If you have a firewall enabled on your WorkSpace, make sure that it isn't blocking any necessary ports. For more information, see IP address and port requirements for WorkSpaces Personal.

- For Windows WorkSpaces, don't configure any Group Policy Objects (GPOs) before image creation.
- For Windows WorkSpaces, do not customize the default user profile (`C:\Users\Default`) before creating an image. We recommend making any customizations to the user profile through GPOs, and applying them after image creation. GPOs can be easily modified or rolled back, and are therefore less prone to error than customizations made to the default user profile.
- Ensure you update networking dependency drivers like ENA, NVMe, and PV drivers on your WorkSpaces. You should do this at least once every 6 months. For more information, see Install or upgrade Elastic Network Adapter (ENA) driver , AWS NVMe drivers for Windows instances, and Upgrade PV drivers on Windows instances.
- Ensure you update the EC2Config, EC2Launch, and EC2Launch V2 agents to the latest versions periodically. You should do this at least once every 6 months. For more information, see Update EC2Config and EC2Launch.

(Optional) Step 1: Specify a custom computer name format for your image

For the WorkSpaces launched from your custom images, you can specify a custom prefix for the computer name format instead of using the default computer name format. By default, the format of the computer name for Windows 10 WorkSpaces is `DESKTOP-XXXXX` and for Windows 11 WorkSpaces, `WORKSPA-XXXXX`. Complete the following procedure to specify a custom prefix.

1. On the WorkSpace that you're using to create your custom image, open `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml` in Notepad or another text editor. For more information about working with the `Unattend.xml` file, see Answer files (unattend.xml) in the Microsoft documentation.

   To access the `C:` drive from the Windows File Explorer on your WorkSpace, enter `C:\` in the address bar.
2. In the `<settings pass="specialize">` section, make sure that `<ComputerName>` is set to an asterisk (`*`). If `<ComputerName>` is set to any other value, your custom computer name settings will be ignored. For more information about the `<ComputerName>` setting, see ComputerName in the Microsoft documentation.
3. In the `<settings pass="specialize">` section, set `<RegisteredOrganization>` and `<RegisteredOwner>` to your preferred values.

During Sysprep, the values that you specify for `<RegisteredOwner>` and `<RegisteredOrganization>` are concatenated together, and the first 7 characters of the combined string are used to create the computer name. For example, if you specify `Amazon.com` for `<RegisteredOrganization>` and **EC2** for `<RegisteredOwner>`, the computer names for the WorkSpaces created from your custom bundle will start with `EC2AMAZ-`*`xxxxxxx`*.

The `<RegisteredOrganization>` and `<RegisteredOwner>` values in the `<settings pass="oobeSystem">` section are ignored by Sysprep.

4. Save your changes to the `Unattend.xml` file.

Step 2: Run the Image Checker

To confirm that your Windows WorkSpace meets the requirements for image creation, we recommend running the Image Checker application. The Image Checker performs a series of tests on the WorkSpace that you want to use to create your image, and provides guidance on how to resolve any issues it finds. The Image Checker is available only for Windows WorkSpaces.

Important

- The WorkSpace must pass all of the tests run by the Image Checker before you can use it for image creation.
- Before you run the Image Checker, verify that the latest Windows security and cumulative updates are installed on your WorkSpace.

To get the Image Checker, do one of the following:

- Reboot your WorkSpace. The Image Checker is downloaded automatically during the reboot and installed at `C:\Program Files\Amazon\ImageChecker.exe`.
- Download the Amazon WorkSpaces Image Checker from https://tools.amazonworkspaces.com/ImageChecker.zip and extract the `ImageChecker.exe` file. Copy this file to `C:\Program Files\Amazon\`.

To run the Image Checker

1. Open the `C:\Program Files\Amazon\ImageChecker.exe` file.
2. In the **Amazon WorkSpaces Image Checker** dialog box, choose **Run**.
3. After each test is completed, you can view the status of the test.

   For any test with a status of **FAILED**, choose **Info** to display information about how to resolve the issue that caused the failure. For more information about how to resolve these issues, see Tips for resolving issues detected by the Image Checker.

   If any tests display a status of **WARNING**, choose the **Fix All Warnings** button.

   The tool generates an output log file in the same directory where the Image Checker is located. By default, this file is located at `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`. Don't delete this log file. If an issue occurs, this log file might be helpful in troubleshooting.
4. If applicable, resolve any issues that cause test failures and warnings, and repeat the process of running the Image Checker until the WorkSpace passes all tests. All failures and warnings must be resolved before you can create an image.
5. After your WorkSpace passes all tests, you see a **Validation Successful** message. You are now ready to create a custom bundle.

Tips for resolving issues detected by the Image Checker

In addition to consulting the following tips for resolving issues that are detected by the Image Checker, be sure to review the Image Checker log file at `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`.

PowerShell version 3.0 or later must be installed

Install the latest version of Microsoft Windows PowerShell.

> **Important**
>
> The PowerShell execution policy for a WorkSpace must be set to allow **RemoteSigned** scripts. To check the execution policy, run the **Get-ExecutionPolicy** PowerShell command. If the execution policy is not set to **Unrestricted** or **RemoteSigned**, run the **Set-ExecutionPolicy –ExecutionPolicy RemoteSigned** command to change the value of the

execution policy. The **RemoteSigned** setting allows the execution of scripts on Amazon WorkSpaces, which is required to create an image.

Only the C and D drives can be present

Only the C and D drives can be present on a WorkSpace that's used for imaging. Remove all other drives, including virtual drives.

No pending reboot due to Windows Updates can be detected

- The Create Image process can't run until Windows is rebooted to finish installing security or cumulative updates. Reboot Windows to apply these updates, and make sure that no other pending Windows security or cumulative updates need to be installed.
- Image creation is not supported on Windows 10 systems that have been upgraded from one version of Windows 10 to a newer version of Windows 10 (a Windows feature/version upgrade). However, Windows cumulative or security updates are supported by the WorkSpaces image-creation process.

The Sysprep file must exist and can't be blank

If there are problems with your Sysprep file, contact the AWS Support Center to get your EC2Config or EC2Launch repaired.

The user profile size must be less than 10 GB

For Windows 7 WorkSpaces, the user profile (`D:\Users\`*`username`*) must be less than 10 GB total. Remove files as needed to reduce the size of the user profile.

Drive C must have enough free space

For Windows 7 WorkSpaces, you must have at least 12 GB of free space on drive C. Remove files as needed to free up space on drive C. For Windows 10 WorkSpaces, ignore if you receive a `FAILED` message and the disk space is above 2GB.

No services can be running under a domain account

To run the Create Image process, no services on the WorkSpace can be running under a domain account. All services must be running under a local account.

To run services under a local account

1. Open `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log` and find the list of services that are running under a domain account.
2. In the Windows search box, enter **`services.msc`** to open the Windows Services Manager.
3. Under **Log On As**, look for the services that are running under domain accounts. (Services running as **Local System**, **Local Service**, or **Network Service** do not interfere with image creation.)
4. Select a service that is running under a domain account, and then choose **Action**, **Properties**.
5. Open the **Log On** tab. Under **Log on as**, choose **Local System account**.
6. Choose **OK**.

The WorkSpace must be configured to use DHCP

You must configure all network adapters on the WorkSpace to use DHCP instead of static IP addresses.

To set all network adapters to use DHCP

1. In the Windows search box, enter **`control panel`** to open the Control Panel.
2. Choose **Network and Internet**.
3. Choose **Network and Sharing Center**.
4. Choose **Change adapter settings**, and select an adapter.
5. Choose **Change settings of this connection**.
6. On the **Networking** tab, select **Internet Protocol Version 4 (TCP/IPv4)**, and then choose **Properties**.
7. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select **Obtain an IP address automatically**.
8. Choose **OK**.
9. Repeat this process for all network adapters on the WorkSpace.

Remote Desktop Services must be enabled

The Create Image process requires Remote Desktop Services to be enabled.

To enable Remote Desktop Services

1. In the Windows search box, enter **`services.msc`** to open the Windows Services Manager.
2. In the **Name** column, find **Remote Desktop Services**.
3. Select **Remote Desktop Services**, and then choose **Action**, **Properties**.
4. On the **General** tab, for **Startup type**, choose **Manual** or **Automatic**.
5. Choose **OK**.

A user profile must exist

The WorkSpace that you're using to create images must have a user profile (`D:\Users\`*`username`*). If this test fails, contact the AWS Support Center for assistance.

The environment variable path must be properly configured

The environment variable path for the local machine is missing entries for System32 and for Windows PowerShell. These entries are required for Create Image to run.

To configure your environment variable path

1. In the Windows search box, enter **`environment variables`** and then choose **Edit the system environment variables**.
2. In the **System Properties** dialog box, open the **Advanced** tab, and choose **Environment Variables**.
3. In the **Environment Variables** dialog box, under **System variables**, select the **Path** entry and then choose **Edit**.
4. Choose **New**, and add the following path:

   ```
   C:\Windows\System32
   ```

5. Choose **New** again, and add the following path:

   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\
   ```

6. Choose **OK**.
7. Restart the WorkSpace.

> **Tip**
>
> The order in which items appear in the environment variable path matters. To determine the correct order, you might want to compare the environment variable path of your WorkSpace with one from a newly created WorkSpace or a new Windows instance.

Windows Modules Installer must be enabled

The Create Image process requires the Windows Modules Installer service to be enabled.

To enable the Windows Modules Installer service

1. In the Windows search box, enter **`services.msc`** to open the Windows Services Manager.
2. In the **Name** column, find **Windows Modules Installer**.
3. Select **Windows Modules Installer**, and then choose **Action**, **Properties**.
4. On the **General** tab, for **Startup type**, choose **Manual** or **Automatic**.
5. Choose **OK**.

Amazon SSM Agent must be disabled

The Create Image process requires the Amazon SSM Agent service to be disabled.

To disable the Amazon SSM Agent service

1. In the Windows search box, enter **`services.msc`** to open the Windows Services Manager.
2. In the **Name** column, find **Amazon SSM Agent**.
3. Select **Amazon SSM Agent**, and then choose **Action**, **Properties**.
4. On the **General** tab, for **Startup type**, choose **Disabled**.
5. Choose **OK**.

SSL3 and TLS version 1.2 must be enabled

To configure SSL/TLS for Windows, see How to Enable TLS 1.2 in the Microsoft Windows documentation.

Only one user profile can exist on the WorkSpace

There can be only one WorkSpaces user profile (`D:\Users\`*`username`*) on the WorkSpace that you're using to create images. Delete any user profiles that don't belong to the intended user of the WorkSpace.

For image creation to work, your WorkSpace can have only three user profiles on it:

- The user profile of the intended user of the WorkSpace (`D:\Users\`*`username`*)
- The default user profile (also known as Default Profile)
- The Administrator user profile

If there are additional user profiles, you can delete them through the advanced system properties in the Windows Control Panel.

To delete a user profile

1. To access the advanced system properties, do one of the following:
   - Press the **Windows key+Pause Break**, and then choose **Advanced system settings** in the left pane of the **Control Panel** > **System and Security** > **System** dialog box.
   - In the Windows search box, enter **`control panel`**. In the Control Panel, choose **System and Security**, then choose System, and then choose **Advanced system settings** in the left pane of the **Control Panel** > **System and Security** > **System** dialog box.
2. In the **System Properties** dialog box, on the **Advanced** tab, choose **Settings** under **User Profiles**.
3. If any profile is listed other than the Administrator profile, the Default Profile, and the profile of the intended WorkSpaces user, select that additional profile and choose **Delete**.
4. When asked if you want to delete the profile, choose **Yes**.
5. If necessary, repeat Steps 3 and 4 to remove any other profiles that don't belong on the WorkSpace.
6. Choose **OK** twice and close the Control Panel.
7. Restart the WorkSpace.

No AppX packages can be in a staged state

One or more AppX packages are in a staged state. This might cause a Sysprep error during image creation.

To remove all staged AppX packages

1. In the Windows search box, enter **`powershell`**. Choose **Run as Administrator**.
2. When asked "Do you want to allow this app to make changes to your device?", choose **Yes**.
3. In the Windows PowerShell window, enter the following commands to list all staged AppX packages, and press Enter after each one.

```
$workSpaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages |    Where-Object { `
                                 (($_.PackageUserInformation -like "*S-1-5-18*" -
and !($_.PackageUserInformation -like "*$workSpaceUserName*")) -and `
                                 ($_.PackageUserInformation -like "*Staged*" -or
 $_.PackageUserInformation -like "*Installed*")) -or `
                                 ((!($_.PackageUserInformation -like "*S-1-5-18*") -
and $_.PackageUserInformation -like "*$workSpaceUserName*") -and `
                                 $_.PackageUserInformation -like "*Staged*")
                                 }
```

4. Enter the following command to remove all staged AppX packages, and press Enter.

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. Run the Image Checker again. If this test still fails, enter the following commands to remove all AppX packages, and press Enter after each one.

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

Windows must not have been upgraded from a previous version

Image creation is not supported on Windows systems that have been upgraded from one version of Windows 10 to a newer version of Windows 10 (a Windows feature/version upgrade).

To create images, use a WorkSpace that has not undergone a Windows feature/version upgrade.

The Windows rearm count must not be 0

The rearm feature allows you to extend the activation period for the trial version of Windows. The Create Image process requires that the rearm count be a value other than 0.

To check the Windows rearm count

1. On the Windows **Start** menu, choose **Windows System**, then choose **Command Prompt**.
2. In the Command Prompt window, enter the following command, and then press Enter.

   ```
   cscript C:\Windows\System32\slmgr.vbs /dlv
   ```

To reset the rearm count to a value other than 0, see Sysprep (Generalize) a Windows installation in the Microsoft Windows documentation.

Other troubleshooting tips

If your WorkSpace passes all of the tests run by the Image Checker, but you are still unable to create an image from the WorkSpace, check for the following issues:

- Make sure that the WorkSpace isn't assigned to a user within a **Domain Guests** group. To check if there are any domain accounts, run the following PowerShell command.

  ```
  Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*
  $env:USERDOMAIN*" }
  ```

- Some Group Policy Objects (GPOs) restrict access to the RDP certificate thumbprint when it is requested by the EC2Config service or the EC2Launch scripts during Windows instance configuration. Before you try to create an image, move the WorkSpace to a new organizational unit (OU) with blocked inheritance and no GPOs applied.
- Make sure that the Windows Remote Management (WinRM) service is configured to start automatically. Do the following:

  1. In the Windows search box, enter `services.msc` to open the Windows Services Manager.

2. In the **Name** column, find **Windows Remote Management (WS-Management)**.
3. Select **Windows Remote Management (WS-Management)**, and then choose **Action**, **Properties**.
4. On the **General** tab, for **Startup type**, choose **Automatic**.
5. Choose **OK**.

Step 3: Create a custom image and custom bundle

After you have validated your WorkSpace image, complete the following procedure to create your custom image and custom bundle using the WorkSpaces console. To create an image programmatically, use the CreateWorkspaceImage API action. For more information, see CreateWorkspaceImage in the *Amazon WorkSpaces API Reference*. To create a bundle programmatically, use the **CreateWorkspaceBundle** API action. For more information, see CreateWorkspaceBundle in the *Amazon WorkSpaces API Reference*.

To create a custom image and custom bundle using the WorkSpaces console

1. If you are still connected to the WorkSpace, disconnect by choosing **Amazon WorkSpaces** and **Disconnect** in the WorkSpaces client application.
2. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
3. In the navigation pane, choose **WorkSpaces**.
4. Select the WorkSpace to open its details page and choose **Create image**. If the status of the WorkSpace is **Stopped**, you must start it first (choose **Actions**, **Start WorkSpaces**) before you can choose **Actions**, **Create Image**.
5. A message displays, prompting you to reboot (restart) your WorkSpace before continuing. Rebooting your WorkSpace updates your Amazon WorkSpaces software to the latest version.

   Reboot your WorkSpace by closing the message and following the steps in Reboot a WorkSpace in WorkSpaces Personal. When you're done, repeat Step 4 of this procedure, but this time choose **Next** when the reboot message appears. To create an image, the status of the WorkSpace must be **Available** and its modification state must be **None**.
6. Enter an image name and a description that will help you identify the image, and then choose **Create Image**. While the image is being created, the status of the WorkSpace is **Suspended** and the WorkSpace is unavailable.

   Don't use a dash (-) special character in the description. It will cause an error.

7. In the navigation pane, choose **Images**. The image is complete when the status of the WorkSpace changes to **Available** (this can take up to 45 minutes).
8. Select the image and choose **Actions**, **Create bundle**.
9. Enter a bundle name and a description, and then do the following:

   - For **Bundle hardware type**, choose the hardware to use when launching WorkSpaces from this custom bundle.
   - For **Storage settings**, select one of the default combinations for the root volume and user volume size, or select **Custom**, and then enter values (up to 2000 GB) for **Root volume size** and **User volume size**.

     The default available size combinations for the root volume (for Microsoft Windows, the C drive, for Linux, /) and the user volume (for Windows, the D drive; for Linux, /home) are as follows:

     - Root: 80 GB, User: 10 GB, 50 GB, or 100 GB
     - Root: 175 GB, User: 100 GB
     - For Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro WorkSpaces only: Root: 100 GB, User: 100 GB

     Alternatively, you can expand the root and user volumes up to 2000 GB each.

     > **Note**
     >
     > To ensure that your data is preserved, you cannot decrease the size of the root or user volumes after you launch a WorkSpace. Instead, make sure that you specify the minimum sizes for these volumes when launching a WorkSpace. You can launch a Value, Standard, Performance, Power, or PowerPro WorkSpace with a minimum of 80 GB for the root volume and 10 GB for the user volume. You can launch a Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro WorkSpace with a minimum of 100 GB for the root volume and 100 GB for the user volume.

10. Choose **Create bundle**.
11. To confirm that your bundle has been created, choose **Bundles** and verify that the bundle is listed.

What's included with Windows WorkSpaces custom images

When you create an image from a Windows WorkSpace, the entire contents of the C drive are included.

- Contacts
- Downloads
- Music
- Pictures
- Saved games
- Videos
- Podcasts
- Virtual machines
- .virtualbox
- Tracing
- appdata\local\temp
- appdata\roaming\apple computer\mobilesync\
- appdata\roaming\apple computer\logs\
- appdata\roaming\apple computer\itunes\iphone software updates\
- appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\
- appdata\roaming\macromedia\flash player\#sharedobjects\
- appdata\roaming\adobe\flash player\assetcache\
- appdata\roaming\microsoft\windows\recent\
- appdata\roaming\microsoft\office\recent\
- appdata\roaming\microsoft office\live meeting
- appdata\roaming\microsoft shared\livemeeting shared\
- appdata\roaming\mozilla\firefox\crash reports\
- appdata\roaming\mcafee\common framework\
- appdata\local\microsoft\feeds cache
- appdata\local\microsoft\windows\temporary internet files\

- appdata\local\microsoft\windows\history\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\locallow\microsoft\internet explorer\iconcache\
- appdata\locallow\microsoft\internet explorer\domstore\
- appdata\locallow\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\recovery\
- appdata\local\mozilla\firefox\profiles\

Manage custom images and bundles for WorkSpaces Pools

The process to manage custom images and bundles is the same between WorkSpaces Personal and WorkSpaces Pool. For more information about how to manage images and bundles, refer to the following documentation within the WorkSpaces Personal section of this guide:

Note

The primary difference between custom bundles that you can use for WorkSpaces Personal and ones that you can use for WorkSpaces Pool is the operating system and base public bundle that can be used. For the operating systems and bundles that are supported in WorkSpaces Pool, see

A *WorkSpace bundle* is a combination of an operating system, and storage, compute, and software resources. When you launch a WorkSpace, you select the bundle that meets your needs. The default bundles available for WorkSpaces are called *public bundles*. For more information about the various public bundles available for WorkSpaces, see Amazon WorkSpaces Bundles.

The following table provides information about the licensing, streaming protocols, and bundles that are supported by each OS.

Windows Server 2019	Included	WSP	Value, Standard, Performance, Power, PowerPro

Windows Server 2022	Included	WSP	Standard, Performance, Power, PowerPro

Operating System	Licenses	Streaming protocols	Supported bundles

Note

- Operating system versions that are no longer supported by the vender are not guaranteed to work and are not supported by AWS support.

.

- Update a custom bundle for WorkSpaces Personal.
- Copy a custom image in WorkSpaces Personal.
- Share or unshare a custom image in WorkSpaces Personal.
- Delete a custom bundle or image in WorkSpaces Personal.

Use session scripts to manage your users' streaming experience

WorkSpaces Pool provides on-instance session scripts. You can use these scripts to run your own custom scripts when specific events occur in users' streaming sessions. For example, you can use custom scripts to prepare your WorkSpaces Pools environment before your users' streaming sessions begin. You can also use custom scripts to clean up streaming instances after users complete their streaming sessions.

Session scripts are specified within a WorkSpace image. These scripts are run within the user context or the system context. If your session scripts use the standard out to write information, error, or debugging messaging, these can be optionally saved to an Amazon S3 bucket within your Amazon Web Services account.

Contents

- Run Scripts After Streaming Sessions End
- Create and Specify Session Scripts
- Session Scripts Configuration File
- Using Windows PowerShell Files
- Logging Session Script Output
- Use persistent storage with session scripts
- Enable Amazon S3 Bucket Storage for Session Script Logs

Run Scripts Before Streaming Sessions Begin

You can configure your scripts to run for a maximum of 60 seconds before your users' applications launch and their streaming sessions begin. Doing so enables you to customize the WorkSpaces Pools environment before users start streaming their applications. When the session scripts run, a loading spinner displays for your users. When your scripts complete successfully or the maximum waiting time elapses, your users' streaming session will begin. If your scripts don't complete successfully, an error message displays for your users. However, your users are not prevented from using their streaming session.

When you specify a file name on a Windows instance, you must use a double backslash. For example:

```
C:\\Scripts\\Myscript.bat
```

If you don't use a double backslash, an error displays to notify you that the `.json` file is incorrectly formatted.

> **Note**
>
> When your scripts complete successfully, they must return a value of 0. If your scripts return a value other than 0, WorkSpaces displays the error message to the user.

When you run scripts before streaming sessions begin, the following process occurs:

1. Your users connect to a WorkSpace in a WorkSpaces Pool that is not domain-joined. They connect by using SAML 2.0.

2. One of the following occurs:
   - If application settings persistence is enabled for your users, the application settings Virtual Hard Disk (VHD) file that stores your users' customizations and Windows settings is downloaded and mounted. Windows user login is required in this case.

     For information about application settings persistence, see Enable application settings persistence for your WorkSpaces Pools users.
   - If application settings persistence is not enabled, the Windows user is already logged in.
3. Your session scripts start. If persistent storage is enabled for your users, storage connector mounting also starts. For information about persistent storage, see Enable and Administer Persistent Storage for WorkSpaces Pools.

   > **Note**
   >
   > The storage connector mount doesn't need to complete for the streaming session to start. If the session scripts complete before the storage connector mount completes, the streaming session starts.
   > For information about monitoring the mount status of storage connectors, see Use persistent storage with session scripts.
4. Your session scripts complete or time out.
5. The users' streaming session starts.

Run Scripts After Streaming Sessions End

You can also configure your scripts to run after users' streaming sessions end. For example, you can run a script when users select **End Session** from the WorkSpaces client toolbar, or when they reach the maximum allowed duration for the session. You can also use these session scripts to clean up your WorkSpaces environment before a streaming instance is terminated. For example, you can use scripts to release file locks or upload log files. When you run scripts after streaming sessions end, the following process occurs:

1. Your users' WorkSpaces streaming session ends.
2. Your session termination scripts start.
3. The session termination scripts complete or time out.
4. Windows user logout occurs.

5. One or both of the following occur in parallel, if applicable:
   - If application settings persistence is enabled for your users, the application settings VHD file that stores your users' customizations and Windows settings is unmounted and uploaded to an Amazon S3 bucket in your account.
   - If persistent storage is enabled for your users, the storage connector completes a final synchronization and is unmounted.
6. The WorkSpace is terminated.

Create and Specify Session Scripts

Complete the following procedure to create and specify session scripts for your WorkSpaces in a WorkSpaces Pool.

1. Connect to the Windows WorkSpace from which you are creating a custom image.
2. Navigate to `C:\AWSEUC\SessionScripts`, and open the `config.json` configuration file.

   For information about session script parameters, see Session Scripts Configuration File.
3. After you finish making your changes, save and close the `config.json` file.
4. Complete the steps to create an image from the WorkSpace. For more information, see Create a custom image and bundle for WorkSpaces Pools.

Session Scripts Configuration File

To locate the session scripts configuration file in a Windows instance, navigate to `C:\AWSEUC\SessionScripts\config.json`. The file is formatted as follows.

> **Note**
>
> The configuration file is in JSON format. Verify that any text you type in this file is in valid JSON format.

```
{
  "SessionStart": {
    "executables": [
      {
```

```
        "context": "system",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      },
      {
        "context": "user",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      }
    ],
    "waitingTime": 30
  },
  "SessionTermination": {
    "executables": [
      {
        "context": "system",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      },
      {
        "context": "user",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      }
    ],
    "waitingTime": 30
  }
}
```

You can use the following parameters in the session scripts configuration file.

`SessionStart/SessionTermination`

The session scripts to run in the appropriate session event based on the name of the object.

Type: String

Required: No

Allowed values: `SessionStart`, `SessionTermination`

`WaitingTime`

The maximum duration of the session scripts in seconds.

Type: Integer

Required: No

Constraints: The maximum duration is 60 seconds. If the session scripts don't complete within this duration, they will be stopped. If you require a script to continue running, launch it as a separate process.

`Executables`

The details for the session scripts to run.

Type: String

Required: Yes

Constraints: The maximum number of scripts that can run per session event is 2 (one for the user context, one for the system context).

`Context`

The context in which to run the session script.

Type: String

Required: Yes

Allowed values: `user`, `system`

`Filename`

The full path to the session script to run. If this parameter is not specified, the session script is not run.

Type: String

Required: No

Constraints: The maximum length for the file name and full path is 1,000 characters.

Allowed values: `.bat`, `.exe`, `.sh`

> **Note**
>
> You can also use Windows PowerShell files. For more information, see Using Windows PowerShell Files.

`Arguments`

The arguments for your session script or executable file.

Type: String

Required: No

Length constraints: The maximum length is 1,000 characters.

`S3LogEnabled`

When the value for this parameter is set to **`True`**, an S3 bucket is created within your Amazon Web Services account to store the logs created by the session script. By default, this value is set to **`True`**. For more information, see the *Logging Session Script Output* section later in this topic.

Type: Boolean

Required: No

Allowed values: `True`, `False`

Using Windows PowerShell Files

To use Windows PowerShell files, specify the full path to the PowerShell file in the `filename` parameter:

```
"filename":
"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
```

Then specify your session script in the **`arguments`** parameter:

```
"arguments": "-File \"C:\\path\\to\\session\\script.ps1\"",
```

Finally, verify that the PowerShell Execution Policy allows your PowerShell file to run.

Logging Session Script Output

When this option is enabled in the configuration file, WorkSpaces Pool automatically captures the output from the session script that is written to the standard out. This output is uploaded to an Amazon S3 bucket in your account. You can review the log files for troubleshooting or debugging purposes.

> **Note**
>
> The log files are uploaded when the session script returns a value, or the value set in **`WaitingTime`** has elapsed, whichever comes first.

Use persistent storage with session scripts

When WorkSpaces persistent storage is enabled, the storage begins mounting when the session start scripts run. If your script relies on persistent storage being mounted, you can wait for the connectors to be available. WorkSpaces maintains the mount status of the storage connectors in the Windows registry on Windows WorkSpaces, at the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\AppStream\Storage\<provided user
               name>\<Storage connector>
```

The registry key values are as follows:

- Provided user name — The user ID provided through the access mode. The access modes and value for each mode are as follows:
  - User Pool — The email address for the user
  - Streaming URL — The UserID
  - SAML — The NameID. If the user name includes a slash (for example, a domain user's SAMAccountName), the slash is replaced by a "-" character.
- Storage connector — The connector for the persistent storage option that is enabled for the user. The storage connector values are as follows:

- HomeFolder

Each storage connector registry key contains a **MountStatus** DWORD value. The following table lists the possible values for **MountStatus**.

> **Note**
>
> To view these registry keys, you must have Microsoft .NET Framework version 4.7.2 or later installed on your image.

Value	Description
0	Storage connector not be enabled for this user
1	Storage connector mounting is in progress
2	Storage connector mounted successfully
3	Storage connector mounting failed
4	Storage connector mounting is enabled, but not mounted yet

Enable Amazon S3 Bucket Storage for Session Script Logs

When you enable Amazon S3 logging in your session script configuration, WorkSpaces Pool captures standard output from your session script. The output is periodically uploaded to an S3 bucket within your Amazon Web Services account. For every AWS Region, WorkSpaces Pool creates a bucket in your account that is unique to your account and the Region.

You do not need to perform any configuration tasks to manage these S3 buckets. They are fully managed by the WorkSpaces service. The log files that are stored in each bucket are encrypted in transit using Amazon S3's SSL endpoints and at rest using Amazon S3-managed encryption keys. The buckets are named in a specific format as follows:

```
wspool-logs-<region-code>-<account-id-without-hyphens>-random-identifier
```

<region-code>

This is the AWS Region code in which the WorkSpaces Pool is created with Amazon S3 bucket storage enabled for session script logs.

<account-id-without-hyphens>

Your Amazon Web Services account identifier. The random ID ensures that there is no conflict with other buckets in that Region. The first part of the bucket name, `appstream-logs`, does not change across accounts or Regions.

For example, if you specify session scripts in an image in the US West (Oregon) Region (`us-west-2`) on account number `123456789012`, WorkSpaces Pool creates an Amazon S3 bucket within your account in that Region with the name shown. Only an administrator with sufficient permissions can delete this bucket.

```
wspool-logs-us-west-2-1234567890123-abcdefg
```

Disabling session scripts does not delete log files stored in the S3 bucket. To permanently delete log files, you or another administrator with adequate permissions must do so by using the Amazon S3 console or API. WorkSpaces Pools adds a bucket policy that prevents accidental deletion of the bucket.

When session scripts are enabled, a unique folder is created for each streaming session that is started.

The path for the folder where the log files are stored in the S3 bucket in your account uses the following structure:

```
<bucket-name>/<stack-name>/<fleet-name>/<access-mode>/<user-id-SHA-256-hash>/<session-id>/SessionScriptsLogs/<session-event>
```

<bucket-name>

The name of the S3 bucket in which the session scripts are stored. The name format is described earlier in this section.

<stack-name>

The name of the stack the session came from.

<fleet-name>

The name of the WorkSpaces Pool the session script is running on.

<access-mode>

The identity method of the user: `custom` for the WorkSpaces API or CLI, `federated` for SAML, and `userpool` for users in the user pool.

<user-id-SHA-256-hash>

The user-specific folder name. This name is created using a lowercase SHA-256 hash hexadecimal string generated from the user identifier.

<session-id>

The identifier of the user's streaming session. Each user streaming session generates a unique ID.

<session-event>

The event that generated the session script log. The event values are: `SessionStart` and `SessionTermination`.

The following example folder structure applies to a streaming session started from the test-stack and test-fleet. The session uses the API of user ID `testuser@mydomain.com`, from an AWS account ID of `123456789012`, and the settings group `test-stack` in the US West (Oregon) Region (`us-west-2`):

```
wspool-logs-us-west-2-1234567890123-abcdefg/test-stack/test-fleet/custom/
a0bcb1da11f480d9b5b3e90f91243143eac04cfccfbdc777e740fab628a1cd13/05yd1391-4805-3da6-
f498-76f5x6746016/SessionScriptsLogs/SessionStart/
```

This example folder structure contains one log file for a user context session start script, and one log file for a system context session start script, if applicable.

Monitoring WorkSpaces Pools

Monitoring is an important part of maintaining the reliability, availability, and performance of your WorkSpaces Pools.

Contents

WorkSpaces Pools metrics and dimensions

Amazon WorkSpaces sends the following WorkSpaces Pools metrics and dimension information to Amazon CloudWatch.

WorkSpaces Pools sends metrics to CloudWatch one time every minute. The `AWS/Workspaces` namespace includes the following metrics.

Pools usage metrics

Metric	Description
`ActiveUserSessionCapacity`	The number of user sessions currently being used for streaming sessions. Units: Count Valid statistics: Average, Minimum, Maximum
`ActualUserSessionCapacity`	The total number of pool sessions that are available for streaming or are currently streaming. `ActualUserSessionCapacity = AvailableUserSessionCapacity + ActiveUserSessionCapacity` Units: Count Valid statistics: Average, Minimum, Maximum
`AvailableUserSessionCapacity`	The number of idle pool sessions currently available for user streaming. `AvailableUserSessionCapacity = ActualUserSessionCapacity - ActiveUserSessionCapacity` Units: Count Valid statistics: Average, Minimum, Maximum

Metric	Description
PendingUserSessionCapacity	The number of sessions being provisioned for your pool. Represents the additional number of streaming sessions the pool can support after provisioning is complete. Units: Count Valid statistics: Average, Minimum, Maximum
UserSessionsCapacityUtilization	The percentage of sessions in a pool that are being used, using the following formula. `UserSessionCapacityUtilization = (ActiveUserSessionCapacity / ActualUserSessionCapacity) * 100` Monitoring this metric helps with decisions about increasing or decreasing the value of a pool's desired capacity. Units: Percent Valid statistics: Average, Minimum, Maximum
DesiredUserSessionCapacity	The total number of sessions that are either running or pending. This represents the total number of concurrent streaming sessions your pool can support in a steady state. `DesiredUserSessionCapacity = ActualUserSessionCapacity + PendingUserSessionCapacity` Units: Count Valid statistics: Average, Minimum, Maximum

Metric	Description
`InsufficientCapacityError`	The number of session requests rejected due to lack of capacity. You can set alarms to use this metric to be notified of users waiting for streaming sessions. Units: Count Valid statistics: Average, Minimum, Maximum, Sum

Enable and Administer Persistent Storage for WorkSpaces Pools

WorkSpaces Pools supports home folders for persistent storage. As a WorkSpaces Pools administrator, you must understand how to perform the following tasks to enable and administer persistent storage for your users.

Contents

Enable and Administer Home Folders for Your WorkSpaces Pools Users

When you enable home folders for WorkSpaces Pools, users can access a persistent storage folder during their streaming sessions. No further configuration is required for your users to access their home folder. Data stored by users in their home folder is automatically backed up to an Amazon Simple Storage Service bucket in your Amazon Web Services account and is made available to those users in subsequent sessions.

Files and folders are encrypted in transit using Amazon S3's SSL endpoints. Files and folders are encrypted at rest using Amazon S3-managed encryption keys.

Home folders are stored on WorkSpaces in WorkSpaces Pools in the following default locations:

- For single-session, non-domain-joined Windows WorkSpaces: `C:\Users\PhotonUser\My Files\Home Folder`
- Domain-joined Windows WorkSpaces: `C:\Users\%username%\My Files\Home Folder`

As an administrator, use the applicable path if you configure your applications to save to the home folder. In some cases, your users may not be able to find their home folder because some applications do not recognize the redirect that displays the home folder as a top-level folder in File Explorer. If this is the case, your users can access their home folder by browsing to the same directory in File Explorer.

Contents

Files and Directories Associated with Compute-Intensive Applications

During WorkSpaces Pools streaming sessions, saving large files and directories associated with compute-intensive applications to persistent storage can take longer than saving files and directories required for basic productivity applications. For example, it might take longer for applications to save a large amount of data or frequently modify the same files than it would to save files created by applications that perform a single write action. It might also take longer to save many small files.

If your users save files and directories associated with compute-intensive applications and WorkSpaces Pools persistent storage options aren't performing as expected, we recommend that you use a Server Message Block (SMB) solution such as Amazon FSx for Windows File Server or an AWS Storage Gateway file gateway. Following are examples of files and directories associated with compute-intensive applications that are more suitable for use with these SMB solutions:

- Workspace folders for integrated development environments (IDEs)
- Local database files
- Scratch space folders created by graphics simulation applications

For more information, see File gateways in the *AWS Storage Gateway User Guide*.

Enable Home Folders for Your WorkSpaces Pools Users

Before enabling home folders, you must do the following:

- Check that you have the correct AWS Identity and Access Management (IAM) permissions for Amazon S3 actions.
- Use an image that was created from an AWS base image released on or after May 18, 2017.
- Enable network connectivity to Amazon S3 from your virtual private cloud (VPC) by configuring internet access or a VPC endpoint for Amazon S3. For more information, see Networking and Access for WorkSpaces Pools and Using Amazon S3 VPC Endpoints for WorkSpaces Pools Features.

You can enable or disable home folders while creating a directory (see Configure SAML 2.0 and create a WorkSpaces Pools directory), or after the directory is created by using the AWS Management Console for WorkSpaces Pools. For each AWS Region, home folders are backed up by an Amazon S3 bucket.

The first time you enable home folders for an WorkSpaces Pools directory in an AWS Region, the service creates an Amazon S3 bucket in your account in that same Region. The same bucket is used to store the content of home folders for all users and all directories in that Region. For more information, see Amazon S3 Bucket Storage.

To enable home folders while creating a directory

- Follow the steps in Configure SAML 2.0 and create a WorkSpaces Pools directory, and make sure that **Enable Home Folders** is selected.

To enable home folders for an existing directory

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the left navigation pane, choose **Directories**, and select the directory for which to enable home folders.
3. Below the directories list, choose **Storage** and select **Enable Home Folders**.
4. In the **Enable Home Folders** dialog box, choose **Enable**.

Administer Your Home Folders

Contents

- Home Folder Content Synchronization
- Home Folder Formats
- Additional Resources

Disable Home Folders

You can disable home folders for a directory without losing user content already stored in home folders. Disabling home folders for a directory has the following effects:

- Users who are connected to active streaming sessions for the directory receive an error message. They are informed that they can no longer store content in their home folder.
- Home folders do not appear for any new sessions that use the directory with home folders disabled.
- Disabling home folders for one directory does not disable it for other directories.
- Even if home folders are disabled for all directories, WorkSpaces Pools does not delete the user content.

To restore access to home folders for the directory, enable home folders again by following the steps described earlier in this topic.

To disable home folders while creating a directory

- Follow the steps in Configure SAML 2.0 and create a WorkSpaces Pools directory and make sure that the **Enable Home Folders** option is cleared.

To disable home folders for an existing directory

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the left navigation pane, choose **Directories**, and select the directory for which to enable home folders.
3. Below the directories list, choose **Storage** and clear **Enable Home Folders**.
4. In the **Disable Home Folders** dialog box, type `CONFIRM` (case-sensitive) to confirm your choice, then choose **Disable**.

Amazon S3 Bucket Storage

WorkSpaces Pools manages user content stored in home folders by using Amazon S3 buckets created in your account. For every AWS Region, WorkSpaces Pools creates a bucket in your account. All user content generated from streaming sessions of directories in that Region is stored in that bucket. The buckets are fully managed by the service without any input or configuration from an administrator. The buckets are named in a specific format as follows:

```
wspool-home-folder-<region-code>-<account-id-without-hyphens>-<random-identifier>
```

Where *<region-code>* is the AWS Region code in which the directory is created and *<account-id-without-hyphens>* is your Amazon Web Services account ID, and *>random-identifier<* is a random identifier number generated by the WorkSpaces service. The first part of the bucket name, `wspool-home-folder-`, does not change across accounts or Regions.

For example, if you enable home folders for directories in the US West (Oregon) Region (us-west-2) on account number 123456789012, the service creates an Amazon S3 bucket in that Region with the name shown. Only an administrator with sufficient permissions can delete this bucket.

```
wspool-home-folder-us-west-2-123456789012
```

As mentioned earlier, disabling home folders for directories does not delete any user content stored in the Amazon S3 bucket. To permanently delete user content, an administrator with adequate access must do so from the Amazon S3 console. WorkSpaces Pools adds a bucket policy that prevents accidental deletion of the bucket.

Home Folder Content Synchronization

When home folders are enabled, WorkSpaces Pools creates a unique folder for each user in which to store their content. The folder is created as a unique Amazon S3 prefix that uses a hash of the user name within an S3 bucket for your Amazon Web Services account and Region. After WorkSpaces Pools creates the home folder in Amazon S3, it copies the accessed content in that folder from the S3 bucket to the WorkSpace. This enables the user to access their home folder content quickly, from the WorkSpace in the WorkSpace Pool, during their streaming session. Changes that you make to a user's home folder content in an S3 bucket and that the user makes to their home folder content on a WorkSpace in the WorkSpace Pool are synchronized between Amazon S3 and WorkSpaces Pools as follows.

1. At the beginning of a user's WorkSpaces Pools streaming session, WorkSpaces Pools catalogs the home folder files that are stored for that user in the Amazon S3 bucket for your Amazon Web Services account and Region.
2. A user's home folder content is also stored on the WorkSpace in WorkSpaces Pools from which they stream. When a user accesses their home folder on the WorkSpace, the list of cataloged files is displayed.
3. WorkSpaces Pools downloads a file from the S3 bucket to the WorkSpace only after the user uses a streaming application to open the file during their streaming session.
4. After WorkSpaces Pools downloads the file to the WorkSpace, synchronization occurs after the file is accessed
5. If the user changes the file during their streaming session, WorkSpaces Pools uploads the new version of the file from the WorkSpace to the S3 bucket periodically or at the end of the streaming session. However, the file is not downloaded from the S3 bucket again during the streaming session.

The following sections describe synchronization behavior when you add, replace, or remove a user's home folder file in Amazon S3.

Contents

Synchronization of files that you add to a user's home folder in Amazon S3

If you add a new file to a user's home folder in an S3 bucket, WorkSpaces Pools catalogs the file and displays it in the list of files in the user's home folder within a few minutes. However, the file isn't downloaded from the S3 bucket to the WorkSpace until the user opens the file with an application during their streaming session.

Synchronization of files that you replace in a user's home folder in Amazon S3

If a user opens a file in their home folder on the WorkSpace in the WorkSpace Pool during their streaming session, and you replace the same file in their home folder in an S3 bucket with a new version during that user's active streaming session, the new version of the file is not immediately

downloaded to the WorkSpace. The new version is downloaded from the S3 bucket to the WorkSpace only after the user starts a new streaming session and opens the file again.

Synchronization of files that you remove from a user's home folder in Amazon S3

If a user opens a file in their home folder on the WorkSpace in the WorkSpace Pool during their streaming session, and you remove the file from their home folder in an S3 bucket during that user's active streaming session, the file is removed from the WorkSpace after the user does either of the following:

- Opens the home folder again
- Refreshes the home folder

Home Folder Formats

The hierarchy of a user folder depends on how a user launches a streaming session, as described in the following section.

SAML 2.0

For sessions created using SAML federation, the user folder structure is as follows:

```
bucket-name/user/federated/user-id-SHA-256-hash/
```

In this case, *user-id-SHA-256-hash* is the folder name created using a lowercase SHA-256 hash hexadecimal string generated from the `NameID` SAML attribute value passed in the SAML federation request. To differentiate users who have the same name but belong to two different domains, send the SAML request with `NameID` in the format `domainname\username`. For more information, see Configure SAML 2.0 and create a WorkSpaces Pools directory.

The following example folder structure applies to session access using SAML federation with `NameID` SAMPLEDOMAIN\testuser, account ID 123456789012 in the US West (Oregon) Region:

```
wspool-home-folder-us-west-2-123456789012/user/
federated/8dd9a642f511609454d344d53cb861a71190e44fed2B8aF9fde0C507012a9901
```

When part or all of the NameID string is capitalized (as the domain name *SAMPLEDOMAIN* is in the example), WorkSpaces Pools generates the hash value based on the capitalization used in the string. Using this example, the hash value for SAMPLEDOMAIN\testuser is

8DD9A642F511609454D344D53CB861A71190E44FED2B8AF9FDE0C507012A9901.
In the folder for that user, this value is displayed in lowercase, as follows:
8dd9a642f511609454d344d53cb861a71190e44fed2B8aF9fde0C507012a9901.

You can identify the folder for a user by generating the SHA-256 hash value of the `NameID` using websites or open source coding libraries available online.

Additional Resources

For more information about managing Amazon S3 buckets and best practices, see the following topics in the *Amazon Simple Storage Service User Guide*:

- You can provide offline access to user data for your users with Amazon S3 policies. For more information, see Amazon S3: Allows IAM Users Access to Their S3 Home Directory, Programmatically and In the Console in the *IAM User Guide*.
- You can enable file versioning for content stored in Amazon S3 buckets used by WorkSpaces Pools. For more information, see Using Versioning.

Enable application settings persistence for your WorkSpaces Pools users

WorkSpaces Pools supports persistent application settings for Windows-based directories. This means that your users' application customizations and Windows settings are automatically saved after each streaming session and applied during the next session. Examples of persistent application settings that your users can configure include, but are not limited to, browser favorites, settings, webpage sessions, application connection profiles, plugins, and UI customizations. These settings are saved to an Amazon Simple Storage Service (Amazon S3) bucket in your account, within the AWS Region in which application settings persistence is enabled. They are available in each WorkSpaces Pools streaming session.

> **Note**
>
> Standard Amazon S3 charges may apply to data that is stored in your S3 bucket. For more information, see Amazon S3 Pricing.

Contents

How application settings persistence works

Persistent application settings are saved to a Virtual Hard Disk (VHD) file. This file is created the first time a user streams an application from a directory on which application settings persistence is enabled. If the WorkSpace Pool associated with the directory is based on an image that contains default application and Windows settings, the default settings are used for the user's first streaming session.

When the streaming session ends, the VHD is unmounted and uploaded to an Amazon S3 bucket within your account. The bucket is created when you enable persistent application settings for the first time for a directory in an AWS Region. The bucket is unique to your AWS account and the Region. The VHD is encrypted in transit using Amazon S3 SSL endpoints, and at rest using AWS Managed CMKs.

The VHD is mounted to the WorkSpace in both `C:\Users\%username%` and `D:\%username%`. If your WorkSpace is not joined to an Active Directory domain, the Windows user name is PhotonUser. If your WorkSpace is joined to an Active Directory domain, the Windows user name is that of the logged in user.

Application settings persistence does not work across different operating system versions. For example, if you enable application settings persistence for a WorkSpace Pool that uses a Windows Server 2019 image, if you update the WorkSpace Pool to use an image that runs a different operating system (such as Windows Server 2022), settings from previous streaming sessions are not saved for users of the directory. Instead, after you update the WorkSpace Pool to use the new image, when users launch a streaming session from a WorkSpace, a new Windows user profile is created. However, if you apply an update to the same operating system on the image, users' customizations and settings from previous streaming sessions are saved. When updates to the same operating system are applied to an image, the same Windows user profile is used when users launch a streaming session from the WorkSpace.

Important

WorkSpaces Pools supports applications that rely on the Microsoft Data Protection API only when the WorkSpace is joined to a Microsoft Active Directory domain. In cases where

a WorkSpace is not joined to an Active Directory domain, the Windows user, PhotonUser, is different on each WorkSpace. Due to the way in which the DPAPI security model works, users' passwords don't persist for applications that use DPAPI in this scenario. In cases where WorkSpaces are joined to an Active Directory domain and the user is a domain user, the Windows user name is that of the logged in user, and users' passwords persist for applications that use DPAPI.

WorkSpaces Pools automatically saves all files and folders in this path, except for the following folders:

- Contacts
- Desktop
- Documents
- Downloads
- Links
- Pictures
- Saved Games
- Searches
- Videos

Files and folders created outside of these folders are saved within the VHD and synced to Amazon S3. The default VHD maximum size is 1GB. The size of the saved VHD is the total size of the files and folders that it contains. WorkSpaces Pools automatically saves the `HKEY_CURRENT_USER` registry hive for the user. For new users (users whose profiles don't exist in Amazon S3), WorkSpaces Pools creates the initial profile by using the default profile. This profile is created in the following location on the image builder: `C:\users\default`.

Note

The entire VHD must be downloaded to the WorkSpace before a streaming session can begin. For this reason, a VHD that contains a large amount of data can delay the start of the streaming session. For more information, see Best practices for enabling application settings persistence.

When you enable application settings persistence, you must specify a settings group. The settings group determines which saved application settings are used for a streaming session from this directory. WorkSpaces Pools creates a new VHD file for the settings group that is stored separately within the S3 bucket in your AWS account. If the settings group is shared between directories, the same application settings are used in each directory. If a directory requires its own application settings, specify a unique settings group for the directory.

Enabling application settings persistence

Contents

Prerequisites for enabling application settings persistence

To enable application settings persistence, you must first do the following:

- Use an image that was created from a base image published by AWS on or after December 7, 2017.
- Enable network connectivity to Amazon S3 from your virtual private cloud (VPC) by configuring internet access or a VPC endpoint for Amazon S3. For more information, see the *Home Folders and VPC Endpoints* section in Networking and Access for WorkSpaces Pools.

Best practices for enabling application settings persistence

To enable application settings persistence without providing internet access to your WorkSpaces, use a VPC endpoint. This endpoint must be in the VPC to which your WorkSpaces in WorkSpaces Pools are connected. You must attach a custom policy to enable WorkSpaces Pools access to the endpoint. For information about how to create the custom policy, see the *Home Folders and VPC Endpoints* section in Networking and Access for WorkSpaces Pools. For more information about private Amazon S3 endpoints, see VPC Endpoints and Endpoints for Amazon S3 in the *Amazon VPC User Guide*.

How to enable application settings persistence

You can enable or disable application settings persistence while creating a directory or after the directory is created by using the WorkSpaces console. For each AWS Region, persistent application settings are stored in an S3 bucket in your account.

The first time you enable application settings persistence for a directory in an AWS Region, WorkSpaces Pools creates an S3 bucket in your AWS account in the same Region. The same bucket stores the application settings VHD file for all users and all directories in that AWS Region. For more information, see *Amazon S3 Bucket Storage* in Administer the VHDs for your users' application settings.

To enable application settings persistence while creating a directory

- Follow the steps in Configure SAML 2.0 and create a WorkSpaces Pools directory, and make sure that **Enable Application Settings Persistence** is selected.

To enable application settings persistence for an existing directory

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the left navigation pane, choose **Pools**, and select the pool for which to enable application persistence.
3. Choose **Edit** in the **Settings** section of the page.
4. In the **Application Persistence** section of the page, select **Enable Application settings persistence**.
5. Choose **Save changes**.

New streaming sessions now have application settings persistence enabled.

Administer the VHDs for your users' application settings

Contents

Amazon S3 bucket storage

When you enable application settings persistence, your users' application customizations and Windows settings are automatically saved to a Virtual Hard Disk (VHD) file that is stored in an Amazon S3 bucket created in your AWS account. For every AWS Region, WorkSpaces Pools creates a bucket in your account that is unique to your account and the Region. All application settings configured by your users are stored in the bucket for that Region.

You do not need to perform any configuration tasks to manage these S3 buckets; they are fully managed by the WorkSpaces Pools service. The VHD file that is stored in each bucket is encrypted in transit using Amazon S3's SSL endpoints and at rest using AWS Managed CMKs. The buckets are named in a specific format as follows:

```
wspool-app-settings-<region-code>-<account-id-without-hyphens>-<random-identifier>
```

region-code

This is the AWS Region code in which the directory is created with application settings persistence.

account-id-without-hyphens

Your AWS account ID. The random identifier ensures there is no conflict with other buckets in that Region. The first part of the bucket name, `wspool-app-settings`, does not change across accounts or Regions.

For example, if you enable application settings persistence for directories in the US West (Oregon) Region (us-west-2) on account number 123456789012, WorkSpaces Pools creates an Amazon S3 bucket within your account in that Region with the name shown. Only an administrator with sufficient permissions can delete this bucket.

```
wspool-app-settings-us-west-2-1234567890123-abcdefg
```

Disabling application settings persistence does not delete any VHDs stored in the S3 bucket. To permanently delete settings VHDs, you or another administrator with adequate permissions must do so by using the Amazon S3 console or API. WorkSpaces Pools adds a bucket policy that prevents accidental deletion of the bucket.

When application settings persistence is enabled, a unique folder is created for each settings group to store the settings VHD. The hierarchy of the folder in the S3 bucket depends on how the user launches a streaming session, as described in the following section.

The path for the folder where the settings VHD is stored in the S3 bucket in your account uses the following structure:

```
bucket-name/Windows/prefix/settings-group/access-mode/user-id-SHA-256-hash
```

bucket-name

The name of the S3 bucket in which users' application settings are stored. The name format is described earlier in this section.

prefix

The Windows version-specific prefix. For example, v4 for Windows Server 2012 R2.

settings-group

The settings group value. This value is applied to one or more directories that share the same the same application settings.

access-mode

The identity method of the user: `custom` for the WorkSpaces Pools API or CLI, `federated` for SAML, and `userpool` for user pool users.

user-id-SHA-256-hash

The user-specific folder name. This name is created using a lowercase SHA-256 hash hexadecimal string generated from the user ID.

The following example folder structure applies to a streaming session that is accessed using the API or CLI with a user ID of `testuser@mydomain.com`, an AWS account ID of `123456789012`, and the settings group `test-stack` in the US West (Oregon) Region (us-west-2):

```
wspool-app-settings-us-west-2-1234567890123-abcdefg/Windows/v4/test-stack/custom/
a0bcb1da11f480d9b5b3e90f91243143eac04cfccfbdc777e740fab628a1cd13
```

You can identify the folder for a user by generating the lowercase SHA-256 hash value of the user ID using websites or open source coding libraries available online.

Reset a user's application settings

To reset a user's application settings, you must find and delete the VHD and associated metadata file from the S3 bucket in your AWS account. Make sure that you do not do this during a user's active streaming session. After you delete the user's VHD and the metadata file, the next time the user launches a session from a streaming instance that has application settings persistence enabled, WorkSpaces Pools creates a new settings VHD for that user.

To reset a user's application settings

1. Open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the S3 bucket that contains the application settings VHD that you want to reset.
3. Locate the folder that contains the VHD. For more information about how to navigate the S3 bucket folder structure, see *Amazon S3 Bucket Storage* earlier in this topic.
4. In the **Name** list, select the check box next to the VHD and the REG, choose **More**, and then choose **Delete**.
5. In the **Delete objects** dialog box, verify that the VHD and the REG are listed, and then choose **Delete**.

The next time the user streams from a pool on which application settings persistence is enabled with the applicable settings group, a new application settings VHD is created. This VHD is saved to the S3 bucket at the end of the session.

Enable Amazon S3 object versioning and revert a user's application settings

You can use Amazon S3 object versioning and lifecycle policies to manage your users' application settings when your users change them. With Amazon S3 object versioning, you can preserve, retrieve, and restore every version of the settings VHD. This enables you to recover from both unintended user actions and application failures. When versioning is enabled, after each streaming session, a new version of the application settings VHD is synced to Amazon S3. The new version does not overwrite the previous version, so if an issue with your users' settings occurs, you can revert to a previous version of the VHD.

> **Note**
>
> Each version of the application settings VHD is saved to Amazon S3 as a separate object and is charged accordingly.

Object versioning is not enabled by default in your S3 bucket, so you must explicitly enable it.

To enable object versioning for your application settings VHD

1. Open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the S3 bucket that contains the application settings VHD on which to enable object versioning.
3. Choose **Properties**.
4. Choose **Versioning**, **Enable versioning**, and then choose **Save**.

To expire older versions of your application settings VHDs, you can use Amazon S3 lifecycle policies. For information, see How Do I Create a Lifecycle Policy for an S3 Bucket? in the *Amazon Simple Storage Service User Guide*.

To revert a user's application settings VHD

You can revert to a previous version of a user's application settings VHD by deleting newer versions of the VHD from the applicable S3 bucket. Do not do this when the user has an active streaming session.

1. Open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the S3 bucket that contains the user's application settings VHD version to revert to.
3. Locate and select the folder that contains the VHD. For information about how to navigate the S3 bucket folder structure, see *Amazon S3 Bucket Storage* earlier in this topic.

   When you select the folder, the settings VHD and associated metadata file display.
4. To display a list of the VHD and metadata file versions, choose **Show**.
5. Locate the version of the VHD to revert to.
6. In the **Name** list, select the check boxes next to the newer versions of the VHD and associated metadata files, choose **More**, and then choose **Delete**.

7. Verify that the application settings VHD that you want to revert to and the associated metadata file are the newest versions of these files.

The next time the user streams from a pool on which application settings persistence is enabled with the applicable settings group, the reverted version of the user's settings displays.

Increase the size of the application settings VHD

The default VHD maximum size is 1 GB. If a user requires additional space for application settings, you can download the applicable application settings VHD to a Windows computer to expand it. Then, replace the current VHD in the S3 bucket with the larger one. Do not do this when the user has an active streaming session.

To increase the size of the application settings VHD

> **Note**
>
> The full VHD must be downloaded before a user can stream applications. Increasing the size of an application settings VHD can increase the time it takes for users to start application streaming sessions.

1. Open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the S3 bucket that contains the application settings VHD to expand.
3. Locate and select the folder that contains the VHD. For information about how to navigate the S3 bucket folder structure, see Amazon S3 bucket storage earlier in this topic.

   When you select the folder, the settings VHD and associated metadata file display.
4. Download the `Profile.vhdx` file to a directory on your Windows computer. Do not close your browser after the download completes, because you'll use the browser again later to upload the expanded VHD.
5. To use Diskpart to increase the size of the VHD to 2 GB, open the command prompt as an administrator, and type the following commands.

   ```
   diskpart
   ```

```
select vdisk file="C:\path\to\application\settings\profile.vhdx"
```

```
expand vdisk maximum=2000
```

6. Then, type the following Diskpart commands to find and attach the VHD, and display the list of volumes:

```
elect vdisk file="C:\path\to\application\settings\profile.vhdx"
```

```
attach vdisk
```

```
list volume
```

In the output, make note of the volume number with the label "AwsEucUsers". In the next step, you select this volume so that you can enlarge it.

7. Type the following command in which *<volume-number>* is the number in the list volume output.

```
select volume <volume-number>
```

8. Type the following command:

```
extend
```

9. Type the following commands to confirm that the size of the partition on the VHD increased as expected (2 GB in this example):

```
diskpart
```

```
select vdisk file="C:\path\to\application\settings\profile.vhdx"
```

```
list volume
```

10. Type the following command to detach the VHD so that it can be uploaded:

```
detach vdisk
```

11. Return to your browser with the Amazon S3 console, choose **Upload**, **Add files**, and then select the enlarged VHD.
12. Choose **Upload**.

After the VHD is uploaded, the next time the user streams from a pool on which application settings persistence is enabled with the applicable settings group, the larger application settings VHD is available.

WorkSpaces Pools troubleshooting notification codes

The following are notification codes and resolution steps for issues with domain join that you might encounter when you set up and use Active Directory with WorkSpaces.

DOMAIN_JOIN_ERROR_ACCESS_DENIED

Message: Access is denied.

Resolution: The service account specified in the directory does not have permissions to create the computer object or reuse an existing one. Validate the permissions and start the WorkSpaces pool.

DOMAIN_JOIN_ERROR_LOGON_FAILURE

Message: The username or password is incorrect.

Resolution: The service account specified in the directory has an invalid username or password. Update the credentials in the AWS Secrets Manager secret configured in the directory, and start the WorkSpaces pool again.

DOMAIN_JOIN_NERR_PASSWORD_EXPIRED

Message: The password of this user has expired.

Resolution: The password for the service account in the AWS Secrets Manager secret has expired. First, stop the WorkSpaces pool. Next, change the password for the secret specified in the WorkSpaces directory. Then, start the WorkSpaces pool.

DOMAIN_JOIN_ERROR_DS_MACHINE_ACCOUNT_QUOTA_EXCEEDED

Message: Your computer could not be joined to the domain. You have exceeded the maximum number of computer accounts you are allowed to create in this domain. Contact your system administrator to have this limit reset or increased.

Resolution: The service account specified on the directory does not have permissions to create the computer object or reuse an existing one. Validate the permissions and start the WorkSpaces pool.

DOMAIN_JOIN_ERROR_INVALID_PARAMETER

Message: A parameter is incorrect. This error is returned if the `LpName` parameter is NULL or the `NameType` parameter is specified as `NetSetupUnknown` or an unknown nametype.

Resolution: This error can occur when the distinguished name for the OU is incorrect. Validate the OU and try again. If you continue to encounter this error, contact AWS Support. For more information, see AWS Support Center.

DOMAIN_JOIN_ERROR_MORE_DATA

Message: More data is available.

Resolution: This error can occur when the distinguished name for the OU is incorrect. Validate the OU and try again. If you continue to encounter this error, contact AWS Support. For more information, see AWS Support Center.

DOMAIN_JOIN_ERROR_NO_SUCH_DOMAIN

Message: The specified domain either does not exist or could not be contacted.

Resolution: The streaming instance was unable to contact your Active Directory domain. To ensure network connectivity, confirm your VPC, subnet, and security group settings.

DOMAIN_JOIN_NERR_WORKSTATION_NOT_STARTED

Message: The Workstation service has not been started.

Resolution: An error occurred starting the Workstation service. Ensure that the service is enabled in your image. If you continue to encounter this error, contact AWS Support. For more information, see AWS Support Center.

DOMAIN_JOIN_ERROR_NOT_SUPPORTED

Message: The request is not supported. This error is returned if a remote computer was specified in the `lpServer` parameter and this call is not supported on the remote computer.

Resolution: Contact AWS Support for assistance. For more information, see AWS Support Center.

DOMAIN_JOIN_ERROR_FILE_NOT_FOUND

Message: The system cannot find the file specified.

Resolution: This error occurs when an invalid organizational unit (OU) distinguished name is provided. The distinguished name must start with **OU=**. Validate the OU distinguished name and try again.

DOMAIN_JOIN_INTERNAL_SERVICE_ERROR

Message: The account already exists.

Resolution: This error can occur in the following scenarios:

- If the issue isn't permissions-related, check the Netdom logs for errors and make sure that you provided the correct OU.
- The service account specified in the directory does not have permissions to create the computer object or reuse an existing one. If this is the case, validate the permissions and start the WorkSpaces pool.
- After WorkSpaces creates the computer object, it is moved from the OU in which it was created. In this case, the first WorkSpaces pool is created successfully, but any new WorkSpaces pool that uses the computer object fails. When Active Directory searches for the computer object in the specified OU and detects that an object with the same name exists elsewhere in the domain, the domain join is not successful.
- The name of the OU specified in the WorkSpaces directory includes spaces before or after the commas in the directory. In this case, when a WorkSpaces pool attempts to rejoin the Active Directory domain, WorkSpaces cannot cycle the computer objects correctly and the domain rejoin does not succeed. To resolve this issue for a WorkSpaces pool, do the following:

  1. Stop the WorkSpaces pool.
  2. Edit the Active Directory domain settings for the WorkSpaces pool to remove the directory and Directory OU to which the WorkSpaces pool is joined.
  3. Update the WorkSpaces directory to specify an OU that doesn't contain spaces.
  4. Edit the Active Directory domain settings for the WorkSpaces pool to specify the directory with the updated Directory OU.

  To resolve this issue for a WorkSpaces pool, do the following:

1. Delete the WorkSpaces pool.
2. Update the WorkSpaces directory to specify an OU that doesn't contain spaces.
3. Create a new WorkSpaces pool and specify the directory with the updated Directory OU.

WORKSPACES_POOL_SESSION_RESERVATION_ERROR

Message: We currently do not have sufficient capacity for requested sessions in the availability zones [us-west-1] for subnets associated with your WorkSpaces Pool. Our system will be working on provisioning additional capacity. Meanwhile, please change or associate a different subnet using one of the following AZs [us-west-2, us-west-3].

Resolution: Wait until EC2 has enough capacity or update subnets in other AZs on the directory.

INSUFFICIENT_CAPACITY_ERROR_WORKSPACES_POOL_AZ

Message: We currently don't have sufficient capacity for requested sessions in availability zone (AZs) [<impacted az>]. Our system will be working on provisioning additional capacity. Meanwhile please change or associate another subnet using other AZs to your WorkSpaces Pool.

Resolution: Wait until Amazon EC2 has enough capacity or update subnets in other AZs on the directory.

INVALID_CUSTOMER_SUBNET_CIDR_BLOCK

Message: Your subnet includes use of an unavailable CIDR range. Please update your subnets outside of the current /18 range.”.

Resolution: Wait until EC2 has enough capacity or update subnets in other AZs on the directory.

Bring Your Own Windows desktop licenses in WorkSpaces

If your licensing agreement with Microsoft allows it, you can bring and deploy your Windows 10 or 11 desktop on your WorkSpaces. To do this, you must enable Bring Your Own License (BYOL) and provide a Windows 10 or 11 license that meets the requirements below. For more information about using Microsoft software on AWS, see Amazon Web Services and Microsoft.

To stay compliant with Microsoft licensing terms, AWS runs your BYOL WorkSpaces on hardware that is dedicated to you in the AWS Cloud. By bringing your own license, you can provide a consistent experience for your users. For more information, see WorkSpaces Pricing.

> **Important**
>
> Image creation is not supported on Windows 10 or 11 systems that have been upgraded from one version of Windows 10 or 11 to a newer version of Windows 10 or 11 (a Windows feature/version upgrade). However, Windows cumulative or security updates are supported by the WorkSpaces image-creation process.

Contents

- Step 9: Launch your BYOL WorkSpaces
- Link BYOL accounts

Requirements

Before you begin, verify the following:

- Your Microsoft licensing agreement allows Windows to run in a virtual hosted environment.
- If you will be using non-GPU-enabled bundles (bundles other than Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro), verify that you will use a minimum of 100 WorkSpaces per Region. These 100 WorkSpaces can be any mix of AlwaysOn and AutoStop WorkSpaces. Using a minimum of 100 WorkSpaces per Region is a requirement for running your WorkSpaces on dedicated hardware. Running your WorkSpaces on dedicated hardware is necessary to comply with Microsoft licensing requirements. The dedicated hardware is provisioned on the AWS side, so your VPC can stay on default tenancy.

  If you plan to use GPU-enabled (Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro) bundles, verify that you will run a minimum of 4 AlwaysOn or 20 AutoStop GPU-enabled WorkSpaces in a Region per month on dedicated hardware.

  Note

  - Graphics bundle is no longer supported after November 30, 2023. We recommend migrating your WorkSpaces to Graphics.g4dn bundle. For more information, see Migrate a WorkSpace in WorkSpaces Personal.
  - Graphics and GraphicsPro bundles aren't available in the Asia Pacific (Mumbai) Region.
  - Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro bundles are not available in the Africa (Cape Town) Region and the Israel (Tel Aviv) Region.
  - To run your WorkSpaces in the Africa (Cape Town) Region, you are required to run a minimum of 400 WorkSpaces in the Africa (Cape Town) Region.
  - Windows 11 bundles can be created for the WSP protocol for WorkSpaces. Windows 11 bundles are also supported for partner protocols with WorkSpaces Core.
  - Graphics and GraphicsPro bundles are not supported for Windows 11.
  - Value bundles are not available for Windows 11 and WorkSpaces Pools. For more information about migrating your existing value bundle WorkSpaces see Migrate a WorkSpace in WorkSpaces Personal.

- For the best video conferencing experience we recommend using Power or PowerPro bundles
- Windows 11 requires the Unified Extensible Firmware Interface (UEFI) boot mode to function. Make sure you specify the optional `--boot-mode` parameter as UEFI to successfully import of your VM.

- WorkSpaces can use a management interface in the /16 IP address range. The management interface is connected to a secure WorkSpaces management network used for interactive streaming. This allows WorkSpaces to manage your WorkSpaces. For more information, see Network interfaces. You must reserve a /16 netmask from at least one of the following IP address ranges for this purpose:
  - 10.0.0.0/8
  - 100.64.0.0/10
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 198.18.0.0/15

  Note
  - As you adopt the WorkSpaces service, the available management interface IP address ranges frequently change. To determine which ranges are currently available, run the list-available-management-cidr-ranges AWS Command Line Interface (AWS CLI) command.
  - In addition to the /16 CIDR block that you select, the 54.239.224.0/20 IP address range is used for management interface traffic in all AWS Regions.
- Make sure you have opened the necessary management interface ports for Microsoft Windows and Microsoft Office KMS activation for BYOL WorkSpaces. For more information, see Management interface ports.
- You have a virtual machine (VM) that runs a supported 64-bit version of Windows. For a list of supported versions, see the next section in this topic, Windows versions supported for BYOL. The VM must also meet these requirements:
  - The Windows operating system must be activated against your key management servers.
  - The Windows operating system must have **English (United States)** as the primary language.

- No software beyond what is included with Windows can be installed on the VM. You can add additional software, such as an antivirus solution, when you later create a custom image.
- Do not customize the default user profile (`C:\Users\Default`) or make other customizations before creating an image. All customizations should be made after image creation. We recommend making any customizations to the user profile through Group Policy Objects (GPOs) and applying them after image creation. This is because customizations done through GPOs can be easily modified or rolled back and are less prone to error than customizations made to the default user profile.
- You must create a **WorkSpaces_BYOL** account with local administrator access before you share the image. The password for this account might be required later, so make note of it.
- The VM must be on a single volume with a maximum size of 70 GB and at least 10 GB of free space. If you're also planning to subscribe to Microsoft Office for your BYOL image, the VM must be on a single volume with a maximum size of 70 GB and at least 20 GB of free space. The DISK that the root volume is on cannot exceed 70GB.
- Your VM must run Windows PowerShell version 4 or later.

- Make sure that you have installed the latest Microsoft Windows patches before you run the BYOL checker script in Step 3: Run the BYOL Checker PowerShell script on a Windows VM.
- The Windows default system unattend files in the `%WINDIR%\panther` and `%WINDIR%\panther\unattend` paths should not be modified.

> **Note**
>
> - For BYOL AutoStop WorkSpaces, a large number of concurrent logins could result in significantly increased time for WorkSpaces to be available. If you expect many users to log into your BYOL AutoStop WorkSpaces at the same time, please consult your account manager for advice.
> - Encrypted AMIs are not supported in the importing process. Ensure you disable the instance used to create the EC2 AMI has EBS encryption. Encryption can be enabled after the final WorkSpaces is provisioned.

Windows versions supported for BYOL

Your VM must run one of the following Windows versions:

- Windows 10 Version 22H2 (November 2022 Update)
- Windows 10 Enterprise LTSC 2019 (1809)
- Windows 10 Enterprise LTSC 2021 (21H2)
- Windows 11 Enterprise 23H2 (October 2023 release)
- Windows 11 Enterprise 22H2 (October 2022 release)

All supported OS versions support all of the compute types available in the AWS Region where you're using WorkSpaces. Versions of Windows that are no longer supported by Microsoft are not guaranteed to work and are not supported by AWS Support.

> **Note**
>
> Windows 10 N and Windows 11 N versions are not supported for BYOL at this time.

Add Microsoft Office to Your BYOL image

During the BYOL image ingestion process, if you are using Windows 10, you have the option to subscribe to Microsoft Office Professional 2016 (32-bit) or 2019 (64-bit) through AWS. If you are using Windows 11, you can subscribe to Microsoft Office Professional 2019 (64-bit). If you choose either of these options, Microsoft Office is pre-installed in your BYOL image and included on any WorkSpaces that you launch from this image.

> **Note**
>
> - Graphics.g4dn and GraphicsPro.g4dn BYOL images with PCoIP support only Office 2019. They don't support Office 2016.
>
> - Graphics.g4dn and GraphicsPro.g4dn BYOL images with WSP support Office bundles through Manage applications in WorkSpaces Personal.

If you choose to subscribe to Office through AWS, additional charges will apply. For more information, see WorkSpaces Pricing.

Important

- If Microsoft Office is already installed on the VM that you are using to create your BYOL image, you must uninstall it from the VM if you want to subscribe to Office through AWS.
- If you plan to subscribe to Office through AWS, make sure that your VM has at least 20 GB of free disk space.
- During image import, you can subscribe to Office 2016 or 2019 but not to Office 2021. For Office 2021 and other applications such as Microsoft Visual Studio 2022, Microsoft Visio 2021, and Microsoft Project 2021, see Manage applications.
- To bring your own Microsoft 365 licenses for both browser-based and desktop applications on Amazon WorkSpaces, install Microsoft 365 applications on your BYOL image after the BYOL image ingestion process is complete.

Note

Graphics.g4dn and GraphicsPro.g4dn BYOL images only support Office 2019 and do not support Office 2016.

If you choose to subscribe to Office, the BYOL image ingestion process takes a minimum of 3 hours.

For details about subscribing to Office during the BYOL ingestion process, see Step 6: Create a BYOL image using the WorkSpaces console.

Office language settings

We choose the language used for your Office subscription based on the AWS Region where you're performing your BYOL image ingestion. For example, if you're performing your BYOL image ingestion in the Asia Pacific (Tokyo) Region, your Office subscription has Japanese as its language.

By default, we install a number of frequently used Office language packs on your WorkSpaces. If the language pack that you want isn't installed, you can download additional language packs from Microsoft. For more information, see Language Accessory Pack for Office in the Microsoft documentation.

To change the language for Office, you have several options:

Option 1: Allow individual users to customize their Office language settings

Individual users can adjust the Office language settings on their WorkSpaces. For more information, see Add an editing or authoring language or set language preferences in Office in the Microsoft documentation.

Option 2: Use GPO administrative templates (.admx/.adml) to enforce default Office language settings for all of your WorkSpaces users

You can use Group Policy Object (GPO) settings to enforce default Office language settings for your WorkSpaces users.

> **Note**
>
> Your WorkSpaces users will not be able to override language settings enforced through GPO.

For more information about using GPO to set the language for Office, see Customize language setup and settings for Office in the Microsoft documentation. Office 2016 and Office 2019 use the same GPO settings (labeled with Office 2016).

To work with GPOs, you must install the Active Directory administration tools. For information about using the Active Directory administration tools to work with GPOs, see Set up Active Directory Administration Tools for WorkSpaces Personal.

Before you can configure Office 2016 or Office 2019 policy settings, you must download the administrative template files (.admx/.adml) for Office from the Microsoft Download Center. After you download the administrative template files, you must add the `office16.admx` and `office16.adml` files to the Central Store of the domain controller for your WorkSpaces directory. (The `office16.admx` and `office16.adml` files apply to both Office 2016 and Office 2019.) For more information about working with `.admx` and `.adml` files, see How to create and manage the Central Store for Group Policy Administrative Templates in Windows in the Microsoft documentation.

The following procedure describes how to create the Central Store and add the administrative template files to it. Perform the following procedure on a directory administration WorkSpace or Amazon EC2 instance that is joined to your WorkSpaces directory.

To install the Group Policy administrative template files for Office

1. Download the administrative template files (.admx/.adml) for Office from the Microsoft Download Center.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open Windows File Explorer, and in the address bar, enter your organization's fully qualified domain name (FQDN), such as `\\example.com`.
3. Open the `SYSVOL` folder.
4. Open the folder with the *FQDN* name.
5. Open the `Policies` folder. You should now be in `\\`*FQDN*`\SYSVOL\`*FQDN*`\Policies`.
6. If it doesn't already exist, create a folder named `PolicyDefinitions`.
7. Open the `PolicyDefinitions` folder.
8. Copy the `office16.admx` file into the `\\`*FQDN*`\SYSVOL\`*FQDN*`\Policies\PolicyDefinitions` folder.
9. Create a folder named `en-US` in the `PolicyDefinitions` folder.
10. Open the `en-US` folder.
11. Copy the `office16.adml` file into the `\\`*FQDN*`\SYSVOL\`*FQDN*`\Policies\PolicyDefinitions\en-US` folder.

To configure the GPO language settings for Office

1. On your directory administration WorkSpace or Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**).
2. Expand the forest (**Forest:*FQDN***).
3. Expand **Domains**.
4. Expand your FQDN (for example, `example.com`).
5. Select your FQDN, open the context (right-click) menu or open the **Action** menu, and choose **Create a GPO in this domain, and Link it here**.
6. Name your GPO (for example, **`Office`**).
7. Select your GPO, open the context (right-click) menu or open the **Action** menu, and choose **Edit**.

8. In the Group Policy Management Editor, choose **User Configuration**, **Policies**, **Administrative Template Policy definitions (ADMX files) retrieved from the local computer**, **Microsoft Office 2016**, and **Language Preferences**.

   > **Note**
   >
   > Office 2016 and Office 2019 use the same GPO settings (labeled with Office 2016). If you don't see **Administrative Template Policy definitions (ADMX files) retrieved from the local computer** under **User Configuration**, **Policies**, the `office16.admx` and `office16.adml` files aren't correctly installed on your domain controller.

9. Under **Language Preferences**, specify the language that you want for the following settings. Be sure to set each setting to **Enabled**, and then under **Options**, select the language you want. Choose **OK** to save each setting.

   - **Display Language** > **Display help in**
   - **Display Language** > **Display menus and dialog boxes in**
   - **Editing languages** > **Primary Editing Language**

10. Close the Group Policy Management tool when you're finished.
11. Group Policy setting changes take effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

    - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
    - From an administrative command prompt, enter **gpupdate /force**.

Option 3: Update the Office language registry settings on your WorkSpaces

To set the Office language settings through the registry, update the following registry settings:

- **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\UILanguage**
- **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\HelpLanguage**

For these settings, add a DWORD key value with the appropriate Office locale ID (LCID). For example, the LCID for English (US) is 1033. Because LCIDs are decimal values, you must set the **Base** option for the DWORD value to **Decimal**. For a list of the Office LCIDs, see Language identifiers and OptionState Id values in Office 2016 in the Microsoft documentation.

You can apply these registry settings to your WorkSpaces through GPO settings or a logon script.

For more information about working with the language settings for Office, see Customize language setup and settings for Office in the Microsoft documentation.

Add Office to your existing BYOL WorkSpaces

You can also add a subscription to Office to your existing BYOL WorkSpaces by doing the following.

- **Manage applications** (recommended) - You can install and configure Microsoft Office, Microsoft Visual Studio 2022, Microsoft Visio, or Microsoft Project 2021 on your existing WorkSpaces. For more information, see Manage applications.
- **Migrate a WorkSpace** - After you have a BYOL bundle with Office installed, you can use the WorkSpaces migration feature to migrate your existing BYOL WorkSpaces to the BYOL bundle that's subscribed to Office. For more information, see Migrate a WorkSpace in WorkSpaces Personal.

> **Note**
>
> The manage applications option is available for installing Microsoft Office 2021 and other applications, such as Microsoft Visual Studio 2022, Microsoft Visio 2021, and Microsoft Project 2021 to your WorkSpaces. For installing Microsoft Office 2016 or 2019 on your WorkSpaces, use Migrate a WorkSpace in WorkSpaces Personal.

Migrate between versions of Microsoft Office

To migrate from one Microsoft Office version to another, you have the following options:

- **Manage applications** (recommended) – You can uninstall the original Office version and install Office 2021 and other applications, such as Microsoft Visual Studio 2022, Microsoft Visio 2021, and Microsoft Project 2021, on your existing WorkSpaces. For example, to migrate from Microsoft Office 2019 to Microsoft Office 2021, use the manage applications workflow to

uninstall Microsoft Office 2019 and install Microsoft Office 2021. For more information, see Manage applications.

- **Migrate a WorkSpace** – To migrate from Microsoft Office 2016 to Microsoft Office 2019 or from Microsoft Office 2019 to Microsoft Office 2016, you must create a BYOL bundle that's subscribed to the version of Office that you want to migrate to. Then, use the WorkSpaces migration feature to migrate your existing BYOL WorkSpaces that are subscribed to Office to the BYOL bundle that's subscribed to the version of Office that you want to migrate to. For example, to migrate from Microsoft Office 2016 to Microsoft Office 2019, create a BYOL bundle that's subscribed to Microsoft Office 2019. Then use the WorkSpaces migration feature to migrate your existing BYOL WorkSpaces that are subscribed to Office 2016 to the BYOL bundle that's subscribed to Office 2019. For more information, see Migrate a WorkSpace.

You can use these options to migrate your WorkSpaces that are subscribed to Microsoft Office through AWS to Microsoft 365 applications. However, manage applications is limited to uninstalling Microsoft Office from your WorkSpace. You must bring in your own tools and installers to install Microsoft 365 applications on your WorkSpaces.

> **Note**
>
> Using manage applications, you can install or uninstall Microsoft Office, Microsoft Visio, or MicrosoftProject 2021 on your WorkSpaces. For Microsoft Office 2016 or 2019 versions, you can only remove them from your WorkSpaces. To install Microsoft Office 2016 or 2019 on your WorkSpaces, migrate a WorkSpace.

For more information about the migration process, see Migrate a WorkSpace in WorkSpaces Personal.

Unsubscribe from Office

To unsubscribe from Office, you have the following options.

- **Manage applications** (recommended) - You can uninstall Microsoft Office and other applications such as Microsoft Visio and Microsoft Project from your WorkSpaces. For more information, see Manage applications.
- **Migrate a WorkSpace** - You can create a BYOL bundle that is not subscribed to Office. Then use the WorkSpaces migration feature to migrate your existing BYOL WorkSpaces to the BYOL

bundle that is not subscribed to Office. For more information, see Migrate a WorkSpace in WorkSpaces Personal.

Office updates

If you have subscribed to Office through AWS, Office updates are included as part of your regular Windows updates. To stay current on all security patches and updates, we recommend that you periodically update your BYOL base images.

Step 1: Check the eligibility of your account for BYOL using the Amazon WorkSpaces console

Before you can enable your account for BYOL, you must go through a verification process to confirm your eligibility for BYOL. Until you go through this process, the **Enable BYOL** option will not be available in your Amazon WorkSpaces console.

> **Note**
>
> The verification process takes at least one business day. If you want to apply the CIDR range and BYOL configurations of an existing AWS account to a different one, you can link them together to use the same underlying hardware. To link your AWS accounts, you don't need to submit a support ticket. You can use APIs, such as CreateAccountLinkInvitations and AcceptAccountLinkInvitation to connect your AWS accounts. For more information, see Link BYOL accounts.

To check the eligibility of your account for BYOL by using the Amazon WorkSpaces console

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Account Settings**, and then under **Bring your own license (BYOL)**, choose **View WorkSpaces BYOL settings**. If your account is not currently eligible for BYOL, a message provides guidance for next steps. To get started, contact your AWS account manager or sales representative, or contact the AWS Support Center. Your contact will verify your eligibility for BYOL.

   To determine your eligibility for BYOL, your contact will need certain information from you. For example, you might be asked to answer the following questions.

- Have you reviewed and accepted the BYOL requirements listed earlier?
- In which AWS Regions do you need your account enabled for BYOL?
- How many BYOL WorkSpaces do you plan to deploy per AWS Region?
- What is your ramp-up plan?
- Are you purchasing WorkSpaces from a reseller?
- What bundle types do you need for BYOL?
- Does your organization have any other AWS accounts enabled for BYOL in the same Region? If yes, do you want to link these accounts so that they use the same underlying hardware?

  If the accounts are linked, the total number of WorkSpaces deployed in these accounts is aggregated together for the purposes of determining your eligibility for BYOL. If the answer to both of these questions is yes, you can link your accounts together. You can use APIs, such as CreateAccountLinkInvitations and AcceptAccountLinkInvitation to connect your AWS accounts. If you want to link other BYOL-enabled accounts, but want to use a different BYOL setup (CIDR range and image), contact to AWS Support to enable your new account for BYOL.

3. After your eligibility is confirmed for BYOL, you can proceed to the next step, where you enable BYOL for your account in the Amazon WorkSpaces console.

Step 2: Enable BYOL for your account for BYOL using the Amazon WorkSpaces console

To enable BYOL for your account, you must specify a management network interface. This interface is connected to a secure Amazon WorkSpaces management network. It is used for interactive streaming of the WorkSpace desktop to Amazon WorkSpaces clients, and to allow Amazon WorkSpaces to manage the WorkSpace.

> **Note**
>
> You only need to perform the steps in this procedure once per Region to enable BYOL for your account.

To enable BYOL for your account by using the Amazon WorkSpaces console

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Account Settings**, and then under **Bring your own license (BYOL)**, choose **View WorkSpaces BYOL settings**.
3. On the **Account Settings** page, under **Bring Your Own License (BYOL)**, choose **Enable BYOL**.

   If you don't see the **Enable BYOL** option, this means that your account is not currently eligible for BYOL. For more information, see Step 1: Check the eligibility of your account for BYOL using the Amazon WorkSpaces console.
4. Under **Bring Your Own License (BYOL)**, in the **Management network interface IP address range** area, choose an IP address range, and then choose **Display available CIDR blocks**.

   Amazon WorkSpaces searches for and displays available IP address ranges as IPv4 Classless Inter-Domain Routing (CIDR) blocks, within the range that you specify. If you require a specific IP address range, you can edit the search range.

   > **Important**
   >
   > **After you specify an IP address range, you cannot modify it.** Make sure to specify an IP address range that doesn't conflict with the ranges used by your internal network. If you have any questions about which range to specify, contact your AWS account manager or sales representative, or contact the AWS Support Center before proceeding.
5. Choose the CIDR block that you want from the list of results, and then choose **Enable BYOL**.

   This process may take several hours. While WorkSpaces is enabling your account for BYOL, proceed to the next step.

Step 3: Run the BYOL Checker PowerShell script on a Windows VM

After you enable BYOL for your account, you must confirm that your VM meets the requirements for BYOL. To do so, perform these steps to download and run the WorkSpaces BYOL Checker PowerShell script. The script performs a series of tests on the VM that you plan to use to create your image.

> **Important**
>
> The VM must pass all tests before you can use it for BYOL.

To download the BYOL Checker script

Before you download and run the BYOL Checker script, verify that the latest Windows security updates are installed on your VM. While this script runs, it disables the Windows Update service.

1. Download the BYOL Checker script .zip file from https://tools.amazonworkspaces.com/BYOLChecker.zip to your `Downloads` folder.
2. In your `Downloads` folder, create a `BYOL` folder.
3. Extract the files from `BYOLChecker.zip` and copy them to the `Downloads\BYOL` folder.
4. Delete the `Downloads\BYOLChecker.zip` folder so that only the extracted files remain.

Perform these steps to run the BYOL Checker script.

To run the BYOL Checker script

1. From the Windows desktop, open Windows PowerShell. Choose the Windows **Start** button, right-click **Windows PowerShell**, and choose **Run as administrator**. If you are prompted by **User Account Control** to choose whether you want PowerShell to make changes to your device, choose **Yes**.
2. At the PowerShell command prompt, change to the directory where the BYOL Checker script is located. For example, if the script is located in the `Downloads\BYOL` directory, enter the following command and press **Enter**:

   ```
   cd C:\Users\username\Downloads\BYOL
   ```

3. Enter the following command to update the PowerShell execution policy on the computer. Doing so allows the BYOL Checker script to run:

   ```
   Set-ExecutionPolicy AllSigned
   ```

4. When prompted to confirm whether to change the PowerShell execution policy, enter **A** to specify Yes to All.
5. Enter the following command to run the BYOL Checker script:

```
.\BYOLChecker.ps1
```

6. If a security notification appears, press the **R** key to Run Once.
7. In the **WorkSpaces Image Validation** dialog box, choose **Begin Tests**.
8. After each test is completed, you can view the status of the test. For any test with a status of **FAILED**, choose **Info** to display information about how to resolve the issue that caused the failure. If any tests display a status of **WARNING**, choose the **Fix All Warnings** button.
9. If applicable, resolve any issues that cause test failures and warnings, and repeat Step 7 and Step 8 until the VM passes all tests. All failures and warnings must be resolved before you export the VM.
10. The BYOL script checker generates two log files, `BYOLPrevalidationlog`*`YYYY-MM-DD_HHmmss`*`.txt` and `ImageInfo.text`. These files are located in the directory that contains the BYOL Checker script files.

    > **Tip**
    >
    > Do not delete these files. If an issue occurs, they might be helpful in troubleshooting.

11. After your VM passes all tests, you get a **Validation Successful** message.

    You will also see a prompt to run Sysprep. Close the prompt and don't run Sysprep yet.
12. Shut down the VM and export it.
13. (Optional) Start the VM and run the BYOL Checker script one more time. All validations should pass. A screen will pop up again with a button to run Sysprep. Choose **Run Sysprep**. If Sysprep is successful, your exported VM that you exported from step 12 can be imported into Amazon Elastic Compute Cloud (Amazon EC2).

    If Sysprep is unsuccessful, review the Sysprep logs in the `%WINDIR%\System32\Sysprep\Panther` path, roll back to the exported VM from step 12, resolve the reported issues, and complete step 12 again by exporting the fixed VM. You will then re-run the BYOL Checker script to ensure the issues have been resolved.

    The most common reason for a Sysprep failure is that the Modern AppX Packages have not been uninstalled for all users. Use the `Remove-AppxPackage` PowerShell cmdlet to remove the AppX Packages.
14. Import the VM that you exported in step 12 into Amazon EC2.

List of BYOL Checker error messages and error fixes

BYOL import requires Powershell 4.0 or higher. The installed version of PowerShell is not supported.

PowerShell version 4.0 or later must be installed. For more information, see Microsoft Windows PowerShell.

BYOL import does not support systems with active Microsoft Office installed.

Microsoft Office must be uninstalled before import. For more information, see Uninstall Office from a PC.

BYOL import requires a system without a PCoIP Agent.

Uninstall the PCoIP Agent. For information about uninstalling the PCoIP agent, see Uninstalling the Teradici PCoIP Software Client for Mac

BYOL import requires that Windows updates are disabled.

Disable Windows updates by following the following steps:

1. Press **Windows key** + **R**. Type `services.msc`, then press **Enter**.
2. Right-click on **Windows Update**, then choose **Properties**.
3. Under the **General** tab, set the **Startup type** to **Disabled**.
4. Choose **Stop**.
5. Click **Apply**, and then choose **OK**.
6. Restart your computer.

BYOL import requires that Automount is enabled.

You must enable Automount. Run the following command in powershell as an administrator.

```
C:\> diskpart
DISKPART> automount enable
```

Automatic mounting of new volumes enabled.

BYOL import requires the WorkSpaces_BYOL account to be enabled

WorkSpaces_BYOL account must be enabled. For more information, see Enable BYOL for your account for BYOL using the Amazon WorkSpaces console.

BYOL import requires the network interface to use DHCP to automatically assign an IP address. The network interface is currently using a static IP address.

Network interface must be changed to use DHCP. For more information, see Change TCP/IP settings.

BYOL import requires more than 20 GB of space on the local disk.

Local disk must have enough space and requires you to free up 20 GB or more.

BYOL import requires systems with 1 local drive. There are additional Local, Removable or Network drives.

Only the C and D drives can be present on a WorkSpace that's used for importing an image. Remove all other drives, including virtual drives.

BYOL import requires Windows 10 or Windows 11.

Use a Windows 10 or Windows 11 operating system.

BYOL import requires systems that are not AD domain joined.

System must be unjoined from AD domain. For more information, see Azure Active Directory device management FAQ.

BYOL import requires systems that are not Azure domain joined.

System must be unjoined from Azure domain. For more information, see Azure Active Directory device management FAQ.

BYOL import requires Windows Public Firewall disabled.

Public firewall profile must be disabled. For more information, see Turn Microsoft Defender Firewall on or off.

BYOL import requires a system without VMware tools.

VMWare tools must be uninstalled. For more information, see Uninstalling and manually installing VMware Tools in VMware Fusion (1014522).

BYOL import requires the local disk to be less than 80 GB.

The disk must be smaller than 80 GB. Reduce the disk size.

BYOL import requires less than 2 partitions on the local drive. In addition, all Windows 10 partitions must be MBR partitioned and all Windows 11 partitions must be GPT partitioned.

Volumes must be MBR partitioned for Windows 10 and GPT partitioned for Windows 11. For more information, see Manage disks.

BYOL import requires all pending updates that require reboots are complete.

Install all updates and reboot the operating system.

BYOL import requires that AutoLogon is disabled.

To disable the AutoLogon registry:

1. Press **Windows key** + **R** and type `Regedit.exe` in the command prompt.
2. Scroll down to `HKEY_LOCAL_Machine\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`
3. Add a value for `DontDisplayLastUserName`.
4. For **Type**, enter `REG_SZ`.
5. For **Value**, enter `0`.

> **Note**
>
> - The value `DontDisplayLastUserName` determines whether the logon dialog box displays the username of the last user that logged onto the PC.
> - The value does not exist by default. If it exists, you must set it to `0` or the value of `DefaultUser` will be wiped and AutoLogon will fail.

BYOL import requires `RealTimeIsUniversal` to be enabled.

RealTimeUniversal Registry Key must be enabled. For more information, see Configure time settings for Windows Server 2008 and later.

BYOL import requires a system with one bootable partition.

Number of bootable partitions must not exceed one.

To remove additional partitions

1. Press the **Windows logo** + **R** keys to open **Run** box. Enter `msconfig` and press the **Enter** key on the keyboard to open the System Configuration window.
2. Choose the **Boot** tab from the window and check if the OS you want to use is set to **Current OS; Default OS**. If it isn't set, choose your desired OS from the window and choose **Set as default** on the same window.
3. To delete another partition, choose that partition, then select **Delete**, **Apply**, **OK**.

If the error still shows up, boot your computer from the installation or repair disc, and follow these steps.

1. Skip the initial languages screen, and then choose **Repair your computer** on the main install screen.
2. On the **Choose an option** screen, choose **Troubleshoot**.
3. On the **Advanced options** screen, choose **Command Prompts**.
4. In the command prompt, enter `bootrec.exe /fixmbr`, then press **Enter**.

BYOL import requires a 64 bit system.

A 64 bit OS image must be used. For more information, see Windows versions supported for BYOL.

BYOL import requires a system that has not been rearmed.

The Image Rearm count must not be 0. The rearm feature allows you to extend the activation period for the trial version of Windows. The Create Image process requires that the rearm count be a value other than 0.

To check the Windows rearm count

1. On the Windows Start menu, choose **Windows System**, then choose **Command Prompt**.
2. In the Command Prompt, enter `cscript C:\Windows\System32\slmgr.vbs /dlv`, and then press **Enter**.

3. To reset the rearm count to a value other than 0. For more information, see Sysprep (Generalize) a Windows installation.

BYOL import requires a system that has not been upgraded in-place. This system has been upgraded in-place.

Windows must not have been upgraded from a previous version.

BYOL import requires that no antivirus is installed on the system.

You must uninstall your antivirus software. Run BYOLChecker to get details for the antivirus software to uninstall.

BYOL import requires Windows 10 systems to have a legacy Boot mode.

The Legacy BIOS BootMode must be used for Windows 10.For more information, see Boot modes.

List of SysPrep error messages and error fixes

The AMI you are importing has AppX packages installed. Remove them and re-import the image.

Modern AppX Packages might still be installed for your users. Remove the AppX package by running the Powershell `cmdlet`, `Remove-AppxPackage`.

The AMI you are importing has reserved storage enabled. Disable it after Windows updates and re-import the image.

To disable reserved storage

1. Open the Registry Editor but entering `regedit.exe`.
2. Navigate to the registry key: `HKLM\Software\Microsoft\Windows\CurrentVersion\ReserveManager`.
3. Change the value of the `ShippedWithReserves` parameter from `1` to `0`.
4. Change the value of `ActiveScenario` to `0`.
5. Disable Reserved Storage in Windows using the following command:

```
DISM.exe /Online /Set-ReservedStorageState /State:Disabled
```

The AMI you are importing has anti-virus or anti-spyware software installed. Remove it and re-import the image.

You must uninstall your antivirus software. Run the BYOLChecker to get details for the antivirus software to uninstall. For more information, see Step 3: Run the BYOL Checker PowerShell script on a Windows VM.

An unknown error has occurred to the AMI you are importing during AMI SysPrep.

SysPrep failure reason couldn't be determined. Contact AWS support at https://aws.amazon.com/support.

Step 4: Export the VM from your virtualization environment

To create an image for BYOL, you must first export the VM from your virtualization environment. The VM must be on a single volume with a maximum size of 70 GB and at least 10 GB of free space. For more information, see the documentation for your virtualization environment and Export Your VM from its Virtualization Environment in the *VM Import/Export User Guide*.

Windows 11 sets new hardware requirements for Unified Extensible Firmware Interface (UEFI), Trusted Platform Module (TPM) 2.0 and Secure Boot support. Unique to Windows 11 imports, VM Import/Export automatically enables UEFI Secure Boot using Microsoft keys and NitroTPM. For more information, see Bringing your Windows 11 image to AWS with VM Import/Export.

Step 5: Import the VM as an image into Amazon EC2

After you export your VM, review the requirements for importing Windows operating systems from a VM. Take action as needed. For more information, see VM Import/Export Requirements.

> **Note**
>
> Importing a VM with an encrypted disk is not supported. If you've opted in to default encryption for Amazon Elastic Block Store (Amazon EBS) volumes, you must deselect that option before importing your VM.

Import your VM into Amazon EC2 as an Amazon Machine Image (AMI). Use one of the following methods:

- Use the **import-image** command with the AWS CLI. For more information, see import-image in the *AWS CLI Command Reference*.
- Use the **ImportImage** API operation. For more information, see ImportImage in the *Amazon EC2 API Reference*.

For more information, see Importing a VM as an Image in the *VM Import/Export User Guide*.

Step 6: Create a BYOL image using the WorkSpaces console

Perform these steps to create an WorkSpaces BYOL image.

> **Note**
>
> To perform this procedure, verify that you have AWS Identity and Access Management (IAM) permissions to:
>
> - Call WorkSpaces **`ImportWorkspaceImage`**.
> - Call Amazon EC2 **`DescribeImages`** on the Amazon EC2 image that you want to use to create the BYOL image.
> - Call Amazon EC2 **`ModifyImageAttribute`** on the Amazon EC2 image that you want to use to create the BYOL image. Make sure that the launch permissions on the Amazon EC2 image are not restricted. The image must be shareable throughout the BYOL image creation process.
>
> For an example IAM policy specific to BYOL WorkSpaces, see Identity and access management for WorkSpaces. For more information about working with IAM permissions, see Changing Permissions for an IAM User in the *IAM User Guide*.
> To create a Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro bundle from your image, contact the AWS Support Center to get your account added to the allow list. After your account is on the allow list, you can use the AWS CLI **import-workspace-image** command to ingest the Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro image. For more information, see import-workspace-image in the *AWS CLI Command Reference*.

To create an image from the Windows VM

1. Open the WorkSpaces console at https://console.aws.amazon.com/workspaces/.

2. In the navigation pane, choose **Images**.
3. Choose **Create BYOL image**.
4. On the **Create BYOL image** page, do the following:

   - For **AMI ID**, choose the **EC2 Console** link, and choose the Amazon EC2 image that you imported as described in the previous section (Step 5: Import the VM as an image into Amazon EC2). The image name must begin with `ami-` and be followed by the identifier for the AMI (for example, `ami-1234567e`).
   - For **Image name**, enter a unique name for the image.
   - For **Description**, enter a description to help you quickly identify the image.
   - For **Instance type**, choose the appropriate bundle type (either **Regular**, **Graphics.g4dn**, **Graphics**, or **GraphicsPro**), depending on which protocol you want to use for your image, either PCoIP or WorkSpaces Streaming Protocol (WSP). If you want to create a GraphicsPro.g4dn bundle, choose **Graphics.g4dn**. For non-GPU-enabled bundles (bundles other than Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro), choose **Regular**.

     > **Note**
     >
     > - GraphicsPro images can be created only for the PCoIP protocol.
     > - Windows 11 images can be created only for the WSP protocol.
     > - Graphics and GraphicsPro Images are not supported for Windows 11.

   - (Optional) For **Select applications**, choose which version of Microsoft Office you want to subscribe to. For more information, see Add Microsoft Office to Your BYOL image.
   - (Optional) For **Tags**, choose **Add new tag** to associate tags with this image. For more information, see Tag resources in WorkSpaces Personal.
5. Choose **Create BYOL image**.

   While your image is being created, the image's status on the **Images** page of the console appears as **Pending**. The BYOL ingestion process takes a minimum of 90 minutes. If you have subscribed to Office as well, expect the process to take a minimum of 3 hours.

   If the image validation does not succeed, the console displays an error code. When the image creation is complete, the status changes to **Available**.

Step 7: Create a custom bundle from the BYOL image

After your BYOL image is created, you can use the image to create a custom bundle. For information, see Create a custom WorkSpaces image and bundle for WorkSpaces Personal.

Step 8: Create a dedicated directory for WorkSpaces

To use BYOL images for WorkSpaces, you must create a directory for this purpose.

To create a directory for WorkSpaces, see Create a directory for WorkSpaces Personal. Ensure you choose **Enable Dedicated WorkSpaces** when creating the directory.

If you've already registered an AWS Managed Microsoft AD directory or an AD Connector directory for WorkSpaces that doesn't run on dedicated hardware, you can set up a new AWS Managed Microsoft AD directory or AD Connector directory for this purpose. You can also deregister the directory and then register it again as a directory for dedicated WorkSpaces. To learn more about registering and deregistering an existing AWS Directory Service directory, see Register an existing AWS Directory Service directory with WorkSpaces Personal.

Step 9: Launch your BYOL WorkSpaces

After you register a directory for dedicated WorkSpaces, you can launch your BYOL WorkSpaces in this directory. You can either launch personal or pooled WorkSpaces.

For information about how to launch WorkSpaces Personal, see Create a WorkSpace in WorkSpaces Personal.

To launch a WorkSpaces Pool, you have to launch a personal WorkSpace, create an image of that personal WorkSpace, then use that image to launch a pool.

To create an image for BYOL WorkSpaces Pools

1. Launch a personal WorkSpace with the BYOL image you want to use for your WorkSpaces Pools. For information about how to launch WorkSpaces Personal, see Create a directory for WorkSpaces Personal.
2. Login in to the personal WorkSpace and make sure all your Windows updates are installed.
3. Update your Amazon EC2 configurations. To update your EC2 configurations using Windows 10, see Install the latest version of EC2Config. To update your EC2 configurations using Windows 11, see Install the latest version of EC2Launch.

4. Add a Windows defender exclusion list. For more information, see Add an exclusion to Windows Security .

   Add the following folders to the exclusion list in Windows Defender:

   - `C:\Program Files\Amazon\*`
   - `C:\ProgramData\Amazon\*`
   - `C:\Program Files\NICE\*`
   - `C:\ProgramData\NICE\*`
   - `C:\Program Files (x86)\AWS Tools\*`
   - `C:\Program Files (x86)\AWS SDK for .NET\*`
   - `C:\AWSEUC\*` (This is for the session script)

5. Disable Windows update on startup by entering the following command.

```
Open powershell as admin-
Run following command -

New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" -Force
New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Force
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU"
 -Name "NoAutoUpdate" -Value 1 -Force
```

6. Reboot the WorkSpace. For more information, see Reboot a WorkSpace in WorkSpaces Personal.

   Note

   We recommend doing the following before you begin creating an image for BYOL WorkSpaces Pools

   - Remove unnecessary startup applications.
   - Remove or disable unnecessary scheduled tasks. Open the start menu, choose **Scheduled tasks**, select the tasks you want to disable and then choose **Disable**.

7. Run image checker after the reboot by entering the following command.

```
C:\Program Files\Amazon\ImageChecker.exe
```

For more information on creating a custom WorkSpaces image, see Create a custom WorkSpaces image and bundle for WorkSpaces Personal.

8. Resolve any errors found by the image checker. For more information, see Tips for resolving issues detected by the Image Checker.
9. After all tests have passed the image checker, go back to the WorkSpaces console.
10. In the navigation pane, under WorkSpaces, choose **Personal**. Choose the BYOL personal WorkSpaces, then choose **Actions**, **Create image**.
11. In the navigation pane, choose **Images**. Under **Images**, check if the image is created.

You can now launch WorkSpaces Pools with the image you created. For more information about launching WorkSpaces Pools, see Create a WorkSpaces Pool.

Link BYOL accounts

You can use BYOL linking to link accounts and share BYOL configurations. BYOL configurations include the CIDR range used by your accounts and the images you use to create WorkSpaces with your Windows license. All accounts that are linked share the same underlying hardware infrastructure.

The account enabled for BYOL linking is the primary owner of the underlying hardware infrastructure, and is called the Source account. The Source account manages access to the underlying hardware infrastructure. Target accounts are the accounts that are linked to the Source account.

Important

APIs for BYOL account linking are not available in the AWS GovCloud (US) Region.

Note

The AWS accounts that you want to link with must be part of your organization and under the same payer account. You can only link accounts within the same Region.

To link the Source and Target accounts

1. Send an invitation link from your Source account to the Target account by using the **CreateAccountLinkInvitation** API.
2. Accept the pending link from your Target account by using the **AcceptAccountLinkInvitation** API.
3. Verify the link has been established by using the **GetAccountLink** or **ListAccountLinks** API.

Security in Amazon WorkSpaces

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to WorkSpaces, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations

This documentation helps you understand how to apply the shared responsibility model when using WorkSpaces. It shows you how to configure WorkSpaces to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your WorkSpaces resources.

Contents

Data protection in Amazon WorkSpaces

The AWS shared responsibility model applies to data protection in Amazon WorkSpaces. As described in this model, AWS is responsible for protecting the global infrastructure that runs all

of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail. For information about using CloudTrail trails to capture AWS activities, see Working with CloudTrail trails in the *AWS CloudTrail User Guide*.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-3 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-3.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with WorkSpaces or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

For more information about WorkSpaces and FIPS endpoint encryption, see Configure FedRAMP authorization or DoD SRG compliance for WorkSpaces Personal.

Encryption at rest

You can encrypt the storage volumes for your WorkSpaces using AWS KMS Key from AWS Key Management Service. For more information, see Encrypted WorkSpaces in WorkSpaces Personal.

When you create WorkSpaces with encrypted volumes, WorkSpaces uses Amazon Elastic Block Store (Amazon EBS) to create and manage those volumes. EBS encrypts your volumes with a data key using the industry-standard AES-256 algorithm. For more information, see Amazon EBS Encryption in the *Amazon EC2 User Guide*.

Encryption in transit

For PCoIP, data in-transit is encrypted using TLS 1.2 encryption and SigV4 request signing. The PCoIP protocol uses encrypted UDP traffic, with AES encryption, for streaming pixels.The streaming connection, using port 4172 (TCP and UDP), is encrypted by using AES-128 and AES-256 ciphers, but the encryption defaults to 128-bit. You can change this default to 256-bit, either by using the **Configure PCoIP Security Settings** Group Policy setting for Windows WorkSpaces, or by modifying the **PCoIP Security Settings** in the `pcoip-agent.conf` file for Amazon Linux WorkSpaces.

To learn more about Group Policy administration for Amazon WorkSpaces, see Configure PCoIP security settings in Manage your Windows WorkSpaces in WorkSpaces Personal. To learn more about modifying the `pcoip-agent.conf` file, see Control PCoIP Agent behavior on Amazon Linux WorkSpaces and PCoIP Security Settings in the Teradici documentation.

For WorkSpaces Streaming Protocol (WSP), streaming and control data in-transit is encrypted using TLS 1.3 encryption for UDP traffic and TLS 1.2 encryption for TCP traffic, with AES-256 ciphers.

Identity and access management for WorkSpaces

By default, IAM users don't have permissions for WorkSpaces resources and operations. To allow IAM users to manage WorkSpaces resources, you must create an IAM policy that explicitly grants them permissions, and attach the policy to the IAM users or groups that require those permissions.

> **Note**
>
> Amazon WorkSpaces doesn’t support the provisioning of IAM credentials into a WorkSpace (such as with an instance profile).

To provide access, add permissions to your users, groups, or roles:

- Users and groups in AWS IAM Identity Center:

Create a permission set. Follow the instructions in Create a permission set in the *AWS IAM Identity Center User Guide*.

- Users managed in IAM through an identity provider:

  Create a role for identity federation. Follow the instructions in Creating a role for a third-party identity provider (federation) in the *IAM User Guide*.

- IAM users:
  - Create a role that your user can assume. Follow the instructions in Creating a role for an IAM user in the *IAM User Guide*.
  - (Not recommended) Attach a policy directly to a user or add a user to a user group. Follow the instructions in Adding permissions to a user (console) in the *IAM User Guide*.

Following are additional resources for IAM:

- For more information about IAM policies, see Policies and Permissions in the *IAM User Guide* guide.
- For more information about IAM, see Identity and Access Management (IAM) and the *IAM User Guide*.
- For more information about WorkSpaces-specific resources, actions, and condition context keys for use in IAM permission policies, see Actions, Resources, and Condition Keys for Amazon WorkSpaces in the *IAM User Guide*.
- For a tool that helps you create IAM policies, see the AWS Policy Generator. You can also use the IAM Policy Simulator to test whether a policy would allow or deny a specific request to AWS.

Contents

Example policies

The following examples show policy statements that you could use to control the permissions that IAM users have to Amazon WorkSpaces.

Example 1: Grant access to perform WorkSpaces personal and pools tasks

The following policy statement grants an IAM user permission to perform WorkSpaces personal and pools tasks.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "workspaces:*",
                "application-autoscaling:DeleteScalingPolicy",
                "application-autoscaling:DeleteScheduledAction",
                "application-autoscaling:DeregisterScalableTarget",
                "application-autoscaling:DescribeScalableTargets",
                "application-autoscaling:DescribeScalingActivities",
                "application-autoscaling:DescribeScalingPolicies",
                "application-autoscaling:DescribeScheduledActions",
                "application-autoscaling:PutScalingPolicy",
                "application-autoscaling:PutScheduledAction",
                "application-autoscaling:RegisterScalableTarget",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateInternetGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVpc",
```

```
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreateRole",
                "iam:GetRole",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "kms:ListAliases",
                "kms:ListKeys",
                "secretsmanager:ListSecrets",
                "tag:GetResources",
                "workdocs:AddUserToGroup",
                "workdocs:DeregisterDirectory",
                "workdocs:RegisterDirectory",
                "sso-directory:SearchUsers",
                "sso:CreateApplication",
                "sso:DeleteApplication",
                "sso:DescribeApplication",
                "sso:DescribeInstance",
                "sso:GetApplicationGrant",
                "sso:ListInstances",
                "sso:PutApplicationAssignment",
                "sso:PutApplicationAssignmentConfiguration",
                "sso:PutApplicationAuthenticationMethod",
                "sso:PutApplicationGrant"
            ],
            "Resource": "*"
        },
        {
            "Sid": "iamPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
```

```
                "StringEquals": {
                    "iam:PassedToService": "workspaces.amazonaws.com"
                }
            }
        }
    ]
}
```

Example 2: Grant access to perform WorkSpaces Personal tasks

The following policy statement grants an IAM user permission to perform all WorkSpaces Personal tasks.

Although Amazon WorkSpaces fully supports the `Action` and `Resource` elements when using the API and command line tools, to use Amazon WorkSpaces from the AWS Management Console, an IAM user must have permissions for the following actions and resources:

- Actions: `"workspaces:*"` and `"ds:*"`
- Resources: `"Resource": "*"`

The following example policy shows how to allow an IAM user to use Amazon WorkSpaces from the AWS Management Console.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
```

```
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup",
        "secretsmanager:ListSecrets",
        "sso-directory:SearchUsers",
        "sso:CreateApplication",
        "sso:DeleteApplication",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:GetApplicationGrant",
        "sso:ListInstances",
        "sso:PutApplicationAssignment",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
```

```
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

Example 3: Grant access to perform WorkSpaces Pools tasks

The following policy statement grants an IAM user permission to perform all WorkSpaces Pools tasks.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "workspaces:*",
                "application-autoscaling:DeleteScalingPolicy",
                "application-autoscaling:DeleteScheduledAction",
                "application-autoscaling:DeregisterScalableTarget",
                "application-autoscaling:DescribeScalableTargets",
                "application-autoscaling:DescribeScalingActivities",
                "application-autoscaling:DescribeScalingPolicies",
                "application-autoscaling:DescribeScheduledActions",
                "application-autoscaling:PutScalingPolicy",
                "application-autoscaling:PutScheduledAction",
                "application-autoscaling:RegisterScalableTarget",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
```

```
                "iam:CreateRole",
                "iam:GetRole",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "secretsmanager:ListSecrets",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "iamPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "workspaces.amazonaws.com"
                }
            }
        }
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/aws-service-role/workspaces.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_WorkSpacesPool",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "workspaces.application-
autoscaling.amazonaws.com"
                }
            }
        }
    ]
}
```

Example 4: Perform all WorkSpaces tasks for BYOL WorkSpaces

The following policy statement grants an IAM user permission to perform all WorkSpaces tasks, including those Amazon EC2 tasks necessary for creating Bring Your Own License (BYOL) WorkSpaces.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "workspaces:*",
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateInternetGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVpc",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:ModifyImageAttribute",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "iam:CreateRole",
                "iam:GetRole",
                "iam:PutRolePolicy",
                "kms:ListAliases",
                "kms:ListKeys",
                "workdocs:AddUserToGroup",
                "workdocs:DeregisterDirectory",
                "workdocs:RegisterDirectory"
            ],
            "Resource": "*"
        },
        {
            "Sid": "iamPassRole",
```

```
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "workspaces.amazonaws.com"
                }
            }
        }
    ]
}
```

Specify WorkSpaces resources in an IAM policy

To specify an WorkSpaces resource in the `Resource` element of the policy statement, use the Amazon Resource Name (ARN) of the resource. You control access to your WorkSpaces resources by either allowing or denying permissions to use the API actions that are specified in the `Action` element of your IAM policy statement. WorkSpaces defines ARNs for WorkSpaces, bundles, IP groups, and directories.

WorkSpace ARN

A WorkSpace ARN has the syntax shown in the following example.

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

region

The Region that the WorkSpace is in (for example, `us-east-1`).

account_id

The ID of the AWS account, with no hyphens (for example, `123456789012`).

workspace_identifier

The ID of the WorkSpace (for example, `ws-a1bcd2efg`).

The following is the format of the `Resource` element of a policy statement that identifies a specific WorkSpace.

```
"Resource": "arn:aws:workspaces:region:account_id:workspace/workspace_identifier"
```

You can use the * wildcard to specify all WorkSpaces that belong to a specific account in a specific Region.

WorkSpace pool ARN

A WorkSpace pool ARN has the syntax shown in the following example.

```
arn:aws:workspaces:region:account_id:workspacespool/workspacespool_identifier
```

region

The Region that the WorkSpace is in (for example, `us-east-1`).

account_id

The ID of the AWS account, with no hyphens (for example, `123456789012`).

workspacespool_identifier

The ID of the WorkSpace pool (for example, `ws-a1bcd2efg`).

The following is the format of the `Resource` element of a policy statement that identifies a specific WorkSpace.

```
"Resource":
 "arn:aws:workspaces:region:account_id:workspacespool/workspacespool_identifier"
```

You can use the * wildcard to specify all WorkSpaces that belong to a specific account in a specific Region.

Image ARN

A WorkSpace image ARN has the syntax shown in the following example.

```
arn:aws:workspaces:region:account_id:workspaceimage/image_identifier
```

region

The Region that the WorkSpace image is in (for example, `us-east-1`).

account_id

The ID of the AWS account, with no hyphens (for example, `123456789012`).

bundle_identifier

The ID of the WorkSpace image (for example, `wsi-a1bcd2efg`).

The following is the format of the `Resource` element of a policy statement that identifies a specific image.

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceimage/image_identifier"
```

You can use the * wildcard to specify all images that belong to a specific account in a specific Region.

Bundle ARN

A bundle ARN has the syntax shown in the following example.

```
arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier
```

region

The Region that the WorkSpace is in (for example, `us-east-1`).

account_id

The ID of the AWS account, with no hyphens (for example, `123456789012`).

bundle_identifier

The ID of the WorkSpace bundle (for example, `wsb-a1bcd2efg`).

The following is the format of the `Resource` element of a policy statement that identifies a specific bundle.

```
"Resource": "arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier"
```

You can use the * wildcard to specify all bundles that belong to a specific account in a specific Region.

IP Group ARN

An IP group ARN has the syntax shown in the following example.

```
arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier
```

region

The Region that the WorkSpace is in (for example, `us-east-1`).

account_id

The ID of the AWS account, with no hyphens (for example, `123456789012`).

ipgroup_identifier

The ID of the IP group (for example, `wsipg-a1bcd2efg`).

The following is the format of the `Resource` element of a policy statement that identifies a specific IP group.

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier"
```

You can use the * wildcard to specify all IP groups that belong to a specific account in a specific Region.

Directory ARN

A directory ARN has the syntax shown in the following example.

```
arn:aws:workspaces:region:account_id:directory/directory_identifier
```

region

The Region that the WorkSpace is in (for example, `us-east-1`).

account_id

The ID of the AWS account, with no hyphens (for example, `123456789012`).

directory_identifier

The ID of the directory (for example, `d-12345a67b8`).

The following is the format of the `Resource` element of a policy statement that identifies a specific directory.

```
"Resource": "arn:aws:workspaces:region:account_id:directory/directory_identifier"
```

You can use the * wildcard to specify all directories that belong to a specific account in a specific Region.

Connection alias ARN

A connection alias ARN has the syntax shown in the following example.

```
arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier
```

region

The Region that the connection alias is in (for example, `us-east-1`).

account_id

The ID of the AWS account, with no hyphens (for example, `123456789012`).

connectionalias_identifier

The ID of the connection alias (for example, `wsca-12345a67b8`).

The following is the format of the `Resource` element of a policy statement that identifies a specific connection alias.

```
"Resource":
 "arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier"
```

You can use the * wildcard to specify all connection aliases that belong to a specific account in a specific Region.

API actions with no support for resource-level permissions

You can't specify a resource ARN with the following API actions:

- `AssociateIpGroups`
- `CreateIpGroup`
- `CreateTags`
- `DeleteTags`

- DeleteWorkspaceImage
- DescribeAccount
- DescribeAccountModifications
- DescribeIpGroups
- DescribeTags
- DescribeWorkspaceDirectories
- DescribeWorkspaceImages
- DescribeWorkspaces
- DescribeWorkspacesConnectionStatus
- DisassociateIpGroups
- ImportWorkspaceImage
- ListAvailableManagementCidrRanges
- ModifyAccount

For API actions that don't support resource-level permissions, you must specify the resource statement shown in the following example.

```
"Resource": "*"
```

API actions that don't support account-level restrictions on shared resources

For the following API actions, you can't specify an account ID in the resource ARN when the resource isn't owned by the account:

- AssociateConnectionAlias
- CopyWorkspaceImage
- DisassociateConnectionAlias

For these API actions, you can specify an account ID in the resource ARN only when that account owns the resources to be acted upon. When the account doesn't own the resources, you must specify * for the account ID, as shown in the following example.

```
"arn:aws:workspaces:region:*:resource_type/resource_identifier"
```

Create the workspaces_DefaultRole Role

Before you can register a directory using the API, you must verify that a role named `workspaces_DefaultRole` exists. This role is created by the Quick Setup or if you launch a WorkSpace using the AWS Management Console, and it grants Amazon WorkSpaces permission to access specific AWS resources on your behalf. If this role does not exist, you can create it using the following procedure.

To create the workspaces_DefaultRole role

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane on the left, choose **Roles**.
3. Choose **Create role**.
4. Under **Select type of trusted entity**, choose **Another AWS account**.
5. For **Account ID**, enter your account ID with no hyphens or spaces.
6. For **Options**, do not specify multi-factor authentication (MFA).
7. Choose **Next: Permissions**.
8. On the **Attach permissions policies** page, select the AWS managed policies **AmazonWorkSpacesServiceAccess**, **AmazonWorkSpacesSelfServiceAccess**, and **AmazonWorkSpacesPoolServiceAccess**. For more information about these managed policies, see AWS managed policies for WorkSpaces.
9. Under **Set permissions boundary**, we recommend that you not use a permissions boundary because of the potential for conflicts with the policies that are attached to this role. Such conflicts could block certain necessary permissions for the role.
10. Choose **Next: Tags**.
11. On the **Add tags (optional)** page, add tags if needed.
12. Choose **Next: Review**.
13. On the **Review** page, for **Role name**, enter **`workspaces_DefaultRole`**.
14. (Optional) For **Role description**, enter a description.
15. Choose **Create Role**.
16. On the **Summary** page for the workspaces_DefaultRole role, choose the **Trust relationships** tab.

17. On the **Trust relationships** tab, choose **Edit trust relationship**.
18. On the **Edit Trust Relationship** page, replace the existing policy statement with the following statement.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

19. Choose **Update Trust Policy**.

Create the AmazonWorkSpacesPCAAccess service role

Before users can login using certificate-based authentication, you must verify that a role named `AmazonWorkSpacesPCAAccess` exists. This role is created when you enable certificate-based authentication on a Directory using the AWS Management Console, and it grants Amazon WorkSpaces permission to access AWS Private CA resources on your behalf. If this role does not exist because you are not using the console to manage certificate-based authentication, you can create it using the following procedure.

To create the AmazonWorkSpacesPCAAccess service role using the AWS CLI

1. Create a JSON file named `AmazonWorkSpacesPCAAccess.json` with the following text.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "prod.euc.ecm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
```

```
    ]
}
```

2. Adjust the `AmazonWorkSpacesPCAAccess.json` path as needed and run the following AWS CLI commands to create the service role and attach the AmazonWorkspacesPCAAccess managed policy.

```
aws iam create-role --path /service-role/ --role-name AmazonWorkSpacesPCAAccess --
assume-role-policy-document file://AmazonWorkSpacesPCAAccess.json
```

```
aws iam attach-role-policy –role-name AmazonWorkSpacesPCAAccess –policy-arn
 arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess
```

AWS managed policies for WorkSpaces

Using AWS managed policies makes adding permissions to users, groups, and roles easier than writing policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. Use AWS managed policies to get started quickly. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services may occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services don't remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the `ReadOnlyAccess` AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the *IAM User Guide*.

AWS managed policy: AmazonWorkSpacesAdmin

This policy provides access to Amazon WorkSpaces administrative actions. It provides the following permissions:

- `workspaces` - Allows access to perform administrative actions on WorkSpaces Personal and WorkSpaces Pools resources.
- `kms` - Allows access to list and describe KMS keys, as well as list aliases.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonWorkSpacesAdmin",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeys",
                "workspaces:CreateTags",
                "workspaces:CreateWorkspaceImage",
                "workspaces:CreateWorkspaces",
                "workspaces:CreateWorkspacesPool",
                "workspaces:CreateStandbyWorkspaces",
                "workspaces:DeleteTags",
                "workspaces:DeregisterWorkspaceDirectory",
                "workspaces:DescribeTags",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspacesPools",
                "workspaces:DescribeWorkspacesPoolSessions",
                "workspaces:DescribeWorkspacesConnectionStatus",
                "workspaces:ModifyCertificateBasedAuthProperties",
                "workspaces:ModifySamlProperties",
                "workspaces:ModifyStreamingProperties",
                "workspaces:ModifyWorkspaceCreationProperties",
                "workspaces:ModifyWorkspaceProperties",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:RegisterWorkspaceDirectory",
                "workspaces:RestoreWorkspace",
                "workspaces:StartWorkspaces",
                "workspaces:StartWorkspacesPool",
                "workspaces:StopWorkspaces",
                "workspaces:StopWorkspacesPool",
                "workspaces:TerminateWorkspaces",
```

```
                "workspaces:TerminateWorkspacesPool",
                "workspaces:TerminateWorkspacesPoolSession",
                "workspaces:UpdateWorkspacesPool"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS managed policy: AmazonWorkspacesPCAAccess

This managed policy provides access to AWS Certificate Manager Private Certificate Authority (Private CA) resources in your AWS account for certificate-based authentication. It is included in the AmazonWorkSpacesPCAAccess role, and it provides the following permissions:

- `acm-pca` - Allows access to AWS Private CA to manage certificate-based authentication.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "acm-pca:IssueCertificate",
                "acm-pca:GetCertificate",
                "acm-pca:DescribeCertificateAuthority"
            ],
            "Resource": "arn:*:acm-pca:*:*:*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/euc-private-ca": "*"
                }
            }
        }
    ]
}
```

AWS managed policy: AmazonWorkSpacesSelfServiceAccess

This policy provides access to the Amazon WorkSpaces service to perform WorkSpaces self-service actions initiated by a user. It is included in the `workspaces_DefaultRole` role, and it provides the following permissions:

- `workspaces` - Allows access to self-service WorkSpaces management capabilities for users.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:ModifyWorkspaceProperties"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS managed policy: AmazonWorkSpacesServiceAccess

This policy provides customer account access to the Amazon WorkSpaces service for launching a WorkSpace. It is included in the `workspaces_DefaultRole` role, and it provides the following permissions:

- `ec2` - Allows access to manage Amazon EC2 resources associated with a WorkSpace, such as network interfaces.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS managed policy: AmazonWorkSpacesPoolServiceAccess

This policy is used in the workspaces_DefaultRole, which WorkSpaces uses to access required resources in the customer AWS account for WorkSpaces Pools. For more information see Create the workspaces_DefaultRole Role. It provides the following permissions:

- `ec2` - Allows access to manage Amazon EC2 resources associated with a WorkSpaces Pool, such as VPCs, subnets, availability zones, security groups, and route tables.
- `s3` - Allows access to perform actions on Amazon S3 buckets required for logs, application settings, and the Home Folder feature.

Commercial AWS Regions

The following policy JSON applies to the commercial AWS Regions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ProvisioningWorkSpacesPoolPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRouteTables",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
```

```
            }
        },
        {
            "Sid": "WorkSpacesPoolS3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:GetObjectVersion",
                "s3:DeleteObjectVersion",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::wspool-logs-*",
                "arn:aws:s3:::wspool-app-settings-*",
                "arn:aws:s3:::wspool-home-folder-*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        }
    ]
}
```

AWS GovCloud (US) Regions

The following policy JSON applies to the commercial AWS GovCloud (US) Regions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ProvisioningWorkSpacesPoolPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRouteTables",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "WorkSpacesPoolS3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:GetObjectVersion",
                "s3:DeleteObjectVersion",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::wspool-logs-*",
                "arn:aws-us-gov:s3:::wspool-app-settings-*",
                "arn:aws-us-gov:s3:::wspool-home-folder-*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        }
    ]
}
```

WorkSpaces updates to AWS managed policies

View details about updates to AWS managed policies for WorkSpaces since this service began tracking these changes.

Change	Description	Date
the section called "AmazonWorkSpacesPoolServiceAcces" - Added new policy	WorkSpaces added a new managed policy to grant permission to view Amazon EC2 VPCs and related resources, and to view and manage Amazon S3 buckets for WorkSpaces Pools.	June 24, 2024
the section called "AmazonWorkSpacesAdmin" - Updated policy	WorkSpaces added several actions for WorkSpaces Pools to the Amazon WorkSpaceAdmin managed policy, granting admins access to manage WorkSpace Pool resources.	June 24, 2024
the section called "AmazonWorkSpacesAdmin" - Updated policy	WorkSpaces added the `workspaces:RestoreWorkspace` action to the Amazon WorkSpacesAdmin managed policy, granting admins access to restore WorkSpaces.	June 25, 2023
the section called "AmazonWorkspacesPCAAccess" - Added new policy	WorkSpaces added a new managed policy to grant `acm-pca` permission to manage AWS Private CA to manage certificate-based authentication.	November 18, 2022

Change	Description	Date
WorkSpaces started tracking changes	WorkSpaces started tracking changes for its WorkSpaces managed policies.	March 1, 2021

Access to WorkSpaces and scripts on streaming instances

Applications and scripts that run on WorkSpaces streaming instances must include AWS credentials in their AWS API requests. You can create an IAM role to manage these credentials. An IAM role specifies a set of permissions that you can use to access AWS resources. This role is not uniquely associated with one person, however. Instead, it can be assumed by anyone that needs it.

You can apply an IAM role to a WorkSpaces streaming instance. When the streaming instance switches to (assumes) the role, the role provides temporary security credentials. Your application or scripts use these credentials to perform API actions and management tasks on the streaming instance. WorkSpaces manages the temporary credential switch for you.

Contents

Best Practices for Using IAM Roles With WorkSpaces Streaming Instances

When you use IAM roles with WorkSpaces streaming instances, we recommend that you follow these practices:

- Limit the permissions that you grant to AWS API actions and resources.

  Follow least privilege principles when you create and attach IAM policies to the IAM roles associated with WorkSpaces streaming instances. When you use an application or script that requires access to AWS API actions or resources, determine the specific actions and resources that are required. Then, create policies that allow the application or script to perform only those actions. For more information, see Grant Least Privilege in the *IAM User Guide*.

- Create an IAM role for each WorkSpaces resource.

  Creating a unique IAM role for each WorkSpaces resource is a practice that follows least privilege principles. Doing so also lets you modify permissions for a resource without affecting other resources.

- Limit where the credentials can be used.

  IAM policies let you define the conditions under which your IAM role can be used to access a resource. For example, you can include conditions to specify a range of IP addresses that requests can come from. Doing so prevents the credentials from being used outside of your environment. For more information, see Use Policy Conditions for Extra Security in the *IAM User Guide*.

Configuring an Existing IAM Role to Use With WorkSpaces Streaming Instances

This topic describes how to configure an existing IAM role so that you can use it with WorkSpaces .

Prerequisites

The IAM role that you want to use with WorkSpaces must meet the following prerequisites:

- The IAM role must be in the same Amazon Web Services account as the WorkSpaces streaming instance.
- The IAM role cannot be a service role.
- The trust relationship policy that is attached to the IAM role must include the WorkSpaces service as the principal. A *principal* is an entity in AWS that can perform actions and access resources. The policy must also include the `sts:AssumeRole` action. This policy configuration defines WorkSpaces as a trusted entity.

- If you are applying the IAM role to WorkSpaces, the WorkSpaces must run a version of the WorkSpaces agent released on or after September 3, 2019. If you are applying the IAM role to WorkSpaces, the WorkSpaces must use an image that uses a version of the agent released on or after the same date.

To enable the WorkSpaces service principal to assume an existing IAM role

To perform the following steps, you must sign into the account as an IAM user who has the permissions required to list and update IAM roles. If you don't have the required permissions, ask

your Amazon Web Services account administrator either to perform these steps in your account or to grant you the required permissions.

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Roles**.
3. In the list of roles in your account, choose the name of the role that you want to modify.
4. Choose the **Trust relationships** tab, and then choose **Edit trust relationship**.
5. Under **Policy Document**, verify that the trust relationship policy includes the `sts:AssumeRole` action for the `workspaces.amazonaws.com` service principal:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "workspaces.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

6. When you are finished editing your trust policy, choose **Update Trust Policy** to save your changes.
7. The IAM role that you selected will display in the WorkSpaces console. This role grants permissions to applications and scripts to perform API actions and management tasks on streaming instances.

How to Create an IAM Role to Use With WorkSpaces Streaming Instances

This topic describes how to create a new IAM role so that you can use it with WorkSpaces

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Roles**, and then choose **Create role**.
3. For **Select type of trusted entity**, choose **AWS service**.

4. From the list of AWS services, choose **WorkSpaces**.
5. Under **Select your use case**, **WorkSpaces — Allows WorkSpaces instances to call AWS services on your behalf** is already selected. Choose **Next: Permissions**.
6. If possible, select the policy to use for the permissions policy or choose **Create policy** to open a new browser tab and create a new policy from scratch. For more information, see step 4 in the procedure Creating IAM Policies (Console) in the *IAM User Guide*.

   After you create the policy, close that tab and return to your original tab. Select the check box next to the permissions policies that you want WorkSpaces to have.
7. (Optional) Set a permissions boundary. This is an advanced feature that is available for service roles, but not service-linked roles. For more information, see Permissions Boundaries for IAM Entities in the *IAM User Guide*.
8. Choose **Next: Tags**. You can optionally attach tags as key-value pairs. For more information, see Tagging IAM Users and Roles in the *IAM User Guide*.
9. Choose **Next: Review**.
10. For **Role name**, type a role name that is unique within your Amazon Web Services account. Because other AWS resources might reference the role, you can't edit the name of the role after it has been created.
11. For **Role description**, keep the default role description or type a new one.
12. Review the role, and then choose **Create role**.

How to Use the IAM Role With WorkSpaces Streaming Instances

After you create an IAM role, you can apply it to WorkSpaces when you launch WorkSpaces. You can also apply an IAM role to existing WorkSpaces.

When you apply an IAM role to WorkSpaces, WorkSpaces retrieves temporary credentials and creates the **workspaces_machine_role** credential profile on the instance. The temporary credentials are valid for 1 hour, and new credentials retrieved every hour. The previous credentials do not expire, so you can use them for as long as they are valid. You can use the credential profile to call AWS services programmatically by using the AWS Command Line Interface (AWS CLI), AWS Tools for PowerShell, or the AWS SDK with the language of your choice.

When you make the API calls, specify **workspaces_machine_role** as the credential profile. Otherwise, the operation fails due to insufficient permissions.

WorkSpaces assumes the specified role while the streaming instance is provisioned. Because WorkSpaces uses the elastic network interface that is attached to your VPC for AWS API calls, your application or script must wait for the elastic network interface to become available before making AWS API calls. If API calls are made before the elastic network interface is available, the calls fail.

The following examples show how you can use the **workspaces_machine_role** credential profile to describe streaming instances (EC2 instances) and to create the Boto client. Boto is the Amazon Web Services (AWS) SDK for Python.

Describe Streaming Instances (EC2 instances) by Using the AWS CLI

```
aws ec2 describe-instances --region us-east-1 --profile workspaces_machine_role
```

Describe Streaming Instances (EC2 instances) by Using AWS Tools for PowerShell

You must use AWS Tools for PowerShell version 3.3.563.1 or later, with the Amazon Web Services SDK for .NET version 3.3.103.22 or later. You can download the AWS Tools for Windows installer, which includes AWS Tools for PowerShell and the Amazon Web Services SDK for .NET, from the AWS Tools for PowerShell website.

```
Get-EC2Instance -Region us-east-1 -ProfileName workspaces_machine_role
```

Creating the Boto Client by Using the AWS SDK for Python

```
session = boto3.Session(profile_name=workspaces_machine_role')
```

Compliance validation for Amazon WorkSpaces

Third-party auditors assess the security and compliance of Amazon WorkSpaces as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

For more information about WorkSpaces and FedRAMP, see Configure FedRAMP authorization or DoD SRG compliance for WorkSpaces Personal.

Your compliance responsibility when using WorkSpaces is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- Evaluating Resources with Rules in the *AWS Config Developer Guide* – AWS Config; assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Resilience in Amazon WorkSpaces

The AWS global infrastructure is built around AWS Regions and Availability Zones. Regions provide multiple physically separated and isolated Availability Zones, which are connected through low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

Amazon WorkSpaces also provides cross-Region redirection, a feature that works with your Domain Name System (DNS) failover routing policies to redirect your WorkSpaces users to alternative WorkSpaces in another AWS Region when their primary WorkSpaces aren't available. For more information, see Cross-Region redirection for WorkSpaces Personal.

Infrastructure security in Amazon WorkSpaces

As a managed service, Amazon WorkSpaces is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see AWS Cloud

Security. To design your AWS environment using the best practices for infrastructure security, see Infrastructure Protection in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access WorkSpaces through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

Network isolation

A virtual private cloud (VPC) is a virtual network in your own logically isolated area in the AWS Cloud. You can deploy your WorkSpaces in a private subnet in your VPC. For more information, see Configure a VPC for WorkSpaces Personal.

To allow traffic only from specific address ranges (for example, from your corporate network), update the security group for your VPC or use an IP access control group.

You can restrict WorkSpace access to trusted devices with valid certificates. For more information, see Restrict access to trusted devices for WorkSpaces Personal.

Isolation on physical hosts

Different WorkSpaces on the same physical host are isolated from each other through the hypervisor. It is as though they are on separate physical hosts. When a WorkSpace is deleted, the memory allocated to it is scrubbed (set to zero) by the hypervisor before it is allocated to a new WorkSpace.

Authorization of corporate users

With WorkSpaces, directories are managed through the AWS Directory Service. You can create a standalone, managed directory for users. Or you can integrate with your existing Active Directory

environment so that your users can use their current credentials to obtain seamless access to corporate resources. For more information, see Manage directories for WorkSpaces Personal.

To further control access to your WorkSpaces, use multi-factor authentication. For more information, see How to Enable Multi-Factor Authentication for AWS Services.

Make Amazon WorkSpaces API requests through a VPC interface endpoint

You can connect directly to Amazon WorkSpaces API endpoints through an interface endpoint in your virtual private cloud (VPC) instead of connecting over the internet. When you use a VPC interface endpoint, communication between your VPC and the Amazon WorkSpaces API endpoint is conducted entirely and securely within the AWS network.

> **Note**
>
> This feature can be used only for connecting to WorkSpaces API endpoints. To connect to WorkSpaces using the WorkSpaces clients, internet connectivity is required, as described in IP address and port requirements for WorkSpaces Personal.

The Amazon WorkSpaces API endpoints support Amazon Virtual Private Cloud (Amazon VPC) interface endpoints that are powered by AWS PrivateLink. Each VPC endpoint is represented by one or more network interfaces (also known as elastic network interfaces, or ENIs) with private IP addresses in your VPC subnets.

The VPC interface endpoint connects your VPC directly to the Amazon WorkSpaces API endpoint without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. The instances in your VPC don't need public IP addresses to communicate with the Amazon WorkSpaces API endpoint.

You can create an interface endpoint to connect to Amazon WorkSpaces with either the AWS Management Console or AWS Command Line Interface (AWS CLI) commands. For instructions, see Creating an Interface Endpoint.

After you have created a VPC endpoint, you can use the following example CLI commands that use the `endpoint-url` parameter to specify interface endpoints to the Amazon WorkSpaces API endpoint:

```
aws workspaces copy-workspace-image --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com

aws workspaces delete-workspace-image --endpoint-
url VPC_Endpoint_ID.api.workspaces.Region.vpce.amazonaws.com

aws workspaces describe-workspace-bundles --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com  \
   --endpoint-name Endpoint_Name \
   --body "Endpoint_Body" \
   --content-type "Content_Type" \
       Output_File
```

If you enable private DNS hostnames for your VPC endpoint, you don't need to specify the endpoint URL. The Amazon WorkSpaces API DNS hostname that the CLI and Amazon WorkSpaces SDK use by default (https://api.workspaces.*Region*.amazonaws.com) resolves to your VPC endpoint.

The Amazon WorkSpaces API endpoint supports VPC endpoints in all AWS Regions where both Amazon VPC and Amazon WorkSpaces are available. Amazon WorkSpaces supports making calls to all of its public APIs inside your VPC.

To learn more about AWS PrivateLink, see the AWS PrivateLink documentation. For the price of VPC endpoints, see VPC Pricing. To learn more about VPC and endpoints, see Amazon VPC.

To see a list of Amazon WorkSpaces API endpoints by Region, see WorkSpaces API Endpoints.

> **Note**
>
> Amazon WorkSpaces API endpoints with AWS PrivateLink are not supported for Federal Information Processing Standard (FIPS) Amazon WorkSpaces API endpoints.

Create a VPC endpoint policy for Amazon WorkSpaces

You can create a policy for Amazon VPC endpoints for Amazon WorkSpaces to specify the following:

- The principal that can perform actions.
- The actions that can be performed.

- The resources on which actions can be performed.

For more information, see Controlling Access to Services with VPC Endpoints in the *Amazon VPC User Guide*.

> **Note**
>
> VPC endpoint policies aren't supported for Federal Information Processing Standard (FIPS) Amazon WorkSpaces endpoints.

The following example VPC endpoint policy specifies that all users who have access to the VPC interface endpoint are allowed to invoke the Amazon WorkSpaces hosted endpoint named `ws-f9abcdefg`.

```
{
     "Statement": [
         {
             "Action": "workspaces:*",
             "Effect": "Allow",
             "Resource": "arn:aws:workspaces:us-west-2:1234567891011:workspace/ws-
f9abcdefg",
             "Principal": "*"
         }
     ]
}
```

In this example, the following actions are denied:

- Invoking Amazon WorkSpaces hosted endpoints other than `ws-f9abcdefg`.
- Performing an action on any resource besides the one specified (WorkSpace ID: `ws-f9abcdefg`).

> **Note**
>
> In this example, users can still take other Amazon WorkSpaces API actions from outside the VPC. To restrict API calls to those from within the VPC, see Identity and access management for WorkSpaces for information about using identity-based policies to control access to Amazon WorkSpaces API endpoints.

Connect your private network to your VPC

To call the Amazon WorkSpaces API through your VPC, you have to connect from an instance that is inside the VPC, or connect your private network to your VPC by using AWS Virtual Private Network (AWS VPN) or AWS Direct Connect. For information, see VPN Connections in the *Amazon Virtual Private Cloud User Guide*. For information about AWS Direct Connect, see Creating a Connection in the *AWS Direct Connect User Guide*.

Update management in WorkSpaces

We recommend that you regularly patch, update, and secure the operating system and applications on your WorkSpaces. You can configure your WorkSpaces to be updated by WorkSpaces during a regular maintenance window or you can update them yourself. For more information, see Maintenance in WorkSpaces Personal.

For applications on your WorkSpaces, you can use any automatic update services provided or follow the recommendations for installing updates provided by the application vendor.

Amazon WorkSpaces quotas

Amazon WorkSpaces provides different resources that you can use in your account in a given Region, including WorkSpaces, images, bundles, directories, connection aliases, and IP control groups. When you create your Amazon Web Services account, we set default quotas (also referred to as limits) on the number of resources that you can create.

The following are the default quotas for WorkSpaces for your AWS account. You can use the Service Quotas console to view the default quota and applied quota, or to request quota increases for adjustable quotas.

In some Regions, where Service Quotas is not available, you must submit a support case to request limit increase. For more information, see Viewing service quotas and Requesting a quota increase in the *Service Quotas User Guide*.

Resource	Default	Description	Adjustable
WorkSpaces	1	The maximum number of WorkSpaces in this account in the current Region.	Yes
Graphics WorkSpaces	0	The maximum number of Graphics WorkSpaces in this account in the current Region. **Note** Graphics bundle is no longer supported after November	Yes

Resource	Default	Description	Adjustable
		30, 2023. We recommend migrating your WorkSpaces to Graphics.g4dn bundle. For more information, see Migrate a WorkSpace in WorkSpaces Personal.	
Graphics.g4dn WorkSpaces	0	The maximum number of Graphics.g4dn WorkSpaces in this account in the current Region.	Yes
GraphicsPro WorkSpaces	0	The maximum number of GraphicsPro WorkSpaces in this account in the current Region.	Yes
GraphicsPro.g4dn WorkSpaces	0	The maximum number of GraphicsPro.g4dn WorkSpaces in this account in the current Region.	Yes

Resource	Default	Description	Adjustable
Standby WorkSpaces	0	The maximum number of WorkSpaces in this account in the current Region.	Yes
Bundles	50	The maximum number of bundles in this account in the current Region. This quota applies only to custom bundles, not to public bundles.	No
Connection aliases	20	The maximum number of connection aliases in this account in the current Region.	No
Directories	50	The maximum number of directories that can be registered for use with Amazon WorkSpaces in this account in the current Region.	No
Images	40	The maximum number of images in this account in the current Region.	Yes

Resource	Default	Description	Adjustable
IP access control groups	100	The maximum number of IP access control groups in this account in the current Region.	No
IP access control groups per directory	25	The maximum number of IP access control groups per directory in this account in the current Region.	No
Rules per IP access control group	10	The maximum number of rules per IP access control group in this account in the current Region.	No
WorkSpaces Pools	10	The maximum number of WorkSpaces Pools in this account in the current Region.	Yes
General Purpose Value streaming instances for WorkSpaces Pools	10	The maximum number of General Purpose Value streaming instances that can be used for WorkSpaces Pools in this account in the current Region.	Yes

Resource	Default	Description	Adjustable
General Purpose Standard streaming instances for WorkSpaces Pools	10	The maximum number of General Purpose Standard instances that can be used for WorkSpaces Pools in this account in the current Region.	Yes
General Purpose Performance streaming instances for WorkSpaces Pools	10	The maximum number of General Purpose Performance streaming instances that can be used for WorkSpaces Pools in this account in the current Region.	Yes
General Purpose Power streaming instances for WorkSpaces Pools"	10	The maximum number of General Purpose Power streaming instances that can be used for WorkSpaces Pools in this account in the current Region.	Yes
General Purpose PowerPro streaming instances for WorkSpaces Pools"	10	The maximum number of General Purpose PowerPro streaming instances that can be used for WorkSpaces Pools in this account in the current Region.	Yes

Resource	Default	Description	Adjustable
Graphics.g4dn xlarge streaming instances for WorkSpaces Pools	0	The maximum number of Graphics.g4dn xlarge streaming instances that can be used for WorkSpaces Pools in this account in the current Region.	No
Graphics.g4dn 4xlarge streaming instances for WorkSpaces Pools	0	The maximum number of Graphics.g4dn 4xlarge streaming instances that can be used for WorkSpaces Pools in this account in the current Region.	No

API throttling

The allowed rate is two calls per second. For more information, see Throttling exceptions.

WorkSpaces Streaming Protocol (WSP) host agent versions

The WorkSpaces Streaming Protocol (WSP) host agent is a host agent that runs inside your WorkSpace. It streams the pixels of your WorkSpace to a client application and includes in-session features, such as two-way audio and video, and printing. For more information about the WorkSpaces Streaming Protocol (WSP), see Protocols for Amazon WorkSpaces.

We recommend keeping your host agent software updated with the latest version. You can manually reboot your WorkSpaces to update the WSP host agent. The WSP host agent is also updated automatically during the regular WorkSpaces default maintenance window. For more information about maintenance windows, see WorkSpace maintenance. Some of these features require the latest WorkSpaces client version. For more information about the latest client versions, see WorkSpaces Clients.

The following table describes the changes in each version of the WSP host agent.

Release	Date	Changes
• Windows WorkSpaces - 2.1.0.1757	August 19, 2024	• Added support for integration with IAM Identity Center (IdC). • Bug fixes and performance improvements.
• Windows WorkSpaces - 2.1.0.1696	July 29, 2024	• Added support for Windows Graphics hosts. • Added WebRTC redirection support for Amazon Connect. • Fixed an issue that could prevent the service from running at system start. • Bug fixes and performance improvements.
• Windows WorkSpaces - 2.1.0.1554	May 15, 2024	• Added support for Idle Disconnect Timeout.

Release	Date	Changes
		• Added new Group Policy setting to configure Idle Disconnect Timeout. • Fixed an issue where WorkSpaces got disconnected and displayed a white screen when users modified the display settings. • Bug fixes and performance improvements.
• Ubuntu WorkSpaces - 2.1.0.1342	February 29, 2024	• Changed preferred webcam resolution to between 480x360 and 640x480. • Bug fixes and performance improvements.
• Windows WorkSpaces - 2.0.0.1425	February 22, 2024	• Added support for in-session WebAuthn redirection requests from web applications running in remote Google Chrome or Microsoft Edge browsers. This feature adds a one-time browser prompt that asks the user to enable the DCV WebAuthn Redirection Extension. It is only supported on Windows WorkSpaces and WorkSpaces native clients. • Fixed an issue where a white or frozen screen sometimes appeared when logging in. • Bug fixes and performance improvements.

Release	Date	Changes
• Windows WorkSpaces - 2.0.0.1304	January 11, 2024	• Fixed a bug related to potential streaming freezes during login. • Fixed a logging-related bug.
• Windows WorkSpaces - 2.0.0.1288	November 16, 2023	• Added support for Indirect Display Driver (IDD) on Windows 10+, which lowers CPU consumpti on and improves streaming performance. • Added new Group Policy setting to enable or disable IDD driver. • Fixed bugs related to clipboard image transparency. • Fixed bugs preserving Windows scale factors. • Bug fixes and performance improvements.
• Windows WorkSpaces - 2.0.0.1164	October 13, 2023	• Added support for VSync in the virtual display driver. • Added new Group Policy setting to enable or disable VSync. • Improved reconnection and reliability issues. • Bug fixes and performance improvements.

Release	Date	Changes
• Amazon Linux WorkSpaces - 2.0.0.1086 • Ubuntu WorkSpaces - 2.1.0.1086	August 18, 2023	• Added new setting to enable or disable time zone redirection. • Extended logon timeout and added a configuration option. • Improved gateway to enable faster reconnections after disruption. • Bug fixes and performance improvements.
• Amazon Linux WorkSpaces - 2.0.0.907	June 30, 2023	• Added support for the DCV Extension SDK to enable ISV-specific integrations. • Changed the disconnect behavior so that logging out terminates the user's session. • Added support for time zone redirection. • Extended logon timeout and added a configuration option. • Fixed upgrade issues. • Bug fixes and performance improvements.
• Windows WorkSpaces - 2.0.0.829	June 8, 2023	• Changed disconnect behavior so that logging out terminates the user's session. • Fixed bugs related to A/V sync and Japanese keyboards. • Improved WSP installer reliability.

Release	Date	Changes
• Ubuntu WorkSpaces - 2.1.0.829	May 16, 2023	• Changed disconnect behavior so that logging out terminates the user's session. • Added support for the DCV Extension SDK to enable ISV-specific integrations. • Added support for time zone redirection. • Fixed upgrade issues.
• Windows WorkSpaces - 2.0.0.799	May 8, 2023	• Enhanced UDP-based QUIC transport with several image quality and performance optimizations. • Added support for the DCV Extension SDK to enable ISV-specific integrations. • Added new Group Policy settings to enable or disable the Extension SDK. • Improved Korean, Japanese, and German keyboard layouts. • Fixed bugs related to session freeze issues, hardware acceleration, printer redirection, log verbosity, and target-fps Group Policy settings.

Note

- For information about how to check your host agent version, see What client and host operating systems are supported by the latest version of WSP?.

- For information about how to update your host agent version, see If I already have a WSP WorkSpace, how do I update it?.
- For WSP macOS client version release notes, see Release notes in the WorkSpaces macOS client application section of the WorkSpaces User Guide.
- For WSP Windows client version release notes, see Release notes in the WorkSpaces Windows client application section of the WorkSpaces User Guide.

SDK extension supported by WSP

Amazon WorkSpaces Streaming Protocol (WSP) is built using NICE DCV technology, enabling high-performance remote access to WorkSpaces instances for a wide range of workloads and use cases. With the NICE DCV Extension SDK, developers can customize WSP WorkSpaces experience for end users, including:

- Facilitating custom hardware support.
- Enhancing the usability of third-party applications in remote sessions. For example, adding local audio termination for VoIP applications or local video playback for conferencing applications
- Providing accessibility software like screen readers with information about the remote session and applications running remotely.
- Allowing security software to analyze the security posture of the local endpoint to allow conditional access policies.
- Performing arbitrary data transfers over an established remote session.

To get started with NICE DCV Extension SDK, see NICE DCV Extension SDK documentation. You can find the SDK itself at NICE DCV Extension SDK GitHub repository. In addition, you can also find integration examples of SDK at NICE DCV Extension SDK samples GitHub repository.

The following are supported by WorkSpaces.

- Streaming protocol – WorkSpaces Streaming Protocol (WSP)
- WorkSpaces Windows client – Windows: 5.9.0.4110 and above.

> **Note**
>
> WorkSpaces Android, iOS clients, web access does not support NICE DCV Extension SDK.

- WorkSpaces supported – Windows, Linux, and Ubuntu servers

Document history for WorkSpaces

The following table describes the important changes to the WorkSpaces service and to the *Amazon WorkSpaces Administration Guide* from January 1, 2018, onward. We also update the documentation frequently to address the feedback that you send us.

For notification about these updates, you can subscribe to the WorkSpaces RSS feed.

Change	Description	Date
Microsoft Entra ID directory	You can create a dedicated Microsoft Entra ID directory.	August 26, 2024
Microsoft Visual Studio	Microsoft Visual Studio bundles are supported for Manage applications.	August 1, 2024
Amazon DCV WebRTC Redirection Extension	You can install the Amazon DCV WebRTC Redirection Extension to use WebRTC redirection.	August 1, 2024
WorkSpaces Pools is now available in AWS GovCloud (US) Region	WorkSpaces Pools offers non-persistent virtual desktops tailored for users who need on-demand access to highly-curated desktop environments hosted on ephemeral infrastructure.	July 23, 2024
WorkSpaces Pools is now available	WorkSpaces Pools offers non-persistent virtual desktops tailored for users who need on-demand access to highly-curated desktop environments hosted on ephemeral infrastructure.	June 27, 2024

AmazonWorkSpacesAdmin managed policy update and new AmazonWorkSpacesPoolServiceAccess managed policy	WorkSpaces updated the AmazonWorkSpacesAdmin managed policy and added the new AmazonWorkSpacesPoolServiceAccess managed policy.	June 27, 2024
AmazonWorkSpacesAdmin managed policy update	WorkSpaces added the workspaces:RestoreWorkspace action to the AmazonWorkSpacesAdmin managed policy, granting admins access to restore WorkSpaces.	July 17, 2023
SDK extension supported by WSP	With the NICE DCV Extension SDK, developers can customize WSP WorkSpaces experience for end users.	May 25, 2023
WorkSpaces Streaming Protocol (WSP) host agent versions	Version information for WorkSpaces Streaming Protocol (WSP).	May 8, 2023
Amazon WorkSpaces launched in AWS GovCloud (US-East)	Amazon WorkSpaces is available in the AWS GovCloud (US-East).	May 3, 2023
Amazon WorkSpaces webcam support	Amazon WorkSpaces now supports real-time audio-video (AV) by seamlessly redirecting local webcam video input to Windows WorkSpaces desktops using the WorkSpaces Streaming Protocol (WSP).	April 5, 2021

Amazon WorkSpaces smart card support with the WorkSpaces macOS client application	You can now use the Amazon WorkSpaces macOS client application with Common Access Card (CAC) and Personal Identity Verification (PIV) smart cards. Smart card support is available on WorkSpaces using the WorkSpaces Streaming Protocol (WSP).	April 5, 2021
Amazon WorkSpaces bundle management APIs	Amazon WorkSpaces bundle management APIs are now available. These API actions support creation, deletion, and image association operations for WorkSpaces bundles.	March 15, 2021
Amazon WorkSpaces launched in Asia Pacific (Mumbai)	Amazon WorkSpaces is available in the Asia Pacific (Mumbai) Region.	March 8, 2021
WorkSpaces Streaming Protocol (WSP)	The WorkSpaces Streaming Protocol (WSP) is now available for both license-included (Windows Server 2016) and BYOL Windows 10-based WorkSpaces on all bundle types except for Graphics and GraphicsPro. WSP is also available for Linux WorkSpaces in the AWS GovCloud (US-West) Region.	December 1, 2020

Smart Cards	Amazon WorkSpaces now supports pre-session (login) and in-session smart card authentication on Windows and Linux WorkSpaces in the AWS GovCloud (US-West) Region.	December 1, 2020
Share Custom Images	You can now share custom WorkSpaces images across AWS accounts. After an image has been shared, the recipient account can copy the image and use it to create bundles for launching new WorkSpaces.	October 1, 2020
Cross-Region Redirection	You can now use cross-Region redirection, a feature that works with your Domain Name System (DNS) routing policies to redirect your users to alternative WorkSpaces when their primary WorkSpaces aren't available.	September 10, 2020
Subscribe to Microsoft Office 2016 or 2019 for BYOL WorkSpaces	You can now subscribe to Microsoft Office Professional 2016 or 2019 provided by AWS on Bring Your Own Windows License (BYOL) WorkSpaces.	September 3, 2020

BYOL Automation in China (Ningxia)	You can use Bring Your Own License (BYOL) automation to simplify the process of using your Windows 10 desktop licenses for your WorkSpaces in China (Ningxia).	April 2, 2020
Image Checker	The Image Checker tool helps you determine whether your Windows WorkSpace meets the requirements for image creation. The Image Checker performs a series of tests on the WorkSpace that you want to use to create your image, and provides guidance on how to resolve any issues it finds.	March 30, 2020
Migrate WorkSpaces	The Amazon WorkSpace s migrate feature enables you to migrate a WorkSpace from one bundle to another, while retaining the data on the user volume. You can use this feature to migrate WorkSpaces from the Windows 7 desktop experienc e to the Windows 10 desktop experience. You can also use this feature to migrate WorkSpaces from one public or custom bundle to another.	January 9, 2020

PrivateLink integration for Amazon WorkSpaces APIs	You can connect directly to Amazon WorkSpaces API endpoints through an interface endpoint in your Virtual Private Cloud (VPC) instead of connecting over the internet. When you use a VPC interface endpoint, communication between your VPC and the Amazon WorkSpaces API endpoint is conducted entirely and securely within the AWS network.	November 25, 2019
Linux client for Amazon WorkSpaces	Users can now use the Linux client to access their WorkSpaces.	November 25, 2019
Amazon WorkSpaces launched in China (Ningxia)	Amazon WorkSpaces is available in the China (Ningxia) Region.	November 13, 2019
Restore WorkSpaces to last known healthy state	You can use the restore feature to roll back a WorkSpace to its last known healthy state.	September 18, 2019

FIPS endpoint encryption	To comply with the Federal Risk and Authorization Management Program (FedRAMP) or the Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG), you can configure Amazon WorkSpaces to use Federal Information Processing Standards (FIPS) endpoint encryption at the directory level.	September 12, 2019
Copy WorkSpace images	You can copy your images within the same Region or across Regions.	June 27, 2019
Self-Service WorkSpace Management Capabilities for Users	You can enable self-service WorkSpace management capabilities for your users to provide them with more control over their experience.	November 19, 2018
BYOL Automation	You can use Bring Your Own License (BYOL) automation to simplify the process of using your Windows 7 and Windows 10 desktop licenses for your WorkSpaces.	November 16, 2018
PowerPro and GraphicsPro bundles	The PowerPro and GraphicsPro bundles are now available for WorkSpaces.	October 18, 2018

Monitor successful WorkSpace logins	You can use events from Amazon CloudWatch Events to monitor and respond to successful WorkSpace logins.	September 17, 2018
Web Access for Windows 10 WorkSpaces	Users can now use the web access client to access a WorkSpace running the Windows 10 desktop experience.	August 24, 2018
URI login	You can use uniform resource identifiers (URIs) to provide users with access to their WorkSpaces.	July 31, 2018
Amazon Linux WorkSpaces	You can provision Amazon Linux WorkSpaces for your users.	June 26, 2018
IP access control groups	You can control the IP addresses from which users can access their WorkSpaces.	April 30, 2018
In-place upgrades	You can upgrade your Windows 10 BYOL WorkSpaces to a newer version of Windows 10.	March 9, 2018

Earlier Updates

The following table describes important additions to the Amazon WorkSpaces service and its documentation set before January 1, 2018.

Change	Description	Date
Flexible compute options	You can switch your WorkSpaces between the Value, Standard, Performance, and Power bundles	December 22, 2017
Configurable storage	You can configure the size of the root and user volumes for your WorkSpaces when you launch them and increase the size of these volumes later on.	December 22, 2017
Control device access	You can specify the types of devices that have access to WorkSpaces. In addition, you can restrict access to WorkSpaces to trusted devices (also known as managed devices).	June 19, 2017
Inter-forest trusts	You can establish a trust relationship between your AWS Managed Microsoft AD and your on-premises Microsoft Active Directory domain and then provision WorkSpaces for users in the on-premises domain.	February 9, 2017
Windows Server 2016 bundles	WorkSpaces offers bundles that include a Windows 10 desktop experience, powered by Windows Server 2016.	November 29, 2016
Web Access	You can access your Windows WorkSpaces from a web browser using WorkSpaces Web Access.	November 18, 2016
Hourly WorkSpaces	You can configure your WorkSpaces so that users are billed by the hour.	August 18, 2016
Windows 10 BYOL	You can bring your Windows 10 Desktop License to WorkSpaces (BYOL).	July 21, 2016
Tagging support	You can use tags to manage and track your WorkSpaces.	May 17, 2016

Change	Description	Date
Saved registrations	Every time you enter a new registration code, the WorkSpaces client stores it. This makes it easier to switch between WorkSpaces in different directories or Regions.	January 28, 2016
Windows 7 BYOL, Chromebook client, WorkSpace encryption	You can bring your Windows 7 Desktop License to WorkSpaces (BYOL), use the Chromebook client, and use WorkSpace encryption.	October 1, 2015
CloudWatch monitoring	Added information about CloudWatch monitoring.	April 28, 2015
Automatic session reconnect	Added information about the auto session reconnect feature in the WorkSpaces desktop client applications.	March 31, 2015
Public IP addresses	You can automatically assign a public IP address to your WorkSpaces.	January 23, 2015
WorkSpaces launched in Asia Pacific (Singapore)	WorkSpaces is available in the Asia Pacific (Singapore) Region.	January 15, 2015
Value bundle added, Standard bundle updates, Office 2013 added	The Value bundle is available, the Standard bundle hardware has been upgraded, and Microsoft Office 2013 is available in Plus packages.	November 6, 2014
Image and bundle support	You can create an image from a WorkSpace that you've customized and a custom WorkSpace bundle from the image.	October 28, 2014
PCoIP zero client support	You can access WorkSpaces PCoIP zero client devices.	October 15, 2014
WorkSpaces launched in Asia Pacific (Tokyo)	WorkSpaces is available in the Asia Pacific (Tokyo) Region.	August 26, 2014

Change	Description	Date
Local printer support	You can enable local printer support for your WorkSpaces.	August 26, 2014
Multi-factor authentication	You can use multi-factor authentication in connected directories.	August 11, 2014
Default OU support and target domain support	You can select a default Organizational Unit (OU) where your WorkSpace machine accounts are placed, and a separate domain where your WorkSpace machine accounts are created.	July 7, 2014
Add security groups	You can add a security group to your WorkSpaces.	July 7, 2014
WorkSpaces launched in Asia Pacific (Sydney)	WorkSpaces is available in the Asia Pacific (Sydney) Region.	May 15, 2014
WorkSpaces launched in Europe (Ireland)	WorkSpaces is available in the Europe (Ireland) Region.	May 5, 2014
Public beta	WorkSpaces is available as a public beta.	March 25, 2014