# Table of Contents

What Is Amazon WorkSpaces? ....................................................................................................................... 1
Features ..................................................................................................................................................... 1
Architecture .............................................................................................................................................. 1
Accessing Your WorkSpace .......................................................................................................................... 2
Pricing .......................................................................................................................................................... 3
How to Get Started .................................................................................................................................... 3
Get Started: Quick Setup ............................................................................................................................. 4
Before You Begin ....................................................................................................................................... 4
Step 1: Launch the WorkSpace .................................................................................................................... 4
Step 2: Connect to the WorkSpace ............................................................................................................. 6
Step 3: Clean Up (Optional) ....................................................................................................................... 6
Networking and Access .............................................................................................................................. 8
VPC Requirements .................................................................................................................................... 8
- Configure a VPC with Private Subnets and a NAT Gateway ................................................................. 8
- Configure a VPC with Public Subnets ................................................................................................... 11
IP Address and Port Requirements ........................................................................................................... 13
- Ports for Client Applications .................................................................................................................. 14
- Ports for Web Access ............................................................................................................................ 14
- Whitelisted Domains and Ports ............................................................................................................ 15
- PCoIP Health Check Servers ............................................................................................................... 19
- PCoIP Gateway .................................................................................................................................... 20
- Network Interfaces ............................................................................................................................... 20
Network Requirements .............................................................................................................................. 22
Trusted Devices ......................................................................................................................................... 23
- Step 1: Create the Certificates ............................................................................................................ 23
- Step 2: Deploy Client Certificates to the Trusted Devices .................................................................. 24
- Step 3: Configure the Restriction ....................................................................................................... 24
Internet Access .......................................................................................................................................... 24
Security Groups .......................................................................................................................................... 25
IP Access Control Groups ............................................................................................................................ 26
- Create an IP Access Control Group ..................................................................................................... 26
- Associate an IP Access Control Group with a Directory .................................................................... 26
- Copy an IP Access Control Group ...................................................................................................... 27
- Delete an IP Access Control Group ..................................................................................................... 27
PCoIP Zero Client ..................................................................................................................................... 27
FIPS Endpoint Encryption ............................................................................................................................ 28
Enable SSH Connections ............................................................................................................................. 29
- Prerequisites for SSH Connections to Amazon Linux WorkSpaces .................................................... 29
- Enable SSH Connections to All Amazon Linux WorkSpaces in a Directory ..................................... 30
- Enable SSH Connections to a Specific Amazon Linux WorkSpace .................................................. 31
- Connect to an Amazon Linux WorkSpace by Using Linux or PuTTY .................................................. 31
Required Configuration ............................................................................................................................. 32
- Required Routing Table Configuration ................................................................................................ 32
- Required Service Components .............................................................................................................. 32
Directories .................................................................................................................................................. 34
Register a Directory ................................................................................................................................... 34
Update Directory Details ............................................................................................................................ 35
- Select an Organizational Unit ............................................................................................................... 35
- Configure Automatic IP Addresses .................................................................................................... 36
- Control Device Access .......................................................................................................................... 36
- Manage Local Administrator Permissions ............................................................................................ 37
- Update the AD Connector Account (AD Connector) .......................................................................... 37
- Multi-factor Authentication (AD Connector) ......................................................................................... 37
Delete a Directory ..................................................................................................................................... 38
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting</td>
<td>103</td>
</tr>
<tr>
<td>Monitor Your WorkSpaces</td>
<td>86</td>
</tr>
<tr>
<td>Bundles and Images</td>
<td>75</td>
</tr>
<tr>
<td>Enabling Advanced Logging</td>
<td>103</td>
</tr>
<tr>
<td>Update Management</td>
<td>102</td>
</tr>
<tr>
<td>Resilience</td>
<td>99</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>93</td>
</tr>
<tr>
<td>Monitor Using CloudWatch Metrics</td>
<td>86</td>
</tr>
<tr>
<td>Encryption in Transit</td>
<td>95</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>93</td>
</tr>
<tr>
<td>Creating the workspaces_defaultRole Role</td>
<td>95</td>
</tr>
<tr>
<td>Specifying Amazon WorkSpaces Resources in an IAM Policy</td>
<td>96</td>
</tr>
<tr>
<td>Compliance Validation</td>
<td>98</td>
</tr>
<tr>
<td>Resilience</td>
<td>99</td>
</tr>
<tr>
<td>Infrastructure Security</td>
<td>99</td>
</tr>
<tr>
<td>Network Isolation</td>
<td>99</td>
</tr>
<tr>
<td>Isolation on Physical Hosts</td>
<td>100</td>
</tr>
<tr>
<td>Authorization of Corporate Users</td>
<td>100</td>
</tr>
<tr>
<td>Connect to Amazon WorkSpaces Through a VPC Interface Endpoint</td>
<td>100</td>
</tr>
<tr>
<td>Create a VPC Endpoint Policy for Amazon WorkSpaces</td>
<td>101</td>
</tr>
<tr>
<td>Connect Your Private Network to Your VPC</td>
<td>102</td>
</tr>
<tr>
<td>Update Management</td>
<td>102</td>
</tr>
<tr>
<td>Amazon WAM</td>
<td>102</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>103</td>
</tr>
<tr>
<td>Enabling Advanced Logging</td>
<td>103</td>
</tr>
</tbody>
</table>
Troubleshooting for Specific Issues ........................................................................................... 104

I can't create an Amazon Linux WorkSpace because there are non-valid characters in the user name ............................................................................................................................ 105
I changed the shell for my Amazon Linux WorkSpace and now I can't provision a PCoIP session .. 105
Launching WorkSpaces in my connected directory often fails ...................................................... 105
Launching WorkSpaces fails with an internal error ................................................................. 105
My users can't connect to a Windows WorkSpace with an interactive logon banner ............... 105
My users are having issues when they try to log on to BYOL WorkSpaces from WorkSpaces Web Access .......................................................................................................................... 105
The WorkSpaces client gives my users a network error, but they are able to use other network-enabled apps on their devices .......................................................... 106
My WorkSpace users see the following error message: "Device can't connect to the registration service. Check your network settings." ............................................................. 108
My users aren't receiving invitation emails or password reset emails ..................................... 108
I receive the message "The system administrator has set policies to prevent this installation" when I try to install applications on a Windows WorkSpace .............................................. 108
No WorkSpaces in my directory can connect to the internet .................................................. 109
I receive a "DNS unavailable" error when I try to connect to my on-premises directory ............ 109
I receive a "Connectivity issues detected" error when I try to connect to my on-premises directory .................................................................................................................. 109
I receive an "SRV record" error when I try to connect to my on-premises directory .................. 110
My Windows WorkSpace goes to sleep when it's left idle ....................................................... 110
One of my WorkSpaces has a state of "Unhealthy" ................................................................... 110
I receive ThrottlingException errors to some of my API calls ................................................ 111

Quotas .......................................................................................................................................... 113

Document History .......................................................................................................................... 114

Earlier Updates ....................................................................................................................... 115
What Is Amazon WorkSpaces?

Amazon WorkSpaces enables you to provision virtual, cloud-based Microsoft Windows or Amazon Linux desktops for your users, known as WorkSpaces. Amazon 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.

Features

- Choose your operating system (Windows or Amazon Linux) and select from a range of hardware configurations, software configurations, and AWS Regions. For more information, see Amazon WorkSpaces Bundles.
- Connect to your WorkSpace and pick up from right where you left off. Amazon WorkSpaces provides a persistent desktop experience.
- Amazon WorkSpaces provides the flexibility of either monthly or hourly billing for WorkSpaces. For more information, see Amazon WorkSpaces Pricing.
- Deploy and manage applications for your Windows WorkSpaces by using Amazon WorkSpaces Application Manager (Amazon WAM).
- 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 directory for your users, or connect your WorkSpaces to your on-premises directory so that your users can use their existing credentials to obtain seamless access to corporate resources.
- 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.

Architecture

For both Windows and Amazon Linux WorkSpaces, each WorkSpace is associated with a virtual private cloud (VPC), and a directory to store and manage information for your WorkSpaces and users. Directories are managed 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.

Amazon WorkSpaces uses a directory, either AWS Directory Service or AWS Managed Microsoft AD, 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 for pixel streaming to the WorkSpace and for network health checks. For more information, see Ports for Client Applications (p. 14).
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 (p. 20).

The following diagram shows the architecture of Amazon WorkSpaces.

**Accessing Your WorkSpace**

You can connect to your WorkSpaces by using the client application for a supported device or, for Windows WorkSpaces, 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 tablets
- Fire tablets
- Zero client devices

On Windows, macOS, and Linux PCs, you can use the following web browsers to connect to Windows WorkSpaces:
• Chrome 53 and later (Windows and macOS only)
• Firefox 49 and later

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

Pricing

After you sign up for AWS, you can get started with Amazon WorkSpaces for free using the Amazon WorkSpaces free tier offer. For more information, see Amazon WorkSpaces Pricing.

With Amazon WorkSpaces, you pay only for what you use. You are charged based on the bundle and the number of WorkSpaces that you launch. The pricing for Amazon WorkSpaces includes the use of Simple AD and AD Connector but not the use of AWS Managed Microsoft AD.

Amazon WorkSpaces provides monthly or hourly billing for WorkSpaces. With monthly billing, you pay a fixed fee for unlimited usage, which is best for users who use their WorkSpaces full time. With hourly billing, you pay a small fixed monthly fee per WorkSpace, plus a low hourly rate for each hour the WorkSpace is running. For more information, see Amazon WorkSpaces Pricing.

How to Get Started

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

• Get Started with Amazon WorkSpaces Quick Setup (p. 4)
• Launch a WorkSpace Using AWS Managed Microsoft AD (p. 47)
• Launch a WorkSpace Using Simple AD (p. 50)
• Launch a WorkSpace Using AD Connector (p. 52)
• Launch a WorkSpace Using a Trusted Domain (p. 55)
Get Started with Amazon WorkSpaces Quick Setup

In this tutorial, you learn how to provision a virtual, cloud-based Microsoft Windows or Amazon Linux desktop, known as a *WorkSpace*, by using Amazon 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 Launch a Virtual Desktop Using Amazon WorkSpaces (p. 47).

**Note**
Quick Setup is supported only in the following AWS Regions:

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

**Tasks**
- Before You Begin (p. 4)
- Step 1: Launch the WorkSpace (p. 4)
- Step 2: Connect to the WorkSpace (p. 6)
- Step 3: Clean Up (Optional) (p. 6)

**Before You Begin**

- 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.
- 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 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.
- Amazon 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 Amazon WorkSpaces Pricing by AWS Region.

**Step 1: Launch the WorkSpace**

Using Quick Setup, you can launch your first WorkSpace in minutes.

**To launch a WorkSpace**

1. Open the Amazon WorkSpaces console at [https://console.aws.amazon.com/workspaces/](https://console.aws.amazon.com/workspaces/).
2. Choose **Get Started Now**. 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 (p. 4).

3. On the **Get Started with Amazon WorkSpaces** page, next to **Quick Setup**, choose **Launch**.

4. For **Bundles**, select a bundle for the user.

5. For **Enter User Details**, complete **Username**, **First Name**, **Last Name**, and **Email**.

6. Choose **Launch WorkSpaces**.

7. On the confirmation page, choose **View the WorkSpaces Console**. 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 the user.
Quick Setup

Quick Setup completes the following tasks on your behalf:

- Creates an IAM role to allow the Amazon WorkSpaces service to create elastic network interfaces and list your Amazon WorkSpaces directories. This role has the name workspaces_DefaultRole.
- Creates a virtual private cloud (VPC).
- Sets up a Simple AD directory in the VPC that is used to store user and WorkSpace information. The directory has an administrator account and it is enabled for Amazon WorkDocs.
- Creates the specified user accounts and adds them to the directory.
- Creates WorkSpace instances. Each WorkSpace receives a public IP address to provide internet access. The running mode is AlwaysOn. For more information, see Manage the WorkSpace Running Mode (p. 62).
- Sends invitation emails to the specified users.

Note
The first user account created by Quick Setup is your Admin user account. You can't update this user account from the Amazon WorkSpaces Console. Don't share the information for this Admin account with anyone else. If you want to invite other users to use this WorkSpace, create new user accounts for them.

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

2. When prompted, download one of the client applications or launch Web Access. For more information about the requirements for each client, see Amazon WorkSpaces Clients in the Amazon WorkSpaces User Guide.

   If you aren't prompted and you haven't installed a client application already, open https://clients.amazonworkspaces.com/ and follow the directions.

3. Start the client, enter the registration code from the invitation email, and choose Register.

4. When prompted to sign in, enter the user name and password, and then choose Sign In.

5. (Optional) When prompted to save your credentials, choose Yes.

Step 3: Clean Up (Optional)

If you are finished with the WorkSpace that you created for this tutorial, you can delete it.
To delete the WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select your WorkSpace and choose **Actions, Remove WorkSpaces**.
4. When prompted for confirmation, choose **Remove WorkSpaces**.
5. (Optional) If you are not using the directory with another application, such as Amazon WorkDocs, Amazon WorkMail, or Amazon Chime, you can delete it as follows:
   a. In the navigation pane, choose **Directories**.
   b. Select your directory and choose **Actions, Deregister**.
   c. Select your directory again and choose **Actions, Delete**.
   d. When prompted for confirmation, choose **Delete**.
Networking and Access for Amazon WorkSpaces

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

Contents
- Configure a VPC for Amazon WorkSpaces (p. 8)
- IP Address and Port Requirements for Amazon WorkSpaces (p. 13)
- Amazon WorkSpaces Client Network Requirements (p. 22)
- Restrict WorkSpaces Access to Trusted Devices (p. 23)
- Provide Internet Access from Your WorkSpace (p. 24)
- Security Groups for Your WorkSpaces (p. 25)
- IP Access Control Groups for Your WorkSpaces (p. 26)
- Set Up PColP Zero Client for WorkSpaces (p. 27)
- Set Up Amazon WorkSpaces for FedRAMP Authorization or DoD SRG Compliance (p. 28)
- Enable SSH Connections for Your Linux WorkSpaces (p. 29)
- Required Configuration and Service Components for WorkSpaces (p. 32)

Configure a VPC for Amazon WorkSpaces

Amazon WorkSpaces launches your WorkSpaces in a virtual private cloud (VPC). Your WorkSpaces must have access to the internet so that you can install updates to the operating system and deploy applications using Amazon WorkSpaces Application Manager (Amazon WAM).

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 an Elastic IP address with each WorkSpace.

Options
- Configure a VPC with Private Subnets and a NAT Gateway (p. 8)
- Configure a VPC with Public Subnets (p. 11)

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.
Amazon WorkSpaces Administration Guide
Configure a VPC with Private Subnets and a NAT Gateway

Tasks
- Step 1: Allocate an Elastic IP Address (p. 9)
- Step 2: Create a VPC (p. 10)
- Step 3: Add a Second Private Subnet (p. 11)
- Step 4: Verify and Name the Route Tables (p. 11)

Step 1: Allocate an Elastic IP Address

Allocate an Elastic IP address for your NAT gateway as follows. Note that if you are using an alternative method of providing internet access, you can skip this step.

To allocate an Elastic IP address
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose Elastic IPs.
3. Choose Allocate new address.
4. On the Allocate new address page, for IPv4 address pool, choose Amazon pool or Owned by me, and then choose Allocate.
5. Make a note of the Elastic IP address, then choose Close.
Step 2: Create a VPC

Create a VPC with one public subnet and two private subnets as follows.

To create the VPC

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose VPC Dashboard in the upper-left corner.
3. Choose Launch VPC Wizard.
4. Choose VPC with Public and Private Subnets and then choose Select.
5. Configure the VPC as follows:
   a. For IPv4 CIDR block, enter the CIDR block for the VPC. We recommend that you use a CIDR block from the private (non-publicly routable) IP address ranges specified in RFC 1918. For example, 10.0.0.0/16. For more information, see VPC and Subnet Sizing for IPv4 in the Amazon VPC User Guide.
   b. For IPv6 CIDR Block, keep No IPv6 CIDR Block.
   c. For VPC name, enter a name for the VPC.
6. Configure the public subnet as follows:
   a. For IPv4 CIDR block, enter the CIDR block for the subnet.
   b. For Availability Zone, keep No Preference.
   c. For Public subnet name, enter a name for the subnet (for example, WorkSpaces Public Subnet).
7. Configure the first private subnet as follows:
   a. For Private subnet's IPv4 CIDR, enter the CIDR block for the subnet.
   b. For Availability Zone, select the first one in the list (for example, us-west-2a).
   c. For Private subnet name, enter a name for the subnet (for example, WorkSpaces Private Subnet 1).
8. For Elastic IP Allocation ID, choose the Elastic IP address that you created. Note that if you are using an alternative method of providing internet access, you can skip this step.
10. For Enable DNS hostnames, keep Yes.
11. For Hardware tenancy, keep Default.
12. Choose Create VPC. Note that it takes several minutes to set up your VPC. After the VPC is created, choose OK.

Note
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.

For more information about working with IPv6 addresses, see IP Addressing in Your VPC in the Amazon VPC User Guide.
Step 3: Add a Second Private Subnet

In the previous step, you created a VPC with one public subnet and one private subnet. Use the following procedure to add a second private subnet.

To add a private subnet

1. In the navigation pane, choose Subnets.
2. Choose Create Subnet.
3. For Name tag, enter a name for the private subnet (for example, WorkSpaces Private Subnet 2).
4. For VPC, select the VPC that you created.
5. For Availability Zone, select the second one in the list (for example, us-west-2b).
6. For IPv4 CIDR block, enter the CIDR block for the subnet.
7. Choose Create.

Step 4: Verify and Name the Route Tables

You can verify and name the route tables for each subnet.

To verify and name the route tables

1. In the navigation pane, choose Subnets, and select the public subnet that you created.
   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 enter a name (for example, workspaces-public-routetable), and then choose the check mark to save the name.
   c. 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.
2. In the navigation pane, choose Subnets, and select the first private subnet that you created (for example, WorkSpaces Private Subnet 1).
   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 there is one route for local traffic and another route that sends all other traffic to the NAT gateway.
3. In the navigation pane, choose Subnets, and select the second private subnet that you created (for example, WorkSpaces Private Subnet 2). 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.

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 (p. 12)
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. In the navigation pane, choose **VPC Dashboard** in the upper-left corner.
3. Choose **Launch VPC Wizard**.
4. Choose **VPC with a Single Public Subnet** and then choose **Select**.
5. For **IPv4 CIDR block**, enter the CIDR block for the VPC. We recommend that you use a CIDR block from the private (non-publicly routable) IP address ranges specified in RFC 1918. For example, 10.0.0.0/16. For more information, see **VPC and Subnet Sizing for IPv4** in the **Amazon VPC User Guide**.
6. For **IPv6 CIDR block**, keep **No IPv6 CIDR Block**.
7. For **VPC name**, enter a name for the VPC.
8. For **Public subnet’s IPv4 CIDR**, enter the CIDR block for the subnet.
9. For **Availability Zone**, choose the first one in the list.
10. (Optional) For **Subnet name**, enter a name for the subnet.
11. For **Service endpoints**, do nothing.
12. For **Enable DNS hostnames**, keep **Yes**.
13. For **Hardware tenancy**, keep **Default**.
14. Choose **Create VPC**. After the VPC is created, choose **OK**.

**Note**
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**.

For more information about working with IPv6 addresses, see **IP Addressing in Your VPC** in the **Amazon VPC User Guide**.

Step 2: Add a Second Public Subnet

In the previous step, you created a VPC with one public subnet. Use the following procedure to add a second public subnet and associate it with the route table for the first public subnet, which has a route to the internet gateway for the VPC.

**To add a public subnet**

1. In the navigation pane, choose **Subnets**.
2. Choose Create Subnet.
3. For Name tag, enter a name for the subnet.
4. For VPC, select the VPC that you created.
5. For Availability Zone, choose the second one in the list.
6. For IPv4 CIDR block, enter the CIDR block for the subnet.
7. Choose Create. After the subnet is created, choose Close.
8. Associate the new public subnet with the route table created for the first subnet as follows:
   a. In the navigation pane, choose Subnets.
   b. Select the first subnet.
   c. On the Route Table tab, choose the ID of the route table.
   d. On the Subnet Associations tab, choose Edit subnet associations.
   e. Select the check box for the second subnet and choose Save.

Step 3: Assign the Elastic IP Address

You can assign Elastic IP addresses to your WorkSpaces automatically or manually. To use automatic assignment, see Configure Automatic IP Addresses (p. 36). To assign Elastic IP addresses manually, use the following procedure.

For a video tutorial about how to assign an Elastic IP address to a WorkSpace, see How do I associate an Elastic IP Address with a WorkSpace? on the AWS Knowledge Center.

To assign an Elastic IP address to a WorkSpace manually
1. Open the Amazon 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 new address and choose Amazon pool or Owned by me, 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. Note that the value of VPC ID matches the ID of your WorkSpaces VPC and the value of Primary private IPv4 IP matches the primary private IP address of the WorkSpace that you noted earlier.
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.

IP Address and Port Requirements for Amazon WorkSpaces

To connect to your WorkSpaces, the network that your Amazon 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.

## Ports for Client Applications

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

**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. It must be open to the PCoIP Gateway IP address ranges and health check servers in the Region that the WorkSpace is in. For more information, see PCoIP Health Check Servers (p. 19) and PCoIP Gateway (p. 20).

## Ports for Web Access

Amazon WorkSpaces Web Access requires inbound and 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.

Typically, the web browser randomly selects a source port in the high range to use for streaming traffic. Amazon 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.

Amazon WorkSpaces Web Access prefers UDP over TCP for desktop streams, but falls back to TCP if UDP is not available. If all UDP ports are blocked except 53, 80, and 443, Web Access will work on Chrome and Firefox using TCP connections.
Whitelisted Domains and Ports

For the Amazon WorkSpaces client application to be able to access the Amazon WorkSpaces service, the following domains and ports must be whitelisted on the network from which the client is trying to access the service.

### Whitelisted Domains and Ports

<table>
<thead>
<tr>
<th>Category</th>
<th>Whitelisted</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPTCHA</td>
<td><a href="https://opfcaptcha-prod.s3.amazonaws.com/">https://opfcaptcha-prod.s3.amazonaws.com/</a></td>
</tr>
<tr>
<td>Client Auto-update</td>
<td>- <a href="https://d2td7dqidlhjx7.cloudfront.net/">https://d2td7dqidlhjx7.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>- In the AWS GovCloud (US-West) Region:</td>
</tr>
<tr>
<td></td>
<td><a href="https://s3.amazonaws.com/workspaces-client-updates/prod/pdt/windows/">https://s3.amazonaws.com/workspaces-client-updates/prod/pdt/windows/</a></td>
</tr>
<tr>
<td></td>
<td>WorkSpacesAppCast.xml</td>
</tr>
<tr>
<td>Connectivity Check</td>
<td><a href="https://connectivity.amazonworkspaces.com/">https://connectivity.amazonworkspaces.com/</a></td>
</tr>
<tr>
<td>Device Metrics (for 1.0+ and 2.0+ WorkSpaces client applications)</td>
<td><a href="https://device-metrics-us-2.amazon.com/">https://device-metrics-us-2.amazon.com/</a></td>
</tr>
<tr>
<td>Client Metrics (for 3.0+ WorkSpaces client applications)</td>
<td>Domains:</td>
</tr>
<tr>
<td></td>
<td>- <a href="https://skylight-client-ds.us-east-1.amazonaws.com">https://skylight-client-ds.us-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="https://skylight-client-ds.us-west-2.amazonaws.com">https://skylight-client-ds.us-west-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="https://skylight-client-ds.ap-southeast-1.amazonaws.com">https://skylight-client-ds.ap-southeast-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="https://skylight-client-ds.ap-northeast-1.amazonaws.com">https://skylight-client-ds.ap-northeast-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="https://skylight-client-ds.ca-central-1.amazonaws.com">https://skylight-client-ds.ca-central-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="https://skylight-client-ds.eu-central-1.amazonaws.com">https://skylight-client-ds.eu-central-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="https://skylight-client-ds.eu-west-1.amazonaws.com">https://skylight-client-ds.eu-west-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="https://skylight-client-ds.eu-west-2.amazonaws.com">https://skylight-client-ds.eu-west-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="https://skylight-client-ds.sa-east-1.amazonaws.com">https://skylight-client-ds.sa-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>- In the AWS GovCloud (US-West) Region:</td>
</tr>
<tr>
<td></td>
<td><a href="https://skylight-client-ds.us-gov-west-1.amazonaws.com">https://skylight-client-ds.us-gov-west-1.amazonaws.com</a></td>
</tr>
<tr>
<td>Directory Settings</td>
<td>Authentication from the client to the customer directory before login to the WorkSpace:</td>
</tr>
</tbody>
</table>

---
## Whitelisted Domains and Ports

<table>
<thead>
<tr>
<th>Category</th>
<th>Whitelisted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connections from macOS clients:</td>
<td>• <a href="https://d32i4gd7pg4909.cloudfront.net/prod/">https://d32i4gd7pg4909.cloudfront.net/prod/</a>&lt;region&gt;/&lt;directory ID&gt;</td>
</tr>
<tr>
<td>Customer directory settings:</td>
<td>• <a href="https://d21ui22avrxoh6.cloudfront.net/prod/">https://d21ui22avrxoh6.cloudfront.net/prod/</a>&lt;region&gt;/&lt;directory ID&gt;</td>
</tr>
<tr>
<td>Login page graphics for customer directory level co-branding:</td>
<td>• <a href="https://d1cbg795sa4g1u.cloudfront.net/prod/">https://d1cbg795sa4g1u.cloudfront.net/prod/</a>&lt;region&gt;/&lt;directory ID&gt;</td>
</tr>
<tr>
<td>CSS file to style the login pages:</td>
<td>• <a href="https://d3s98kk2h6f4oh.cloudfront.net/">https://d3s98kk2h6f4oh.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://dyqsoz7pkju4e.cloudfront.net/">https://dyqsoz7pkju4e.cloudfront.net/</a></td>
</tr>
<tr>
<td>JavaScript file for the login pages:</td>
<td>• US East (N. Virginia) — <a href="https://d32i4gd7pg4909.cloudfront.net/">https://d32i4gd7pg4909.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• US West (Oregon) — <a href="https://d18af7771co7lp.cloudfront.net/">https://d18af7771co7lp.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• Asia Pacific (Seoul) — <a href="https://dtyv4uwoh7ynt.cloudfront.net/">https://dtyv4uwoh7ynt.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• Asia Pacific (Singapore) — <a href="https://d3qzmd7y07pz0i.cloudfront.net/">https://d3qzmd7y07pz0i.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• Asia Pacific (Sydney) — <a href="https://dwcpoxuuza83q.cloudfront.net/">https://dwcpoxuuza83q.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• Asia Pacific (Tokyo) — <a href="https://d2c2t8mxjqh5z1.cloudfront.net/">https://d2c2t8mxjqh5z1.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• Canada (Central) — <a href="https://d2wfbsypmqjmqog.cloudfront.net/">https://d2wfbsypmqjmqog.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• Europe (Frankfurt) — <a href="https://d1whcm49570ijw.cloudfront.net/">https://d1whcm49570ijw.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• Europe (Ireland) — <a href="https://d3pgffbf39h4k4.cloudfront.net/">https://d3pgffbf39h4k4.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• Europe (London) — <a href="https://d16q6638mh01s7.cloudfront.net/">https://d16q6638mh01s7.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• South America (São Paulo) — <a href="https://d2lh2qc5bdoq4b.cloudfront.net/">https://d2lh2qc5bdoq4b.cloudfront.net/</a></td>
</tr>
</tbody>
</table>

In the AWS GovCloud (US-West) Region:
## Whitelisted Domains and Ports

<table>
<thead>
<tr>
<th>Category</th>
<th>Whitelisted</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Customer directory settings:</td>
</tr>
<tr>
<td></td>
<td><a href="https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/">https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/</a>&lt;directory ID&gt;</td>
</tr>
<tr>
<td></td>
<td>• Login page graphics for customer directory level co-branding:</td>
</tr>
<tr>
<td></td>
<td><a href="https://s3.amazonaws.com/workspaces-client-assets/prod/pdt/">https://s3.amazonaws.com/workspaces-client-assets/prod/pdt/</a>&lt;directory ID&gt;</td>
</tr>
<tr>
<td></td>
<td>• CSS file to style the login pages:</td>
</tr>
<tr>
<td></td>
<td><a href="https://s3.amazonaws.com/workspaces-client-css/workspaces_v2.css">https://s3.amazonaws.com/workspaces-client-css/workspaces_v2.css</a></td>
</tr>
<tr>
<td></td>
<td>• JavaScript file for the login pages:</td>
</tr>
<tr>
<td></td>
<td>Not applicable</td>
</tr>
<tr>
<td>Forrester Log Service</td>
<td><a href="https://fls-na.amazon.com/">https://fls-na.amazon.com/</a></td>
</tr>
<tr>
<td>PCoIP Health Check (DRP)</td>
<td>PCoIP Health Check Servers (p. 19)</td>
</tr>
<tr>
<td>PCoIP Session Gateway (PSG)</td>
<td>PCoIP Gateway (p. 20)</td>
</tr>
<tr>
<td>Registration Dependency</td>
<td><a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
</tr>
<tr>
<td>Session Broker (PCM)</td>
<td>Domains:</td>
</tr>
<tr>
<td></td>
<td><a href="https://skylight-cm.us-east-1.amazonaws.com">https://skylight-cm.us-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://skylight-cm-ap-northeast-1.amazonaws.com">https://skylight-cm-ap-northeast-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://skylight-cm-ap-southeast-1.amazonaws.com">https://skylight-cm-ap-southeast-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://skylight-cm-ap-northeast-2.amazonaws.com">https://skylight-cm-ap-northeast-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://skylight-cm-us-east-1.amazonaws.com">https://skylight-cm-us-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://skylight-cm-us-west-1.amazonaws.com">https://skylight-cm-us-west-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://skylight-cm-us-west-2.amazonaws.com">https://skylight-cm-us-west-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://skylight-cm-fips.us-east-1.amazonaws.com">https://skylight-cm-fips.us-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://skylight-cm-fips.us-west-2.amazonaws.com">https://skylight-cm-fips.us-west-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://skylight-cm-fips.us-west-1.amazonaws.com">https://skylight-cm-fips.us-west-1.amazonaws.com</a></td>
</tr>
</tbody>
</table>
## Whitelisted Domains and Ports

<table>
<thead>
<tr>
<th>Category</th>
<th>Whitelisted</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Login Pages</td>
<td>https://&lt;directory id&gt;.awsapps.com/ (where &lt;directory id&gt; is the customer's domain)</td>
</tr>
<tr>
<td>Web Access TURN Servers</td>
<td>Servers:</td>
</tr>
<tr>
<td></td>
<td>• turn:*-us-east-1.rdn.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>• turn:*-us-west-2.rdn.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>• turn:*-ap-northeast-2.rdn.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>• turn:*-ap-southeast-1.rdn.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>• turn:*-ap-southeast-2.rdn.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>• turn:*-ap-northeast-1.rdn.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>• turn:*-ca-central-1.rdn.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>• turn:*-eu-central-1.rdn.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>• turn:*-eu-west-1.rdn.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>• turn:*-eu-west-2.rdn.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>• turn:*-sa-east-1.rdn.amazonaws.com</td>
</tr>
<tr>
<td>WS Broker</td>
<td>Domains:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service.us-east-1.amazonaws.com">https://ws-broker-service.us-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service-fips.us-east-1.amazonaws.com">https://ws-broker-service-fips.us-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service.us-west-2.amazonaws.com">https://ws-broker-service.us-west-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service-fips.us-west-2.amazonaws.com">https://ws-broker-service-fips.us-west-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service.ap-northeast-2.amazonaws.com">https://ws-broker-service.ap-northeast-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service.ap-southeast-1.amazonaws.com">https://ws-broker-service.ap-southeast-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service.ap-southeast-2.amazonaws.com">https://ws-broker-service.ap-southeast-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service.ap-northeast-1.amazonaws.com">https://ws-broker-service.ap-northeast-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service.ca-central-1.amazonaws.com">https://ws-broker-service.ca-central-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service.eu-central-1.amazonaws.com">https://ws-broker-service.eu-central-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service.eu-west-1.amazonaws.com">https://ws-broker-service.eu-west-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service.eu-west-2.amazonaws.com">https://ws-broker-service.eu-west-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service.sa-east-1.amazonaws.com">https://ws-broker-service.sa-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service.us-gov-west-1.amazonaws.com">https://ws-broker-service.us-gov-west-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-broker-service-fips.us-gov-west-1.amazonaws.com">https://ws-broker-service-fips.us-gov-west-1.amazonaws.com</a></td>
</tr>
</tbody>
</table>
PCoIP Health Check Servers

The Amazon WorkSpaces client applications perform PCoIP health checks over port 4172. These checks validate whether TCP or UDP traffic streams from the Amazon WorkSpaces servers to the client applications. For these checks to finish successfully, your firewall policies must take into account the following Regional PCoIP health check servers.

<table>
<thead>
<tr>
<th>Region</th>
<th>Health check server</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>drp-iad.amazonworkspaces.com</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>drp-pdx.amazonworkspaces.com</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>drp-icn.amazonworkspaces.com</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>drp-sin.amazonworkspaces.com</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>drp-syd.amazonworkspaces.com</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>drp-nrt.amazonworkspaces.com</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>drp-yul.amazonworkspaces.com</td>
</tr>
</tbody>
</table>
PCoIP Gateway

Amazon WorkSpaces uses PCoIP to stream the desktop session to clients over port 4172. Amazon WorkSpaces uses a small range of Amazon EC2 public IP addresses for its PCoIP gateway servers. This enables you to set more finely grained firewall policies for devices that access Amazon WorkSpaces.

<table>
<thead>
<tr>
<th>Region</th>
<th>Health check server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>drp-fra.amazonworkspaces.com</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>drp-dub.amazonworkspaces.com</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>drp-lhr.amazonworkspaces.com</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>drp-gru.amazonworkspaces.com</td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td>drp-pdt.amazonworkspaces.com</td>
</tr>
</tbody>
</table>

## Public IP Address Range

<table>
<thead>
<tr>
<th>Region</th>
<th>Public IP Address Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>52.23.61.0 - 52.23.62.255, 3.217.228.0 - 3.217.231.255</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>54.244.46.0 - 54.244.47.255</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>13.124.247.0 - 13.124.247.255</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>52.76.127.0 - 52.76.127.255</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>54.153.254.0 - 54.153.254.255</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>54.250.251.0 - 54.250.251.255</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>35.183.255.0 - 35.183.255.255</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>52.59.127.0 - 52.59.127.255</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>52.19.124.0 - 52.19.125.255</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>35.176.32.0 - 35.176.32.255</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>54.233.204.0 - 54.233.204.255</td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td>52.61.193.0 - 52.61.193.255</td>
</tr>
</tbody>
</table>

## Network Interfaces

Each WorkSpace has the following network interfaces:

- The primary network interface 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 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.
Amazon 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, Amazon 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.

Do not modify or delete any of the network interfaces attached to a WorkSpace. Doing so might cause the WorkSpace to become unreachable.

Management Interface IP Ranges

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

<table>
<thead>
<tr>
<th>Region</th>
<th>IP Address Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>192.168.0.0/16 and 198.19.0.0/16</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>172.31.0.0/16, 192.168.0.0/16, and 198.19.0.0/16</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>198.19.0.0/16</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>198.19.0.0/16</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>172.31.0.0/16, 192.168.0.0/16, and 198.19.0.0/16</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>198.19.0.0/16</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>198.19.0.0/16</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>198.19.0.0/16</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>172.31.0.0/16, 192.168.0.0/16, and 198.19.0.0/16</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>198.19.0.0/16</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>198.19.0.0/16</td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td>198.19.0.0/16</td>
</tr>
</tbody>
</table>

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.
- Inbound UDP on port 4172. This is used for streaming user input.
- Inbound TCP on port 4489. This is for access using the web client.
- Inbound TCP on port 8200. This is used for management and configuration of the WorkSpace.
- Outbound TCP on ports 8443 and 9997. This is used for access using the web client.
- Outbound UDP on ports 3478 and 4172. This is used for access using the web client.
- Outbound UDP on ports 50002 and 55002. This is used for PCoIP 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 need to open ephemeral ports 49152 - 65535 to allow return communication.

- Outbound TCP on port 80 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 and Office activation.

Under normal circumstances, the Amazon 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 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.

### Amazon WorkSpaces Client Network Requirements

Your Amazon 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.

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.
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 Amazon WorkSpaces (p. 13).

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 250ms, the user can access the WorkSpace but performance is degraded.

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.

The clients require HTTPS access to Amazon 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 launch and configure an EC2 instance with PCoIP Connection Manager for Amazon WorkSpaces. For more information, see Deploying the PCoIP Connection Manager for Amazon WorkSpaces in the PCoIP Connection Manager User Guide.

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

To verify client networking requirements

1. Open the Amazon 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 WorkSpaces Access to Trusted Devices

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.

When you enable this feature, Amazon 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, Amazon 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.

Important
This feature is supported for Windows computers and macOS computers.

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

- Certificates must be Base64-encoded certificate files in CRT, CERT, or PEM format.
- Certificates must include a Common Name.
- The maximum length of certificate chain supported is 4.
Step 2: Deploy Client Certificates to the Trusted Devices

You must install client certificates on the trusted devices for your users. 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.

On Windows, the WorkSpaces client application searches for client certificates in both the user and root certificate stores. On macOS, the WorkSpaces client application searches for client certificates in the entire keychain.

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 Amazon 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.
6. [macOS] Choose Only Allow Trusted macOS Devices to Access WorkSpaces.
7. 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.
8. Choose Update and Exit.

Provide Internet Access from Your WorkSpace

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 configure automatic assignment of public IP addresses.
- Launch your WorkSpaces in public subnets and manually assign public IP addresses to your WorkSpaces.

For more information, see Configure a VPC for Amazon WorkSpaces (p. 8).

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 WAM

If you are using Amazon WorkSpaces Application Manager (Amazon WAM) to deploy applications to your WorkSpaces, your WorkSpaces must have access to the internet.

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.

```json
{
  "Statement": [
    {
      "Sid": "AmazonLinux2AMIMRepositoryAccess",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amazonlinux.*.amazonaws.com/*"
      ]
    }
  ]
}
```

Security Groups for Your WorkSpaces

When you register a directory with Amazon 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-92673056e8_controllers) and the security group for WorkSpaces has a name that consists of the directory identifier followed by _workspacesMembers (for example, d-926720fc18_workspacesMembers).

**Important**

Do not delete the _workspacesMembers security group. If you delete this security group, your WorkSpaces won't function correctly and you won't be able to recreate this group and add it back.
You can have an additional security group for WorkSpaces. After you add the security group to the directory, it is associated with new WorkSpaces that you launch or existing WorkSpaces that you rebuild.

**To add a security group to a directory**

1. Open the Amazon 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**.

**IP Access Control Groups for Your WorkSpaces**

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

There is a default IP access control group associated with each directory. The default group allows all traffic. 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.

You can use this feature with Web Access and the client applications for macOS, iPad, Windows, Chromebook, and Android. To use this feature with a PCoIP zero client, you cannot use PCoIP Connection Manager.

**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 Amazon 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 Amazon 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 Amazon 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 Amazon 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 Client for WorkSpaces**

If your zero client device has firmware version 6.0.0 or later, your users can connect to their WorkSpaces directly. Otherwise, if the firmware is between 4.6.0 and 6.0.0, you must set up Teradici PCoIP Connection Manager for Amazon WorkSpaces and provide your users with server URIs to connect to their WorkSpaces through Teradici PCoIP Connection Manager for Amazon WorkSpaces.

To set up PCoIP Connection Manager for Amazon WorkSpaces on an EC2 instance, go to AWS Marketplace and find an Amazon Machine Image (AMI) that you can use to launch an instance with PCoIP Connection Manager. For more information, see **Deploying the PCoIP Connection Manager for Amazon WorkSpaces** in the **PCoIP Connection Manager User Guide**.
For information about setting up and connecting with a PCoIP zero client device, see PCoIP Zero Client in the Amazon WorkSpaces User Guide.

Set Up Amazon WorkSpaces for FedRAMP Authorization or DoD SRG Compliance

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.

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.

- 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
  - 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

To use FIPS endpoint encryption

1. Open the Amazon 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 (p. 28) section.

Enable SSH Connections for Your Linux WorkSpaces

If you or your users want to connect to your Amazon 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 Amazon Linux WorkSpaces.

Contents
- Prerequisites for SSH Connections to Amazon Linux WorkSpaces (p. 29)
- Enable SSH Connections to All Amazon Linux WorkSpaces in a Directory (p. 30)
- Enable SSH Connections to a Specific Amazon Linux WorkSpace (p. 31)
- Connect to an Amazon Linux WorkSpace by Using Linux or PuTTY (p. 31)

Prerequisites for SSH Connections to Amazon Linux WorkSpaces

- Enabling inbound SSH traffic to a WorkSpace — To add a rule to allow inbound SSH traffic to one or more Amazon 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 an Amazon 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 Amazon Linux WorkSpace you want to connect to and your user name

1. Open the Amazon 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
2. In the list of directories, click the Directory ID link of the directory for the WorkSpace.

Enable SSH Connections to All Amazon Linux WorkSpaces in a Directory

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

To create a security group with a rule to allow inbound SSH traffic to all Amazon 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.
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, 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 Create.
Enable SSH Connections to a Specific Amazon Linux WorkSpace

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

**To add a rule to an existing security group to allow inbound SSH traffic to a specific Amazon 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 an Amazon Linux WorkSpace by 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 Amazon Linux WorkSpaces” earlier in this topic.

**To connect to an Amazon Linux WorkSpace by 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

<table>
<thead>
<tr>
<th>ssh  &quot;anycompany\junedoe&quot;@203.0.113.25</th>
</tr>
</thead>
</table>

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

To connect to an Amazon Linux WorkSpace by 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

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

**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**

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.

**Note**

If antivirus software is installed on the WorkSpace, exclude the following locations.
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.

- `/var/lib/skylight`
- `/var/lib/pcoip-agent`
- `/var/log/skylight`
- `/var/log/pcoip-agent`
- `/etc/pam.d/pcoip`
- `/etc/pam.d/pcoip-session`
- `/etc/X11/default-display-manager`
- `/etc/os-release`
- `/etc/profile.d/system-restart-check.sh`
- `/etc/yum/pluginconf.d/halt_os_update_check.conf`
- `/usr/lib/skylight`
- `/usr/lib/pcoip-agent`
- `/usr/lib/systemd/system/pcoip.service.d/`
- `/usr/lib/systemd/system/pcoip.service`
- `/usr/lib/system.d/system/skylight-agent.service`
- `/usr/lib/yum-plugins/halt_os_update_check.p`
Manage Directories for Amazon WorkSpaces

Amazon 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.
- **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 Microsoft AD directory and your on-premises domain.

For tutorials that demonstrate how to set up these directories and launch WorkSpaces, see Launch a Virtual Desktop Using Amazon WorkSpaces (p. 47).

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 Amazon WorkSpaces console and other tasks using Group Policy.

**Note**
Shared directories are not currently supported with WorkSpaces.

**Contents**
- Register a Directory with Amazon WorkSpaces (p. 34)
- Update Directory Details for Your WorkSpaces (p. 35)
- Delete the Directory for Your WorkSpaces (p. 38)
- Enable Amazon WorkDocs for Microsoft Active Directory (p. 38)
- Set Up Active Directory Administration Tools for Amazon WorkSpaces (p. 39)
- Manage Your Windows WorkSpaces Using Group Policy (p. 40)
- Manage Your Amazon Linux WorkSpaces (p. 44)

## Register a Directory with Amazon WorkSpaces

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

**To register a directory**

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select the directory.
4. Choose **Actions, Register**.
5. Select two subnets that are not from the same Availability Zone.

6. 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.

7. 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 Microsoft Active Directory (AD). If you’re using Microsoft AD, finish registering your directory, and then see **Enable Amazon WorkDocs for Microsoft Active Directory** (p. 38).

8. Choose Register. Initially the value of Registered is REGISTERING. After registration is complete, the value is Yes.

When you are finished using the directory with Amazon WorkSpaces, you can deregister it. Note that you must deregister a directory before you can delete it. If you have any Amazon WAM applications assigned to your users, you must remove those assignments before you can delete a directory. For more information, see **Removing Application Assignments** in the **Amazon WAM Administration Guide**.

**To deregister a directory**

1. Open the Amazon 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.

---

**Update Directory Details for Your WorkSpaces**

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

**Tasks**
- Select an Organizational Unit (p. 35)
- Configure Automatic IP Addresses (p. 36)
- Control Device Access (p. 36)
- Manage Local Administrator Permissions (p. 37)
- Update the AD Connector Account (AD Connector) (p. 37)
- Multi-factor Authentication (AD Connector) (p. 37)

**Select an Organizational Unit**

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 Amazon 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 Target Domain and Organizational Unit.
5. To find an OU, you can type all or part of the OU name and choose Search OU. Alternatively, you can choose List all OU to list all OUs.
6. Select the OU and choose Update and Exit.
7. (Optional) Rebuild the existing WorkSpaces to update the OU. For more information, see Rebuild a WorkSpace (p. 69).

To specify a target domain and organizational unit

1. Open the Amazon 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 Target Domain and Organizational Unit.
5. For Selected OU, type the full LDAP distinguished name for the target domain and OU and then choose Update and Exit. For example, OU=WorkSpaces_machines,DC=machines,DC=example,DC=com.
6. (Optional) Rebuild the existing WorkSpaces to update the OU. For more information, see Rebuild a WorkSpace (p. 69).

Configure Automatic IP Addresses

After you enable automatic assignment of Elastic public IP addresses, each WorkSpace that you launch is assigned an Elastic public IP address. This allows WorkSpaces in public subnets to access the internet. WorkSpaces that exist at the time that you enable automatic assignment do not receive an Elastic public IP address until you rebuild them.

Note that you do not need to enable automatic assignment of Elastic public IP 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 manually assigned Elastic IP addresses. For more information, see Configure a VPC for Amazon WorkSpaces (p. 8).

To configure Elastic public IP addresses

1. Open the Amazon 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 restrict access to WorkSpaces to trusted devices (also known as managed devices).
To control device access to WorkSpaces

1. Open the Amazon 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 and find the Other Platforms section. By default, WorkSpaces Web Access and Linux clients are disabled, and users can access their WorkSpaces from their iOS devices, Android devices, Chromebooks, and PCoIP zero client devices.
5. Select the device types to enable and clear the device types to disable. To block access from all selected device types, choose Block.
6. (Optional) You can restrict access to trusted devices. For more information, see Restrict WorkSpaces Access to Trusted Devices (p. 23).
7. Choose Update and Exit.

Manage Local Administrator Permissions

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 Amazon 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 Local Administrator Setting.
5. To ensure that users are local administrators, choose Enable. Otherwise, choose Disable.
6. Choose Update and Exit.

Update the AD Connector Account (AD Connector)

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

To update the AD Connector account

1. Open the Amazon 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 Update AD Connector Account.
5. Type the user name and password for the new account.
6. Choose Update and Exit.

Multi-factor Authentication (AD Connector)

You can enable multi-factor authentication for your AD Connector directory.
To enable multi-factor authentication

1. Open the Amazon 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 (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 20.
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.

Delete the Directory for Your WorkSpaces

You can delete the directory for your WorkSpaces if it is no longer in use by other WorkSpaces or applications such as Amazon WorkDocs, Amazon WorkMail, or Amazon Chime. Note that you must deregister a directory before you can delete it.

To delete a directory

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose Directories.
3. Select the directory and choose Actions, Deregister.
4. When prompted for confirmation, choose Deregister.
5. Select the directory again and choose Actions, Delete.
6. When prompted for confirmation, choose Delete.

Enable Amazon WorkDocs for Microsoft Active Directory

If you're using Microsoft Active Directory (AD) with Amazon WorkSpaces, you can enable Amazon WorkDocs for your directory through either the Amazon WorkDocs console or the AWS Directory Service console.

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**

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 Amazon WorkSpaces**

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 Amazon WorkSpaces console to perform some directory-related tasks. For more information, see Manage Directories for Amazon WorkSpaces (p. 34).

If you create a directory with 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 a Windows instance and join it to your WorkSpaces directory.
   
   You can join an Amazon EC2 Windows instance to your directory domain when you launch the instance. For more information, see Joining a Windows Instance to an AWS Directory Service Domain in the Amazon EC2 User Guide for Windows Instances.
   
   Alternatively, you can join the instance to your directory manually. For more information, see Manually Add a Windows Instance (Simple AD and Microsoft AD) in the AWS Directory Service Administration Guide.
   
2. Install the Active Directory Administration Tools on the instance. For more information, see Installing the Active Directory Administration Tools in the AWS Directory Service Administration Guide.
3. Run the tools as a directory administrator as follows:
   
   a. Open the **Administrative Tools**.
   b. Hold down the Shift key, right-click the tool shortcut, and choose **Run as different user**.
c. Type the username and password for the administrator. With Simple AD, the username is **Administrator** and with 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**

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 user 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 use whichever Active Directory tools you are familiar with to manage user objects. Note that before you can remove a user, you must delete the WorkSpace assigned to that user. For more information, see Delete a WorkSpace (p. 74).

**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.

---

Manage Your Windows WorkSpaces Using Group Policy

You can use Group Policy objects to apply settings to manage Windows WorkSpaces or users that are part of your Windows WorkSpaces directory.

**Note**

Linux instances do not adhere to Group Policy. For information about managing Amazon Linux WorkSpaces, see Manage Your Amazon Linux WorkSpaces (p. 44).

We recommend that you create an organizational unit for your WorkSpaces Computer Objects and an organizational unit for your WorkSpaces User Objects.

Group Policy settings can affect a WorkSpace user’s experience as follows:

- Some Group Policy settings force a user to log off when they are disconnected from a session. Any applications that a user has open on the WorkSpace are closed.
• Implementing an interactive logon message to display a logon banner prevents users from being able to access their WorkSpace. The interactive logon message Group Policy setting is not currently supported by Amazon WorkSpaces.
• Disabling removable storage through Group Policy settings will cause a login failure that results in users being logged in to a temporary profile with no access to drive D.
• 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 WorkSpace. To prevent this issue from occurring, make sure that your users can access drive C and drive D.

Contents
• Install the Group Policy Administrative Template (p. 41)
• Configure Printer Support for Windows WorkSpaces (p. 41)
• Enable or Disable Clipboard Redirection for Windows WorkSpaces (p. 42)
• Set the Session Resume Timeout for Windows WorkSpaces (p. 43)
• Set the Maximum Lifetime for a Kerberos Ticket (p. 44)

Install the Group Policy Administrative Template

To use the Group Policy settings that are specific to Amazon WorkSpaces, you must install the Group Policy administrative template. Perform the following procedure on a directory administration WorkSpace or Amazon EC2 instance that is joined to your directory.

To install the Group Policy administrative template
1. From a running Windows WorkSpace client, make a copy of the pcoip.adm file in the C:\Program Files (x86)\Teradici\PCoIP Agent\configuration directory.
2. Open the Group Policy Management tool 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 Group Policy object, 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 Group Policy object 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 Group Policy object to modify the Group Policy settings that are specific to Amazon WorkSpaces.

Configure Printer Support for Windows WorkSpaces

By default, Amazon 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. The Group Policy setting change takes effect after the WorkSpace's next Group Policy settings update and the session is restarted.

To configure printer support

1. Make sure that the most recent Amazon WorkSpaces Group Policy administrative template (p. 41) 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. Choose Action, Edit in the main menu.
3. In the Group Policy Management Editor, choose Computer Configuration, Policies, Administrative Templates, Classic Administrative Templates, PCoIP Session Variables, and Overridable Administrator Defaults.
4. Open the Configure remote printing setting.
5. 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.
6. Choose OK.

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 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 the most recent Amazon WorkSpaces Group Policy administrative template (p. 41) is installed in your domain.
2. Open the Group Policy Management tool and navigate to and select the WorkSpaces Group Policy object for your WorkSpaces machine accounts. Choose Action, Edit in the main menu.
3. In the Group Policy Management Editor, choose Computer Configuration, Policies, Administrative Templates, Classic Administrative Templates, PCoIP Session Variables, and Overridable Administrator Defaults.
4. Open the Configure remote printing setting.
5. Choose Enabled, and then under Options, Configure remote printing, choose either Basic and Advanced printing for Windows clients or choose Basic printing, select Automatically set default printer, and then choose OK.

Enable or Disable Clipboard Redirection for Windows WorkSpaces

By default, Amazon WorkSpaces supports clipboard redirection. If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

The Group Policy setting change takes effect after the WorkSpace's next Group Policy settings update and the client session is restarted.
To enable or disable clipboard redirection for Windows WorkSpaces

1. Make sure that the most recent Amazon WorkSpaces Group Policy administrative template (p. 41) is installed in your domain.
2. Open the Group Policy Management tool and navigate to and select the WorkSpaces Group Policy object for your WorkSpaces machine accounts. Choose Action, Edit in the main menu.
3. In the Group Policy Management Editor, choose Computer Configuration, Policies, Administrative Templates, Classic Administrative Templates, PCoIP Session Variables, and Overridable Administrator Defaults.
4. Open the Configure clipboard redirection setting.
5. 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

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 Windows WorkSpaces

When using the Amazon WorkSpaces client applications, an interruption of network connectivity causes an active session to be disconnected. This can be caused by events such as closing the laptop lid, or the loss of your wireless network connection. The Amazon WorkSpaces client applications for Windows and macOS attempt to reconnect the session automatically if network connectivity is regained 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.

The Group Policy setting change takes effect after the WorkSpace's next Group Policy settings update and the session is restarted.

To set the automatic session resume timeout value

1. Make sure that the most recent Amazon WorkSpaces Group Policy administrative template (p. 41) is installed in your domain.
2. Open the Group Policy Management tool and navigate to and select the WorkSpaces Group Policy object for your WorkSpaces machine accounts. Choose Action, Edit in the main menu.
3. In the Group Policy Management Editor, choose Computer Configuration, Policies, Administrative Templates, Classic Administrative Templates, and PCoIP Session Variables.
   To allow the user to override your setting, choose Overridable Administrator Defaults; otherwise, choose Not Overridable Administrator Defaults.
4. Open the Configure Session Automatic Reconnection Policy setting.
5. 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.
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 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 WorkSpace Management Capabilities for Your Users (p. 60).

Manage Your Amazon Linux WorkSpaces

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.

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. For a full listing of the available settings, run man pcoip-agent.conf from the terminal on any Amazon Linux WorkSpace.

Enable or Disable Clipboard Redirection for Amazon Linux WorkSpaces

By default, Amazon WorkSpaces supports clipboard redirection. Use the PCoIP Agent conf to disable this feature, if needed.

The Group Policy setting change takes effect after the WorkSpace's next Group Policy settings update and the session is restarted.

To enable or disable clipboard redirection for 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.
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.

   ```bash
   [example\username@workspace-id ~]$ sudo visudo
   ```

2. Add the following line.

   ```bash
   %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.

   ```bash
   [example\username@workspace-id ~]$ sudo vi /etc/security/access.conf
   ```

2. Add the following line.

   ```bash
   +:(example\Linux_WorkSpaces_Admins):ALL
   ```

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.
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 from Your WorkSpace (p. 24).
Launch a Virtual Desktop Using Amazon WorkSpaces

With Amazon WorkSpaces, you can provision virtual, cloud-based Microsoft Windows or Amazon Linux desktops for your users, known as WorkSpaces.

Amazon WorkSpaces uses a directory to store and manage information for your WorkSpaces and users. You can do any 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.

The following tutorials show you how to launch a WorkSpace by using the supported directory service options.

Tutorials
• Launch a WorkSpace Using AWS Managed Microsoft AD (p. 47)
• Launch a WorkSpace Using Simple AD (p. 50)
• Launch a WorkSpace Using AD Connector (p. 52)
• Launch a WorkSpace Using a Trusted Domain (p. 55)

Launch a WorkSpace Using AWS Managed Microsoft AD

Amazon WorkSpaces enables you to provision virtual, cloud-based Windows desktops for your users, known as WorkSpaces.

Amazon WorkSpaces uses directories to store and manage information for your WorkSpaces and users. For your directory, you can choose from Simple AD, AD Connector, or AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD. In addition, you can establish a trust relationship between your AWS Managed Microsoft AD directory and your on-premises domain.

In this tutorial, we launch a WorkSpace that uses AWS Managed Microsoft AD. For tutorials that use the other options, see Launch a Virtual Desktop Using Amazon WorkSpaces (p. 47).

Tasks
• Before You Begin (p. 48)
• Step 1: Create an AWS Managed Microsoft AD Directory (p. 48)
• Step 2: Create a WorkSpace (p. 48)
• Step 3: Connect to the WorkSpace (p. 49)
• Next Steps (p. 49)
Before You Begin

- Amazon 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 Amazon WorkSpaces Pricing by AWS Region.
- When you launch a WorkSpace, you must select a WorkSpace bundle. A bundle is a combination of an operating system, and storage, compute, and software resources. For more information, see Amazon WorkSpaces Bundles.
- When you create a directory using AWS Directory Service or launch a WorkSpace, you must create or select a virtual private cloud configured with a public subnet and two private subnets. For more information, see Configure a VPC for Amazon WorkSpaces (p. 8).

Step 1: Create an AWS Managed Microsoft AD Directory

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.

To create an AWS Managed Microsoft AD directory

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Choose **Set up Directory, Create Microsoft AD**.
4. 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).
   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**.
5. Choose **Create Microsoft AD**.
6. Choose **Done**. The initial status of the directory is **Creating**. When directory creation is complete, the status is **Active**.

Step 2: Create a WorkSpace

Now that you have created an AWS Managed Microsoft AD directory, you are ready to create a WorkSpace.
To create a WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose WorkSpaces.
3. Choose Launch WorkSpaces.
4. On the Select a Directory page, choose the directory that you created, and then choose Next Step. Amazon WorkSpaces registers your directory.
5. On the Identify Users page, add a new user to your directory as follows:
   a. Complete Username, First Name, Last Name, and Email. Use an email address that you have access to.
   b. Choose Create Users.
   c. Choose Next Step.
6. On the Select Bundle page, select a bundle and then choose Next Step.
7. On the WorkSpaces Configuration page, choose a running mode and then choose Next Step.
8. On the Review & Launch WorkSpaces page, choose Launch WorkSpaces. 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 the user.

Step 3: Connect to the WorkSpace

After you receive the invitation email, 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. When prompted, specify a password and activate the user. Remember this password as you will need it to sign in 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 three of the following categories: lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9), and ~!@#$%^&*_-+=`|}{\:[;"'<>,.?/.
2. When prompted, download one of the client applications or, for Windows WorkSpaces, launch Web Access.
   Note
   You cannot use a web browser to connect to Amazon Linux WorkSpaces.
   If you aren’t prompted and you haven’t installed a client application already, open https://clients.amazonworkspaces.com/ and follow the directions.
3. Start the client, enter the registration code from the invitation email, and choose Register.
4. When prompted to sign in, enter the user name and password for the user, and then choose Sign In.
5. (Optional) When prompted to save your credentials, choose Yes.

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. If you are finished with your WorkSpace, you can delete it. For more information, see the following documentation.

- Create a Custom WorkSpaces Bundle (p. 75)
Launch a WorkSpace Using Simple AD

Amazon WorkSpaces enables you to provision virtual, cloud-based Microsoft Windows desktops for your users, known as WorkSpaces.

Amazon WorkSpaces uses directories to store and manage information for your WorkSpaces and users. For your directory, you can choose from Simple AD, AD Connector, or AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD. In addition, you can establish a trust relationship between your AWS Managed Microsoft AD directory and your on-premises domain.

In this tutorial, we launch a WorkSpace that uses Simple AD. For tutorials that use the other options, see Launch a Virtual Desktop Using Amazon WorkSpaces (p. 47).

Tasks
- Before You Begin (p. 50)
- Step 1: Create a Simple AD Directory (p. 50)
- Step 2: Create a WorkSpace (p. 51)
- Step 3: Connect to the WorkSpace (p. 52)
- Next Steps (p. 52)

Before You Begin

- 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, see the Simple AD table under AWS Directory Service.
- Amazon 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 Amazon WorkSpaces Pricing by AWS Region.
- When you launch a WorkSpace, you must select a WorkSpace bundle. A bundle is a combination of an operating system, and storage, compute, and software resources. For more information, see Amazon WorkSpaces Bundles.
- When you create a directory using AWS Directory Service or launch a WorkSpace, you must create or select a virtual private cloud configured with a public subnet and two private subnets. For more information, see Configure a VPC for Amazon WorkSpaces (p. 8).

Step 1: Create a Simple AD Directory

Create a Simple 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 create the WorkSpace.

To create a Simple AD directory
1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose Directories.
3. Choose Set up Directory, Create Simple AD.
4. 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**, enter the fully-qualified name for the directory (for example, example.com).
   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. Keep **Directory size** as **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 Step**.
5. Choose **Create Simple AD**.
6. Choose **Done**. The initial status of the directory is Requested and then Creating. When directory creation is complete, the status is Active.

**Directory Creation**

Amazon WorkSpaces completes the following tasks on your behalf:

- Creates an IAM role to allow the Amazon WorkSpaces service to create elastic network interfaces and list your Amazon 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.

**Step 2: Create a WorkSpace**

Now you are ready to launch the WorkSpace.

**To create a WorkSpace for a user**

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Choose **Launch WorkSpaces**.
4. On the **Select a Directory** page, do the following:
   a. For **Directory**, choose the directory that you created.
   b. For **Enable Amazon WorkDocs**, choose **Yes**.
      **Note**
      This option is available only if Amazon WorkDocs is available in the selected Region.
   c. Choose **Next**. Amazon WorkSpaces registers your Simple AD directory.
5. On the **Identify Users** page, add a new user to your directory as follows:
   a. Complete **Username, First Name, Last Name**, and **Email**. Use an email address that you have access to.
Step 3: Connect to the WorkSpace

After you receive the invitation email, 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. When prompted, enter a password and activate the user. Remember this password as you will need it to sign in 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 four of the following categories: lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9), and ~!@#$%^&*_-+=`\{}[]:;"'<>,.?/

2. 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 follow the directions.

3. Start the client, enter the registration code from the invitation email, and choose Register.

4. When prompted to sign in, enter the user name and password for the user, and then choose Sign In.

5. (Optional) When prompted to save your credentials, choose Yes.

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. If you are finished with your WorkSpace, you can delete it. For more information, see the following documentation.

- Create a Custom WorkSpaces Bundle (p. 75)
- Administer Your WorkSpaces (p. 62)
- Manage Directories for Amazon WorkSpaces (p. 34)
- Delete a WorkSpace (p. 74)

Launch a WorkSpace Using AD Connector

Amazon WorkSpaces enables you to provision virtual, cloud-based Microsoft Windows desktops for your users, known as WorkSpaces.

Amazon WorkSpaces uses directories to store and manage information for your WorkSpaces and users. For your directory, you can choose from Simple AD, AD Connector, or AWS Directory Service for Microsoft
Active Directory, also known as AWS Managed Microsoft AD. In addition, you can establish a trust relationship between your AWS Managed Microsoft AD directory and your on-premises domain.

In this tutorial, we launch a WorkSpace that uses AD Connector. For tutorials that use the other options, see Launch a Virtual Desktop Using Amazon WorkSpaces (p. 47).

Tasks
- Before You Begin (p. 53)
- Step 1: Create an AD Connector (p. 53)
- Step 2: Create a WorkSpace (p. 54)
- Step 3: Connect to the WorkSpace (p. 54)
- Next Steps (p. 55)

Before You Begin
- Amazon 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 Amazon WorkSpaces Pricing by AWS Region.
- When you launch a WorkSpace, you must select a WorkSpace bundle. A bundle is a combination of an operating system, and storage, compute, and software resources. For more information, see Amazon WorkSpaces Bundles.
- Create a virtual private cloud with at least two private subnets. 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 from Your WorkSpace (p. 24).

Step 1: Create an AD Connector

To create an AD Connector

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose Directories.
3. Choose Set up Directory, Create AD Connector.
4. 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.
5. For Connected directory DNS, enter the fully-qualified name of your on-premises directory (for example, example.com).
6. For Connected directory NetBIOS name, enter the short name of your on-premises directory (for example, example).
7. 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.
8. For Connector account password and Confirm password, enter the password for the on-premises user account.
9. For DNS address, enter the IP address of at least one DNS server in your on-premises directory.
10. (Optional) For Description, enter a description for the directory.
11. Keep Size as Small.
12. For VPC, select your VPC.
Step 2: Create a WorkSpace

Now you are ready to launch WorkSpaces for one or more users in your on-premises directory.

To launch a WorkSpace for an existing user

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose WorkSpaces.
3. Choose Launch WorkSpaces.
4. For Directory, choose the directory that you created.
5. (Optional) If this is the first time you have launched a WorkSpace in this directory, and Amazon WorkDocs is supported in the Region, you can enable or disable Amazon WorkDocs for all users in the directory. For more information, see Amazon WorkDocs Sync Client Help in the Amazon WorkDocs Administration Guide.
6. Choose Next. Amazon WorkSpaces registers your AD Connector.
7. Select one or more existing users from your on-premises directory. Do not add new users to an on-premises directory through the Amazon WorkSpaces console.

   To find users to select, you can enter all or part of the user's name and choose Search or choose Show All Users. Note that you cannot select a user that does not have an email address.

   After you select the users, choose Add Selected and then choose Next Step.
8. Under Select Bundle, choose the default WorkSpace bundle to be used for the WorkSpaces. Under Assign WorkSpace Bundles, you can choose a different the bundle for an individual WorkSpace if needed. When you have finished, choose Next Step.
9. Choose a running mode for your WorkSpaces and then choose Next Step. For more information, see Manage the WorkSpace Running Mode (p. 62).
10. Choose Launch WorkSpaces. The initial status of the WorkSpace is PENDING. When the launch is complete, the status is AVAILABLE.
11. Send invitations to the email address for each user. For more information, see Send an Invitation Email (p. 58).

Step 3: 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. 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 follow the directions.
3. Start the client, enter the registration code from the invitation email, and choose **Register**.
4. When prompted to sign in, enter the user name and password for the user, and then choose **Sign In**.
5. (Optional) When prompted to save your credentials, choose **Yes**.

**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. If you are finished with your WorkSpace, you can delete it. For more information, see the following documentation.

- Create a Custom WorkSpaces Bundle (p. 75)
- Administer Your WorkSpaces (p. 62)
- Manage Directories for Amazon WorkSpaces (p. 34)
- Delete a WorkSpace (p. 74)

**Launch a WorkSpace Using a Trusted Domain**

Amazon WorkSpaces enables you to provision virtual, cloud-based Microsoft Windows desktops for your users, known as **WorkSpaces**.

Amazon WorkSpaces uses directories to store and manage information for your WorkSpaces and users. For your directory, you can choose from Simple AD, AD Connector, or AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD. In addition, you can establish a trust relationship between your AWS Managed Microsoft AD directory and your on-premises domain.

In this tutorial, we launch a WorkSpace that uses a trust relationship. For tutorials that use the other options, see **Launch a Virtual Desktop Using Amazon WorkSpaces** (p. 47).

**Tasks**

- Before You Begin (p. 55)
- Step 1: Establish a Trust Relationship (p. 55)
- Step 2: Create a WorkSpace (p. 56)
- Step 3: Connect to the WorkSpace (p. 56)
- Next Steps (p. 57)

**Before You Begin**

- Amazon 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 **Amazon WorkSpaces Pricing by AWS Region**.
- When you launch a WorkSpace, you must select a WorkSpace bundle. A bundle is a combination of storage, compute, and software resources. For more information, see **Amazon WorkSpaces Bundles**.

**Step 1: Establish a Trust Relationship**

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**.
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 two-way trust is required so that on-premises credentials can be used to manage and authenticate with WorkSpaces, and so that WorkSpaces can be provisioned to on-premises users and groups.

**Step 2: Create a WorkSpace**

After you establish a trust relationship between your AWS Managed Microsoft AD and your on-premises Microsoft Active Directory domain, you can provision WorkSpaces for users in the on-premises domain.

Note that you must ensure that GPO settings are replicated across domains before you can apply them to Amazon WorkSpaces.

**To launch workspaces for users in a trusted on-premises domain**

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose WorkSpaces.
3. Choose Launch WorkSpaces.
4. On the Select a Directory page, choose the directory that you just registered and then choose Next Step.
5. On the Identify Users page, do the following:
   a. For Select trust from forest, select the trust relationship that you created.
   b. Select the users from the on-premises domain and then choose Add Selected.
   c. Choose Next Step.
6. Select the bundle to be used for the WorkSpaces and then choose Next Step.
7. Choose the running mode, choose the encryption settings, and configure any tags. When you are finished, choose Next Step.
8. Choose Launch WorkSpaces. Note that it can take up to 20 minutes for the WorkSpaces to become available, and up to 40 minutes if encryption is enabled. The initial status of the WorkSpace is PENDING. When the launch is complete, the status is AVAILABLE.
9. Send invitations to the email address for each user. For more information, see Send an Invitation Email (p. 58).

**Step 3: Connect to the WorkSpace**

After you receive the invitation email, you can connect to your WorkSpace. Users can enter their user names as username, corp\username, or corp.example.com\username.

**To connect to the WorkSpace**

1. Open the link in the invitation email. When prompted, enter a password and activate the user. Remember this password as you will need it to sign in 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 three of the following categories: lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9), and ~!#$%^&*_-+=`\{|}[]:;"'<>,.?/.

2. 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 follow the directions.

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

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. If you are finished with your WorkSpace, you can delete it. For more information, see the following documentation.

- Create a Custom WorkSpaces Bundle (p. 75)
- Administer Your WorkSpaces (p. 62)
- Manage Directories for Amazon WorkSpaces (p. 34)
- Delete a WorkSpace (p. 74)
Administer WorkSpace Users

Each WorkSpace is assigned to a single user and cannot be shared by multiple users. Whenever you launch a WorkSpace, you must assign it to a user that does not already have a WorkSpace.

Contents
- Manage WorkSpaces Users (p. 58)
- Customize How Users Log in to their WorkSpaces (p. 59)
- Enable Self-Service WorkSpace Management Capabilities for Your Users (p. 60)

Manage WorkSpaces Users

As an administrator for Amazon WorkSpaces, you can use the Amazon WorkSpaces console to perform the following tasks to manage WorkSpaces users.

Edit User Information

You can use the Amazon WorkSpaces console to edit the user information for a WorkSpace.

Note
This feature is available only if you use Microsoft AD or Simple AD. If you use Microsoft Active Directory through AD Connector or a trust relationship, you can manage users and groups by using Active Directory.

To edit user information
1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose WorkSpaces.
3. Select a user and choose Actions, Edit User.
4. Update First Name, Last Name, and Email as needed.
5. Choose Update.

Note
To delete or otherwise manage users, you must do this through your directory. 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 Active Directory.

Send an Invitation Email

You can send an invitation email to a user manually if needed.

To resend an invitation email
1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose WorkSpaces.
3. Select the user to send the invitation to and choose Actions, Invite User.
4. Copy the email body text and paste it into an email to the user using your own email application. You can modify the body text if desired. When the invitation email is ready, send it to the user.

Customize How Users Log in to their WorkSpaces

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 user names are automatically entered on their WorkSpaces client login page.
- If multi-factor authentication (MFA) is used in your organization, their user names and MFA codes are automatically entered on their client login page.

You can configure URI access to WorkSpaces for client applications on the following supported devices:

- Windows computers
- macOS computers
- Ubuntu Linux 18.04 computers
- iPads
- Android tablets

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 computers, and on the Internet Explorer and Microsoft Edge browsers on Windows computers. For more information about WorkSpaces clients, see Amazon 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 user names that include any of these characters, you should percent-encode those user names in your URI. For more information, see Uniform Resource Identifier (URI): Generic Syntax.

<table>
<thead>
<tr>
<th>Supported Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>workspaces:///</td>
<td>Opens the WorkSpaces client application. (Note: Using workspaces:/// by itself is not currently supported in the Linux client application.)</td>
</tr>
<tr>
<td>workspaces://@registrationcode</td>
<td>Registers a user by using their WorkSpaces registration code. Also displays the client login page.</td>
</tr>
</tbody>
</table>
Enable Self-Service WorkSpace Management Capabilities for Your Users

In Amazon 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 Amazon WorkSpaces. When you enable self-service capabilities, you can allow users to perform one or more of the following tasks directly from their Windows, macOS, or Linux client for Amazon WorkSpaces:

- Cache their credentials on their client. This lets them reconnect to their WorkSpace without re-entering their credentials.
- Restart their WorkSpace.
- Increase the volume size of the C: drive and D: drive on their WorkSpace.
- Change the compute type (bundle) for their WorkSpace.
- Switch the running mode of their WorkSpace.
- Rebuild their WorkSpace.

To enable one or more of these capabilities for your users, perform the following steps.

To enable self-service management capabilities for your users

1. Open the Amazon 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 **User Self-Service Permissions**. 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 (p. 44).

- **Restart WorkSpace from client**— Users can restart their WorkSpace. Restarting disconnects users from their WorkSpace, shuts it down, and restarts 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 (C: drive) up to 175 GB, and the size of the user volume (D: drive) 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 1000, 100 to 1000].

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. When 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.

**Note**

If users increase the volume size on their WorkSpace, this will increase 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. This process may take up to an hour.

**Note**

If users change their WorkSpace compute type, this may change 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 WorkSpace Running Mode (p. 62).

**Note**

If users switch the running mode of their WorkSpace, this will change 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.

5. Choose **Update** or **Update and Exit**.
Administer Your WorkSpaces

You can administer your WorkSpaces using the Amazon WorkSpaces console.

Contents
• Manage the WorkSpace Running Mode (p. 62)
• Modify a WorkSpace (p. 63)
• Tag WorkSpaces Resources (p. 64)
• WorkSpace Maintenance (p. 65)
• Encrypted WorkSpaces (p. 66)
• Restart a WorkSpace (p. 69)
• Rebuild a WorkSpace (p. 69)
• Restore a WorkSpace (p. 70)
• Upgrade Windows 10 BYOL WorkSpaces (p. 70)
• Delete a WorkSpace (p. 74)

Manage the WorkSpace Running Mode

The running mode of a WorkSpaces determines its immediate availability and how you pay for it. 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 inactivity and the state of apps and data is saved. To set the automatic stop time, use **AutoStop Time (hours)**.

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.

For more information, see Amazon WorkSpaces Pricing.

Modify the Running Mode

You can switch between running modes at any time.

To modify the running mode of a WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose WorkSpaces.
3. Select the WorkSpaces to modify and choose Actions, Modify Running Mode Properties.
4. Select the new running mode, AlwaysOn or AutoStop, and then choose Modify.
Stop and Start an AutoStop WorkSpace

When your AutoStop WorkSpaces are not in use, they are automatically stopped after a specified period of inactivity, and hourly metering is suspended. To further optimize costs, you can suspend the hourly charges associated with AutoStop WorkSpaces. The WorkSpace is stopped and all apps and data saved for the next time a user logs in to the WorkSpace.

Note
Amazon WorkSpaces can detect inactivity only when users are using Amazon WorkSpaces clients. If users are using third-party clients, Amazon WorkSpaces might not be able to detect inactivity, and therefore the WorkSpace might not automatically stop and metering might not be suspended.

When a user reconnects to a stopped WorkSpace, it resumes from where it left off, typically in under 90 seconds.

You can restart AutoStop WorkSpaces that are available or in an error state.

To stop an AutoStop WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose WorkSpaces.
3. Select the WorkSpaces to be stopped and choose Actions, Stop WorkSpaces.
4. When prompted for confirmation, choose Stop.

To start an AutoStop WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose WorkSpaces.
3. Select the WorkSpaces to be started and choose Actions, Start WorkSpaces.
4. When prompted for confirmation, choose Start.

To remove the fixed infrastructure costs associated with AutoStop WorkSpaces, remove the WorkSpace from your account. For more information, see Delete a WorkSpace (p. 74).

Modify a WorkSpace

You can increase the size of the root and user volumes for a WorkSpace, up to 2000 GB each. You can expand these volumes whether they are encrypted or unencrypted. You can request a volume expansion once in a 6-hour period. To ensure that your data is preserved, you cannot decrease the size of the root or user volumes after you launch a WorkSpace.

Note
When you expand a volume for a WorkSpace, Amazon WorkSpaces automatically extends the volume's partition within Windows. However, for this change to take effect, you must restart the WorkSpace.

You can switch a WorkSpace between the Value, Standard, Performance, Power, and PowerPro bundles. When you request a bundle change, Amazon WorkSpaces restarts the WorkSpace using the new bundle. Amazon WorkSpaces preserves the operating system, applications, data, and storage settings for the WorkSpace. You can request a larger bundle once in a 6-hour period or a smaller bundle once every 30 days. For a newly launched WorkSpace, you must wait 6 hours before requesting a larger bundle.
The current modification state of a WorkSpace is displayed in the State setting in the Amazon WorkSpaces console. The possible values for State are Modifying Compute, Modifying Storage, and None.

**To modify the configuration of a WorkSpace**

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose WorkSpaces.
3. Select the WorkSpace and choose Actions, Modify WorkSpace.
4. To increase the size of the root volume or user volume, choose Modify Volume Sizes and enter the new values.
   
   **Note**
   
   You can only resize SSD volumes.
5. To change the bundle, choose Change Compute Type and select the new bundle type.
6. Choose Modify.

**Tag WorkSpaces Resources**

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 organize data, including billing data.

Tags added to an existing resource appear in your cost allocation report on the first of the following month for WorkSpaces renewed in that month. For more information, see Using Cost Allocation Tags in the AWS Billing and Cost Management User Guide.

**Resources 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 value 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**

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose one of the following resource types: Directories, WorkSpaces, Bundles, Images, or IP Access Controls.
3. Select the resource and choose Actions, Manage Tags.

4. Do one or more of the following:
   a. To update a tag, edit the values of Key and Value.
   b. To add a tag, choose Add Tag and then edit the values of Key and Value.
   c. 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 AWS CLI

Use the create-tags and delete-tags commands.

WorkSpace Maintenance

We recommend that you maintain your WorkSpaces on a regular basis. Amazon WorkSpaces schedules maintenance windows for your WorkSpaces by default. During the maintenance window, the WorkSpace installs important updates and reboots as necessary. During maintenance, your WorkSpaces might be unavailable.

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 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 disconnect, the time zone of the WorkSpace is updated to the time zone of the Region that you connected from.

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. Starting 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 the maintenance window, the state of the WorkSpace is set to MAINTENANCE.

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 Amazon 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 ADMIN_MAINTENANCE. When you are finished, change the state of the WorkSpace to AVAILABLE.

When a WorkSpace is in ADMIN_MAINTENANCE mode, 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 have a status of AVAILABLE. The Modify State setting is not available when a WorkSpace has a status of STOPPED.

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose WorkSpaces.
3. Select your WorkSpace, and choose Actions, Modify WorkSpace.
4. Choose Modify State. For Intended State, select ADMIN_MAINTENANCE or AVAILABLE.
5. Choose Modify.

To change the state of the WorkSpace using the AWS CLI

Use the modify-workspace-state command.

Encrypted WorkSpaces

Amazon WorkSpaces is integrated with the AWS Key Management Service (AWS KMS). This enables you to encrypt storage volumes of WorkSpaces using customer master keys (CMK). When you launch a WorkSpace, you can encrypt the root volume (for Microsoft Windows, the drive C, for Linux, /) and the user volume (for Windows, the drive D; 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.

Prerequisites

You need an AWS KMS CMK before you can begin the encryption process.

The first time you launch a WorkSpace from the Amazon WorkSpaces console in a Region, an AWS managed CMK is created for you automatically. You can select this AWS managed CMK to encrypt the user and root volumes of your WorkSpace.

Alternately, you can select a CMK that you created using AWS KMS. For more information about creating CMKs, see Creating Keys in the AWS Key Management Service Developer Guide. For more information
You must meet the following requirements to use an AWS KMS CMK to encrypt your WorkSpaces:

- The CMK must be symmetric. Amazon WorkSpaces does not support asymmetric CMKs. For information about distinguishing between symmetric and asymmetric CMKs, see Identifying Symmetric and Asymmetric CMKs in the AWS Key Management Service Developer Guide.
- The CMK must be enabled. To determine whether a CMK is enabled, see Displaying CMK Details in the AWS Key Management Service Developer Guide.
- You must have the correct permissions and policies associated with the key. For more information, see IAM Permissions and Roles for Encryption (p. 67).

Limits

- 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 CMK is enabled; otherwise, the WorkSpace becomes unusable.

Encrypting WorkSpaces

To encrypt a WorkSpace

1. Open the Amazon 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, choose your AWS KMS CMK. The CMK must be symmetric. Amazon WorkSpaces does not support asymmetric CMKs.
   c. Choose Next Step.

Viewing Encrypted WorkSpaces

To see which WorkSpaces and volumes have been encrypted from the Amazon 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.

IAM Permissions and Roles for Encryption

Amazon WorkSpaces encryption privileges require limited AWS KMS access on a given key for the IAM user who launches encrypted WorkSpaces. The following is a sample key policy that can be used. This policy enables you to separate the principals that can manage the AWS KMS CMK from those that can use it. The account ID and IAM user name must be modified to match your account.

The first statement matches the default AWS KMS key policy. The second and third statements define which AWS principals can manage and use the key, respectively. The fourth statement enables AWS

about creating CMKs using the AWS KMS API, see Working With Keys in the AWS Key Management Service Developer Guide.
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 condition uses a context key that is set only for AWS KMS calls made by AWS services on behalf of the customers.

```json
{
   "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:Get*",
            "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 should include usage permissions on the CMK, as well as access to WorkSpaces. The following is a sample policy that can be attached to an IAM user to grant them WorkSpaces privileges.

```json
{
   "Version": "2012-10-17",
   "Statement": [
```
Restart a WorkSpace

Occasionally, you might need to restart a WorkSpace manually. Restarting a WorkSpace performs a shutdown and restart of the WorkSpace. The user data, operating system, and system settings are not affected.

To restart a WorkSpace
1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose WorkSpaces.
3. Select the WorkSpaces to be restarted and choose Actions, Reboot WorkSpaces.
4. When prompted for confirmation, choose Reboot WorkSpaces.

Rebuild a WorkSpace

Automatic snapshots for use when rebuilding a WorkSpace are scheduled every 12 hours. If the WorkSpace is healthy, a snapshot of the user volume is created. If the WorkSpace is unhealthy, the snapshot is not created.
If needed, you can rebuild a WorkSpace. This recreates both the root volume and the user volume.

Rebuilding a WorkSpace causes the following to occur:

- The system 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.
- The primary elastic network interface (ENI) is recreated. The WorkSpace receives a new private IP address.

To rebuild a WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose WorkSpaces.
3. Select the WorkSpace to be rebuilt and choose Actions, Rebuild / Restore WorkSpace.
4. When prompted for confirmation, choose Rebuild WorkSpace.

Restore a WorkSpace

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, these snapshots are not created.

If needed, you can restore a WorkSpace to its last known healthy state. This 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.

Restoring a WorkSpace causes the following to occur:

- The system is restored to the most recent snapshot of the root volume. Any applications that were installed, or system settings that were changed after the most recent snapshot 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.

To restore a WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose WorkSpaces.
3. Select the WorkSpace to be restored and choose Actions, Rebuild / Restore WorkSpace.

Upgrade Windows 10 BYOL WorkSpaces

On your Windows 10 Bring Your Own License (BYOL) WorkSpaces, you can upgrade to a newer version of Windows 10 by 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 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.

Prerequisites

- If you have deferred or paused Windows 10 upgrades by using Group Policy or System Center Configuration Manager (SCCM), enable operating system upgrades for your Windows 10 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 be stopped automatically while updates are being applied. For more information, see Modify the Running Mode (p. 62). 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 re-creates the user profile by making a copy of a special profile named Default User (C:\Users\Default). To preserve custom Windows preferences and application settings stored in the Windows registry, modify C:\Users\Default\NTUSER.DAT on the WorkSpace before you perform the in-place upgrade.

To perform an in-place upgrade of Windows 10

1. Check the version of Windows currently running on the Windows 10 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.

    You can do this manually. If you have multiple WorkSpaces to update, you can use Group Policy or SCCM to push a PowerShell script (p. 73).

    • 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

    (Optional) By default, WorkSpaces redirects user shell folders to drive D. To prevent user shell folder redirection, set the following key value to 0.

    HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1\UserShellFoldersRedirection

3. 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 may see placeholder icons in the Start menu. This behavior is automatically resolved after the in-place upgrade is complete.

    (Optional) Confirm that the following key value is set to 1, which unblocks the WorkSpace for updating.
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 version and how many apps were installed, this process can take 40-120 minutes.

5. 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 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 were successfully executed, verify that the following key value is set to 1.

HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1\scriptExecutionComplete

(Optional) 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 (p. 62).

After in-place upgrades, the NTUSER.DAT file of the user is regenerated and placed on the C drive, so that you do not have to go through the above steps again for future Windows 10 in-place upgrades. By default, WorkSpaces redirects the following shell folders to the D drive.

- 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\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.

**Known Limitations**

The NTUSER.DAT location change does not happen during WorkSpace rebuilds. If you perform an in-place upgrade on a Windows 10 BYOL WorkSpace and then rebuild it, the new WorkSpace uses the NTUSER.DAT file on the D drive. Also, if your default BYOL bundle contains an image that is based on an
earlier release of Windows 10, you need to perform the in-place upgrade again after the WorkSpace is rebuilt.

Troubleshooting

If you encounter any issues with the update, you can check the following items to troubleshoot.

- 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

- 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 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 steps in the previous section, but use this script to update the registry on each WorkSpace.

```powershell
# AWS WorkSpaces 2.13.18
# Enable In-Place Update Sample Scripts
# These registry keys and values will enable scripts to execute on next reboot of the WorkSpace.

$scriptlist = (@"update-pvdrivers.ps1","enable-inplace-upgrade.ps1")
$wsConfigRegistryRoot="HKLM:\Software\Amazon\WorkSpacesConfig"
$Enabled = 1

foreach ($scriptName in $scriptlist)
{
    $scriptRegKey = "$wsConfigRegistryRoot\$scriptName"
    if (-not(Test-Path $scriptRegKey))
    {
        Write-Host "Registry key not found. Creating registry key '$scriptRegKey' with 'Update' enabled."
        New-Item -Path $wsConfigRegistryRoot -Name $scriptName -ErrorAction SilentlyContinue | 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)'"
        }
    }
}
```
Delete a WorkSpace

When you are finished with a WorkSpace, you can delete it. You can also delete related resources.

Warning
This 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.

To delete a WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose WorkSpaces.
3. Select your WorkSpace and choose Actions, Remove WorkSpaces.
4. When prompted for confirmation, choose Remove WorkSpaces. The status of the WorkSpace is set to TERMINATING. When the termination is complete, the status is set to TERMINATED.
5. (Optional) To delete any custom bundles and images that you are finished with, see Delete a Custom WorkSpaces Bundle (p. 79).
6. (Optional) After you delete all WorkSpaces in a directory, you can delete the directory. For more information, see Delete the Directory for Your WorkSpaces (p. 38).
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.
WorkSpace Bundles and Images

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. For more information, see Amazon WorkSpaces Bundles.

You can create an image from a Windows or Amazon Linux WorkSpace that you've customized, create a custom WorkSpace bundle from the image, and launch WorkSpaces from your custom bundle. By creating a custom bundle, you can ensure that the WorkSpaces for your users have everything that they need already installed. If you need to perform software updates or install additional software on your WorkSpaces, you can update your custom bundle and rebuild your WorkSpaces.

Contents
- Create a Custom WorkSpaces Bundle (p. 75)
- Update a Custom WorkSpaces Bundle (p. 78)
- Copy a Custom WorkSpaces Image (p. 79)
- Delete a Custom WorkSpaces Bundle (p. 79)
- Bring Your Own Windows Desktop Images (p. 80)

Create a Custom WorkSpaces Bundle

After you've launched a Windows or Amazon Linux WorkSpace and customized it, you can create an image from the WorkSpace and then create a custom bundle from the image. You can specify this bundle when you launch new WorkSpaces to ensure that they have the same configuration and software as the WorkSpace you used to create the 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.

Requirements to create Windows custom images
- All applications and user profiles on WorkSpaces images must be compatible with Microsoft Sysprep.
- All applications to be included in the image must be installed on the C: drive.
- Customized Windows user profiles for Windows 7 Bring Your Own Windows License (BYOL) or Windows Server 2008 R2 custom images must be placed in D:\Users\username before you run Create Image on the WorkSpace.
- Customized Windows user profiles for Windows 10 BYOL or Windows Server 2016 custom images must be placed in C:\Users\Default before you run Create Image on the WorkSpace.
- The user profile must exist and its total size (files and data) must be less than 10 GB.
- The C:\ drive must have enough available space for the contents of the user profile, plus an additional 2 GB.
- 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 following components are required in an image; otherwise, the WorkSpaces you launch from the image will not function correctly:
Create a Custom Bundle

- PowerShell
- Remote Desktop Services
- AWS PV drivers
- EC2Config or EC2Launch (Windows Server 2016)
- [EC2Launch 1.2.0 or earlier] Windows Remote Management (WinRM)
- Teradici PCoIP agents and drivers
- STXHD agents and drivers
- AWS and WorkSpaces certificates
- Skylight agent

Requirements to create Amazon Linux custom images

- All applications to be included in the image must be installed outside of the /home directory (or user volume).
- The root volume (/) should be less than 97% full.
- The following components are required in an image; otherwise, the WorkSpaces you launch from the image will not function correctly:
  - Cloud-init
  - Teradici PCoIP agents and drivers
  - Skylight agent

Best Practices

Before you create an image from a WorkSpace, do the following:

- Install all operating system updates (except Windows feature/version updates) and all application updates on the WorkSpace. For more information, see the Important note (p. 75) 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.

To create a custom bundle

1. If you are still connected to the WorkSpace, disconnect.
2. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
3. In the navigation pane, choose WorkSpaces.
4. Select the WorkSpace and choose Actions, Create Image.
5. A message displays prompting you to restart your WorkSpace before continuing, to update your WorkSpaces software to the latest version necessary. Restart your WorkSpace if needed by closing the message and following the steps in Restart a WorkSpace (p. 69). When you're done, repeat the previous step, and choose Next when this 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.
7. In the navigation pane, choose **Images**. The image is complete when the status changes to **Available**.

8. Select the image and choose **Actions, Create Bundle**.

9. Enter a bundle name and a description, and then do the following:

   - For **Bundle Type**, choose the hardware from which your WorkSpace is launched.
   - For **Root Volume Size**, leave the default value or enter a new value that is equal or greater than the current size. Then, enter a value for **User Volume Size**.

     The available sizes 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

     Alternatively, you can expand the root and user volumes up to 1000 GB each.

10. Choose **Create Bundle**.

### Image Creation for Windows WorkSpaces

When you create an image from a Windows WorkSpace, the entire contents of the C:\ drive are included. 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
Update a Custom Bundle

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 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
- /etc/security/access.conf
- /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

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

Image Creation for Amazon Linux WorkSpaces

Update a Custom WorkSpaces Bundle

You can update an existing custom WorkSpaces bundle by modifying a WorkSpace based on the bundle, creating an image from the WorkSpace, and updating the bundle with the new image. You can launch
new WorkSpaces using the updated bundle. To update existing WorkSpaces that are based on the bundle, rebuild the WorkSpace.

**To update a bundle**

1. Connect to a WorkSpace that is based on the bundle and make any changes. For example, you can apply the latest operating system and application patches and install additional applications.

   Alternatively, you can create a WorkSpace with the same base software package (Plus or Standard) as the image used to create the bundle and make changes.

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

3. In the navigation pane, choose **WorkSpaces**.

4. Select the WorkSpace and choose **Actions, Create Image**.

5. Enter an image name and a description, and then choose **Create Image**. The WorkSpace is unavailable while the image is being created.

6. In the navigation pane, choose **Bundles**.

7. Select the bundle and choose **Actions, Update Bundle**.

8. For **Update WorkSpace Bundle**, select the image that you created and choose **Update Bundle**.

9. (Optional) Rebuild the existing WorkSpaces based on the bundle. For more information, see Rebuild a WorkSpace (p. 69).

**Copy a Custom WorkSpaces Image**

You can copy a custom WorkSpaces image within or across AWS Regions. Copying an image results in an identical image with its own unique identifier.

There are no additional charges for copying an image across Regions. The quota for the number of images in the destination Region applies.

**To copy an image**

1. Open the Amazon 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. Provide a name, description and Region for the copied image, and then choose **Copy Image**.

**Delete a Custom WorkSpaces Bundle**

You can delete unused custom bundles as needed. If you delete a bundle that is being used by a WorkSpace, the bundle is placed in a delete queue and will be deleted after all WorkSpaces based on the bundle have been deleted.

**To delete a bundle**

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

2. In the navigation pane, choose **Bundles**.

3. Select the bundle and choose **Actions, Delete Bundle**.

4. When prompted for confirmation, choose **Delete Bundle**.

After you delete a custom bundle, you can delete the image you used to create or update the bundle.
To delete an image
1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose Images.
3. Select the image and choose Actions, Delete Image.
4. When prompted for confirmation, choose Delete Image.

Bring Your Own Windows Desktop Images

If your licensing agreement with Microsoft allows it, you can use your Windows 7, Windows 10 Enterprise, or Windows 10 Pro desktop images for your WorkSpaces. To do this, you must Bring Your Own License (BYOL) and provide a Windows 7 or Windows 10 image that meets the following requirements. To stay compliant with Microsoft licensing terms, run your Amazon 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 Amazon WorkSpaces Pricing.

Important
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.

To get started, open the Amazon WorkSpaces console and choose Account Settings to enable your account for BYOL.

Contents
- Requirements (p. 80)
- Windows Versions That Are Supported for BYOL (p. 81)
- Step 1: Enable BYOL for Your Account by Using the Amazon WorkSpaces Console (p. 81)
- Step 2: Run the BYOL Checker PowerShell Script on a Windows VM (p. 82)
- Step 3: Export the VM from Your Virtualization Environment (p. 83)
- Step 4: Import the VM as an Image into EC2 (p. 83)
- Step 5: Create a BYOL Image by Using the Amazon WorkSpaces Console (p. 84)
- Step 6: Create a Custom Bundle From the BYOL Image (p. 84)
- Step 7: Register a Directory for Dedicated WorkSpaces (p. 85)
- Step 8: Launch Your BYOL WorkSpaces (p. 85)

Requirements

Before you begin, verify the following:

- Your Microsoft licensing agreement allows Windows to be run in a virtual hosted environment.
- You will use a minimum of 200 Amazon WorkSpaces. This is a requirement for running your Amazon WorkSpaces on dedicated hardware. Running your Amazon WorkSpaces on dedicated hardware is necessary to comply with Microsoft licensing requirements.
- If you plan to use GPU-enabled (Graphics and Graphics Pro) 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.
- Amazon WorkSpaces can use a management interface in the /16 IP address range. The management interface is connected to a secure Amazon WorkSpaces management network used for interactive streaming. This allows Amazon WorkSpaces to manage your WorkSpaces. For more information, see
Network Interfaces (p. 20). At least one of the following IP address ranges must be available 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

You have a virtual machine (VM) that runs a supported 64-bit version of Windows 7 or Windows 10. For a list of supported versions, see the next section in this topic, Windows Versions That Are Supported for BYOL (p. 81). 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 7 or Windows 10 can be installed on the VM.
  You can add additional software, such as an antivirus solution, when you later create a custom image.
- If the VM is running Windows 10, the user profile must be placed in C:\Users\Default.
- We recommend that you create a WorkSpaces_BYOL account with local administrator access before you share the image. The password for this account may be required later.
- Your VM must also run PowerShell version 4 or later.

Windows Versions That Are Supported for BYOL

Your VM must run one of the following Windows versions:

- Windows 7 Service Pack 1
- Windows 10 Version 1607 (Anniversary Update)
- Windows 10 Version 1703 (Creators Update)
- Windows 10 Version 1709 (Fall Creators Update)
- Windows 10 Version 1803 (April 2018 Update)
- Windows 10 Version 1809 (October 2018 Update)
- Windows 10 Version 1903 (May 2019 Update)

Step 1: Enable BYOL for Your Account by 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
The steps in this procedure for enabling BYOL for your account need to be performed only once per account, per Region.

To enable BYOL for your account by using the Amazon WorkSpaces console

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose Account Settings. If your account is not currently eligible for BYOL, a message provides guidance for next steps.
3. 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 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.

4. Choose the CIDR block that you want from the list of results, and then choose **Enable BYOL**.

This process may take several hours. While Amazon WorkSpaces is enabling your account for BYOL, proceed to the next step.

### Step 2: 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 Amazon 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. Open the following URL to download the BYOL Checker script .zip file: [https://d2zdca6k60k1ljz.cloudfront.net/BYOLChecker.zip](https://d2zdca6k60k1ljz.cloudfront.net/BYOLChecker.zip).
2. When prompted, right-click the **Download** link and choose **Save target as**.
3. In the **Save as** dialog box, navigate to the location where you want to save the script file, and choose **Save**. We recommend that you create a folder in the Windows Temp folder for this purpose. For example, **C:\Windows\Temp\byol**.
4. When a message notifies you that the BYOL Checker script .zip file has finished downloading, choose **OK** to close the message.
5. Windows Explorer opens in the location where you saved the .zip file. Right-click the file, and choose **Extract All**.
6. In the **Select a Destination and Extract Files** dialog box, navigate to the location where you want to extract the script (for example, **C:\Windows\Temp\byol\**), and choose **Extract**.
7. If you created a folder for the BYOL script, you can copy the extracted files to the root of the folder.
8. Delete the original .zip files so that only the extracted files remain. Close any open applications and windows (for example, close Windows Explorer and your browser, if they are open).

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, enter the commands required to change to the directory where the BYOL Checker script is located. For example, if the script is located in the BYOL directory, enter the following commands. After each command, press Enter:

   cd/

   cd C:\Windows\Temp\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 Unrestricted

4. When prompted to confirm whether to change the PowerShell execution policy, enter A to specify Yes for 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 Amazon 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 steps 7 and 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, BYOLPrevalidationlogYYYYMMDDT 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 may be helpful in troubleshooting.

11. After your VM passes all test, you get a Validation Successful message. Review the VM locale settings displayed in the tool. To update the locale settings, follow these instructions in the Microsoft documentation and run the BYOL Checker script again.

12. Choose Run Sysprep. If Sysprep is successful, your VM shuts down. Otherwise, review the Sysprep logs, resolve the reported issues, and run the BYOL Checker script again.

   The most common reason that Sysprep fails is that the Modern Appx Packages are not installed for all users. Use the Remove-AppxPackage cmdlet to remove the Appx Packages.

---

**Step 3: 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 that is at least 10 GB and smaller than 80 GB. 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.

**Step 4: Import the VM as an Image into 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.
Step 5: Create a BYOL Image by Using the Amazon WorkSpaces Console

Perform these steps to create an Amazon WorkSpaces BYOL image.

Note
To perform this procedure, verify that you have permissions to:

- Call Amazon WorkSpaces ImportWorkspaceImage.
- Call EC2 DescribeImages on the EC2 image that you want to use to create the BYOL image.
- Call EC2 ModifyImageAttribute on the EC2 image that you want to use to create the BYOL image.

For more information, see Changing Permissions for an IAM User in the IAM User Guide.

To create a 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 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 Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose Images.
4. In the Create BYOL Image dialog box, do the following:
   - For AMI ID, click the EC2 Console link, and choose the EC2 image that you imported as described in the previous section (Step 4: Import the VM as an Image into EC2). The image name must begin with ami- and be followed by the identifier for the AMI (for example, ami-5731123e).
   - For BYOL image name, enter a unique name for the image.
   - For Image description, enter a description to help you quickly identify the image.
5. Choose Create.

While your image is being created, the image status in the image registry of the console appears as Pending. 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 6: 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 Bundle (p. 75).
Step 7: Register a Directory for Dedicated WorkSpaces

To use BYOL images for WorkSpaces, you must register a directory for this purpose. To do so, perform these steps.

To register a directory for dedicated WorkSpaces

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose Directories.
3. Select the directory and choose Actions, Register.
4. In the Register directory dialog box, for Enable Dedicated WorkSpaces, choose Yes.
5. Choose Register.

If you have already registered AWS Directory Service for Microsoft Active Directory or an AD Connector directory for WorkSpaces that does not run on dedicated hardware, you can set up a new Microsoft Active Directory or AD Connector directory for this purpose. You can also deregister the directory and then reregister it as a directory for dedicated WorkSpaces. To do so, perform these steps.

Note
You can only perform this procedure if no WorkSpaces are associated with the directory.

To deregister a directory and reregister it for dedicated WorkSpaces

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Terminate existing WorkSpaces.
3. In the navigation pane, choose Directories.
4. Select the directory and choose Actions, Deregister.
5. When prompted for confirmation, choose Deregister.
6. Select the directory again and choose Actions, Register.
7. In the Register directory dialog box, for Enable Dedicated WorkSpaces, choose Yes.
8. Choose Register.

Step 8: Launch Your BYOL WorkSpaces

After you register a directory for dedicated WorkSpaces, you can launch your BYOL WorkSpaces in this directory. For information about how to launch WorkSpaces, see Launch a Virtual Desktop Using Amazon WorkSpaces (p. 47).
Monitor Your WorkSpaces

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 (p. 86).

**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 CloudWatch Events (p. 90).

**CloudTrail logs**

AWS CloudTrail provides a record of actions taken by a user, role, or an AWS service in Amazon WorkSpaces. Using the information collected by CloudTrail, you can determine the request that was made to Amazon 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 Amazon WorkSpaces API Calls by Using CloudTrail.

Monitor Your WorkSpaces Using CloudWatch Metrics

Amazon 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 Amazon WorkSpaces (p. 13).

**Contents**

- Amazon WorkSpaces Metrics (p. 86)
- Dimensions for Amazon WorkSpaces Metrics (p. 88)
- Monitoring Example (p. 88)

**Amazon WorkSpaces Metrics**

The AWS/WorkSpaces namespace includes the following metrics.
<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Dimensions</th>
<th>Statistics Available</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available&lt;sup&gt;1&lt;/sup&gt;</td>
<td>The number of WorkSpaces that returned a healthy status.</td>
<td>DirectoryId</td>
<td>Average, Sum, Maximum, Minimum, Data Samples</td>
<td>Count</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WorkspaceId</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unhealthy&lt;sup&gt;1&lt;/sup&gt;</td>
<td>The number of WorkSpaces that returned an unhealthy status.</td>
<td>DirectoryId</td>
<td>Average, Sum, Maximum, Minimum, Data Samples</td>
<td>Count</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WorkspaceId</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ConnectionAttempt&lt;sup&gt;2&lt;/sup&gt;</td>
<td>The number of connection attempts.</td>
<td>DirectoryId</td>
<td>Average, Sum, Maximum, Minimum, Data Samples</td>
<td>Count</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WorkspaceId</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ConnectionSuccess&lt;sup&gt;2&lt;/sup&gt;</td>
<td>The number of successful connections.</td>
<td>DirectoryId</td>
<td>Average, Sum, Maximum, Minimum, Data Samples</td>
<td>Count</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WorkspaceId</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ConnectionFailure&lt;sup&gt;2&lt;/sup&gt;</td>
<td>The number of failed connections.</td>
<td>DirectoryId</td>
<td>Average, Sum, Maximum, Minimum, Data Samples</td>
<td>Count</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WorkspaceId</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SessionLaunchTime&lt;sup&gt;2&lt;/sup&gt;</td>
<td>The amount of time it takes to initiate a WorkSpaces session.</td>
<td>DirectoryID</td>
<td>Average, Sum, Maximum, Minimum, Data Samples</td>
<td>Second (time)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WorkspaceID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>InSessionLatency&lt;sup&gt;2&lt;/sup&gt;</td>
<td>The round trip time between the WorkSpaces client and the WorkSpace.</td>
<td>DirectoryID</td>
<td>Average, Sum, Maximum, Minimum, Data Samples</td>
<td>Millisecond (time)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WorkspaceID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SessionDisconnect&lt;sup&gt;2&lt;/sup&gt;</td>
<td>The number of connections that were closed, including user-initiated and failed connections.</td>
<td>DirectoryID</td>
<td>Average, Sum, Maximum, Minimum, Data Samples</td>
<td>Count</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WorkspaceID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UserConnected&lt;sup&gt;3&lt;/sup&gt;</td>
<td>The number of WorkSpaces that have a user connected.</td>
<td>DirectoryID</td>
<td>Average, Sum, Maximum, Minimum, Data Samples</td>
<td>Count</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WorkspaceID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stopped</td>
<td>The number of WorkSpaces that are stopped.</td>
<td>DirectoryID</td>
<td>Average, Sum, Maximum, Minimum, Data Samples</td>
<td>Count</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WorkspaceID</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Dimensions for Amazon WorkSpaces Metrics

To filter the metric data, use the following dimensions.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DirectoryId</td>
<td>Filters the metric data to the WorkSpaces in the specified directory. The form of the directory ID is d-XXXXXXXXXX.</td>
</tr>
<tr>
<td>WorkspaceId</td>
<td>Filters the metric data to the specified WorkSpace. The form of the workspace ID is ws-XXXXXXXXXX.</td>
</tr>
</tbody>
</table>

### 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.

   ```bash
   aws cloudwatch describe-alarms --state-value "ALARM"
   ```
Monitoring Example

2. Get the list of WorkSpaces in the specified directory using the `describe-workspaces` command.

```bash
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.

```bash
aws cloudwatch get-metric-statistics \
  --namespace AWS/WorkSpaces \ 
  --metric-name ConnectionFailure \ 
  --start-time 2015-04-27T00:00:00Z \ 
  --end-time 2015-04-28T00:00Z \ 
  --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 CloudWatch Events

You can use events from Amazon CloudWatch Events 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 CloudWatch Event type of WorkSpaces Access.
- Analyze login data, which is available in near real-time, and perform automated actions by using AWS Lambda.
- Use policy controls to block access to files and applications from unauthorized IP addresses.

For more information about events, see the Amazon CloudWatch Events User Guide.

WorkSpaces Events

Amazon WorkSpaces client applications send WorkSpaces Access events to CloudWatch Events when a user successfully logs in to a WorkSpace. All Amazon WorkSpaces clients send these events.

Events are represented as JSON objects. The following is example data for a WorkSpaces Access event.

```json
{
  "version": "0",
  "id": "64ca0eda-9751-dc55-c41a-1bd50b4fc9b7",
  "detail-type": "WorkSpaces Access",
  "source": "aws.workspaces",
  "account": "123456789012",
  "time": "2018-07-01T17:53:06Z",
  "region": "us-east-2",
  "resources": [],
  "detail": {
    "clientIpAddress": "192.0.2.3",
    "actionType": "successfulLogin",
    "workspacesClientProductName": "WorkSpaces Desktop client",
    "loginTime": "2018-07-01T17:52:51.595Z",
    "clientPlatform": "Windows",
    "directoryId": "d-123456789",
    "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.
Create a Rule to Handle WorkSpaces Events

Use the following procedure to create a CloudWatch Events rule to handle the WorkSpaces events.

To create a rule to handle WorkSpaces events

2. In the navigation pane, choose Events.
3. Choose Create rule.
4. For Event Source, do the following:
   a. Choose Event Pattern and Build event pattern to match events by service (the default).
   b. For Service Name, choose WorkSpaces.
   c. For Event Type, choose WorkSpaces Access.
5. For Targets, choose Add target, and then choose the service that is to act when a WorkSpaces event is detected. Provide any information required by this service.
6. Choose Configure details. For Rule definition, enter a name and description.
7. Choose Create rule.
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 Amazon 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 Amazon WorkSpaces. It shows you how to configure Amazon 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 Amazon WorkSpaces resources.

Contents
- Data Protection in Amazon WorkSpaces (p. 92)
- Identity and Access Management for Amazon WorkSpaces (p. 93)
- Compliance Validation for Amazon WorkSpaces (p. 98)
- Resilience in Amazon WorkSpaces (p. 99)
- Infrastructure Security in Amazon WorkSpaces (p. 99)
- Update Management in Amazon WorkSpaces (p. 102)

Data Protection in Amazon WorkSpaces

Amazon WorkSpaces conforms to the AWS shared responsibility model, which includes regulations and guidelines for data protection. AWS is responsible for protecting the global infrastructure that runs all the AWS services. AWS maintains control over data hosted on this infrastructure, including the security configuration controls for handling customer content and personal data. AWS customers and APN partners, acting either as data controllers or data processors, are responsible for any personal data that they put in the AWS Cloud.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM), so that 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 TLS to communicate with AWS resources.
- Set up API and user activity logging with AWS CloudTrail.
- 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 personal data that is stored in Amazon S3.
We strongly recommend that you never put sensitive identifying information, such as your customers' account numbers, into free-form fields or metadata, such as function names and tags. Any data that you enter into metadata might get picked up for inclusion in diagnostic logs. When you provide a URL to an external server, don't include credentials information in the URL to validate your request to that server.

For more information about data protection, see the AWS Shared Responsibility Model and GDPR blog post on the AWS Security Blog.

**Encryption at Rest**

You can encrypt the storage volumes for your WorkSpaces using customer master keys (CMK) from AWS Key Management Service. For more information, see Encrypted WorkSpaces (p. 66).

**Encryption in Transit**

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.

**Identity and Access Management for Amazon WorkSpaces**

By default, IAM users don't have permissions for Amazon WorkSpaces resources and operations. To allow IAM users to manage Amazon 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. For more information about IAM policies, see Policies and Permissions in the IAM User Guide guide.

Amazon WorkSpaces also creates an IAM role to allow the Amazon WorkSpaces service access to required resources.

For more information about IAM, see Identity and Access Management (IAM) and the IAM User Guide.

**Example 1: Perform all Amazon WorkSpaces tasks**

The following policy statement grants an IAM user permission to perform all Amazon WorkSpaces tasks, including creating and managing directories. It also grants permission to run the quick setup procedure.

Note that although Amazon WorkSpaces fully supports the Action and Resource elements when using the API and command line tools, you must set them both to "*" in order to use the Amazon WorkSpaces console successfully.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:PassRole",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
```
Example 2: Perform WorkSpace-specific tasks

The following policy statement grants an IAM user permission to perform WorkSpace-specific tasks, such as launching and removing WorkSpaces. In the policy statement, the `ds:*` action grants broad permissions — full control over all Directory Services objects in the account.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["workspaces:*", "ds:*", "iam:PutRolePolicy"],
            "Resource": "*",
        }
    ]
}
```

To also grant the user the ability to enable Amazon WorkDocs for users within Amazon WorkSpaces, add the `workdocs` operations as shown in the following example.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["workspaces:*"],
            "Resource": "*",
        }
    ]
}
```
To also grant the user the ability to use the Launch WorkSpaces wizard, add the kms operations as shown in the following example.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup",
        "workdocs:RemoveUserFromGroup",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Creating the workspaces_DefaultRole Role

Before you can register a directory using the API, you must create the workspaces_DefaultRole role, if it doesn't already exist.

**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 and AmazonWorkSpacesSelfServiceAccess.
9. Under Set permissions boundary, do not use a permissions boundary.
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.

```json
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "workspaces.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

19. Choose Update Trust Policy.

Specifying Amazon WorkSpaces Resources in an IAM Policy

To specify an Amazon WorkSpaces resource in the Resource element of the policy statement, use the Amazon Resource Name (ARN) of the resource. You control access to your Amazon WorkSpaces resources by either allowing or denying permissions to use the API actions specified in the Action element of your IAM policy statement. Amazon 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-2).
- **account_id**
  - The ID of the AWS account, with no hyphens (for example, 123456789012).
- **workspace_identifier**
  - The ID of the WorkSpace (for example, ws-0123456789).

The following is the format of the Resource element of a policy statement that identifies a specific WorkSpace.

```
```

You can use the * wildcard to specify all WorkSpaces that belong to a specific account in a specific Region.

**Bundle ARN**

A bundle ARN has the syntax shown in the following example.
Specifying Amazon WorkSpaces Resources in an IAM Policy

The Region that the WorkSpace is in (for example, us-east-2).

The ID of the AWS account, with no hyphens (for example, 123456789012).

The ID of the WorkSpace bundle (for example, wsb-0123456789).

The following is the format of the Resource element of a policy statement that identifies a specific bundle.


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"

The Region that the WorkSpace is in (for example, us-east-2).

The ID of the AWS account, with no hyphens (for example, 123456789012).

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.


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"

The Region that the WorkSpace is in (for example, us-east-2).
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.


You can use the * wildcard to specify all directories 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
- 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": "*"

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 Amazon WorkSpaces and FedRAMP, see Set Up Amazon WorkSpaces for FedRAMP Authorization or DoD SRG Compliance (p. 28).

Your compliance responsibility when using Amazon 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 Whitepaper** – 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.

### Infrastructure Security in Amazon WorkSpaces

As a managed service, Amazon WorkSpaces is protected by the AWS global network security procedures that are described in the *Amazon Web Services: Overview of Security Processes* whitepaper.

You use AWS published API calls to access Amazon WorkSpaces through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed 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 Amazon WorkSpaces (p. 8).
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 (p. 26).

You can restrict WorkSpace access to trusted devices with valid certificates. For more information, see Restrict WorkSpaces Access to Trusted Devices (p. 23).

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 Amazon 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 Amazon WorkSpaces (p. 34).

To further control access to your WorkSpaces, use multi-factor authentication. For more information, see How to Enable Multi-Factor Authentication for AWS Services.

Connect to Amazon WorkSpaces 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.

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 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"
```
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 (p. 19).

**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`.

```json
{
   "Statement": [
   {
      "Action": "workspaces:*",
      "Effect": "Allow",
      "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 Amazon WorkSpaces (p. 93) 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 an Amazon Virtual Private Network (VPN) or AWS Direct Connect. For information about Amazon VPN, 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 Amazon 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 Amazon WorkSpaces during a regular maintenance window or you can update them yourself. For more information, see WorkSpace Maintenance (p. 65).

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 WAM
Amazon WorkSpaces Application Manager (Amazon WAM) offers a fast, flexible, and secure way to deploy and manage applications for your Windows WorkSpaces. For more information, see the Amazon WAM Administration Guide.
Troubleshooting Amazon WorkSpaces Issues

The following information can help you troubleshoot issues with your WorkSpaces.

Enabling Advanced Logging

To help troubleshoot issues that your users may experience, you can enable advanced logging on any Amazon WorkSpaces client. Advanced logging is enabled for every subsequent client session until you disable it.

Advanced logging generates log files that contain diagnostic information and debugging-level details, including verbose performance data. These files are automatically uploaded to a database in AWS.

**Note**

To have AWS review the log files that are generated by advanced logging 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 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
   ```

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
   ```
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.

Troubleshooting for 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 (p. 105)
- I changed the shell for my Amazon Linux WorkSpace and now I can't provision a PCoIP session (p. 105)
- Launching WorkSpaces in my connected directory often fails (p. 105)
- Launching WorkSpaces fails with an internal error (p. 105)
- My users can't connect to a Windows WorkSpace with an interactive logon banner (p. 105)
- My users are having issues when they try to log on to BYOL WorkSpaces from WorkSpaces Web Access (p. 105)
- The WorkSpaces client gives my users a network error, but they are able to use other network-enabled apps on their devices (p. 106)
- My WorkSpace users see the following error message: "Device can't connect to the registration service. Check your network settings." (p. 108)
- My users aren't receiving invitation emails or password reset emails (p. 108)
- I receive the message "The system administrator has set policies to prevent this installation" when I try to install applications on a Windows WorkSpace (p. 108)
- No WorkSpaces in my directory can connect to the internet (p. 109)
- I receive a "DNS unavailable" error when I try to connect to my on-premises directory (p. 109)
- I receive a "Connectivity issues detected" error when I try to connect to my on-premises directory (p. 109)
- I receive an "SRV record" error when I try to connect to my on-premises directory (p. 110)
- My Windows WorkSpace goes to sleep when it's left idle (p. 110)
- One of my WorkSpaces has a state of "Unhealthy" (p. 110)
- I receive ThrottlingException errors to some of my API calls (p. 111)
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 only up to 20 letters, spaces, and numbers that are representable in UTF-8, plus the following special characters:

_.-#

Additionally, you can't use 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 (p. 45).

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 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.

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 Amazon WorkSpaces.

My users are having issues when they try to log on to BYOL WorkSpaces from WorkSpaces Web Access

BYOL WorkSpaces rely 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 BYOL WorkSpaces, you must configure a Group Policy setting and a Local Security Policy setting. If these two settings are not
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.

Amazon 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 Amazon 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 (p. 107)
- PCoIP Zero Clients (p. 107)
- Other Client Applications (p. 108)

**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 Amazon WorkSpaces Client Downloads. 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**

2. Download the Starfield certificate in DER format (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92).
3. Open the Microsoft Management Console. (From a Command Prompt window, run `mmc`.)
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.
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 users aren't receiving invitation emails or password reset emails

Users might not receive welcome or password reset emails for WorkSpaces that were created using AD Connector.

To manually send welcome emails to these users, see Send an Invitation Email (p. 58).

To assist users with resetting their passwords, see your documentation for Microsoft Active Directory.

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 Amazon WorkSpaces Group Policy object.
1. Make sure that the most recent Amazon WorkSpaces Group Policy administrative template (p. 41) 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. Choose Action, Edit in the main menu.


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 Amazon 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 from Your WorkSpace (p. 24).

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)
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 and Sound.
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. If this plan isn't visible, choose the arrow to the right of Show additional plans to display it.

If the preceding steps do not solve the issue, do the following:

1. 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.
2. 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.
3. 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).
4. Choose the plus sign to the left of PCI Express, and do the same for Link State Power Management.
5. Verify that the Link State Power Management settings are Off.
6. Choose OK (or Apply if you changed any settings) to close the dialog box.
7. 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 Amazon 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.
I receive ThrottlingException errors to some of my API calls

The default allowed rate for Amazon 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.

<table>
<thead>
<tr>
<th>Second</th>
<th>Number of Requests Sent</th>
<th>Net Requests Allowed</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>5</td>
<td>During the first second (second 1), five requests are allowed, up to the burst rate maximum of five calls per second.</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>Because two or fewer calls were issued in second 1, the full burst capacity of five calls is still available.</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>5</td>
<td>Because only two calls were issued in second 2, the full burst capacity of five calls is still available.</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>2</td>
<td>Because the full burst capacity was used in second 3, only the constant rate of two calls per second is available.</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>2</td>
<td>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.</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>1</td>
<td>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.</td>
</tr>
</tbody>
</table>
I receive ThrottlingException errors to some of my API calls

<table>
<thead>
<tr>
<th>Second</th>
<th>Number of Requests Sent</th>
<th>Net Requests Allowed</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>0</td>
<td>3</td>
<td>Now that there are no longer throttled API calls in the queue, the rate limit will continue to increase, up to the burst rate limit of five calls.</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>5</td>
<td>Because no calls were issued in second 7, the maximum number of requests is allowed.</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>5</td>
<td>Even though no calls were issued in second 8, the rate limit does not increase above five.</td>
</tr>
</tbody>
</table>
Amazon WorkSpaces Quotas

The following are the quotas (also referred to as limits) for Amazon WorkSpaces for your AWS account. To request a quota increase, use the Amazon WorkSpaces Limits form.

WorkSpace and Image Quotas

- WorkSpaces per Region: 1
- Graphics WorkSpaces per Region: 0
- GraphicsPro WorkSpaces per Region: 0
- Images per Region: 5

IP Access Control Quotas

- IP access control groups per Region: 100
- Rules per IP access control group: 10
- IP access control groups per directory: 25
Document History

The following table describes the important changes to the Amazon 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 Amazon WorkSpaces RSS feed.

<table>
<thead>
<tr>
<th>update-history-change</th>
<th>update-history-description</th>
<th>update-history-date</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrivateLink integration for Amazon WorkSpaces APIs</td>
<td>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.</td>
<td>November 25, 2019</td>
</tr>
<tr>
<td>Amazon WorkSpaces launched in China (Ningxia)</td>
<td>Amazon WorkSpaces is available in the China (Ningxia) Region.</td>
<td>November 13, 2019</td>
</tr>
<tr>
<td>Restore WorkSpaces to last known healthy state</td>
<td>You can use the restore feature to roll back a WorkSpace to its last known healthy state.</td>
<td>September 18, 2019</td>
</tr>
<tr>
<td>FIPS endpoint encryption</td>
<td>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.</td>
<td>September 12, 2019</td>
</tr>
<tr>
<td>Copy WorkSpace images</td>
<td>You can copy your images within the same Region or across Regions.</td>
<td>June 27, 2019</td>
</tr>
<tr>
<td>Self-Service WorkSpace Management Capabilities for Users</td>
<td>You can enable self-service WorkSpace management capabilities for your users to provide them with more control over their experience.</td>
<td>November 19, 2018</td>
</tr>
<tr>
<td>BYOL Automation</td>
<td>You can use Bring Your Own License (BYOL) automation to simplify the process of using Windows 7 and Windows</td>
<td>November 16, 2018</td>
</tr>
</tbody>
</table>
Earlier Updates

The following table describes important additions to the Amazon WorkSpaces service and its documentation set before January 1, 2018.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexible compute options</td>
<td>You can switch your WorkSpaces between the Value, Standard, Performance, and Power bundles.</td>
<td>December 22, 2017</td>
</tr>
<tr>
<td>Configurable storage</td>
<td>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.</td>
<td>December 22, 2017</td>
</tr>
<tr>
<td>Control device access</td>
<td>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).</td>
<td>June 19, 2017</td>
</tr>
<tr>
<td>Inter-forest trusts</td>
<td>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.</td>
<td>February 9, 2017</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Windows Server 2016 bundles</td>
<td>Amazon WorkSpaces offers bundles that include a Windows 10 desktop experience, powered by Windows Server 2016.</td>
<td>November 29, 2016</td>
</tr>
<tr>
<td>Web Access</td>
<td>You can access your Windows WorkSpaces from a web browser using Amazon WorkSpaces Web Access.</td>
<td>November 18, 2016</td>
</tr>
<tr>
<td>Hourly WorkSpaces</td>
<td>You can configure your WorkSpaces so that users are billed by the hour.</td>
<td>August 18, 2016</td>
</tr>
<tr>
<td>Windows 10 BYOL</td>
<td>You can bring your Windows 10 Desktop License to Amazon WorkSpaces (BYOL).</td>
<td>July 21, 2016</td>
</tr>
<tr>
<td>Tagging support</td>
<td>You can use tags to manage and track your WorkSpaces.</td>
<td>May 17, 2016</td>
</tr>
<tr>
<td>Saved registrations</td>
<td>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.</td>
<td>January 28, 2016</td>
</tr>
<tr>
<td>Windows 7 BYOL, Chromebook client, WorkSpace encryption</td>
<td>You can bring your Windows 7 Desktop License to Amazon WorkSpaces (BYOL), use the Chromebook client, and use WorkSpace encryption.</td>
<td>October 1, 2015</td>
</tr>
<tr>
<td>CloudWatch monitoring</td>
<td>Added information about CloudWatch monitoring.</td>
<td>April 28, 2015</td>
</tr>
<tr>
<td>Automatic session reconnect</td>
<td>Added information about the auto session reconnect feature in the WorkSpaces desktop client applications.</td>
<td>March 31, 2015</td>
</tr>
<tr>
<td>Public IP addresses</td>
<td>You can automatically assign a public IP address to your WorkSpaces.</td>
<td>January 23, 2015</td>
</tr>
<tr>
<td>Amazon WorkSpaces launched in Asia Pacific (Singapore)</td>
<td>Amazon WorkSpaces is available in the Asia Pacific (Singapore) Region.</td>
<td>January 15, 2015</td>
</tr>
<tr>
<td>Value bundle added, Standard bundle updates, Office 2013 added</td>
<td>The Value bundle is available, the Standard bundle hardware has been upgraded, and Microsoft Office 2013 is available in Plus packages.</td>
<td>November 6, 2014</td>
</tr>
<tr>
<td>Image and bundle support</td>
<td>You can create an image from a WorkSpace that you've customized and a custom WorkSpace bundle from the image.</td>
<td>October 28, 2014</td>
</tr>
<tr>
<td>PCoIP zero client support</td>
<td>You can access Amazon WorkSpaces PCoIP zero client devices.</td>
<td>October 15, 2014</td>
</tr>
<tr>
<td>Amazon WorkSpaces launched in Asia Pacific (Tokyo)</td>
<td>Amazon WorkSpaces is available in the Asia Pacific (Tokyo) Region.</td>
<td>August 26, 2014</td>
</tr>
<tr>
<td>Local printer support</td>
<td>You can enable local printer support for your WorkSpaces.</td>
<td>August 26, 2014</td>
</tr>
<tr>
<td>Multi-factor authentication</td>
<td>You can use multi-factor authentication in connected directories.</td>
<td>August 11, 2014</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Default OU support and target domain support</td>
<td>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.</td>
<td>July 7, 2014</td>
</tr>
<tr>
<td>Add security groups</td>
<td>You can add a security group to your WorkSpaces.</td>
<td>July 7, 2014</td>
</tr>
<tr>
<td>Amazon WorkSpaces launched in Asia Pacific (Sydney)</td>
<td>Amazon WorkSpaces is available in the Asia Pacific (Sydney) Region.</td>
<td>May 15, 2014</td>
</tr>
<tr>
<td>Amazon WorkSpaces launched in Europe (Ireland)</td>
<td>Amazon WorkSpaces is available in the Europe (Ireland) Region.</td>
<td>May 5, 2014</td>
</tr>
<tr>
<td>Public beta</td>
<td>Amazon WorkSpaces is available as a public beta.</td>
<td>March 25, 2014</td>
</tr>
</tbody>
</table>