# Table of Contents

What is WorkSpaces? .......................................................................................................................... 1
  Features ........................................................................................................................................ 1
  Architecture ................................................................................................................................. 1
  Access your WorkSpace .............................................................................................................. 2
  Pricing ......................................................................................................................................... 3
  How to get started ....................................................................................................................... 3
Get started: Quick Setup .................................................................................................................. 4
  Before you begin .......................................................................................................................... 4
  What Quick Setup does .............................................................................................................. 5
  Step 1: Launch the WorkSpace .................................................................................................... 5
  Step 2: Connect to the WorkSpace ............................................................................................... 7
  Step 3: Clean up (Optional) ......................................................................................................... 7
  Next steps .................................................................................................................................... 8
Networking and access .................................................................................................................... 9
  Protocols for Amazon WorkSpaces ............................................................................................ 9
  VPC requirements ....................................................................................................................... 10
    Requirements ............................................................................................................................ 10
    Configure a VPC with private subnets and a NAT gateway .................................................... 10
    Configure a VPC with public subnets ....................................................................................... 12
  Availability Zones for WorkSpaces .............................................................................................. 13
  IP address and port requirements ............................................................................................... 14
    Ports for client applications ...................................................................................................... 15
    Ports for Web Access ................................................................................................................ 15
    Domains and IP addresses to add to your allow list .................................................................. 16
    .................................................................................................................................................. 21
    .................................................................................................................................................. 22
    Health check servers ............................................................................................................... 22
    PCoIP gateway servers .............................................................................................................. 24
    WSP gateway servers ............................................................................................................... 26
    Network interfaces ................................................................................................................... 26
    IP address and port requirements by Region ............................................................................ 30
  Network requirements ................................................................................................................. 54
  Trusted devices ............................................................................................................................ 55
    Step 1: Create the certificates .................................................................................................... 56
    Step 2: Deploy client certificates to the trusted devices ......................................................... 56
    Step 3: Configure the restriction .............................................................................................. 57
  SAML 2.0 integration .................................................................................................................... 57
    Authentication workflow ............................................................................................................. 57
    Setting up SAML 2.0 (preview) .................................................................................................. 59
  Smart card authentication ............................................................................................................ 66
    Requirements ............................................................................................................................ 67
    Limitations ................................................................................................................................ 67
    Directory configuration .............................................................................................................. 68
    Enable smart cards for Windows WorkSpaces ......................................................................... 68
    Enable smart cards for Linux WorkSpaces .............................................................................. 70
  Internet access ............................................................................................................................ 74
  Security groups ............................................................................................................................. 75
  IP access control groups ............................................................................................................. 76
    Create an IP access control group ............................................................................................. 76
    Associate an IP access control group with a directory ............................................................ 76
    Copy an IP access control group ............................................................................................... 77
    Delete an IP access control group ............................................................................................ 77
  PCoIP zero client .......................................................................................................................... 77
  Set up Android for Chromebooks ............................................................................................... 78
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Access</td>
<td>78</td>
</tr>
<tr>
<td>Step 1: Enable Web Access to your WorkSpaces</td>
<td>79</td>
</tr>
<tr>
<td>Step 2: Configure inbound and outbound access to ports for Web Access</td>
<td>79</td>
</tr>
<tr>
<td>Step 3: Configure Group Policy and security policy settings to enable users to log on</td>
<td>79</td>
</tr>
<tr>
<td>FIPS endpoint encryption</td>
<td>81</td>
</tr>
<tr>
<td>Enable SSH connections</td>
<td>82</td>
</tr>
<tr>
<td>Prerequisites for SSH connections to Amazon Linux WorkSpaces</td>
<td>83</td>
</tr>
<tr>
<td>Enable SSH connections to all Amazon Linux WorkSpaces in a directory</td>
<td>84</td>
</tr>
<tr>
<td>Enable SSH connections to a specific Amazon Linux WorkSpace</td>
<td>84</td>
</tr>
<tr>
<td>Connect to an Amazon Linux WorkSpace using Linux or PuTTY</td>
<td>85</td>
</tr>
<tr>
<td>Required configuration</td>
<td>86</td>
</tr>
<tr>
<td>Routing table configuration</td>
<td>86</td>
</tr>
<tr>
<td>Components for Windows</td>
<td>86</td>
</tr>
<tr>
<td>Components for Linux</td>
<td>87</td>
</tr>
<tr>
<td>Directories</td>
<td>89</td>
</tr>
<tr>
<td>Register a directory</td>
<td>90</td>
</tr>
<tr>
<td>Update directory details</td>
<td>91</td>
</tr>
<tr>
<td>Select an organizational unit</td>
<td>91</td>
</tr>
<tr>
<td>Configure automatic public IP addresses</td>
<td>92</td>
</tr>
<tr>
<td>Control device access</td>
<td>93</td>
</tr>
<tr>
<td>Manage local administrator permissions</td>
<td>93</td>
</tr>
<tr>
<td>Update the AD Connector account (AD Connector)</td>
<td>93</td>
</tr>
<tr>
<td>Multi-factor authentication (AD Connector)</td>
<td>94</td>
</tr>
<tr>
<td>Update DNS servers for WorkSpaces</td>
<td>94</td>
</tr>
<tr>
<td>Best practices</td>
<td>95</td>
</tr>
<tr>
<td>Step 1: Update the DNS server settings on your WorkSpaces</td>
<td>95</td>
</tr>
<tr>
<td>Step 2: Update the DNS server settings for Active Directory</td>
<td>97</td>
</tr>
<tr>
<td>Step 3: Test the updated DNS server settings</td>
<td>97</td>
</tr>
<tr>
<td>Delete a directory</td>
<td>99</td>
</tr>
<tr>
<td>Enable Amazon WorkDocs for AWS Managed Microsoft AD</td>
<td>100</td>
</tr>
<tr>
<td>Set up Directory Administration</td>
<td>101</td>
</tr>
<tr>
<td>Launch a WorkSpace</td>
<td>103</td>
</tr>
<tr>
<td>Launch using AWS Managed Microsoft AD</td>
<td>104</td>
</tr>
<tr>
<td>Before you begin</td>
<td>104</td>
</tr>
<tr>
<td>Step 1: Create an AWS Managed Microsoft AD Directory</td>
<td>105</td>
</tr>
<tr>
<td>Step 2: Create a WorkSpace</td>
<td>105</td>
</tr>
<tr>
<td>Step 3: Connect to the WorkSpace</td>
<td>106</td>
</tr>
<tr>
<td>Next steps</td>
<td>107</td>
</tr>
<tr>
<td>Launch using Simple AD</td>
<td>107</td>
</tr>
<tr>
<td>Before you begin</td>
<td>107</td>
</tr>
<tr>
<td>Step 1: Create a Simple AD directory</td>
<td>108</td>
</tr>
<tr>
<td>Step 2: Create a WorkSpace</td>
<td>109</td>
</tr>
<tr>
<td>Step 3: Connect to the WorkSpace</td>
<td>109</td>
</tr>
<tr>
<td>Next steps</td>
<td>107</td>
</tr>
<tr>
<td>Launch using AD Connector</td>
<td>110</td>
</tr>
<tr>
<td>Before you begin</td>
<td>111</td>
</tr>
<tr>
<td>Step 1: Create an AD Connector</td>
<td>111</td>
</tr>
<tr>
<td>Step 2: Create a WorkSpace</td>
<td>112</td>
</tr>
<tr>
<td>Step 3: Connect to the WorkSpace</td>
<td>112</td>
</tr>
<tr>
<td>Next steps</td>
<td>110</td>
</tr>
<tr>
<td>Launch using a trusted domain</td>
<td>113</td>
</tr>
<tr>
<td>Before you begin</td>
<td>114</td>
</tr>
<tr>
<td>Step 1: Establish a trust relationship</td>
<td>114</td>
</tr>
<tr>
<td>Step 2: Create a WorkSpace</td>
<td>114</td>
</tr>
<tr>
<td>Step 3: Connect to the WorkSpace</td>
<td>115</td>
</tr>
<tr>
<td>Next steps</td>
<td>116</td>
</tr>
<tr>
<td>Administer WorkSpace users</td>
<td>117</td>
</tr>
</tbody>
</table>
Troubleshooting ............................................................................................................................. 249
Security ......................................................................................................................................... 233
Troubleshoot specific issues ..................................................................................................... 252
Enabling advanced logging ...................................................................................................... 249
Update management .............................................................................................................. 248
Infrastructure security ............................................................................................................. 246
Resilience .............................................................................................................................. 245
Compliance validation ............................................................................................................. 245
Identity and access management .............................................................................................. 234
Data protection ...................................................................................................................... 233
Encryption at rest ................................................................................................................... 234
Encryption in transit ............................................................................................................... 234
Example policies ..................................................................................................................... 235
Specify WorkSpaces resources in an IAM policy ................................................................. 238
Create the workspaces_DefaultRole Role ........................................................................... 242
AWS managed policies for WorkSpaces .................................................................................. 243
Security considerations if you stop using cross-Region redirection ......................................... 232
Connect your private network to your VPC ........................................................................ 248
Create a VPC endpoint policy for Amazon WorkSpaces ........................................................ 247
Make Amazon WorkSpaces API requests through a VPC interface endpoint ...................... 246
Isolation on physical hosts ............................................................................................... 246
Network isolation ........................................................................................................... 246
Authorization of corporate users .......................................................................................... 246
Make Amazon WorkSpaces API requests through a VPC interface endpoint ...................... 246
Create a VPC endpoint policy for Amazon WorkSpaces ........................................................ 247
Connect your private network to your VPC ........................................................................ 248
Update management ............................................................................................................. 248
Amazon WAM ................................................................................................................... 248
Troubleshooting ..................................................................................................................... 249
Enabling advanced logging .................................................................................................. 249
Troubleshoot specific issues ................................................................................................. 252
I can't create an Amazon Linux WorkSpace because there are non-valid characters in the user name ................................................................. 253
I changed the shell for my Amazon Linux WorkSpace and now I can't provision a PCoIP session ................................................................. 253
My Amazon Linux WorkSpaces won't start ....................................................................... 253
Launching WorkSpaces in my connected directory often fails ............................................... 254
Launching WorkSpaces fails with an internal error ............................................................... 254
When I try to register a directory, the registration fails and leaves the directory in an ERROR state ................................................................. 255
My users can't connect to a Windows WorkSpace with an interactive logon banner ............ 255
My users can't connect to a Windows WorkSpace ............................................................... 255
My users are having issues when they try to log on to WorkSpaces from WorkSpaces Web Access ................................................................................................. 256
The Amazon WorkSpaces client displays a gray "Loading..." screen for a while before returning to the login screen. No other error message appears. ................................................................. 256
My users receive the message "WorkSpace Status: Unhealthy. We were unable to connect you to your WorkSpace. Please try again in a few minutes." ................................................................. 257
My users receive the message "This device is not authorized to access the WorkSpace. Please contact your administrator for assistance." ................................................................................................. 257
My users receive the message "No network. Network connection lost. Check your network connection or contact your administrator for help." when trying to connect to a WSP WorkSpace ................................................................................................. 257
The WorkSpaces client gives my users a network error, but they are able to use other network-enabled apps on their devices .............................................................. 258
My WorkSpace users see the following error message: “Device can't connect to the registration service. Check your network settings.” .......................................................... 259
My PCoIP zero client users are receiving the error “The supplied certificate is invalid due to timestamp” .................................................................................................................... 259
USB printers and other USB peripherals aren't working for PCoIP zero clients ......................... 260
My users skipped updating their Windows or macOS client applications and aren't getting prompted to install the latest version ........................................................................... 260
My users are unable to install the Android client application on their Chromebooks .......... 261
My users aren't receiving invitation emails or password reset emails ................................ 261
My users don't see the Forgot password? option on the client login screen ....................... 261
I receive the message “The system administrator has set policies to prevent this installation” when I try to install applications on a Windows WorkSpace .................................................. 261
No WorkSpaces in my directory can connect to the internet ................................................. 262
My WorkSpace has lost its internet access ........................................................................... 262
I receive a "DNS unavailable" error when I try to connect to my on-premises directory ........ 262
I receive a "Connectivity issues detected" error when I try to connect to my on-premises directory ......................................................................................................................... 263
I receive an "SRV record" error when I try to connect to my on-premises directory ................. 263
My Windows WorkSpace goes to sleep when it's left idle .................................................... 263
One of my WorkSpaces has a state of UNHEALTHY .......................................................... 264
My WorkSpace is unexpectedly crashing or rebooting ........................................................ 265
The same username has more than one WorkSpace, but the user can log in to only one of the WorkSpaces .............................................................................................................. 266
I’m having trouble using Docker with Amazon WorkSpaces .................................................. 267
I receive ThrottlingException errors to some of my API calls ................................................. 267
My WorkSpace keeps disconnecting when I let it run in the background ............................... 268
SAML 2.0 federation isn’t working. My users are not authorized to stream their WorkSpaces desktop. ............................................................................................................................ 268
My users are getting disconnected from their WorkSpaces session every 60 minutes. ............ 269
My users get a redirect URI error when they federate using the SAML 2.0 identity provider (IdP)-initiated flow, or an additional instance of the WorkSpaces client application starts every time my users attempt to sign in from the client after federating to the IdP. ............... 269
My users receive the message, “Something went wrong: An error occurred while launching your WorkSpace” when they attempt to sign in to the WorkSpaces client application after federating to the IdP. ................................................................. 269
My users receive the message, "Unable to validate tags" when they attempt to sign in to the WorkSpaces client application after federating to the IdP. ................................................................. 270
My users receive the message, “The client and the server cannot communicate, because they do not possess a common algorithm” ................................................................. 270
Quotas ...................................................................................................................................... 271
Document history ...................................................................................................................... 273
Earlier Updates ....................................................................................................................... 276
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. 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 and the section called “Create a custom image and bundle” (p. 181).
- Choose your protocol: PCoIP or WorkSpaces Streaming Protocol (WSP). For more information, see Protocols for Amazon WorkSpaces (p. 9).
- Connect to your WorkSpace and pick up from right where you left off. WorkSpaces provides a persistent desktop experience.
- WorkSpaces provides the flexibility of either monthly or hourly billing for WorkSpaces. For more information, see 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. For more information, see Directories (p. 89).
- 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. For more information, see the section called “VPC requirements” (p. 10). 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.

WorkSpaces uses your Simple AD, AD Connector, or AWS Managed Microsoft AD directory to authenticate users. Users access their WorkSpaces by using a client application from a supported device or, for Windows WorkSpaces, a web browser, and they log in by using their directory credentials. The login information is sent to an authentication gateway, which forwards the traffic to the directory for the WorkSpace. After the user is authenticated, streaming traffic is initiated through the streaming gateway.

Client applications use HTTPS over port 443 for all authentication and session-related information. Client applications use port 4172 (PCoIP) and port 4195 (WSP) for pixel streaming to the WorkSpace.
Access 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 devices
- Fire tablets
- Zero client devices (Teradici zero client devices are supported only with PCoIP.)

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

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

Pricing

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

With 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 WorkSpaces includes the use of Simple AD and AD Connector but not the use of AWS Managed Microsoft AD.

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 WorkSpaces Pricing.

For information about supported regions, see WorkSpaces Pricing.

How to get started

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

• Get started with WorkSpaces Quick Setup (p. 4)
• Launch a WorkSpace using AWS Managed Microsoft AD (p. 104)
• Launch a WorkSpace using Simple AD (p. 107)
• Launch a WorkSpace using AD Connector (p. 110)
• Launch a WorkSpace using a trusted domain (p. 113)

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

• Provision Desktops in the Cloud
• Best Practices for Deploying Amazon WorkSpaces
• Amazon WorkSpaces resources — includes whitepapers, blog posts, webinars, and re:Invent sessions
• Amazon WorkSpaces FAQs
Get started with WorkSpaces 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 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 WorkSpaces (p. 103).

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

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

To change your Region, see Choosing a Region.

**Tasks**

- Before you begin (p. 4)
- What Quick Setup does (p. 5)
- Step 1: Launch the WorkSpace (p. 5)
- Step 2: Connect to the WorkSpace (p. 7)
- Step 3: Clean up (Optional) (p. 7)
- Next steps (p. 8)

**Before you begin**

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

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

It’s also helpful to review and understand the following before you proceed:
What Quick Setup does

Quick Setup completes the following tasks on your behalf:

- **Creates an IAM role** to allow the WorkSpaces service to create elastic network interfaces and list your WorkSpaces directories. This role has the name `workspaces_DefaultRole`.

- **Creates a virtual private cloud (VPC)**. If you want to use an existing VPC instead, make sure it meets the requirements noted in Configure a VPC for WorkSpaces (p. 10), and then follow the steps in one of the tutorials listed in Launch a virtual desktop using WorkSpaces (p. 103). Choose the tutorial that corresponds to the type of Active Directory that you want to use.

- **Sets up a Simple AD directory** in the VPC and enables it for Amazon WorkDocs. This Simple AD directory is used to store user and WorkSpace information. The first user account created by Quick Setup is your admin user account. The directory also has an Administrator account. For more information, see What gets created in the AWS Directory Service Administration Guide.

- **Creates the specified user accounts and adds them to the directory**.

- **Creates WorkSpaces**. Each WorkSpace receives a public IP address to provide internet access. The running mode is AlwaysOn. For more information, see Manage the WorkSpace running mode (p. 147).

- **Sends invitation emails to the specified users**. If your users don't receive their invitation emails, see Send an invitation email (p. 118).

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

Step 1: Launch the WorkSpace

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

To launch a WorkSpace

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). In this case, see Launch a virtual desktop using WorkSpaces (p. 103).
3. On the Get Started with WorkSpaces page, next to Quick Setup, choose Launch.
4. For **Bundles**, select a bundle (hardware and software) for the user with the appropriate protocol (PCoIP or WSP). For more information about the various public bundles available for Amazon WorkSpaces, see [Amazon WorkSpaces Bundles](#).

![Bundle Options](#)

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

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

6. Choose **Launch WorkSpaces**.

7. On the confirmation page, choose **View the WorkSpaces Console**. It takes approximately 20 minutes for your WorkSpace to be launched. To monitor the progress, go to the left navigation pane and choose **Directories**. You will see a directory being created with an initial status of **REQUESTED** and then **CREATING**.

   After the directory has been created and has a status of **ACTIVE**, you can choose **WorkSpaces** in the left navigation pane to monitor the progress of the WorkSpace launch process. The initial
status of the WorkSpace is PENDING. When the launch is complete, the status is AVAILABLE and an invitation is sent to the email address that you specified for each user. If your users don't receive their invitation emails, see Send an invitation email (p. 118).

Step 2: Connect to the WorkSpace

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

To connect to the WorkSpace

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

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

2. Review WorkSpaces Clients in the Amazon WorkSpaces User Guide for more information about the requirements for each client, and then do one of the following:
   - When prompted, download one of the client applications or launch Web Access.
   - If you aren't prompted and you haven't installed a client application already, open https://clients.amazonworkspaces.com/ and download one of the client applications or launch Web Access.

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

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

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

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

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

Step 3: Clean up (Optional)

If you are finished with the WorkSpace that you created for this tutorial, you can delete it. For more information, see the section called “Delete a WorkSpace” (p. 179).

Note
Simple AD is made available to you free of charge to use with WorkSpaces. If there are no WorkSpaces being used with your Simple AD directory for 30 consecutive days, this directory will be automatically deregistered for use with Amazon WorkSpaces, and you will be charged for this directory as per the AWS Directory Service pricing terms.
To delete empty directories, see Delete the directory for your WorkSpaces (p. 99). If you delete your Simple AD directory, you can always create a new one when you want to start using WorkSpaces again.
Next steps

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

• Create a custom WorkSpaces image and bundle (p. 181)
• Administer your WorkSpaces (p. 125)
• Manage directories for WorkSpaces (p. 89)

To create additional WorkSpaces, do one of the following:

• If you want to continue using the VPC and the Simple AD directory that were created by Quick Setup, you can add WorkSpaces for additional users by following the steps in the Step 2: Create a WorkSpace (p. 109) section of the Launch a WorkSpace Using Simple AD tutorial.
• If you need to use another directory type or if you need to use an existing Active Directory, see the appropriate tutorial in Launch a virtual desktop using WorkSpaces (p. 103).

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

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

Contents
- Protocols for Amazon WorkSpaces (p. 9)
- Configure a VPC for WorkSpaces (p. 10)
- Availability Zones for Amazon WorkSpaces (p. 13)
- IP address and port requirements for WorkSpaces (p. 14)
- Amazon WorkSpaces client network requirements (p. 54)
- Restrict WorkSpaces access to trusted devices (p. 55)
- WorkSpaces Integration with SAML 2.0 (preview) (p. 57)
- Use smart cards for authentication (p. 66)
- Provide internet access from your WorkSpace (p. 74)
- Security groups for your WorkSpaces (p. 75)
- IP access control groups for your WorkSpaces (p. 76)
- Set up PCoIP zero clients for WorkSpaces (p. 77)
- Set up Android for Chromebooks (p. 78)
- Enable and configure Amazon WorkSpaces Web Access (p. 78)
- Set up Amazon WorkSpaces for FedRAMP authorization or DoD SRG compliance (p. 81)
- Enable SSH connections for your Linux WorkSpaces (p. 82)
- Required configuration and service components for WorkSpaces (p. 86)

Protocols for Amazon WorkSpaces

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

When to use PCoIP
- If you want to use the iPad, Android, or Linux clients.
- If you use Teradici zero client devices.
- If you need to use GPU-based bundles (Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro).
- If you need to use a Linux bundle for non-smart card use cases.
- If you need to use WorkSpaces in the China (Ningxia) Region.

When to use WSP
- If you need higher loss/latency tolerance to support your end user network conditions. For example, you have users who are accessing their WorkSpaces across global distances or using unreliable networks.
If you need your users to authenticate with smart cards or to use smart cards in-session.
• If you need webcam support capabilities in-session.
• If you need to use Web Access with the Windows Server 2019-powered WorkSpaces bundle.

Note
• A directory can have a mix of PCoIP and WSP WorkSpaces in it.
• A user can have both a PCoIP and a WSP WorkSpace as long as the two WorkSpaces are located in separate directories. The same user cannot have a PCoIP and a WSP WorkSpace in the same directory. For more information about creating multiple WorkSpaces for a user, see Create multiple WorkSpaces for a user (p. 118).
• You can migrate a WorkSpace between the two protocols by using the WorkSpaces migration feature, which requires a rebuild of the WorkSpace. For more information, see Migrate a WorkSpace (p. 175).

Configure a VPC for WorkSpaces

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 a public IP address or Elastic IP address with each WorkSpace.

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

Contents
• Requirements (p. 10)
• Configure a VPC with private subnets and a NAT gateway (p. 10)
• Configure a VPC with public subnets (p. 12)

Requirements

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

Note
Amazon WorkSpaces is available in a subset of the Availability Zones in each supported Region. To determine which Availability Zones you can use for the subnets of the VPC that you're using for WorkSpaces, see Availability Zones for Amazon WorkSpaces (p. 13).

Configure a VPC with private subnets and a NAT gateway

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

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

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Choose Create VPC.
3. Under Resources to create, choose VPC and more.
4. For Name tag auto-generation, enter a name for the VPC.
5. To configure the subnets, do the following:
   a. For Number of Availability Zones, choose 1 or 2, depending on your needs.
   b. Expand Customize AZs and choose your Availability Zones. Otherwise, AWS selects them for you. To make an appropriate selection, see Availability Zones for Amazon WorkSpaces (p. 13).
   c. For Number of public subnets, ensure that you have one public subnet per Availability Zone.
   d. For Number of private subnets, ensure that you have at least one private subnet per Availability Zone.
   e. Enter a CIDR block for each subnet. For more information, see Subnet sizing in the Amazon VPC User Guide.
6. For NAT gateways, choose 1 per AZ.
7. Choose Create VPC.

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

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

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

Configure a VPC with public subnets

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

Tasks
- Step 1: Create a VPC (p. 12)
- Step 2: Assign public IP addresses to your WorkSpaces (p. 13)

Step 1: Create a VPC

Create a VPC with one public subnet as follows.

To create the VPC
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Choose Create VPC.
3. Under Resources to create, choose VPC and more.
4. For Name tag auto-generation, enter a name for the VPC.
5. To configure the subnets, do the following:
   a. For Number of Availability Zones, choose 2.
   b. Expand Customize AZs and choose your Availability Zones. Otherwise, AWS selects them for you. To make an appropriate selection, see Availability Zones for Amazon WorkSpaces (p. 13).
   c. For Number of public subnets, choose 2.
   d. For Number of private subnets, choose 0.
   e. Enter a CIDR block for each public subnet. For more information, see Subnet sizing in the Amazon VPC User Guide.
6. Choose Create VPC.

IPv6 CIDR blocks

You can associate an IPv6 CIDR block with your VPC and subnets. However, if you configure your subnets to automatically assign IPv6 addresses to instances launched in the subnet, then you cannot use Graphics bundles. (You can use GraphicsPro bundles, however.) This restriction arises from a hardware limitation of previous-generation instance types that do not support IPv6.
To work around this issue, you can temporarily disable the **auto-assign IPv6 addresses** setting on the WorkSpaces subnets before launching Graphics bundles, and then reenable this setting (if needed) after launching Graphics bundles so that any other bundles receive the desired IP addresses.

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

### Step 2: Assign public IP addresses to your WorkSpaces

You can assign public IP addresses to your WorkSpaces automatically or manually. To use automatic assignment, see the section called “Configure automatic public IP addresses” (p. 92). To assign public IP addresses manually, use the following procedure.

For a video tutorial about how to assign an Elastic IP address to a WorkSpace, see the AWS Knowledge Center video: [How do I associate an Elastic IP Address with a WorkSpace?](https://aws.amazon.com/mp4).

**To assign a public IP address to a WorkSpace manually**

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

### Availability Zones for Amazon WorkSpaces

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

An Availability Zone is represented by a Region code followed by a letter identifier; for example, `us-east-1a`. To ensure that resources are distributed across the Availability Zones for a Region, we independently map Availability Zones to names for each AWS account. For example, the Availability Zone `us-east-1a` for your AWS account might not be the same location as `us-east-1a` for another AWS account.
To coordinate Availability Zones across accounts, you must use the AZ ID, which is a unique and consistent identifier for an Availability Zone. For example, use1-az2 is an AZ ID for the us-east-1 Region and it has the same location in every AWS account.

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

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

<table>
<thead>
<tr>
<th>Region name</th>
<th>Region code</th>
<th>Supported AZ IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td>use1-az2, use1-az4, use1-az6</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
<td>usw2-az1, usw2-az2, usw2-az3</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>ap-south-1</td>
<td>aps1-az1, aps1-az2, aps1-az3</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>ap-northeast-2</td>
<td>apne2-az1, apne2-az3</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>ap-southeast-1</td>
<td>apsel1-az1, apsel1-az2</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2</td>
<td>apse2-az1, apse2-az3</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1</td>
<td>apne1-az1, apne1-az4</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1</td>
<td>cac1-az1, cac1-az2</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>eu-central-1</td>
<td>euc1-az2, euc1-az3</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>eu-west-1</td>
<td>euw1-az1, euw1-az2, euw1-az3</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>eu-west-2</td>
<td>euw2-az2, euw2-az3</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>sa-east-1</td>
<td>sae1-az1, sae1-az3</td>
</tr>
</tbody>
</table>

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

**IP address and port requirements for WorkSpaces**

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

For an architecture diagram, see WorkSpaces Architecture (p. 1). For additional architecture diagrams, see Best Practices for Deploying Amazon WorkSpaces.
Ports for client applications

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

Port 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 and 4195 (UDP and TCP)

These ports are used for streaming the WorkSpace desktop and health checks. The desktop client applications do not support the use of a proxy server for port 4172 and 4195 traffic; they require a direct connection to ports 4172 and 4195. These ports must be open to the PCoIP Gateway and WorkSpaces Streaming Protocol (WSP) Gateway IP address ranges, and to the health check servers in the Region that the WorkSpace is in. For more information, see Health check servers (p. 22), PCoIP gateway servers (p. 24), and WSP gateway servers (p. 26).

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

Ports for Web Access

WorkSpaces Web Access requires outbound access for the following ports:

Port 53 (UDP)

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

Port 80 (UDP and TCP)

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

Port 443 (UDP and TCP)

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

Port 4195 (UDP and TCP)

For WorkSpaces that are configured for WorkSpaces Streaming Protocol (WSP), this port is used for streaming the WorkSpaces desktop. Web access does not support the use of a proxy server for port 4195 traffic. Direct connections are required. This port must be open to the WSP Gateway IP address ranges. For more information, see WSP gateway servers (p. 26).
Note
If your firewall uses stateful filtering, ephemeral ports (also known as dynamic ports) are automatically opened to allow return communication. If your firewall uses stateless filtering, you must open ephemeral ports explicitly to allow return communication. The required ephemeral port range that you must open varies depending on your configuration.

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

Domains and IP addresses to add to your allow list

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

Domains and IP addresses to add to your allow list

<table>
<thead>
<tr>
<th>Category</th>
<th>Domain or IP address</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>
</tbody>
</table>
| Client Auto-update | • https://d2td7dqidlhjx7.cloudfront.net/  
| | • In the AWS GovCloud (US-West) Region:  
| Connectivity Check | https://connectivity.amazonworkspaces.com/ |
| Device Metrics (for 1.0+ and 2.0+ WorkSpaces client applications) | https://device-metrics-us-2.amazon.com/ |
| Client Metrics (for 3.0+ WorkSpaces client applications) | Domains:  
| | • https://skylight-client-ds.us-east-1.amazonaws.com  
| | • https://skylight-client-ds.us-west-2.amazonaws.com  
| | • https://skylight-client-ds.ap-south-1.amazonaws.com  
| | • https://skylight-client-ds.ap-northeast-2.amazonaws.com  
| | • https://skylight-client-ds.ap-southeast-1.amazonaws.com  
| | • https://skylight-client-ds.ap-southeast-2.amazonaws.com  
| | • https://skylight-client-ds.ap-northeast-1.amazonaws.com  
| | • https://skylight-client-ds.ca-central-1.amazonaws.com  
| | • https://skylight-client-ds.eu-central-1.amazonaws.com  
| | • https://skylight-client-ds.eu-west-1.amazonaws.com |
## Domains and IP addresses to add to your allow list

<table>
<thead>
<tr>
<th>Category</th>
<th>Domain or IP address</th>
</tr>
</thead>
<tbody>
<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>Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)</td>
<td>• <a href="https://ws-client-service.us-east-1.amazonaws.com">https://ws-client-service.us-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-client-service.us-west-2.amazonaws.com">https://ws-client-service.us-west-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-client-service.ap-south-1.amazonaws.com">https://ws-client-service.ap-south-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-client-service.ap-northeast-2.amazonaws.com">https://ws-client-service.ap-northeast-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-client-service.ap-southeast-1.amazonaws.com">https://ws-client-service.ap-southeast-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-client-service.ap-southeast-2.amazonaws.com">https://ws-client-service.ap-southeast-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-client-service.ap-northeast-1.amazonaws.com">https://ws-client-service.ap-northeast-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-client-service.ca-central-1.amazonaws.com">https://ws-client-service.ca-central-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-client-service.eu-central-1.amazonaws.com">https://ws-client-service.eu-central-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-client-service.eu-west-1.amazonaws.com">https://ws-client-service.eu-west-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-client-service.eu-west-2.amazonaws.com">https://ws-client-service.eu-west-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ws-client-service.sa-east-1.amazonaws.com">https://ws-client-service.sa-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td>Category</td>
<td>Domain or IP address</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Directory Settings</td>
<td>Authentication from the client to the customer directory before login to the WorkSpace:</td>
</tr>
<tr>
<td></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></td>
<td>Connections from macOS clients:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://d32i4gd7pg4909.cloudfront.net/">https://d32i4gd7pg4909.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>Customer directory settings:</td>
</tr>
<tr>
<td></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></td>
<td>Login page graphics for customer directory level co-branding:</td>
</tr>
<tr>
<td></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></td>
<td>CSS file to style the login pages:</td>
</tr>
<tr>
<td></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></td>
<td>JavaScript file for the login pages:</td>
</tr>
<tr>
<td></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://d18af777lco7lp.cloudfront.net/">https://d18af777lco7lp.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• Asia Pacific (Mumbai) — <a href="https://d78hovzqqtbsb.cloudfront.net/">https://d78hovzqqtbsb.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://d3qzmd7y07p20i.cloudfront.net/">https://d3qzmd7y07p20i.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• Asia Pacific (Sydney) — <a href="https://dwcpxoxuua83q.cloudfront.net/">https://dwcpxoxuua83q.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• Asia Pacific (Tokyo) — <a href="https://d2c2t8mxjhhq5z1.cloudfront.net/">https://d2c2t8mxjhhq5z1.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• Canada (Central) — <a href="https://d2wfbpsypmqjmqog.cloudfront.net/">https://d2wfbpsypmqjmqog.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>• Europe (Frankfurt) — <a href="https://d1whcm49570jjw.cloudfront.net/">https://d1whcm49570jjw.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>
</tbody>
</table>
## Domains and IP addresses to add to your allow list

<table>
<thead>
<tr>
<th>Category</th>
<th>Domain or IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>• South America (São Paulo) — <a href="https://d2lh2qc5bdoq4b.cloudfront.net/">https://d2lh2qc5bdoq4b.cloudfront.net/</a></td>
<td></td>
</tr>
</tbody>
</table>

In the AWS GovCloud (US-West) Region:

- Customer directory settings:
  - https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/<directory ID>
- Login page graphics for customer directory level co-branding:
  - https://s3.amazonaws.com/workspaces-client-assets/prod/pdt/<directory ID>
- CSS file to style the login pages:
  - https://s3.amazonaws.com/workspaces-client-css/workspaces_v2.css
- JavaScript file for the login pages:
  - Not applicable

<table>
<thead>
<tr>
<th>Forrester Log Service</th>
<th><a href="https://fls-na.amazon.com/">https://fls-na.amazon.com/</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Check (DRP) Servers</td>
<td>Health check servers (p. 22)</td>
</tr>
<tr>
<td>Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)</td>
<td><a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
</tr>
<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>
</tbody>
</table>

In the AWS GovCloud (US-West) Region:

- https://login.us-gov-home.awsapps.com/directory/<directory id>/ (where <directory id> is the customer's domain)
<table>
<thead>
<tr>
<th>Category</th>
<th>Domain or IP address</th>
</tr>
</thead>
<tbody>
<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-south-1.amazonaws.com">https://ws-broker-service.ap-south-1.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.eu-east-1.amazonaws.com">https://ws-broker-service.eu-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="https://ws-broker-service.southwest-1.amazonaws.com">https://ws-broker-service.southwest-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="https://ws-broker-service.service.us-gov-west-1.amazonaws.com">https://ws-broker-service.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>
<tr>
<td>Category</td>
<td>Domain or IP address</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WorkSpaces API Endpoints</td>
<td>Domains:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.us-east-1.amazonaws.com">https://workspaces.us-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces-fips.us-east-1.amazonaws.com">https://workspaces-fips.us-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.us-west-2.amazonaws.com">https://workspaces.us-west-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces-fips.us-west-2.amazonaws.com">https://workspaces-fips.us-west-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.ap-south-1.amazonaws.com">https://workspaces.ap-south-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.ap-northeast-2.amazonaws.com">https://workspaces.ap-northeast-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.ap-southeast-1.amazonaws.com">https://workspaces.ap-southeast-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.ap-southeast-2.amazonaws.com">https://workspaces.ap-southeast-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.ap-northeast-1.amazonaws.com">https://workspaces.ap-northeast-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.ca-central-1.amazonaws.com">https://workspaces.ca-central-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.eu-central-1.amazonaws.com">https://workspaces.eu-central-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.eu-west-1.amazonaws.com">https://workspaces.eu-west-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.eu-west-2.amazonaws.com">https://workspaces.eu-west-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.sa-east-1.amazonaws.com">https://workspaces.sa-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.us-gov-west-1.amazonaws.com">https://workspaces.us-gov-west-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces-fips.us-gov-west-1.amazonaws">https://workspaces-fips.us-gov-west-1.amazonaws</a></td>
</tr>
<tr>
<td>PCoIP Session Gateway (PSG)</td>
<td>PCoIP gateway servers (p. 24)</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-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.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-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.ap-south-1.amazonaws.com">https://skylight-cm.ap-south-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.ap-southeast-1.amazonaws.com">https://skylight-cm.ap-southeast-1.amazonaws.com</a></td>
</tr>
</tbody>
</table>
## Health check servers

The WorkSpaces client applications perform health checks over ports 4172 and 4195. These checks validate whether TCP or UDP traffic streams from the WorkSpaces servers to the client applications. For these checks to finish successfully, your firewall policies must allow outbound traffic to the IP addresses of the following Regional health check servers.

<table>
<thead>
<tr>
<th>Category</th>
<th>Domain or IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <a href="https://skylight-cm.ap-southeast-2.amazonaws.com">https://skylight-cm.ap-southeast-2.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.ca-central-1.amazonaws.com">https://skylight-cm.ca-central-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://skylight-cm.eu-central-1.amazonaws.com">https://skylight-cm.eu-central-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://skylight-cm.eu-west-1.amazonaws.com">https://skylight-cm.eu-west-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://skylight-cm.eu-west-2.amazonaws.com">https://skylight-cm.eu-west-2.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://skylight-cm.sa-east-1.amazonaws.com">https://skylight-cm.sa-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://skylight-cm-fips.us-gov-west-1.amazonaws.com">https://skylight-cm-fips.us-gov-west-1.amazonaws.com</a></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Domain or IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSP Session Gateway (WSG)</td>
<td>WSP gateway servers (p. 26)</td>
</tr>
<tr>
<td>Web Access TURN Servers for WSP</td>
<td>WSP gateway servers (p. 26)</td>
</tr>
<tr>
<td>Region</td>
<td>Health check hostname</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>drp-iad.amazonworkspaces.com</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>drp-pdx.amazonworkspaces.com</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>drp-bom.amazonworkspaces.com</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>drp-icn.amazonworkspaces.com</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>drp-sin.amazonworkspaces.com</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>drp-syd.amazonworkspaces.com</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>drp-nrt.amazonworkspaces.com</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>drp-yul.amazonworkspaces.com</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Region</td>
<td>Health check hostname</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>drp-fra.amazonworkspaces.com</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>drp-dub.amazonworkspaces.com</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td>drp-lhr.amazonworkspaces.com</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>drp-gru.amazonworkspaces.com</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td>drp-pdt.amazonworkspaces.com</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PCoIP gateway servers**

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

**Note**

We are regularly updating our IP address ranges in the AWS IP Address Ranges ip-ranges.json file. To ingest the most up-to-date IP address ranges for WorkSpaces, look for entries in the ip-ranges.json file where service: "WORKSPACES_GATEWAYS".

<table>
<thead>
<tr>
<th>Region</th>
<th>Public IP address range</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>3.217.228.0 - 3.217.231.255</td>
</tr>
<tr>
<td>Region</td>
<td>Public IP address range</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>3.235.112.0 - 3.235.119.255</td>
</tr>
<tr>
<td></td>
<td>52.23.61.0 - 52.23.62.255</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>35.80.88.0 - 35.80.95.255</td>
</tr>
<tr>
<td></td>
<td>44.234.54.0 - 44.234.55.255</td>
</tr>
<tr>
<td></td>
<td>54.244.46.0 - 54.244.47.255</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>13.126.243.0 - 13.126.243.255</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>3.34.37.0 - 3.34.37.255</td>
</tr>
<tr>
<td></td>
<td>3.34.38.0 - 3.34.39.255</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>18.141.152.0 - 18.141.152.255</td>
</tr>
<tr>
<td></td>
<td>18.141.154.0 - 18.141.155.255</td>
</tr>
<tr>
<td></td>
<td>52.76.127.0 - 52.76.127.255</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>3.25.43.0 - 3.25.43.255</td>
</tr>
<tr>
<td></td>
<td>3.25.44.0 - 3.25.45.255</td>
</tr>
<tr>
<td></td>
<td>54.153.254.0 - 54.153.254.255</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>18.180.178.0 - 18.180.178.255</td>
</tr>
<tr>
<td></td>
<td>54.250.251.0 - 54.250.251.255</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>15.223.100.0 - 15.223.100.255</td>
</tr>
<tr>
<td></td>
<td>15.223.102.0 - 15.223.103.255</td>
</tr>
<tr>
<td></td>
<td>35.183.255.0 - 35.183.255.255</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>18.156.52.0 - 18.156.52.255</td>
</tr>
<tr>
<td></td>
<td>18.156.54.0 - 18.156.55.255</td>
</tr>
<tr>
<td></td>
<td>52.59.127.0 - 52.59.127.255</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>3.249.28.0 - 3.249.29.255</td>
</tr>
<tr>
<td></td>
<td>52.19.124.0 - 52.19.125.255</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>18.132.21.0 - 18.132.21.255</td>
</tr>
<tr>
<td></td>
<td>18.132.22.0 - 18.132.23.255</td>
</tr>
<tr>
<td></td>
<td>35.176.32.0 - 35.176.32.255</td>
</tr>
</tbody>
</table>
## WSP gateway servers

**Important**

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

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

<table>
<thead>
<tr>
<th>Region</th>
<th>Public IP address range</th>
</tr>
</thead>
<tbody>
<tr>
<td>South America (São Paulo)</td>
<td>18.230.103.0 - 18.230.103.255</td>
</tr>
<tr>
<td></td>
<td>18.230.104.0 - 18.230.105.255</td>
</tr>
<tr>
<td></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 (eth1) provides connectivity to the resources within your VPC and on the internet, and is used to join the WorkSpace to the directory.

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

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

**Warning**

Do not modify or delete any of the network interfaces that are attached to a WorkSpace. Doing so might cause the WorkSpace to become unreachable or lose internet access. For example, if you have enabled automatic assignment of Elastic IP addresses (p. 92) at the directory level, an Elastic IP address (from the Amazon-provided pool) is assigned to your WorkSpace when it is launched. However, if you associate an Elastic IP address that you own to a WorkSpace, and then you later disassociate that Elastic IP address from the WorkSpace, the WorkSpace loses its public IP address, and it doesn’t automatically get a new one from the Amazon-provided pool.

To associate a new public IP address from the Amazon-provided pool with the WorkSpace, you must rebuild the WorkSpace (p. 167). If you don’t want to rebuild the WorkSpace, you must associate another Elastic IP address that you own to the WorkSpace.

### Management interface IP ranges

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

**Note**

- **If you're using Bring Your Own License (BYOL) Windows WorkSpaces**, the IP address ranges in the following table do not apply. Instead, PCoIP BYOL WorkSpaces use the 54.239.224.0/20 IP address range for management interface traffic in all AWS Regions. For WSP BYOL Windows WorkSpaces, both the 54.239.224.0/20 and 10.0.0.0/8 IP address ranges apply in all AWS Regions. (These IP address ranges are used in addition to the /16 CIDR block that you select for management traffic for your BYOL WorkSpaces.)

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

<table>
<thead>
<tr>
<th>Region</th>
<th>IP address range</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16, WSP: 10.0.0.0/8</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, and 198.19.0.0/16, WSP: 10.0.0.0/8</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>PCoIP/WSP: 192.168.0.0/16, WSP: 10.0.0.0/8</td>
</tr>
<tr>
<td>Region</td>
<td>IP address range</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>PCoIP/WSP: 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>WSP: 10.0.0.0/8</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>PCoIP/WSP: 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>WSP: 10.0.0.0/8</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, and 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>WSP: 10.0.0.0/8</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>PCoIP/WSP: 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>WSP: 10.0.0.0/8</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>PCoIP/WSP: 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>WSP: 10.0.0.0/8</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>PCoIP/WSP: 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>WSP: 10.0.0.0/8</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, and 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>WSP: 10.0.0.0/8</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>PCoIP/WSP: 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>WSP: 10.0.0.0/8</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>PCoIP/WSP: 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>WSP: 10.0.0.0/8</td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td>PCoIP/WSP: 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>WSP: 10.0.0.0/8</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 on the PCoIP protocol.
- Inbound UDP on port 4172. This is used for streaming user input on the PCoIP protocol.
- Inbound TCP on port 4489. This is used for access using the web client.
- Inbound TCP on port 8200. This is used for management and configuration of the WorkSpace on the PCoIP protocol.
- Inbound TCP on ports 8201-8250. These ports are used for establishment of the streaming connection and for streaming user input on the WSP protocol.
- Inbound UDP on port 8220. This port is used for establishment of the streaming connection and for streaming user input on the WSP protocol.
• Outbound TCP on ports 8443 and 9997. This is used for access using the web client.
• Outbound UDP on ports 3478, 4172, and 4195. This is used for access using the web client.
• Outbound UDP on ports 50002 and 55002. This is used for streaming. If your firewall uses stateful filtering, the ephemeral ports 50002 and 55002 are automatically opened to allow return communication. If your firewall uses stateless filtering, you must open ephemeral ports 49152 - 65535 to allow return communication.
• Outbound TCP on port 80 to IP address 169.254.169.254 for access to the EC2 metadata service. Any HTTP proxy assigned to your WorkSpaces must also exclude 169.254.169.254.
• Outbound TCP on port 1688 to IP addresses 169.254.169.250 and 169.254.169.251 to allow access to Microsoft KMS for Windows activation for Workspaces that are based on public bundles. If you're using Bring Your Own License (BYOL) Windows WorkSpaces, you must allow access to your own KMS servers for Windows activation.
• Outbound TCP on port 1688 to IP address 54.239.236.220 to allow access to Microsoft KMS for Office activation for BYOL WorkSpaces.

If you're using Office through one of the WorkSpaces public bundles, the IP address for Microsoft KMS for Office activation varies. To determine that IP address, find the IP address for the management interface of the WorkSpace, and then replace the last two octets with 64.250. For example, if the IP address of the management interface is 192.168.3.5, the IP address for Microsoft KMS Office activation is 192.168.64.250.

• Outbound TCP to IP address 127.0.0.2 for WSP WorkSpaces when the WorkSpace host is configured to use a proxy server.

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

Primary interface ports

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

• For internet connectivity, the following ports must be open outbound to all destinations and inbound from the WorkSpaces VPC. You need to add these manually to the security group for your WorkSpaces if you want them to have internet access.
  • TCP 80 (HTTP)
  • TCP 443 (HTTPS)

• To communicate with the directory controllers, the following ports must be open between your WorkSpaces VPC and your directory controllers. For a Simple AD directory, the security group created by AWS Directory Service will have these ports configured correctly. For an AD Connector directory, you might need to adjust the default security group for the VPC to open these ports.
  • TCP/UDP 53 - DNS
  • TCP/UDP 88 - Kerberos authentication
  • UDP 123 - NTP
  • TCP 135 - RPC
  • UDP 137-138 - Netlogon
  • TCP 139 - Netlogon
  • TCP/UDP 389 - LDAP
  • TCP/UDP 445 - SMB
  • TCP 1024-65535 - Dynamic ports for RPC
If any security or firewall software is installed on a WorkSpace that blocks any of these ports, the WorkSpace may not function correctly or may be unreachable.

### IP address and port requirements by Region

#### US East (N. Virginia)

**Domains and IP Addresses to add to your allowlist**

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</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://d2td7dqlhjx7.cloudfront.net/">https://d2td7dqlhjx7.cloudfront.net/</a></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>Domain: <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>Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)</td>
<td>Domain: <a href="https://ws-client-service.us-east-1.amazonaws.com">https://ws-client-service.us-east-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>
<tr>
<td></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></td>
<td>Connections from macOS clients:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://d32i4gd7pg4909.cloudfront.net/">https://d32i4gd7pg4909.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>Customer directory settings:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://d21ui22avroxh6.cloudfront.net/prod/">https://d21ui22avroxh6.cloudfront.net/prod/</a>&lt;region&gt;/&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://d1cbg795sa4g1u.cloudfront.net/prod/">https://d1cbg795sa4g1u.cloudfront.net/prod/</a>&lt;region&gt;/&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://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>Category</td>
<td>Details</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
</tr>
<tr>
<td>JavaScript file for the login pages:</td>
<td></td>
</tr>
<tr>
<td>• US East (N. Virginia) — <a href="https://d32i4gd7pg4909.cloudfront.net/">https://d32i4gd7pg4909.cloudfront.net/</a></td>
<td></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>Health Check (DRP) Servers</td>
<td>Health check servers (p. 22)</td>
</tr>
<tr>
<td>Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)</td>
<td><a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
</tr>
<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>WS Broker</td>
<td>Domains:</td>
</tr>
<tr>
<td>• <a href="https://ws-broker-service.us-east-1.amazonaws.com">https://ws-broker-service.us-east-1.amazonaws.com</a></td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td>WorkSpaces API Endpoints</td>
<td>Domains:</td>
</tr>
<tr>
<td><a href="https://workspaces.us-east-1.amazonaws.com">https://workspaces.us-east-1.amazonaws.com</a></td>
<td></td>
</tr>
<tr>
<td>Session Broker (PCM)</td>
<td>Domains:</td>
</tr>
<tr>
<td>• <a href="https://skylight-cm.us-east-1.amazonaws.com">https://skylight-cm.us-east-1.amazonaws.com</a></td>
<td></td>
</tr>
<tr>
<td>• <a href="https://skylight-cm-fips.us-east-1.amazonaws.com">https://skylight-cm-fips.us-east-1.amazonaws.com</a></td>
<td></td>
</tr>
<tr>
<td>Web Access TURN Servers for PCoIP</td>
<td>Server:</td>
</tr>
<tr>
<td>• turn:*.us-east-1.rdn.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td>Health check hostname</td>
<td>drp-iad.amazonworkspaces.com</td>
</tr>
<tr>
<td>Health check IP addresses</td>
<td></td>
</tr>
<tr>
<td>• 3.209.215.252</td>
<td></td>
</tr>
<tr>
<td>• 3.212.50.30</td>
<td></td>
</tr>
<tr>
<td>• 3.225.55.35</td>
<td></td>
</tr>
<tr>
<td>• 3.226.24.234</td>
<td></td>
</tr>
<tr>
<td>• 34.200.29.95</td>
<td></td>
</tr>
<tr>
<td>• 52.200.219.150</td>
<td></td>
</tr>
<tr>
<td>PCoIP gateway servers public IP address ranges</td>
<td></td>
</tr>
<tr>
<td>• 3.217.228.0 - 3.217.231.255</td>
<td></td>
</tr>
<tr>
<td>• 3.235.112.0 - 3.235.119.255</td>
<td></td>
</tr>
<tr>
<td>• 52.23.61.0 - 52.23.62.255</td>
<td></td>
</tr>
<tr>
<td>WSP gateway servers IP address range</td>
<td></td>
</tr>
<tr>
<td>• 3.227.4.0/22</td>
<td></td>
</tr>
<tr>
<td>• 44.209.84.0/22</td>
<td></td>
</tr>
<tr>
<td>Management interface IP address ranges</td>
<td></td>
</tr>
<tr>
<td>• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16</td>
<td></td>
</tr>
<tr>
<td>• WSP: 10.0.0.0/8</td>
<td></td>
</tr>
</tbody>
</table>
### US West (Oregon)

#### Domains and IP Addresses to add to your allowlist

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</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://d2td7qidlhxj7.cloudfront.net/">https://d2td7qidlhxj7.cloudfront.net/</a></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>Domain: <a href="https://skylight-client-ds.us-west-2.amazonaws.com">https://skylight-client-ds.us-west-2.amazonaws.com</a></td>
</tr>
</tbody>
</table>
| Directory Settings                                  | Authentication from the client to the customer directory before login to the WorkSpace:  
  - https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID>  
  Connections from macOS clients:  
  - https://d32i4gd7pg4909.cloudfront.net/  
  Customer directory settings:  
  - https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID>  
  Login page graphics for customer directory level co-branding:  
  - https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID>  
  CSS file to style the login pages:  
  - https://d3s98kk2h6f4oh.cloudfront.net/  
  - https://dyqsoz7pkju4e.cloudfront.net/  
  JavaScript file for the login pages:  
  - US West (Oregon) — https://d18af7771co7ip.cloudfront.net/ |
<table>
<thead>
<tr>
<th><strong>Category</strong></th>
<th><strong>Details</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Forrester Log Service</td>
<td><a href="https://fls-na.amazon.com/">https://fls-na.amazon.com/</a></td>
</tr>
<tr>
<td>Health Check (DRP) Servers</td>
<td>Health check servers (p. 22)</td>
</tr>
<tr>
<td>Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)</td>
<td><a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
</tr>
<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>Session Broker (PCM)</td>
<td>Domains:&lt;br&gt;• <a href="https://skylight-cm.us-west-2.amazonaws.com">https://skylight-cm.us-west-2.amazonaws.com</a>&lt;br&gt;• <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>Web Access TURN Servers for PCoIP</td>
<td>Server:&lt;br&gt;• turn:<em>.</em>.us-west-2.rdn.amazonaws.com</td>
</tr>
<tr>
<td>Health check hostname</td>
<td>drp-pdx.amazonworkspaces.com</td>
</tr>
<tr>
<td>Health check IP addresses</td>
<td>• 34.217.248.177&lt;br&gt;• 52.34.160.80&lt;br&gt;• 54.68.150.54&lt;br&gt;• 54.185.4.125&lt;br&gt;• 54.188.171.18&lt;br&gt;• 54.244.158.140</td>
</tr>
<tr>
<td>PCoIP gateway servers public IP address ranges</td>
<td>• 35.80.88.0 - 35.80.95.255&lt;br&gt;• 44.234.54.0 - 44.234.55.255&lt;br&gt;• 54.244.46.0 - 54.244.47.255</td>
</tr>
<tr>
<td>WSP gateway servers IP address range</td>
<td>34.223.96.0/22</td>
</tr>
<tr>
<td>Management interface IP address ranges</td>
<td>• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16&lt;br&gt;• WSP: 10.0.0.0/8</td>
</tr>
</tbody>
</table>
## Asia Pacific (Mumbai)

### Domains and IP Addresses to add to your allowlist

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</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://d2td7dqiilhjx7.cloudfront.net/">https://d2td7dqiilhjx7.cloudfront.net/</a></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>Domain: <a href="https://skylight-client-ds.ap-south-1.amazonaws.com">https://skylight-client-ds.ap-south-1.amazonaws.com</a></td>
</tr>
<tr>
<td>Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)</td>
<td>Domain: <a href="https://ws-client-service.ap-south-1.amazonaws.com">https://ws-client-service.ap-south-1.amazonaws.com</a></td>
</tr>
</tbody>
</table>

### Directory Settings

- **Authentication from the client to the customer directory before login to the WorkSpace:**
  - https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID>

- **Connections from macOS clients:**
  - https://d32i4gd7pg4909.cloudfront.net/

- **Customer directory settings:**
  - https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID>

- **Login page graphics for customer directory level co-branding:**
  - https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID>

- **CSS file to style the login pages:**
  - https://d3s98kk2h6f4oh.cloudfront.net/
  - https://dyqsoz7pkju4e.cloudfront.net/

- **JavaScript file for the login pages:**
  - Asia Pacific (Mumbai) — https://d78hovzzqqtbs.cloudfront.net/
### Category | Details
--- | ---
Forrester Log Service | https://fls-na.amazon.com/
Health Check (DRP) Servers | Health check servers (p. 22)
Registration Dependency (for Web Access and Teradici PCoIP Zero Clients) | https://s3.amazonaws.com
User Login Pages | https://<directory id>.awsapps.com/ (where <directory id> is the customer’s domain)
WS Broker | Domain:
  - https://ws-broker-service.ap-south-1.amazonaws.com
WorkSpaces API Endpoints | Domain:
  - https://workspaces.ap-south-1.amazonaws.com
Session Broker (PCM) | Domain:
  - https://skylight-cm.ap-south-1.amazonaws.com
Web Access TURN Servers for PCoIP | Web Access isn't currently available in the Asia Pacific (Mumbai) Region
Health check hostname | drp-bom.amazonworkspaces.com
Health check IP addresses | • 13.127.57.82
  • 13.234.250.73
WSP gateway servers IP address range | 65.1.156.0/22
Management interface IP address ranges | • PCoIP/WSP: 192.168.0.0/16
  • WSP: 10.0.0.0/8

### Asia Pacific (Seoul)

### Domains and IP Addresses to add to your allowlist

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</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>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>
</tbody>
</table>
| Client Metrics (for 3.0+ WorkSpaces client applications) | Domain:
<table>
<thead>
<tr>
<th>Category</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)</strong></td>
<td><strong>Domain:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong><a href="https://ws-client-service.ap-northeast-2.amazonaws.com">https://ws-client-service.ap-northeast-2.amazonaws.com</a></strong></td>
</tr>
<tr>
<td><strong>Directory Settings</strong></td>
<td><strong>Authentication from the client to the customer directory before login to the WorkSpace:</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong><a href="https://d32i4gd7pg4909.cloudfront.net/prod/">https://d32i4gd7pg4909.cloudfront.net/prod/</a>&lt;region&gt;/&lt;directory ID&gt;</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Connections from macOS clients:</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong><a href="https://d32i4gd7pg4909.cloudfront.net/">https://d32i4gd7pg4909.cloudfront.net/</a></strong></td>
</tr>
<tr>
<td></td>
<td><strong>Customer directory settings:</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong><a href="https://d21ui22avrxoh6.cloudfront.net/prod/">https://d21ui22avrxoh6.cloudfront.net/prod/</a>&lt;region&gt;/&lt;directory ID&gt;</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Login page graphics for customer directory level co-branding:</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong><a href="https://d1cbg795sa4g1u.cloudfront.net/prod/">https://d1cbg795sa4g1u.cloudfront.net/prod/</a>&lt;region&gt;/&lt;directory ID&gt;</strong></td>
</tr>
<tr>
<td></td>
<td><strong>CSS file to style the login pages:</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong><a href="https://d3s98kk2h6f4oh.cloudfront.net/">https://d3s98kk2h6f4oh.cloudfront.net/</a></strong></td>
</tr>
<tr>
<td></td>
<td>• <strong><a href="https://dyqsoz7pkju4e.cloudfront.net/">https://dyqsoz7pkju4e.cloudfront.net/</a></strong></td>
</tr>
<tr>
<td></td>
<td><strong>JavaScript file for the login pages:</strong></td>
</tr>
<tr>
<td></td>
<td>• **Asia Pacific (Seoul) — <strong><a href="https://dtyv4uwoh7ynt.cloudfront.net/">https://dtyv4uwoh7ynt.cloudfront.net/</a></strong></td>
</tr>
<tr>
<td><strong>Forrester Log Service</strong></td>
<td><strong><a href="https://fls-na.amazon.com/">https://fls-na.amazon.com/</a></strong></td>
</tr>
<tr>
<td><strong>Health Check (DRP) Servers</strong></td>
<td><strong>Health check servers (p. 22)</strong></td>
</tr>
<tr>
<td><strong>Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)</strong></td>
<td><strong><a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></strong></td>
</tr>
<tr>
<td><strong>User Login Pages</strong></td>
<td><strong>https://&lt;directory id&gt;.awsapps.com/ (where &lt;directory id&gt; is the customer’s domain)</strong></td>
</tr>
<tr>
<td><strong>WS Broker</strong></td>
<td><strong>Domain:</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong><a href="https://ws-broker-service.ap-northeast-2.amazonaws.com">https://ws-broker-service.ap-northeast-2.amazonaws.com</a></strong></td>
</tr>
</tbody>
</table>
### WorkSpaces API Endpoints

**Domain:**
- https://workspaces.ap-northeast-2.amazonaws.com

### Session Broker (PCM)

**Domain:**
- https://skylight-cm.ap-northeast-2.amazonaws.com

### Web Access TURN Servers for PCoIP

**Server:**
- turn:*.ap-northeast-2.rdn.amazonaws.com

### Health check hostname

- drp-icn.amazonworkspaces.com

### Health check IP addresses

- 13.124.44.166
- 13.124.203.105
- 52.78.44.253
- 52.79.54.102

### PCoIP gateway servers public IP address ranges

- 3.34.37.0 - 3.34.37.255
- 3.34.38.0 - 3.34.39.255

### WSP gateway servers IP address range

- 3.35.160.0/22

### Management interface IP address ranges

- PCoIP/WSP: 198.19.0.0/16
- WSP: 10.0.0.0/8

### Asia Pacific (Singapore)

#### Domains and IP Addresses to add to your allowlist

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</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://d2td7dqidljx7.cloudfront.net/">https://d2td7dqidljx7.cloudfront.net/</a></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>Domain: <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>Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)</td>
<td>Domain: <a href="https://ws-client-service.ap-southeast-1.amazonaws.com">https://ws-client-service.ap-southeast-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>
<tr>
<td>Category</td>
<td>Details</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
</tr>
<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>• Asia Pacific (Singapore) — <a href="https://d3qzmd7y07pz0i.cloudfront.net/">https://d3qzmd7y07pz0i.cloudfront.net/</a></td>
</tr>
</tbody>
</table>

**Forrester Log Service**

https://fls-na.amazon.com/

**Health Check (DRP) Servers**

Health check servers (p. 22)

**Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)**

https://s3.amazonaws.com

**User Login Pages**

https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)

**WS Broker**

Domain:

• https://ws-broker-service.ap-southeast-1.amazonaws.com

**WorkSpaces API Endpoints**

Domain:

• https://workspaces.ap-southeast-1.amazonaws.com

**Session Broker (PCM)**

Domain:

• https://skylight-cm.ap-southeast-1.amazonaws.com
<table>
<thead>
<tr>
<th>Category</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Access TURN Servers for PCoIP</td>
<td>Server:</td>
</tr>
<tr>
<td></td>
<td>• turn:*-ap-southeast-1.rdn.amazonaws.com</td>
</tr>
<tr>
<td>Health check hostname</td>
<td>drp-sin.amazonworkspaces.com</td>
</tr>
<tr>
<td>Health check IP addresses</td>
<td>• 3.0.212.144</td>
</tr>
<tr>
<td></td>
<td>• 18.138.99.116</td>
</tr>
<tr>
<td></td>
<td>• 18.140.252.123</td>
</tr>
<tr>
<td></td>
<td>• 52.74.175.118</td>
</tr>
<tr>
<td>PCoIP gateway servers public IP address ranges</td>
<td>• 18.141.152.0 - 18.141.152.255</td>
</tr>
<tr>
<td></td>
<td>• 18.141.154.0 - 18.141.155.255</td>
</tr>
<tr>
<td></td>
<td>• 52.76.127.0 - 52.76.127.255</td>
</tr>
<tr>
<td>WSP gateway servers IP address range</td>
<td>13.212.132.0/22</td>
</tr>
<tr>
<td>Management interface IP address ranges</td>
<td>• PCoIP/WSP: 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>• WSP: 10.0.0.0/8</td>
</tr>
</tbody>
</table>

**Asia Pacific (Sydney)**

### Domains and IP Addresses to add to your allowlist

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</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://d2td7dqiilhjx7.cloudfront.net/">https://d2td7dqiilhjx7.cloudfront.net/</a></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>Domain: <a href="https://skylight-client-ds.ap-southeast-2.amazonaws.com">https://skylight-client-ds.ap-southeast-2.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>
<tr>
<td></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></td>
<td>Connections from macOS clients:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://d32i4gd7pg4909.cloudfront.net/">https://d32i4gd7pg4909.cloudfront.net/</a></td>
</tr>
<tr>
<td>Category</td>
<td>Details</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Customer directory settings:</td>
<td>• <a href="https://d2ui22avroxh6.cloudfront.net/prod/region/directory">https://d2ui22avroxh6.cloudfront.net/prod/region/directory</a> ID</td>
</tr>
<tr>
<td>Login page graphics for customer directory level co-branding:</td>
<td>• <a href="https://d1cb795sa4g1.cloudfront.net/prod/region/directory">https://d1cb795sa4g1.cloudfront.net/prod/region/directory</a> ID</td>
</tr>
<tr>
<td>CSS file to style the login pages:</td>
<td>• <a href="https://d3s9kk2h6f4.cloudfront.net/">https://d3s9kk2h6f4.cloudfront.net/</a></td>
</tr>
<tr>
<td>JavaScript file for the login pages:</td>
<td>• <a href="https://dyqsoz7pkju4.cloudfront.net/">https://dyqsoz7pkju4.cloudfront.net/</a></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>Health Check (DRP) Servers</td>
<td>Health check servers (p. 22)</td>
</tr>
<tr>
<td>Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)</td>
<td><a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
</tr>
<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>WS Broker</td>
<td>Domain:</td>
</tr>
<tr>
<td>WorkSpaces API Endpoints</td>
<td>Domain:</td>
</tr>
<tr>
<td>Session Broker (PCM)</td>
<td>Domain:</td>
</tr>
<tr>
<td>Web Access TURN Servers for PCoIP</td>
<td>Server:</td>
</tr>
<tr>
<td>Health check hostname</td>
<td>drp-syd.amazonworkspaces.com</td>
</tr>
<tr>
<td>Health check IP addresses</td>
<td>• 3.24.11.127</td>
</tr>
<tr>
<td></td>
<td>• 13.237.232.125</td>
</tr>
</tbody>
</table>
### IP address and port requirements by Region

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCoIP gateway servers public IP address ranges</td>
<td>- 3.25.43.0 - 3.25.43.255&lt;br&gt;- 3.25.44.0 - 3.25.45.255&lt;br&gt;- 54.153.254.0 - 54.153.254.255</td>
</tr>
<tr>
<td>WSP gateway servers IP address range</td>
<td>3.25.248.0/22</td>
</tr>
<tr>
<td>Management interface IP address ranges</td>
<td>• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, and 198.19.0.0/16&lt;br&gt;• WSP: 10.0.0.0/8</td>
</tr>
</tbody>
</table>

### Asia Pacific (Tokyo)

#### Domains and IP Addresses to add to your allowlist

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</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://d2td7dqd7hjx7.cloudfront.net/">https://d2td7dqd7hjx7.cloudfront.net/</a></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>Domain:&lt;br&gt;<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>Directory Settings</td>
<td>Authentication from the client to the customer directory before login to the WorkSpace:&lt;br&gt;- <a href="https://d32i4gd7pg4909.cloudfront.net/prod/">https://d32i4gd7pg4909.cloudfront.net/prod/</a>&lt;region&gt;/&lt;directory ID&gt;</td>
</tr>
<tr>
<td></td>
<td>Connections from macOS clients:&lt;br&gt;- <a href="https://d32i4gd7pg4909.cloudfront.net/">https://d32i4gd7pg4909.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>Customer directory settings:&lt;br&gt;- <a href="https://d21ui22avrxoh6.cloudfront.net/prod/">https://d21ui22avrxoh6.cloudfront.net/prod/</a>&lt;region&gt;/&lt;directory ID&gt;</td>
</tr>
<tr>
<td></td>
<td>Login page graphics for customer directory level co-branding:</td>
</tr>
<tr>
<td>Category</td>
<td>Details</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Category</td>
<td>Details</td>
</tr>
<tr>
<td>Details</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>Details</td>
<td>CSS file to style the login pages:</td>
</tr>
<tr>
<td>Details</td>
<td>• <a href="https://d3s98kk2h6f4oh.cloudfront.net/">https://d3s98kk2h6f4oh.cloudfront.net/</a></td>
</tr>
<tr>
<td>Details</td>
<td>• <a href="https://dyqso7pkju4e.cloudfront.net/">https://dyqso7pkju4e.cloudfront.net/</a></td>
</tr>
<tr>
<td>Details</td>
<td>JavaScript file for the login pages:</td>
</tr>
<tr>
<td>Details</td>
<td>• Asia Pacific (Tokyo) — <a href="https://d2c2t8mxjhhq5z1.cloudfront.net/">https://d2c2t8mxjhhq5z1.cloudfront.net/</a></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>Health Check (DRP) Servers</td>
<td>Health check servers (p. 22)</td>
</tr>
<tr>
<td>Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)</td>
<td><a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
</tr>
<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>WS Broker</td>
<td>Domain:</td>
</tr>
<tr>
<td>WorkSpaces API Endpoints</td>
<td>• <a href="https://workspaces.ap-northeast-1.amazonaws.com">https://workspaces.ap-northeast-1.amazonaws.com</a></td>
</tr>
<tr>
<td>Session Broker (PCM)</td>
<td>Domain:</td>
</tr>
<tr>
<td>Web Access TURN Servers for PCoIP</td>
<td>• turn:*.ap-northeast-1.rdn.amazonaws.com</td>
</tr>
<tr>
<td>Health check hostname</td>
<td>drp-nrt.amazonworkspaces.com</td>
</tr>
<tr>
<td>Health check IP addresses</td>
<td>• 18.178.102.247</td>
</tr>
<tr>
<td>PCoIP gateway servers public IP address ranges</td>
<td>• 54.64.174.128</td>
</tr>
<tr>
<td>PCoIP gateway servers public IP address ranges</td>
<td>• 18.180.178.0 - 18.180.180.255</td>
</tr>
<tr>
<td>PCoIP gateway servers public IP address ranges</td>
<td>• 18.180.181.255</td>
</tr>
<tr>
<td>PCoIP gateway servers public IP address ranges</td>
<td>• 54.250.251.0 - 54.250.251.255</td>
</tr>
<tr>
<td>WSP gateway servers IP address range</td>
<td>3.114.164.0/22</td>
</tr>
<tr>
<td>Management interface IP address ranges</td>
<td>• PCoIP/WSP: 198.19.0.0/16</td>
</tr>
<tr>
<td>Management interface IP address ranges</td>
<td>• WSP: 10.0.0.0/8</td>
</tr>
</tbody>
</table>
## Canada (Central)

### Domains and IP Addresses to add to your allowlist

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</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://d2td7dqi6ljx7.cloudfront.net/">https://d2td7dqi6ljx7.cloudfront.net/</a></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>Domain: <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>Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)</td>
<td>Domain: <a href="https://ws-client-service.ca-central-1.amazonaws.com">https://ws-client-service.ca-central-1.amazonaws.com</a></td>
</tr>
</tbody>
</table>
| Directory Settings | Authentication from the client to the customer directory before login to the WorkSpace:  
  - https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID>  
  Connections from macOS clients:  
  - https://d32i4gd7pg4909.cloudfront.net/  
  Customer directory settings:  
  - https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID>  
  Login page graphics for customer directory level co-branding:  
  - https://d1c7g795sa4g1u.cloudfront.net/prod/<region>/<directory ID>  
  CSS file to style the login pages:  
  - https://d3s98kk2h6f4oh.cloudfront.net/  
  - https://dyqsoz7pkju4e.cloudfront.net/  
  JavaScript file for the login pages:  
  - Canada (Central) — https://d2wfbsypmqjomg.cloudfront.net/ |
<table>
<thead>
<tr>
<th>Category</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forrester Log Service</td>
<td><a href="https://fls-na.amazon.com/">https://fls-na.amazon.com/</a></td>
</tr>
<tr>
<td>Health Check (DRP) Servers</td>
<td>Health check servers (p. 22)</td>
</tr>
<tr>
<td>Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)</td>
<td><a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
</tr>
<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>WS Broker</td>
<td>Domain:</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>WorkSpaces API Endpoints</td>
<td>Domain:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.ca-central-1.amazonaws.com">https://workspaces.ca-central-1.amazonaws.com</a></td>
</tr>
<tr>
<td>Session Broker (PCM)</td>
<td>Domain:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://skylight-cm.ca-central-1.amazonaws.com">https://skylight-cm.ca-central-1.amazonaws.com</a></td>
</tr>
<tr>
<td>Web Access TURN Servers for PCoIP</td>
<td>Server:</td>
</tr>
<tr>
<td></td>
<td>• turn:*-ca-central-1.rdn.amazonaws.com</td>
</tr>
<tr>
<td>Health check hostname</td>
<td>drp-yul.amazonworkspaces.com</td>
</tr>
<tr>
<td>Health check IP addresses</td>
<td>• 52.60.69.16</td>
</tr>
<tr>
<td></td>
<td>• 52.60.80.237</td>
</tr>
<tr>
<td></td>
<td>• 52.60.173.117</td>
</tr>
<tr>
<td></td>
<td>• 52.60.201.0</td>
</tr>
<tr>
<td>PCoIP gateway servers public IP address ranges</td>
<td>• 15.223.100.0 - 15.223.100.255</td>
</tr>
<tr>
<td></td>
<td>• 15.223.102.0 - 15.223.103.255</td>
</tr>
<tr>
<td></td>
<td>• 35.183.255.0 - 35.183.255.255</td>
</tr>
<tr>
<td>WSP gateway servers IP address range</td>
<td>3.97.20.0/22</td>
</tr>
<tr>
<td>Management interface IP address ranges</td>
<td>• PCoIP/WSP: 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>• WSP: 10.0.0.0/8</td>
</tr>
</tbody>
</table>

**Europe (Frankfurt)**

**Domains and IP Addresses to add to your allowlist**

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</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://d2td7dqiilhijx7.cloudfront.net/">https://d2td7dqiilhijx7.cloudfront.net/</a></td>
</tr>
<tr>
<td>Connectivity Check</td>
<td><a href="https://connectivity.amazonworkspaces.com/">https://connectivity.amazonworkspaces.com/</a></td>
</tr>
<tr>
<td>Category</td>
<td>Details</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</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>Domain:</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>Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)</td>
<td>Domain:</td>
</tr>
<tr>
<td></td>
<td><a href="https://ws-client-service.eu-central-1.amazonaws.com">https://ws-client-service.eu-central-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>
<tr>
<td></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></td>
<td>Connections from macOS clients:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://d32i4gd7pg4909.cloudfront.net/">https://d32i4gd7pg4909.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>Customer directory settings:</td>
</tr>
<tr>
<td></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></td>
<td>Login page graphics for customer directory level co-branding:</td>
</tr>
<tr>
<td></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></td>
<td>CSS file to style the login pages:</td>
</tr>
<tr>
<td></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></td>
<td>JavaScript file for the login pages:</td>
</tr>
<tr>
<td></td>
<td>• Europe (Frankfurt) — <a href="https://d1whcm49570jjw.cloudfront.net/">https://d1whcm49570jjw.cloudfront.net/</a></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>Health Check (DRP) Servers</td>
<td>Health check servers (p. 22)</td>
</tr>
<tr>
<td>Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)</td>
<td><a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
</tr>
<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>Category</td>
<td>Details</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>WS Broker</td>
<td>Domain:</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>WorkSpaces API Endpoints</td>
<td>Domain:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.eu-central-1.amazonaws.com">https://workspaces.eu-central-1.amazonaws.com</a></td>
</tr>
<tr>
<td>Session Broker (PCM)</td>
<td>Domain:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://skylight-cm.eu-central-1.amazonaws.com">https://skylight-cm.eu-central-1.amazonaws.com</a></td>
</tr>
<tr>
<td>Web Access TURN Servers for PCoIP</td>
<td>Server:</td>
</tr>
<tr>
<td></td>
<td>• turn:*-eu-central-1.rdn.amazonaws.com</td>
</tr>
<tr>
<td>Health check hostname</td>
<td>drp-fra.amazonawsworkspaces.com</td>
</tr>
<tr>
<td>Health check IP addresses</td>
<td>• 52.59.191.224</td>
</tr>
<tr>
<td></td>
<td>• 52.59.191.225</td>
</tr>
<tr>
<td></td>
<td>• 52.59.191.226</td>
</tr>
<tr>
<td></td>
<td>• 52.59.191.227</td>
</tr>
<tr>
<td>PCoIP gateway servers public IP address ranges</td>
<td>• 18.156.52.0 - 18.156.52.255</td>
</tr>
<tr>
<td></td>
<td>• 18.156.54.0 - 18.156.55.255</td>
</tr>
<tr>
<td></td>
<td>• 52.59.127.0 - 52.59.127.255</td>
</tr>
<tr>
<td>WSP gateway servers IP address range</td>
<td>18.192.216.0/22</td>
</tr>
<tr>
<td>Management interface IP address ranges</td>
<td>• PCoIP/WSP: 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>• WSP: 10.0.0.0/8</td>
</tr>
</tbody>
</table>

**Europe (Ireland)**

**Domains and IP Addresses to add to your allowlist**

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</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>Connectivity Check</td>
<td><a href="https://connectivity.amazonawsworkspaces.com/">https://connectivity.amazonawsworkspaces.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.amazonaws.com/">https://device-metrics-us-2.amazonaws.com/</a></td>
</tr>
<tr>
<td>Client Metrics (for 3.0+ WorkSpaces client applications)</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>Category</td>
<td>Details</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)</td>
<td>Domain:</td>
</tr>
<tr>
<td></td>
<td><a href="https://ws-client-service.eu-west-1.amazonaws.com">https://ws-client-service.eu-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>
<tr>
<td></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></td>
<td>Connections from macOS clients:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://d32i4gd7pg4909.cloudfront.net/">https://d32i4gd7pg4909.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>Customer directory settings:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://d21ui22avrxo6.cloudfront.net/prod/">https://d21ui22avrxo6.cloudfront.net/prod/</a>&lt;region&gt;/&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://d1cbg795sa4g1u.cloudfront.net/prod/">https://d1cbg795sa4g1u.cloudfront.net/prod/</a>&lt;region&gt;/&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://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></td>
<td>JavaScript file for the login pages:</td>
</tr>
<tr>
<td></td>
<td>• Europe (Ireland) — <a href="https://d3pgffbf39h4k4.cloudfront.net/">https://d3pgffbf39h4k4.cloudfront.net/</a></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>Health Check (DRP) Servers</td>
<td>Health check servers (p. 22)</td>
</tr>
<tr>
<td>Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)</td>
<td><a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
</tr>
<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>WS Broker</td>
<td>Domain:</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>WorkSpaces API Endpoints</td>
<td>Domain:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.eu-west-1.amazonaws.com">https://workspaces.eu-west-1.amazonaws.com</a></td>
</tr>
</tbody>
</table>
## IP address and port requirements by Region

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Broker (PCM)</td>
<td>Domain:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://skylight-cm.eu-west-1.amazonaws.com">https://skylight-cm.eu-west-1.amazonaws.com</a></td>
</tr>
<tr>
<td>Web Access TURN Servers for PCoIP</td>
<td>Server:</td>
</tr>
<tr>
<td></td>
<td>• turn:<em>.</em>.eu-west-1.rdn.amazonaws.com</td>
</tr>
<tr>
<td>Health check hostname</td>
<td>drp-dub.amazonaws.com</td>
</tr>
<tr>
<td>Health check IP addresses</td>
<td>• 18.200.177.86</td>
</tr>
<tr>
<td></td>
<td>• 52.48.86.38</td>
</tr>
<tr>
<td></td>
<td>• 54.76.137.224</td>
</tr>
<tr>
<td>PCoIP gateway servers public IP address ranges</td>
<td>• 3.249.28.0 - 3.249.29.255</td>
</tr>
<tr>
<td></td>
<td>• 52.19.124.0 - 52.19.125.255</td>
</tr>
<tr>
<td>WSP gateway servers IP address range</td>
<td>3.248.176.0/22</td>
</tr>
<tr>
<td>Management interface IP address ranges</td>
<td>• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>• WSP: 10.0.0.0/8</td>
</tr>
</tbody>
</table>

### Europe (London)

#### Domains and IP Addresses to add to your allowlist

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPTCHA</td>
<td><a href="https://opfaptcha-prod.s3.amazonaws.com/">https://opfaptcha-prod.s3.amazonaws.com/</a></td>
</tr>
<tr>
<td>Client Auto-update</td>
<td><a href="https://d2td7dqidhljx7.cloudfront.net/">https://d2td7dqidhljx7.cloudfront.net/</a></td>
</tr>
<tr>
<td>Connectivity Check</td>
<td><a href="https://connectivity.amazonaws.com/">https://connectivity.amazonaws.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.amazonaws.com/">https://device-metrics-us-2.amazonaws.com/</a></td>
</tr>
<tr>
<td>Client Metrics (for 3.0+ WorkSpaces client applications)</td>
<td>Domain: <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>Directory Settings</td>
<td>Authentication from the client to the customer directory before login to the WorkSpace:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://d32i4gd7pg4909.cloudfront.net/prod/">https://d32i4gd7pg4909.cloudfront.net/prod/</a>&lt;region&gt;/&lt;directory ID&gt;</td>
</tr>
</tbody>
</table>

Connections from macOS clients:
<table>
<thead>
<tr>
<th>Category</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer directory settings:</td>
<td><a href="https://d32i4gd7pg4909.cloudfront.net/">https://d32i4gd7pg4909.cloudfront.net/</a></td>
</tr>
<tr>
<td>Login page graphics for customer directory level co-branding:</td>
<td><a href="https://d21ui22avroxh6.cloudfront.net/prod/%5C">https://d21ui22avroxh6.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>JavaScript file for the login pages:</td>
<td><a href="https://dyqsoz7pkju4e.cloudfront.net/">https://dyqsoz7pkju4e.cloudfront.net/</a></td>
</tr>
<tr>
<td>Europe (London) —</td>
<td><a href="https://d16q6638mh01s7.cloudfront.net/">https://d16q6638mh01s7.cloudfront.net/</a></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>Health Check (DRP) Servers</td>
<td>Health check servers (p. 22)</td>
</tr>
<tr>
<td>Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)</td>
<td><a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
</tr>
<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>WS Broker</td>
<td>Domain:</td>
</tr>
<tr>
<td>WorkSpaces API Endpoints</td>
<td>Domain:</td>
</tr>
<tr>
<td>Session Broker (PCM)</td>
<td>Domain:</td>
</tr>
<tr>
<td>Web Access TURN Servers for PCoIP</td>
<td>Server:</td>
</tr>
<tr>
<td>Health check hostname</td>
<td>drp-lhr.amazonworkspaces.com</td>
</tr>
<tr>
<td>Category</td>
<td>Details</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Health check IP addresses</td>
<td>• 35.176.62.54</td>
</tr>
<tr>
<td></td>
<td>• 35.177.255.44</td>
</tr>
<tr>
<td></td>
<td>• 52.56.46.102</td>
</tr>
<tr>
<td></td>
<td>• 52.56.111.36</td>
</tr>
<tr>
<td>PCoIP gateway servers public IP address ranges</td>
<td>• 18.132.21.0 - 18.132.21.255</td>
</tr>
<tr>
<td></td>
<td>• 18.132.22.0 - 18.132.23.255</td>
</tr>
<tr>
<td></td>
<td>• 35.176.32.0 - 35.176.32.255</td>
</tr>
<tr>
<td>WSP gateway servers IP address range</td>
<td>18.134.68.0/22</td>
</tr>
<tr>
<td>Management interface IP address ranges</td>
<td>• 198.19.0.0/16</td>
</tr>
<tr>
<td></td>
<td>• WSP: 10.0.0.0/8</td>
</tr>
</tbody>
</table>

**South America (São Paulo)**

**Domains and IP Addresses to add to your allowlist**

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</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>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>Domain:</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>Dynamic Messaging Service (for 3.0+ WorkSpaces client applications)</td>
<td>Domain:</td>
</tr>
<tr>
<td></td>
<td><a href="https://ws-client-service.sa-east-1.amazonaws.com">https://ws-client-service.sa-east-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>
<tr>
<td></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></td>
<td>Connections from macOS clients:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://d32i4gd7pg4909.cloudfront.net/">https://d32i4gd7pg4909.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td>Customer directory settings:</td>
</tr>
<tr>
<td></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>Category</td>
<td>Details</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</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>• South America (São Paulo) — <a href="https://d2lh2qc5bdoq4b.cloudfront.net/">https://d2lh2qc5bdoq4b.cloudfront.net/</a></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>Health Check (DRP) Servers</td>
<td>Health check servers (p. 22)</td>
</tr>
<tr>
<td>Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)</td>
<td><a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
</tr>
<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>WS Broker</td>
<td>Domain:</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>WorkSpaces API Endpoints</td>
<td>Domain:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://workspaces.sa-east-1.amazonaws.com">https://workspaces.sa-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td>Session Broker (PCM)</td>
<td>Domain:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://skylight-cm.sa-east-1.amazonaws.com">https://skylight-cm.sa-east-1.amazonaws.com</a></td>
</tr>
<tr>
<td>Web Access TURN Servers for PCoIP</td>
<td>Server:</td>
</tr>
<tr>
<td></td>
<td>• turn:*.sa-east-1.rdn.amazonaws.com</td>
</tr>
<tr>
<td>Health check hostname</td>
<td>drp-gru.amazonworkspaces.com</td>
</tr>
<tr>
<td>Health check IP addresses</td>
<td>• 18.231.0.105</td>
</tr>
<tr>
<td></td>
<td>• 52.67.55.29</td>
</tr>
<tr>
<td></td>
<td>• 54.233.156.245</td>
</tr>
<tr>
<td></td>
<td>• 54.233.216.234</td>
</tr>
<tr>
<td>PCoIP gateway servers public IP address ranges</td>
<td>• 18.230.103.0 - 18.230.103.255</td>
</tr>
<tr>
<td></td>
<td>• 18.230.104.0 - 18.230.105.255</td>
</tr>
<tr>
<td></td>
<td>• 54.233.204.0 - 54.233.204.255</td>
</tr>
<tr>
<td>WSP gateway servers IP address range</td>
<td>15.228.64.0/22</td>
</tr>
</tbody>
</table>


## Amazon WorkSpaces Administration Guide

### IP address and port requirements by Region

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</th>
</tr>
</thead>
</table>
| Management interface IP address ranges | • 198.19.0.0/16  
• WSP: 10.0.0.0/8 |

### AWS GovCloud (US-West) Region

#### Domains and IP Addresses to add to your allowlist

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</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>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>
</tbody>
</table>
| Client Metrics (for 3.0+ WorkSpaces client applications) | Domain:  
https://skylight-client-ds.us-gov-west-1.amazonaws.com |
| Directory Settings | Authentication from the client to the customer directory before login to the WorkSpace:  
• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID>  
Connections from macOS clients:  
• https://d32i4gd7pg4909.cloudfront.net/  
Customer directory settings:  
• https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/<directory ID>  
Login page graphics for customer directory level co-branding:  
• https://s3.amazonaws.com/workspaces-client-assets/prod/pdt/<directory ID>  
CSS file to style the login pages:  
• https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css  
JavaScript file for the login pages: |
<table>
<thead>
<tr>
<th>Category</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<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>Health Check (DRP) Servers</td>
<td>Health check servers (p. 22)</td>
</tr>
<tr>
<td>Registration Dependency (for Web Access and Teradici PCoIP Zero Clients)</td>
<td><a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
</tr>
<tr>
<td>User Login Pages</td>
<td><a href="https://login.us-gov-home.awsapps.com/directory/">https://login.us-gov-home.awsapps.com/directory/</a>&lt;directory id&gt;/ (where &lt;directory id&gt; is the customer's domain)</td>
</tr>
<tr>
<td>WS Broker</td>
<td>Domain:</td>
</tr>
<tr>
<td>WorkSpaces API Endpoints</td>
<td>Domain:</td>
</tr>
<tr>
<td>Session Broker (PCM)</td>
<td>Domain:</td>
</tr>
<tr>
<td>Health check hostname</td>
<td>drp-pdt.amazonworkspaces.com</td>
</tr>
</tbody>
</table>
| Health check IP addresses | • 52.61.60.65  
• 52.61.65.14  
• 52.61.88.170  
• 52.61.137.87  
• 52.61.155.110  
• 52.222.20.88 |
| PCoIP gateway servers public IP address ranges | • 52.61.193.0 - 52.61.193.255 |
| WSP gateway servers IP address range | • 3.32.139.0/24  
• 3.30.129.0/24  
• 3.30.130.0/23 |
| Management interface IP address ranges | • 198.19.0.0/16  
• WSP: 10.0.0.0/8 |
Amazon WorkSpaces client network requirements

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

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

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

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

- The client device must have a broadband internet connection. We recommend planning for a minimum of 1 Mbps per simultaneous user watching a 480p video window. Depending on your user-quality requirements for video resolution, more bandwidth might be required.
- The network that the client device is connected to, and any firewall on the client device, must have certain ports open to the IP address ranges for various AWS services. For more information, see IP address and port requirements for WorkSpaces (p. 14).
- For the best performance for PCoIP, the round trip time (RTT) from the client's network to the Region that the WorkSpaces are in should be less than 100ms. If the RTT is between 100ms and 200ms, the user can access the WorkSpace, but performance is affected. If the RTT is between 200ms and 375ms, the performance is degraded. If the RTT exceeds 375ms, the WorkSpaces client connection is terminated.
- For the best performance for WorkSpaces Streaming Protocol (WSP), the RTT from the client's network to the Region that the WorkSpaces are in should be less than 250ms. If the RTT is between 250ms and 400ms, the user can access the WorkSpace, but the performance is degraded.
- To check the RTT to the various AWS Regions from your location, use the Amazon WorkSpaces Connection Health Check.
- To use webcams with WSP, we recommend a minimum upload bandwidth of 1.7 megabits per second.
- If users will access their WorkSpaces through a virtual private network (VPN), the connection must support a maximum transmission unit (MTU) of at least 1200 bytes.

**Note**
You cannot access WorkSpaces through a VPN connected to your virtual private cloud (VPC). To access WorkSpaces using a VPN, internet connectivity (through the VPN's public IP addresses) is required, as described in IP address and port requirements for WorkSpaces (p. 14).

- The clients require HTTPS access to WorkSpaces resources hosted by the service and Amazon Simple Storage Service (Amazon S3). The clients do not support proxy redirection at the application level. HTTPS access is required so that users can successfully complete registration and access their WorkSpaces.
- To allow access from PCoIP zero client devices, you must be using a PCoIP protocol bundle for WorkSpaces. You must also enable Network Time Protocol (NTP) in Teradici. For more information, see Set up PCoIP zero clients for WorkSpaces (p. 77).
- For 3.0+ clients, if you are using single sign-on (SSO) for Amazon WorkDocs, you must follow the instructions in Single Sign-On in the AWS Directory Service Administration Guide.

You can verify that a client device meets the networking requirements as follows.
To verify networking requirements for 3.0+ clients

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

<table>
<thead>
<tr>
<th>If you're using...</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows or Linux clients</td>
<td>In the upper-right corner of the client application, select the <strong>Network</strong> icon.</td>
</tr>
<tr>
<td>macOS client</td>
<td>Choose <strong>Connections, Network</strong>.</td>
</tr>
</tbody>
</table>

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

To verify networking requirements for 1.0+ and 2.0+ clients

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

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

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

Supported clients

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

**Important**
This feature is not supported by the following clients:

- WorkSpaces client applications for Linux or iPad
- WorkSpaces Web Access
Step 1: Create the certificates

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

Requirements

- Root certificates must be Base64-encoded certificate files in CRT, CERT, or PEM format.
- Root certificates must satisfy the following regular expression pattern, which means that every encoded line, beside the last one, has to be exactly 64 characters long:

```
BEGIN CERTIFICATE
(\[A-Za-z0-9/\+]{64}\s?\n)*\[A-Za-z0-9/\+]{1,64}=0,2\nEND CERTIFICATE
```

- Device certificates must include a Common Name.
- Device certificates must include the following extensions: Key Usage: Digital Signature, and Enhanced Key Usage: Client Authentication.
- All the certificates in the chain from the device certificate to the trusted root Certificate Authority must be installed on the client device.
- The maximum supported length of certificate chain is 4.
- WorkSpaces does not currently support device revocation mechanisms, such as certificate revocation lists (CRL) or Online Certificate Status Protocol (OCSP), for client certificates.
- Use a strong encryption algorithm. We recommend SHA256 with RSA, SHA256 with ECDSA, SHA384 with ECDSA, or SHA512 with ECDSA.
- For macOS, if the device certificate is in the system keychain, we recommend that you authorize the WorkSpaces client application to access those certificates. Otherwise, users must enter keychain credentials when they log in or reconnect.

Step 2: Deploy client certificates to the trusted devices

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

The WorkSpaces client applications search for certificates as follows:

- Android - On Android, searches the keychain for client certificates. On Android-compatible Chrome OS systems, searches the keychain for user certificates.
- macOS - Searches the keychain for client certificates.
- Windows - Searches the user and root certificate stores for client certificates.
Step 3: Configure the restriction

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

To configure the restriction

2. In the navigation pane, choose Directories.
3. Select the directory and then choose Actions, Update Details.
4. Expand Access Control Options.
5. Select the device type under For each device type, specify which devices can access WorkSpaces.
6. Import up to two root certificates. For each root certificate, do the following:
   a. Choose Import.
   b. Copy the body of the certificate to the form.
   c. Choose Import.
7. (Optional) Specify whether other types of devices have access to WorkSpaces.
   a. Scroll down to 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.
   b. Select the device types to enable and clear the device types to disable.
   c. To block access from all selected device types, choose Block.
8. Choose Update and Exit.

WorkSpaces Integration with SAML 2.0 (preview)

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

Authentication workflow

The following sections describe the authentication workflow between WorkSpaces and a SAML 2.0 identity provider (IdP):

- When the flow is initiated by the IdP. For example, when a user clicks on an application in the IdP user portal in a web browser.
- When the flow is initiated by the WorkSpaces client. For example, when a user opens the client and signs in.

In these examples, the user enters user@example.com to sign in to the IdP. The IdP has a SAML 2.0 service provider application configured for a WorkSpaces directory and the user is authorized for the WorkSpaces SAML 2.0 application. The user creates a WorkSpace for the user name, user, in a directory that's enabled for SAML 2.0 authentication. Additionally, the user installs the WorkSpaces client application on their device.
Identity provider (IdP)-initiated flow

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

1. Using their web browser, the user signs in to the IdP.
2. After signing in to the IdP, the user clicks the WorkSpaces application from the IdP user portal.
3. The user is redirected to this page in the browser, and the WorkSpaces client application is opened automatically.

4. The WorkSpaces client is now registered and the user can continue to sign by clicking Continue to sign in to WorkSpaces.

WorkSpaces client-initiated flow

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

1. The user launches the WorkSpaces client application (if it isn't already running) and clicks Continue to sign in to WorkSpaces.
2. The user is redirected to their default web browser to sign in to the IdP. If the user is already signed in to the IdP in their browser, they don't need to sign in again and will skip this step.
3. Once signed in to the IdP, the user is redirected to this page in the browser, and clicks Log in to WorkSpaces.
4. The user is redirected to the WorkSpaces client application to complete sign in to their WorkSpace. The WorkSpaces user name is populated automatically from the IdP SAML 2.0 assertion.

5. The user is signed in to their WorkSpace.

Setting up SAML 2.0 (preview)

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

Contents
- Requirements (preview) (p. 59)
- Prerequisites (p. 60)
- Step 1: Create a SAML identity provider in AWS IAM (p. 61)
- Step 2: Create a SAML 2.0 federation IAM role (p. 61)
- Step 3: Embed an inline policy for the IAM role (p. 62)
- Step 4: Configure your SAML 2.0 identity provider (p. 63)
- Step 5: Create assertions for the SAML authentication response (p. 63)
- Step 6: Configure the relay state of your federation (p. 64)
- Step 7: Enable integration with SAML 2.0 on your WorkSpaces directory (p. 65)

Requirements (preview)

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

During the SAML 2.0 authentication preview, SAML must be configured on a WorkSpaces directory using WorkSpaces API or the AWS CLI. The WorkSpaces management console can't be used to configure SAML properties.

• The user must be able to sign in to WorkSpaces by entering their AD user name without the domain, as username. Directory use cases that require user name formats such as corp\username, corp.example.com\username, or username@corp.example.com aren't supported. As a result, SAML 2.0 authentication isn't supported with WorkSpaces that are launched using AWS Managed Microsoft AD trusted domains.

• To use SAML 2.0 authentication with WorkSpaces, the IdP must support IdP-initiated deep linking for the relay state URL. Examples of IdPs include ADFS, Azure AD, Duo Single Sign-On, Okta, PingFederate, and PingOne. Consult your IdP documentation for more information.

• SAML 2.0 authentication will function with WorkSpaces launched using Simple AD, but this isn't recommended as Simple AD doesn't integrate with SAML 2.0 IdPs.

• SAML 2.0 authentication is supported on the following WorkSpaces clients. Open Amazon WorkSpaces Client Downloads to find the latest versions. Other client versions won't be able to connect to WorkSpaces enabled for SAML 2.0 authentication unless fallback is enabled. For more information, see Enable SAML 2.0 authentication on the WorkSpaces directory:
  • Windows client application version 5.1.0.3029 or later
  • macOS client version 5.x or later

Important
The FIPS 140-2 Validated Mode setting for WorkSpaces endpoint encryption doesn't apply to relay state endpoints that are used for the SAML 2.0 authentication preview. For more information, see FIPS endpoint encryption.

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

1. Configure your IdP to integrate user identities from the Microsoft Active Directory that is used with the WorkSpaces directory. For a user with a WorkSpace, the sAMAccountName and email attributes for the Active Directory user and the IdP user must match for the user to sign in to WorkSpaces using the IdP. For more information about integrating Active Directory with your IdP, consult your IdP documentation.

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

3. Create or register a directory for WorkSpaces by using the WorkSpaces management console. For more information, see Manage directories for WorkSpaces. SAML 2.0 authentication for WorkSpaces is supported for the following directory types:
   • AD Connector
4. Create a WorkSpace for a user who can sign in to the IdP using a supported directory type. You can create a WorkSpace using the WorkSpaces management console, AWS CLI, or WorkSpaces API. For more information, see Launch a virtual desktop using WorkSpaces.

**Step 1: Create a SAML identity provider in AWS IAM**

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

**Step 2: Create a SAML 2.0 federation IAM role**

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

To create an IAM role for SAML IdP

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Roles > Create role.
3. For Role type, choose SAML 2.0 federation.
4. For SAML Provider select the SAML IdP that you created.
   
   **Important**
   
   Don't choose either of the two SAML 2.0 access methods, Allow programmatic access only or Allow programmatic and Amazon Web Services Management Console access.
   
5. For Attribute, choose SAML:sub_type.
6. For Value enter persistent. This value restricts role access to SAML user streaming requests that include a SAML subject type assertion with a value of persistent. If the SAML:sub_type is persistent, your IdP sends the same unique value for the NameID element in all SAML requests from a particular user. For more information about the SAML:sub_type assertion, see the Uniquely identifying users in SAML-based federation section in Using SAML-based federation for API access to AWS.
7. Review your SAML 2.0 trust information, confirming the correct trusted entity and condition, and then choose Next: Permissions.
8. On the Attach permissions policies page, choose Next: Tags.
9. (Optional) Enter a key and value for each tag that you want to add. For more information, see Tagging IAM users and roles.
10. When you're done, choose Next: Review. You'll create and embed an inline policy for this role later.
11. For Role name, enter a name that identifies the purpose of this role. Because multiple entities might reference the role, you can't edit the role's name once it is created.
12. (Optional) For Role description, enter a description for the new role.
13. Review the role details and choose Create role.
14. Add the sts:TagSession permission to your new IAM role's trust policy. For more information, see Attribute-based application entitlements using a third-party SAML 2.0 identity provider and Passing session tags in AWS STS. In your new IAM role's details, choose the Trust relationships tab, and then choose Edit trust relationship*. When Edit Trust Relationship policy editor opens, add the sts:TagSession* permission, as follows:

```json
{
   "Version": "2012-10-17",
   "Statement": [
   
   ```
"Effect": "Allow",
"Principal": {
"Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/IDENTITY-PROVIDER"
},
"Action": [
"sts:AssumeRoleWithSAML",
"sts:TagSession"
],
"Condition": {
"StringEquals": {
"SAML:sub_type": "persistent"
}
}
]
}
]

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

Step 3: Embed an inline policy for the IAM role

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

1. In the details for the IAM role that you created, choose the Permissions tab, and then choose Add inline policy. The Create policy wizard will start.
2. In Create policy, choose the JSON tab.
3. Copy and paste the following JSON policy into the JSON window. Then, modify the resource by entering your AWS Region Code, account ID, and directory ID. In the following policy, "Action": "workspaces:Stream" is the action that provides your WorkSpaces users with permissions to connect to their desktop sessions in the WorkSpaces directory.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "workspaces:Stream",
      "Condition": {
        "StringEquals": {
          "workspaces:userId": "${saml:sub}"
        }
      }
    }
  ]
}
```

Replace REGION-CODE with the AWS Region where your WorkSpaces directory exists. Replace DIRECTORY-ID with the WorkSpaces directory ID, which can be found in the WorkSpaces management console.
4. When you're done, choose Review policy. The Policy Validator will report any syntax errors.
Step 4: Configure your SAML 2.0 identity provider

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

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

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

Step 5: Create assertions for the SAML authentication response

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

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

- **SAML Subject NameID** – The unique identifier for the user who is signing in. The value must match the WorkSpaces user name, and is typically the sAMAccountName attribute for the Active Directory user.
- **SAML Subject Type** (with a value set to persistent) – Setting the value to persistent ensures that your IdP sends the same unique value for the NameID element in all SAML requests from a particular user. Make sure that your IAM policy includes a condition to only allow SAML requests with a SAML sub_type set to persistent, as described in Step 2: Create a SAML 2.0 federation IAM role.
- **Attribute element with the Name attribute set to https://aws.amazon.com/SAML/Attributes/Role** – This element contains one or more AttributeValue elements that list the IAM role and SAML Idp to which the user is mapped by your IdP. The role and Idp are specified as a comma-delimited pair of ARNs.
- **Attribute element with the Name attribute set to https://aws.amazon.com/SAML/Attributes/RoleSessionName** – This element contains one AttributeValue element that provides an identifier for the AWS temporary credentials that are issued for SSO. The value in the AttributeValue element must be between 2 and 64 characters long, can contain only alphanumeric characters, underscores, and the following characters: ., +, =, @, -. It can’t contain spaces. The value is typically an email address or a user principal name (UPN). It shouldn’t be a value that includes a space, such as a user’s display name.
- **Attribute element with the Name attribute set to https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email** – This element contains one AttributeValue element that provides the email address of the user. The value must match the WorkSpaces user email address as defined in the WorkSpaces directory. Tag values may include combinations of letters, numbers, spaces, and _/:,.+,=,@, - characters. For more information, see Rules for tagging in IAM and AWS STS in the IAM User Guide.
- **Attribute element with the Name attribute set to https://aws.amazon.com/SAML/Attributes/SessionDuration (optional)** – This element contains one AttributeValue element that specifies the maximum amount of time that a federated streaming session for a user can remain active before reauthentication is required. The default value is 60 minutes. For more information, see the SAML SessionDurationAttribute.
Note
Although SessionDuration is an optional attribute, we recommend that you include it in the SAML response. If you don't specify this attribute, the session duration is set to a default value of 60 minutes. WorkSpaces desktop sessions are disconnected after their session duration expires.

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

Step 6: Configure the relay state of your federation

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

The following is the relay state URL format:

```
```

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

Optionally, if you are using cross-region redirection for WorkSpaces, you can substitute the registration code with the fully qualified domain name (FQDN) associated with directories in your primary and failover Regions. For more information, see Cross-region redirection for Amazon WorkSpaces. When using cross-region redirection and SAML 2.0 authentication, both primary and failover directories need to be enabled for SAML 2.0 authentication and independently configured with the IdP, using the relay state endpoint associated with each Region. This will allow the FQDN to be configured correctly when users register their WorkSpaces client applications before signing in, and will allow users to authenticate during a failover event.

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

<table>
<thead>
<tr>
<th>Region</th>
<th>Relay state endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia) Region</td>
<td>workspaces.euc-sso.us-east-1.aws.amazon.com</td>
</tr>
<tr>
<td>US West (Oregon) Region</td>
<td>workspaces.euc-sso.us-west-2.aws.amazon.com</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai) Region</td>
<td>workspaces.euc-sso.ap-south-1.aws.amazon.com</td>
</tr>
<tr>
<td>Asia Pacific (Seoul) Region</td>
<td>workspaces.euc-sso.ap-northeast-2.aws.amazon.com</td>
</tr>
<tr>
<td>Asia Pacific (Singapore) Region</td>
<td>workspaces.euc-sso.ap-southeast-1.aws.amazon.com</td>
</tr>
<tr>
<td>Asia Pacific (Sydney) Region</td>
<td>workspaces.euc-sso.ap-southeast-2.aws.amazon.com</td>
</tr>
</tbody>
</table>
### Setting up SAML 2.0 (preview)

<table>
<thead>
<tr>
<th>Region</th>
<th>Relay state endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Tokyo) Region</td>
<td>workspaces.euc-sso.ap-northeast-1.aws.amazon.com</td>
</tr>
<tr>
<td>Canada (Central) Region</td>
<td>workspaces.euc-sso.ca-central-1.aws.amazon.com</td>
</tr>
<tr>
<td>Europe (Frankfurt) Region</td>
<td>workspaces.euc-sso.eu-central-1.aws.amazon.com</td>
</tr>
<tr>
<td>Europe (Ireland) Region</td>
<td>workspaces.euc-sso.eu-west-1.aws.amazon.com</td>
</tr>
<tr>
<td>Europe (London) Region</td>
<td>workspaces.euc-sso.eu-west-2.aws.amazon.com</td>
</tr>
</tbody>
</table>

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

Finally, enable SAML 2.0 authentication on the WorkSpaces directory by performing the following steps. Once this step is completed, you can use the IdP-initiated and client application-initiated flows to register WorkSpaces client applications and sign in to WorkSpaces.

**Note**  
During the SAML 2.0 authentication preview, SAML must be enabled on the WorkSpaces directory using the AWS CLI or WorkSpaces API. For more information, see the [AWS CLI command reference for WorkSpaces](https://docs.aws.amazon.com/workspaces/latest/adg/rpc-reference-create-directory.html), and the [Amazon WorkSpaces API reference](https://docs.aws.amazon.com/workspaces/latest/adg/API_CreateDirectory.html). The following examples reference the AWS CLI.

1. Construct the following "saml.json" file:

```json
{
  "ResourceId": "DIRECTORY-ID",
  "SamlProperties": {
    "Status": "DISABLED | ENABLED | ENABLED_WITH_DIRECTORY_LOGIN_FALLBACK",
    "UserAccessUrl": "USER-ACCESS-URL",
    "RelayStateParameterName": "RELAY-STATE-PARAMETER-NAME"
  }
}
```

Replace `DIRECTORY-ID` with the WorkSpaces directory ID, which can be found in the WorkSpaces management console.

For `Status`, select one of the following valid options: `DISABLED`, `ENABLED`, or `ENABLED_WITH_DIRECTORY_LOGIN_FALLBACK`.

- **DISABLED** is the default status for WorkSpaces directories and doesn't enable SAML 2.0 authentication.
- **ENABLED** status enables SAML 2.0 authentication. Users attempting to connect to WorkSpaces from a client application that doesn't support SAML 2.0 authentication will not be able to connect.
- **ENABLED_WITH_DIRECTORY_LOGIN_FALLBACK** status enables SAML 2.0 authentication with supported client applications, but doesn't prevent clients that don't support SAML 2.0 authentication from connecting as if SAML 2.0 authentication was disabled.

For the `UserAccessUrl` and `RelayStateParameterName`, replace `USER-ACCESS-URL` and `RELAY-STATE-PARAMETER-NAME` with values that are applicable to your IdP and the application you have configured in Step 1. The default value for `RelayStateParameterName` is "RelayState" if you omit...
this parameter. The following table lists user access URL and relay state parameter names that are unique to various identity providers for applications. Use this table to determine the correct values. Typically, the user access URL is the URL a user would navigate to in their web browser in order to federate and directly access the application, without any SAML 2.0 service provider (SP) bindings.

### Domains and IP addresses to add to your allow list

<table>
<thead>
<tr>
<th>Identity provider</th>
<th>Parameter</th>
<th>User access URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure AD</td>
<td>RelayState</td>
<td><a href="https://myapps.microsoft.com/signin/">https://myapps.microsoft.com/signin/</a>&lt;app_name&gt;/app/&lt;app_id&gt;?tenantId=&lt;tenant_id&gt;</td>
</tr>
<tr>
<td>Okta</td>
<td>RelayState</td>
<td>https://&lt;sub_domain&gt;.okta.com/app/&lt;app_name&gt;/&lt;app_id&gt;/sso/saml</td>
</tr>
<tr>
<td>OneLogin</td>
<td>RelayState</td>
<td>https://&lt;sub-domain&gt;.onelogin.com/trust/saml2/http-post/sso/&lt;app-id&gt;</td>
</tr>
<tr>
<td>PingFederate</td>
<td>TargetResource</td>
<td>https://&lt;host&gt;/idp/startSSO.ping?PartnerSpId=&lt;sp_id&gt;</td>
</tr>
<tr>
<td>PingOne</td>
<td>TargetResource</td>
<td><a href="https://sso.connect.pingidentity.com/sso/sp/initssos&amp;saasid=">https://sso.connect.pingidentity.com/sso/sp/initssos&amp;saasid=</a>&lt;app_id&gt;&amp;idpid=&lt;idp_id&gt;</td>
</tr>
</tbody>
</table>

2. Adjust the "saml.json" path as needed and run the following command to modify your WorkSpaces directory to enable SAML authentication:

```bash
aws workspaces modify-saml-properties --region REGION-CODE --cli-input-json file:///saml.json
```

Replace REGION-CODE with the AWS Region where your WorkSpaces directory exists.

### Use smart cards for authentication

Windows and Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) bundles allow the use of Common Access Card (CAC) and Personal Identity Verification (PIV) smart cards for authentication.
Amazon WorkSpaces supports the use of smart cards for both pre-session authentication and in-session authentication. Pre-session authentication refers to smart card authentication that’s performed while users are logging in to their WorkSpaces. In-session authentication refers to authentication that’s performed after logging in.

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

Contents
- Requirements (p. 67)
- Limitations (p. 67)
- Directory configuration (p. 68)
- Enable smart cards for Windows WorkSpaces (p. 68)
- Enable smart cards for Linux WorkSpaces (p. 70)

Requirements
- An Active Directory Connector (AD Connector) directory is required for pre-session authentication. AD Connector uses certificate-based mutual Transport Layer Security (mutual TLS) authentication to authenticate users to Active Directory using a hardware or software-based smart card certificate. For more information about how to configure your AD Connector and your on-premises directory, see Directory configuration (p. 68).
- To use a smart card with a Windows or Linux WorkSpace, the user must use the Amazon WorkSpaces Windows client version 3.1.1 or later or the WorkSpaces macOS client version 3.1.5 or later. For more information about using smart cards with the Windows and macOS clients, see Smart Card Support in the Amazon WorkSpaces User Guide.
- The root CA and smart card certificates must meet certain requirements. For more information, see Enable mTLS authentication in AD Connector for use with smart cards in the AWS Directory Service Administration Guide and Certificate Requirements in the Microsoft documentation.

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

Limitations
- Only the WorkSpaces Windows client application version 3.1.1 or later and the macOS client application version 3.1.5 or later are currently supported for smart card authentication.
- The WorkSpaces Windows client application 3.1.1 or later supports smart cards only when the client is running on a 64-bit version of Windows.
- Only AD Connector directories are currently supported for smart card authentication.
- In-session authentication is available in all Regions where WSP is supported. Pre-session authentication is available in the following Regions:
  - Asia Pacific (Sydney) Region
• Asia Pacific (Tokyo) Region
• Europe (Ireland) Region
• AWS GovCloud (US-West) Region
• US East (N. Virginia) Region
• US West (Oregon) Region

For in-session authentication and pre-session authentication on Linux or Windows WorkSpaces, only one smart card is currently allowed at a time.

For pre-session authentication, enabling both smart card authentication and username and password authentication on the same directory is not currently supported.

Only CAC and PIV cards are supported at this time. Other types of hardware or software-based smart cards might also work, but they haven't been fully tested for use with WSP.

Using a smart card to unlock the screen during a Windows or Linux WorkSpace session currently isn't supported. To work around this issue for Windows WorkSpaces, see To detect the Windows lock screen and disconnect the session (p. 68). To work around this issue for Linux WorkSpaces, see To disable the lock screen on Linux WorkSpaces (p. 71).

Directory configuration

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

AD Connector directory configuration

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

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

On-premises directory configuration

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

Enable smart cards for Windows WorkSpaces

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

To detect the Windows lock screen and disconnect the session

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

You can enable disconnecting the session when the Windows lock screen is detected by using Group Policy settings. For more information, see Enable or disable disconnect session on screen lock for WSP (p. 141).
To enable in-session or pre-session authentication

By default, Windows WorkSpaces are not enabled to support the use of smart cards for pre-session or in-session authentication. If needed, you can enable in-session and pre-session authentication for Windows WorkSpaces by using Group Policy settings. For more information, see Enable or disable smart card redirection for WSP (p. 140).

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

To enable users to use smart cards in a browser

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

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

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

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

Tip

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

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

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

1. If Firefox is already running, close it.
2. Open Firefox. Choose the menu button ☰ in the upper-right corner, and then choose Options.
5. In the Device Manager dialog box, you should see OpenSC smartcard framework (0.21) in the left navigation, and it should have the following values when you select it:

   Module: OpenSC smartcard framework (0.21)
   Path: C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll

Troubleshooting

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

Some common issues that can cause problems:
Incorrect mapping of the slots to the certificates.

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

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

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

### Enable smart cards for Linux WorkSpaces

**Note**

Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) bundles are available only in the AWS GovCloud (US-West) Region at this time.

Linux WorkSpaces on WSP currently have the following limitations:

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

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

**To obtain your root CA certificate**

You can obtain your root CA certificate in several ways:

- You can use a root CA certificate operated by a third-party certification authority.
- You can export your own root CA certificate by using the Web Enrollment site, which is either http://ip_address/certsrv or http://fqdn/certsrv, where ip_address and fqdn are the IP address and the fully qualified domain name (FQDN) of the root certification CA server. For more information about using the Web Enrollment site, see How to export a Root Certification Authority Certificate in the Microsoft documentation.
- You can use the following procedure to export the root CA certificate from a root CA certification server that is running Active Directory Certificate Services (AD CS). For information about installing AD CS, see Install the Certification Authority in the Microsoft documentation.
  1. Log into the root CA server using an administrator account.
  2. From the Windows Start menu, open a command prompt window (Start > Windows System > Command Prompt).
  3. Use the following command to export the root CA certificate to a new file, where rootca.cer is the name of the new file:

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

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

\texttt{openssl x509 -inform der -in rootca.cer -out /tmp/rootca.pem}

To add your root CA certificate to your Linux WorkSpaces

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

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

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

1. Create a new Linux WorkSpace with the WSP protocol enabled. When launching the WorkSpace in the Amazon WorkSpaces console, on the Select Bundles page, be sure to select WSP for the protocol, and then select one of the Amazon Linux 2 public bundles.

2. On the new WorkSpace, run the following command as root, where \texttt{pem-path} is the path to the root CA certificate file in PEM format.

\texttt{/usr/lib/skylight/enable_smartcard --ca-cert pem-path}

**Note**

Linux WorkSpaces assume that the certificates on the smart cards are issued for the user's default user principal name (UPN), such as \texttt{sAMAccountName@domain}, where \texttt{domain} is a fully qualified domain name (FQDN).

To use alternate UPN suffixes, run \texttt{/usr/lib/skylight/enable_smartcard --help} for more information. The mapping for alternate UPN suffixes is unique to each user. Therefore, that mapping must be performed individually on each user's WorkSpace.

3. (Optional) By default, all services are enabled to use smart card authentication on Linux WorkSpaces. To limit smart card authentication to only specific services, you must edit \texttt{/etc/pam.d/system-auth}. Uncomment the \texttt{auth} line for \texttt{pam_succeed_if.so} and edit the list of services as needed.

   After the auth line is uncommented, to allow a service to use smart card authentication, you must add it to the list. To make a service use only password authentication, you must remove it from the list.

4. (Optional) Using a smart card to unlock the screen isn't currently supported. To disable the lock screen on Linux WorkSpaces, create a file named \texttt{/usr/share/glib-2.0/schemas/10_screensaver.gschema.override} with the following contents:

   \[
   \begin{array}{l}
   \text{[org.mate.screensaver]} \\
   \text{lock-enabled=false}
   \end{array}
   \]

   After creating this file, run this command:

   \texttt{sudo glib-compile-schemas /usr/share/glib-2.0/schemas/}

5. Perform any additional customizations to the WorkSpace. For example, you might want to add a system-wide policy to enable users to use smart cards in Firefox (p. 72). (Chrome users must
Enable smart cards for Linux WorkSpaces

6. Create a custom WorkSpace image and bundle (p. 181) from the WorkSpace.
7. Use the new custom bundle to launch WorkSpaces for your users.

To enable users to use smart cards in Firefox

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

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

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

Troubleshooting

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

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

Some common issues that can cause problems:

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

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

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

- opensc-explorer
- opensc-tool
Enable smart cards for Linux WorkSpaces

• pkcs11_inspect
• pkcs11_listcerts
• pkcs15-tool

To enable debug logging

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

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

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

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

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

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

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

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

**Note**

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

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

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

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

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

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

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

Provide internet access 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 automatically or manually assign public IP addresses to your WorkSpaces.

For more information about these options, see the corresponding sections in Configure a VPC for WorkSpaces (p. 10).

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": "AmazonLinux2AMIRepositoryAccess",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amazonlinux.*.amazonaws.com/*"
      ]
    }
  ]
}
```
Security groups for your WorkSpaces

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

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

You can add a default WorkSpaces security group to a directory. After you associate a new security group with a WorkSpaces directory, new WorkSpaces that you launch or existing WorkSpaces that you rebuild will have the new security group. You can also add this new default security group to existing WorkSpaces without rebuilding them (p. 75), as explained later in this topic.

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

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

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

2. In the navigation pane, choose **Directories**.
3. Select the directory and choose **Actions, Update Details**.
4. Expand **Security Group** and select a security group.
5. Choose **Update and Exit**.

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

**To add a security group to an existing WorkSpace**

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

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

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

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

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

Note

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

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

Create an IP access control group

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

To create an IP access control group

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**

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**

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**

2. In the navigation pane, choose **Directories**.
3. For each directory that is associated with the IP access control group, select the directory and choose **Actions, Update Details**. Expand **IP Access Control Groups**, clear the check box for the IP access control group, and choose **Update and Exit**.
4. In the navigation pane, choose **IP Access Controls**.
5. Select the group and choose **Actions, Delete IP Group**.

**Set up PCoIP zero clients for WorkSpaces**

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

If your zero client device has firmware version 6.0.0 or later, your users can connect to their WorkSpaces directly. When your users are connecting directly to their WorkSpaces using a zero client device, we recommend using multi-factor authentication (MFA) with your WorkSpaces directory. For more information about using MFA with your directory, see the following documentation:
• **AWS Managed Microsoft AD** — Enable multi-factor authentication for AWS Managed Microsoft AD in the *AWS Directory Service Administration Guide*

• **AD Connector** — Enable multi-factor authentication for AD Connector in the *AWS Directory Service Administration Guide* and *Multi-factor authentication (AD Connector)* (p. 94)

• **Trusted domains** — Enable multi-factor authentication for AWS Managed Microsoft AD in the *AWS Directory Service Administration Guide*

• **Simple AD** — Multi-factor authentication is not available for Simple AD.

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

**Important**

- In the Teradici PCoIP Administrative Web Interface (AWI) or the Teradici PCoIP Management Console (MC), make sure you enable Network Time Protocol (NTP). For the NTP host DNS name, use pool.ntp.org, and set the NTP host port to 123. If NTP isn’t enabled, your PCoIP zero client users might receive certificate failure errors, such as “The supplied certificate is invalid due to timestamp.”

- Starting with version 20.10.4 of the PCoIP agent, Amazon WorkSpaces disables USB redirection by default through the Windows registry. This registry setting affects the behavior of USB peripherals when your users are using PCoIP zero client devices to connect to their WorkSpaces. For more information, see *USB printers and other USB peripherals aren’t working for PCoIP zero clients* (p. 260).

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

### Set up Android for Chromebooks

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

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

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

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

### Enable and configure Amazon WorkSpaces Web Access

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

- Web Access is currently unavailable in the Asia Pacific (Mumbai) Region.
- Web Access is not available for some Windows 10 WorkSpaces that are using the PCoIP protocol. If your PCoIP WorkSpace is powered by Windows Server 2019, Web Access is not available.
- A web browser cannot be used to connect to Amazon Linux WorkSpaces.

Important

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

Step 1: Enable Web Access to your WorkSpaces

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

To enable Web Access to your WorkSpaces

2. In the navigation pane, choose Directories.
3. Choose the appropriate directory, and then choose Actions, Update Details.
4. Expand Access Control Options and find the Other Platforms section.
6. Choose Update and Exit.

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

Amazon WorkSpaces Web Access requires inbound and outbound access for certain ports. For more information, see Ports for Web Access (p. 15).

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

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

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

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

For information about using the Active Directory administration tools to work with GPOs, see Installing the Active Directory Administration Tools in the AWS Directory Service Administration Guide.
To enable the WorkSpaces logon agent to switch users

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

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

1. Open the Group Policy Management tool (gpmc.msc) and navigate to and select a GPO at the domain or domain controller level of the directory that you use for your WorkSpaces. (If you have the WorkSpaces Group Policy administrative template (p. 127) installed in your domain, you can use the WorkSpaces GPO for your WorkSpaces machine accounts.)

2. Choose Action, Edit in the main menu.


4. Open the Hide entry points for Fast User Switching setting.

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

To hide the last logged on user name

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

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

1. Open the Group Policy Management tool (gpmc.msc) and navigate to and select a GPO at the domain or domain controller level of the directory that you use for your WorkSpaces. (If you have the WorkSpaces Group Policy administrative template (p. 127) installed in your domain, you can use the WorkSpaces GPO for your WorkSpaces machine accounts.)

2. Choose Action, Edit in the main menu.


4. Open one of the following settings:
   - For Windows 7 — Interactive logon: Don't display last signed-in
   - For Windows 10 — Interactive logon: Do not display last user name

5. In the Properties dialog box for the setting, choose Enabled, and then choose OK.

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

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

1. Open the Group Policy Management tool (gpmc.msc) and navigate to and select a GPO at the domain or domain controller level of the directory that you use for your WorkSpaces. (If you have the WorkSpaces Group Policy administrative template (p. 127) installed in your domain, you can use the WorkSpaces GPO for your WorkSpaces machine accounts.)

2. Choose Action, Edit in the main menu.
3. In the Group Policy Management Editor, choose **Computer Configuration, Windows Settings, Security Settings, Local Policies, and Security Options**.

4. Open the **Interactive logon: Do not require CTRL+ALT+DEL** setting.

5. On the **Local Security Setting** tab, choose **Disabled**, and then choose **OK**.

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

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

1. Open the Group Policy Management tool (**gpmc.msc**) and navigate to and select a GPO at the domain or domain controller level of the directory that you use for your WorkSpaces. (If you have the WorkSpaces Group Policy administrative template (p. 127) installed in your domain, you can use the WorkSpaces GPO for your WorkSpaces machine accounts.)

2. Choose **Action, Edit** in the main menu.

3. In the Group Policy Management Editor, choose **Computer Configuration, Windows Settings, Security Settings, Local Policies, and Security Options**.

4. Open the **Interactive logon: Display user information when the session is locked** setting.

5. On the **Local Security Setting** tab, choose **User display name, domain and user names**, and then choose **OK**.

**To apply the Group Policy and Security Policy settings changes**

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

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

---

**Set up Amazon WorkSpaces for FedRAMP authorization or DoD SRG compliance**

To comply with the [Federal Risk and Authorization Management Program (FedRAMP)](https://fedramp.gov) or the [Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG)](https://www.gsa.gov/cloud-computing-security-requirements-guide), 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 eachRegion, see [AWS Services in Scope by Compliance Program](https://aws.amazon.com/about-aws/compliance/).**Note**

In addition to using FIPS endpoint encryption, you can also encrypt your WorkSpaces. For more information, see [Encrypted WorkSpaces](p. 160).

**Requirements**

- You must create your WorkSpaces in a [US AWS Region that has FedRAMP authorization or is DoD SRG-compliant](https://aws.amazon.com/regions/global/).
Enable SSH connections

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. For more information, see the section called “Security groups” (p. 75).

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

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**, specify the CIDR range of the public IP addresses for the computers that users will use to connect to their WorkSpaces. For example, a corporate network or a home network.
   - For **Description** (optional), type a description for the rule.
7. Choose Create.

**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 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 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.

   ```bash
   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

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

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

**To connect to an Amazon Linux WorkSpace using PuTTY**

1. Open PuTTY.
2. In the PuTTY Configuration dialog box, do the following:
• For **Host Name (or IP address)**, enter the following command. Replace the values with the NetBIOS name of the Active Directory domain that you are connected to, the user name that you use to connect to the WorkSpace, and the IP address of the WorkSpace that you want to connect to.

```
\NetBIOS_NAME\Username@WorkSpaceIP
```

• For **Port**, enter 22.

• For **Connection type**, choose **SSH**.

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

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

**Required configuration and service components for WorkSpaces**

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

- the section called “Routing table configuration” (p. 86)
- the section called “Components for Windows” (p. 86)
- the section called “Components for Linux” (p. 87)

**Required routing table configuration**

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

**Required service components for Windows**

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

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

- C:\Program Files\Amazon
- C:\Program Files\NICE
- C:\Program Files\Teradici
- C:\Program Files (x86)\Teradici
- C:\ProgramData\Amazon
- C:\ProgramData\NICE
- C:\ProgramData\Teradici
32-bit PCoIP agent

As of March 29, 2021, we updated the PCoIP agent from 32-bit to 64-bit. For Windows WorkSpaces that are using the PCoIP protocol, this means that the location of the Teradici files changed from `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_server_win32.exe` to `C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_server.exe`. Because we updated PCoIP agents during regular maintenance windows, some of your WorkSpaces might have used the 32-bit agent longer than others during the transition.

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

If you're filtering on the paths to any 32-bit PCoIP components, be sure to add the paths to the 64-bit versions of the components. Because your WorkSpaces might not all be updated at the same time, do not replace the 32-bit path with the 64-bit path, or some of your WorkSpaces might not work. For example, if you're basing your exclusions or communication filters on `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_agent.exe`, you must also add `C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_agent.exe`. Likewise, if you're basing your exclusions or communications filters on `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_arbiter_win32.exe`, the PCoIP arbiter service change — Be aware that the PCoIP arbiter service (`C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_arbiter_win32.exe`) is removed when your WorkSpaces are updated to use the 64-bit agent.

PCoIP zero clients and USB devices — Starting with version 20.10.4 of the PCoIP agent, Amazon WorkSpaces disables USB redirection by default through the Windows registry. This registry setting affects the behavior of USB peripherals when your users are using PCoIP zero client devices to connect to their WorkSpaces. For more information, see USB printers and other USB peripherals aren't working for PCoIP zero clients (p. 260).

Required service components for Linux

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

**Note**

Making changes to files other than `/etc/pcoip-agent/pcoip-agent.conf` might cause your WorkSpaces to stop working and might require you to rebuild them. For information about modifying `/etc/pcoip-agent/pcoip-agent.conf`, see Manage your Amazon Linux WorkSpaces (p. 143).

* `/etc/dhcp/dhclient.conf`
* `/etc/logrotate.d/pcoip-agent`
* `/etc/logrotate.d/pcoip-server`
* `/etc/os-release`
* `/etc/pam.d/pcoip`
* `/etc/pam.d/pcoip-session`
* `/etc/pcoip-agent`
* `/etc/profile.d/system-restart-check.sh`
* `/etc/X11/default-display-manager`
* `/etc/yum/pluginconf.d/halt_os_update_check.conf`
Components for Linux

- /lib/systemd/system/pcoip.service
- /lib/systemd/system/pcoip-agent.service
- /lib64/security/pam_self.so
- /usr/bin/pcoip-fne-view-license
- /usr/bin/pcoip-list-licenses
- /usr/bin/pcoip-validate-license
- /usr/lib/firewalld/services/pcoip-agent.xml
- /usr/lib/modules-load.d/usb-vhci.conf
- /usr/lib/pcoip-agent
- /usr/lib/skylight
- /usr/lib/systemd/system/pcoip.service
- /usr/lib/systemd/system/pcoip.service.d/
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/tmpfiles.d/pcoip-agent.conf
- /usr/lib/yum-plugins/halt_os_update_check.py
- /usr/sbin/pcoip-agent
- /usr/sbin/pcoip-register-host
- /usr/sbin/pcoip-support-bundler
- /usr/share/doc/pcoip-agent
- /usr/share/pcoip-agent
- /usr/share/selinux/packages/pcoip-agent.pp
- /usr/share/X11
- /var/crash/pcoip-agent
- /var/lib/pcoip-agent
- /var/lib/skylight
- /var/log/pcoip-agent
- /var/log/skylight
Manage directories for WorkSpaces

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

- **AD Connector** — Use your existing on-premises Microsoft Active Directory. Users can sign into their WorkSpaces using their on-premises credentials and access on-premises resources from their WorkSpaces.
- **AWS Managed Microsoft AD** — Create a Microsoft Active Directory hosted on AWS.
- **Simple AD** — Create a directory that is compatible with Microsoft Active Directory, powered by Samba 4, and hosted on AWS.
- **Cross trust** — Create a trust relationship between your AWS Managed Microsoft AD directory and your on-premises domain.

For tutorials that demonstrate how to set up these directories and launch WorkSpaces, see Launch a virtual desktop using WorkSpaces (p. 103).

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

After you create a directory, you'll perform most directory administration tasks using tools such as the Active Directory Administration Tools. You can perform some directory administration tasks using the WorkSpaces console and other tasks using Group Policy. For more information about managing users and groups, see Manage WorkSpaces users (p. 117) and Set up Active Directory Administration Tools for WorkSpaces (p. 101).

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

To delete empty directories, see Delete the directory for your WorkSpaces (p. 99). If you delete your Simple AD or AD Connector directory, you can always create a new one when you want to start using WorkSpaces again.

**Contents**
- Register a directory with WorkSpaces (p. 90)
- Update directory details for your WorkSpaces (p. 91)
- Update DNS servers for Amazon WorkSpaces (p. 94)
Register a directory with WorkSpaces

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

Requirements

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

- The directory that you want to register for use with Amazon WorkSpaces must be present in every virtual private cloud (VPC) subnet where you want to launch WorkSpaces.
- If you're using AD Connector, your AD Connector must be directly attached to the subnets of the same VPC that will be used for WorkSpaces deployments.
- If you're using AWS Managed Microsoft AD or Simple AD, your directory can be in a dedicated private subnet, as long as the directory has access to the VPC where the WorkSpaces are located.

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

**Note**

Simple AD and AD Connector are made available to you free of charge to use with WorkSpaces. If there are no WorkSpaces being used with your Simple AD or AD Connector directory for 30 consecutive days, this directory will be automatically deregistered for use with Amazon WorkSpaces, and you will be charged for this directory as per the AWS Directory Service pricing terms.

To delete empty directories, see Delete the directory for your WorkSpaces (p. 99). If you delete your Simple AD or AD Connector directory, you can always create a new one when you want to start using WorkSpaces again.

**To register a directory**

2. In the navigation pane, choose **Directories**.
3. Select the directory.
4. Choose **Actions, Register**.

**Note**

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

5. Select two subnets of your VPC that are not from the same Availability Zone. These subnets will be used to launch your WorkSpaces. For more information, see Availability Zones for Amazon WorkSpaces (p. 13).

**Note**

If you do not know which subnets to choose, select **No Preference**.
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 AWS Managed Microsoft AD. If you’re using AWS Managed Microsoft AD, finish registering your directory, and then see **Enable Amazon WorkDocs for AWS Managed Microsoft AD** (p. 100).

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

**To deregister a directory**

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 WorkSpaces console.

**Tasks**
- Select an organizational unit (p. 91)
- Configure automatic public IP addresses (p. 92)
- Control device access (p. 93)
- Manage local administrator permissions (p. 93)
- Update the AD Connector account (AD Connector) (p. 93)
- Multi-factor authentication (AD Connector) (p. 94)

### 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

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. 167).

To specify a target domain and organizational unit

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. 167).

Configure automatic public IP addresses

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

Note that you do not need to enable automatic assignment of public addresses if your WorkSpaces are in private subnets and you configured a NAT gateway for the virtual private cloud (VPC), or if your WorkSpaces are in public subnets and you assigned them Elastic IP addresses. For more information, see Configure a VPC for WorkSpaces (p. 10).

Warning
If you associate an Elastic IP address that you own to a WorkSpace, and then you later disassociate that Elastic IP address from the WorkSpace, the WorkSpace loses its public IP address, and it doesn't automatically get a new one from the Amazon-provided pool. To associate a new public IP address from the Amazon-provided pool with the WorkSpace, you must rebuild the WorkSpace (p. 167). If you don't want to rebuild the WorkSpace, you must associate another Elastic IP address that you own to the WorkSpace.

To configure Elastic IP addresses

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

### Control device access

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

#### To control device access to WorkSpaces

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 also restrict access to trusted devices only. For more information, see *Restrict WorkSpaces access to trusted devices (p. 55).*
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

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 WorkSpaces machine accounts to your AD Connector directory.

#### To update the AD Connector account

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

**Note**

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

**To enable multi-factor authentication**

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

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

**Update DNS servers for Amazon WorkSpaces**

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

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

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

We recommend updating the DNS settings on the WorkSpaces before updating the DNS settings in Active Directory (as explained in Step 1 (p. 95) of the following procedure).
If you want to rebuild the WorkSpaces instead, update one of the DNS server IP addresses in your Active Directory (Step 2 (p. 97)), and then follow the procedure in Rebuild a WorkSpace (p. 167) to rebuild your WorkSpaces. After you've rebuilt your WorkSpaces, follow the procedure in Step 3 (p. 97) to test your DNS server updates. After completing that step, update the IP address of your second DNS server in Active Directory, and then rebuild your WorkSpaces again. Be sure to follow the procedure in Step 3 (p. 97) to test your second DNS server update. As noted in the Best Practices (p. 95) section, we recommend updating your DNS server IP addresses one at a time.

Best practices

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

- To avoid disconnections and inaccessibility of domain resources, we strongly recommend performing DNS server updates during off-peak hours or during a planned maintenance period.
- Don't launch any new WorkSpaces during the 15 minutes before and the 15 minutes after changing your DNS server settings.
- When updating your DNS server settings, change one DNS server IP address at a time. Verify that the first update is correct before updating the second IP address. We recommend performing the following procedure (Step 1 (p. 95), Step 2 (p. 97), and Step 3 (p. 97)) twice to update the IP addresses one at a time.

Step 1: Update the DNS server settings on your WorkSpaces

In the following procedure, the current and new DNS server IP address values are referred to as follows:

- Current DNS IP addresses: \texttt{OldIP1}, \texttt{OldIP2}
- New DNS IP addresses: \texttt{NewIP1}, \texttt{NewIP2}

\textbf{Note}

If this is the second time you're performing this procedure, replace \texttt{OldIP1} with \texttt{OldIP2} and \texttt{NewIP1} with \texttt{NewIP2}.

Update the DNS server settings for Windows WorkSpaces

If you have multiple WorkSpaces, you can deploy the following registry update to the WorkSpaces by applying a Group Policy Object (GPO) on the Active Directory OU for your WorkSpaces. For more information about working with GPOs, see Manage your Windows WorkSpaces (p. 125).

You can make these updates either by using the Registry Editor or by using Windows PowerShell. Both procedures are described in this section.

To update the DNS registry settings using the Registry Editor

1. On your Windows WorkSpace, open the Windows search box, and enter \texttt{registry editor} to open the Registry Editor (\texttt{regedit.exe}).
2. When asked “Do you want to allow this app to make changes to your device?”, choose Yes.
3. In the Registry Editor, navigate to the following registry entry:

   *HKEY\_LOCAL\_MACHINE\SOFTWARE\Amazon\SkyLight*

4. Open the DomainJoinDns registry key. Update \texttt{OldIP1} with \texttt{NewIP1}, and then choose OK.
5. Close the Registry Editor.
6. Reboot the WorkSpace, or restart the service SkyLightWorkspaceConfigService.
Step 1: Update the DNS server settings on your WorkSpaces

Note
After you restart the service SkyLightWorkspaceConfigService, it can take up to 1 minute for the network adapter to reflect the change.

7. Proceed to Step 2 (p. 97), and update your DNS server settings in Active Directory to replace OldIP1 with NewIP1.

To update the DNS registry settings using PowerShell

The following procedure uses PowerShell commands to update your registry and restart the service SkyLightWorkspaceConfigService.

1. On your Windows WorkSpace, open the Windows search box, and enter powershell. Choose Run as Administrator.
2. When asked “Do you want to allow this app to make changes to your device?”, choose Yes.
3. In the PowerShell window, run the following command to retrieve the current DNS server IP addresses.

   Get-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS

   You should receive the following output.

   | DomainJoinDns | OldIP1,OldIP2 |
   | PSPath        | Microsoft.PowerShell.Core\Registry:\HKEY_LOCAL_MACHINE\SOFTWARE\Amazon | SkyLight |
   | PSParentPath  | Microsoft.PowerShell.Core\Registry:\HKEY_LOCAL_MACHINE\SOFTWARE\Amazon | SkyLight |
   | PSChildName   | SkyLight |
   | PSDrive       | HKLM |
   | PSPortinProvider | Microsoft.PowerShell.Core\Registry |

4. In the PowerShell window, run the following command to change OldIP1 to NewIP1. Be sure to leave OldIP2 as is for now.

   Set-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS -Value "NewIP1,OldIP2"

5. Run the following command to restart the service SkyLightWorkspaceConfigService.

   restart-service -Name SkyLightWorkspaceConfigService

   Note
   After you restart the service SkyLightWorkspaceConfigService, it can take up to 1 minute for the network adapter to reflect the change.

6. Proceed to Step 2 (p. 97), and update your DNS server settings in Active Directory to replace OldIP1 with NewIP1.

Update the DNS server settings for Linux WorkSpaces

If you have more than one Linux WorkSpace, 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.

To update the DNS server settings on a Linux WorkSpace

1. On your Linux WorkSpace, open a Terminal window (Applications > System Tools > MATE Terminal).
2. Use the following Linux command to edit the /etc/dhcp/dhclient.conf file. You must have root user privileges to edit this file. Either become root by using the sudo -i command, or execute all commands with sudo as shown.

```
sudo vi /etc/dhcp/dhclient.conf
```

In the /etc/dhcp/dhclient.conf file, you will see the following prepend command, where `OldIP1` and `OldIP2` are the IP addresses of your DNS servers.

```
prepend domain-name-servers OldIP1, OldIP2; # skylight
```

3. Replace `OldIP1` with `NewIP1`, and leave `OldIP2` as is for now.
4. Save your changes to /etc/dhcp/dhclient.conf.
5. Reboot the WorkSpace.
6. Proceed to Step 2 (p. 97), and update your DNS server settings in Active Directory to replace `OldIP1` with `NewIP1`.

### Step 2: Update the DNS server settings for Active Directory

In this step, you update your DNS server settings for Active Directory. As noted in the Best Practices (p. 95) section, we recommend updating your DNS server IP addresses one at a time.

To update your DNS server settings for Active Directory, see the following documentation in the AWS Directory Service Administration Guide:

- AD Connector: Update the DNS Address for Your AD Connector
- AWS Managed Microsoft AD: Configure DNS Conditional Forwarders for Your On-premises Domain
- Simple AD: Configure DNS

After updating your DNS server settings, proceed to Step 3 (p. 97).

### Step 3: Test the updated DNS server settings

After completing Step 1 (p. 95) and Step 2 (p. 97), use the following procedure to verify that your updated DNS server settings are working as expected.

In the following procedure, the current and new DNS server IP address values are referred to as follows:

- Current DNS IP addresses: `OldIP1, OldIP2`
- New DNS IP addresses: `NewIP1, NewIP2`

**Note**

If this is the second time you're performing this procedure, replace `OldIP1` with `OldIP2` and `NewIP1` with `NewIP2`.

**Test the updated DNS server settings for Windows WorkSpaces**

1. Shut down the `OldIP1` DNS server.
2. Log in to a Windows WorkSpace.
4. Run the following command, where `AD_Name` is the name of your Active Directory (for example, `corp.example.com`).

```
nslookup AD_Name
```

The `nslookup` command should return the following output. (If this is the second time you're performing this procedure, you should see `NewIP2` in place of `OldIP2`.)

```
Server: Full_AD_Name
Address: NewIP1
Name: AD_Name
Addresses: OldIP2
        NewIP1
```

5. If the output is not what you were expecting or if you receive any errors, repeat Step 1 (p. 95).
6. Wait for an hour and confirm that no user issues have been reported. Verify that `NewIP1` is getting DNS queries and responding with answers.
7. After you've verified that the first DNS server is working properly, repeat Step 1 (p. 95) to update the second DNS server, this time replacing `OldIP2` with `NewIP2`. Then repeat Step 2 and Step 3.

**Test the updated DNS server settings for Linux WorkSpaces**

1. Shut down the `OldIP1` DNS server.
2. Log in to a Linux WorkSpace.
3. On your Linux WorkSpace, open a Terminal window (Applications > System Tools > MATE Terminal).
4. The DNS server IP addresses returned in the DHCP response are written to the local `/etc/resolv.conf` file on the WorkSpace. Run the following command to view the contents of the `/etc/resolv.conf` file.

```
cat /etc/resolv.conf
```

You should see the following output. (If this is the second time you're performing this procedure, you should see `NewIP2` in place of `OldIP2`.)

```
; This file is generated by Amazon WorkSpaces
; Modifying it can make your WorkSpace inaccessible until reboot
options timeout:2 attempts:5
search region.compute.internal
nameserver NewIP1
nameserver OldIP2
nameserver WorkSpaceIP
```

**Note**
If you make manual modifications to the `/etc/resolv.conf` file, those changes are lost when the WorkSpace is restarted.

5. If the output is not what you were expecting or if you receive any errors, repeat Step 1 (p. 95).
6. The actual DNS server IP addresses are stored in the `/etc/dhcp/dhclient.conf` file. To see the contents of this file, run the following command.

```
sudo cat /etc/dhcp/dhclient.conf
```
You should see the following output. (If this is the second time you're performing this procedure, you should see *NewIP2* in place of *OldIP2*.)

```
# This file is generated by Amazon WorkSpaces
# Modifying it can make your WorkSpace inaccessible until rebuild
prepend domain-name-servers NewIP1, OldIP2; # skylight
```

7. Wait for an hour and confirm that no user issues have been reported. Verify that *NewIP1* is getting DNS queries and responding with answers.

8. After you've verified that the first DNS server is working properly, repeat Step 1 (p. 95) to update the second DNS server, this time replacing *OldIP2* with *NewIP2*. Then repeat Step 2 and Step 3.

---

**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 other applications, such as Amazon WorkDocs, Amazon WorkMail, or Amazon Chime. Note that you must deregister a directory before you can delete it.

**Note**
Simple AD and AD Connector are made available to you free of charge to use with WorkSpaces. If there are no WorkSpaces being used with your Simple AD or AD Connector directory for 30 consecutive days, this directory will be automatically deregistered for use with Amazon WorkSpaces, and you will be charged for this directory as per the AWS Directory Service pricing terms.

If you delete your Simple AD or AD Connector directory, you can always create a new one when you want to start using WorkSpaces again.

**What happens when you delete a directory**

When a Simple AD or AWS Directory Service for Microsoft Active Directory directory is deleted, all of the directory data and snapshots are deleted and cannot be recovered. After the directory is deleted, any Amazon EC2 instances that are joined to the directory remain intact. You cannot, however, use your directory credentials to log in to these instances. You need to log in to these instances with a user account that is local to the instance.

When an AD Connector directory is deleted, your on-premises directory remains intact. Any Amazon EC2 instances that are joined to the directory also remain intact and remain joined to your on-premises directory. You can still use your directory credentials to log in to these instances.

**To delete a directory**

1. Delete all WorkSpaces in the directory. For more information, see Delete a WorkSpace (p. 179).
2. Find and remove all of the applications and services that are registered to the directory. For more information, see Delete Your Directory in the AWS Directory Service Administration Guide.
4. In the navigation pane, choose **Directories**.
5. Select the directory and choose **Actions, Deregister**.
6. When prompted for confirmation, choose **Deregister**.
7. Select the directory again and choose **Actions, Delete**.
8. When prompted for confirmation, choose **Delete**.

**Note**
Removing application assignments can sometimes take more time than expected. If you receive the following error message, verify that you've removed all application assignments, and then wait 30 to 60 minutes before trying again to delete the directory:
Enable Amazon WorkDocs for AWS Managed Microsoft AD

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

**Note**
Amazon WorkDocs is not available in all of the AWS Regions where Amazon WorkSpaces is available. For more information, see Amazon WorkDocs Pricing.

### To enable WorkDocs through the Amazon WorkDocs console

1. Open the Amazon WorkDocs console at https://console.aws.amazon.com/zocalo/.
2. Choose **Create a New WorkDocs Site**.
3. Under **Standard Setup**, choose **Launch**.
4. Select the directory and create your site name.
5. Specify the user who will administer the WorkDocs site. You can use the admin or any user created in the directory.

For more information, see Getting Started with AWS Managed Microsoft AD in the Amazon WorkDocs Administration Guide.

### To enable WorkDocs through the AWS Directory Service console

2. In the navigation pane, choose **Directories**.
3. On the **Directories** page, choose your directory.
4. On the **Directory details** page, choose the **Application management** tab.
5. In the **Application access URL** section, if an access URL has not been assigned to the directory, the **Create** button is displayed. Enter a directory alias and choose **Create**. For more information, see Creating an Access URL in the AWS Directory Service Administration Guide.
6. In the **Application access URL** section, choose **Enable** to enable single sign-on for Amazon WorkDocs. For more information, see Single Sign-On in the AWS Directory Service Administration Guide.
Set up Active Directory Administration Tools for WorkSpaces

You'll perform most administrative tasks for your WorkSpaces directory using directory management tools, such as the Active Directory Administration Tools. However, you'll use the WorkSpaces console to perform some directory-related tasks. For more information, see Manage directories for WorkSpaces (p. 89).

If you create a directory with AWS Managed Microsoft AD or Simple AD that includes five or more WorkSpaces, we recommend that you centralize administration on an Amazon EC2 instance. Although you can install the directory management tools on a WorkSpace, using an Amazon EC2 instance is a more robust solution.

To set up the Active Directory Administration Tools

1. Launch an Amazon EC2 Windows instance and join it to your WorkSpaces directory by using one of the following options:
   - If you don't already have an existing Amazon EC2 Windows instance, you can join the instance to your directory domain when you launch the instance. For more information, see Seamlessly join a Windows EC2 instance in the AWS Directory Service Administration Guide.
   - If you already have an existing Amazon EC2 Windows instance, you can join it to your directory manually. For more information, see Manually Add a Windows Instance in the AWS Directory Service Administration Guide.

2. Install the Active Directory Administration Tools on the Amazon EC2 Windows instance. For more information, see Installing the Active Directory Administration Tools in the AWS Directory Service Administration Guide.

   **Note**
   When you're installing the Active Directory Administration Tools, make sure to also select Group Policy Management to install the Group Policy Management Editor (gpmc.msc) tool.

   When the feature installation is finished, the Active Directory tools are available on the Windows Start menu under Windows Administrative Tools.

3. Run the tools as a directory administrator as follows:
   - On the Windows Start menu, open Windows Administrative Tools.
   - Hold down the Shift key, right-click the shortcut for the tool you want to use, and choose Run as different user.
   - Type the username and password for the administrator. With Simple AD, the username is Administrator and with AWS Managed Microsoft AD, the administrator is Admin.

You can now perform directory administration tasks using the Active Directory tools that you are familiar with. For example, you can use the Active Directory Users and Computers Tool to add users, remove users, promote a user to directory administrator, or reset a user password. Note that you must be logged into your Windows instance as a user that has permissions to manage users in the directory.

To promote a user to a directory administrator

   **Note**
   This procedure applies only to directories created with Simple AD, not AWS Managed AD. For directories created with AWS Managed AD, see Manage Users and Groups in AWS Managed Microsoft AD in the AWS Directory Service Administration Guide.

1. Open the Active Directory Users and Computers tool.
2. Navigate to the Users folder under your domain and select the user to promote.
4. In the username Properties dialog box, choose Member Of.
5. Add the user to the following groups and choose OK.
   - Administrators
   - Domain Admins
   - Enterprise Admins
   - Group Policy Creator Owners
   - Schema Admins

To add or remove users

You can create new users from the Amazon WorkSpaces console only during the process of launching a WorkSpace, and you cannot delete users through the Amazon WorkSpaces console. Most user management tasks, including managing user groups, must be performed through your directory.

**Important**
Before you can remove a user, you must delete the WorkSpace assigned to that user. For more information, see Delete a WorkSpace (p. 179).

The process you use for managing users and groups depends on which type of directory you’re using.

- If you’re using AWS Managed Microsoft AD, see Manage Users and Groups in AWS Managed Microsoft AD in the AWS Directory Service Administration Guide.
- If you’re using Simple AD, see Manage Users and Groups in Simple AD in the AWS Directory Service Administration Guide.
- If you use Microsoft Active Directory through AD Connector or a trust relationship, you can manage users and groups using the Active Directory module.

To reset a user password

When you reset the password for an existing user, do not set User must change password at next logon. Otherwise, the users cannot connect to their WorkSpaces. Instead, assign a secure temporary password to each user and then ask the users to manually change their passwords from within the WorkSpace the next time they log on.

**Note**
If you’re using AD Connector or if your users are in the AWS GovCloud (US-West) Region, your users won’t be able to reset their own passwords. (The Forgot password? option on the WorkSpaces client application login screen won’t be available.)
Launch a virtual desktop using WorkSpaces

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

**Note**

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

- **Linux**: A-1xxxxxxxxxxxx
- **Windows**: IP-Cxxxxxx or WSAMZN-xxxxxxx or EC2AMAZ-xxxxxxx

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

- Starting June 22, 2020, Windows WorkSpaces launched from public bundles have the WSAMZN-xxxxxxx format for their computer names instead of the IP-Cxxxxxx format.
- For custom bundles based on a public image, if the public image was created before June 22, 2020, the computer names are in the EC2AMAZ-xxxxxxx format. If the public image was created on or after June 22, 2020, the computer names are in the WSAMZN-xxxxxxx format.
- For Bring Your Own License (BYOL) bundles, either the DESKTOP-xxxxxxx or the EC2AMAZ-xxxxxxx format is used for the computer names by default.

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

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.

**Note**

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

To delete empty directories, see Delete the directory for your WorkSpaces (p. 99). If you delete your Simple AD or AD Connector directory, you can always create a new one when you want to start using WorkSpaces again.

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. 104)
- Launch a WorkSpace using Simple AD (p. 107)
- Launch a WorkSpace using AD Connector (p. 110)
- Launch a WorkSpace using a trusted domain (p. 113)

### Launch a WorkSpace using AWS Managed Microsoft AD

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

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 WorkSpaces (p. 103).

**Tasks**
- Before you begin (p. 104)
- Step 1: Create an AWS Managed Microsoft AD Directory (p. 105)
- Step 2: Create a WorkSpace (p. 105)
- Step 3: Connect to the WorkSpace (p. 106)
- Next steps (p. 107)

### Before you begin

- WorkSpaces is not available in every Region. Verify the supported Regions and select a Region for your WorkSpaces. For more information about the supported Regions, see WorkSpaces Pricing by AWS Region.
- 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 WorkSpaces (p. 10).
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.

Note

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

To create an AWS Managed Microsoft AD directory

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).
      Important
      If you need to update your DNS server after launching your WorkSpaces, follow the procedure in Update DNS servers for Amazon WorkSpaces (p. 94) to ensure that your WorkSpaces get properly updated.
   c. For NetBIOS name, enter a short name for the directory (for example, workspaces).
   d. For Admin password and Confirm password, enter a password for the directory administrator account. For more information about the password requirements, see Create Your AWS Managed Microsoft AD Directory in the AWS Directory Service Administration Guide.
   e. (Optional) For Description, enter a description for the directory.
   f. For VPC, select the VPC that you created.
   g. For Subnets, select the two private subnets (with the CIDR blocks 10.0.1.0/24 and 10.0.2.0/24).
   h. Choose Next Step.
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

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. 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.
   **Note**
   Invitation emails aren't sent if the user already exists in Active Directory. Instead, make sure you manually send the user an invitation email. For more information, see Send an invitation email (p. 118).
9. (Optional) If Amazon WorkDocs is supported in the Region, you can enable Amazon WorkDocs for all users in the directory. For more information, see Enable Amazon WorkDocs for AWS Managed Microsoft AD (p. 100). For more information about Amazon WorkDocs, see Amazon WorkDocs Drive in the Amazon WorkDocs Administration Guide.

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 each of the following categories:
   lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9), and ~!@#$%^&*_-+=`\{}[]:;"'<>,.?/
2. Review WorkSpaces Clients in the Amazon WorkSpaces User Guide for more information about the requirements for each client, and then do one of the following:
   - When prompted, download one of the client applications or launch Web Access.
   - If you aren’t prompted and you haven’t installed a client application already, open https://clients.amazonworkspaces.com/ and download one of the client applications or launch Web Access.
   **Note**
   You cannot use a web browser (Web Access) to connect to Amazon Linux WorkSpaces.
3. Start the client, enter the registration code from the invitation email, and choose Register.
4. When prompted to sign in, enter the 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. You can also perform various administrative tasks for your WorkSpaces and your WorkSpaces directory. If you are finished with your WorkSpace, you can delete it. For more information, see the following documentation.

- Create a custom WorkSpaces image and bundle (p. 181)
- Administer your WorkSpaces (p. 125)
- Manage directories for WorkSpaces (p. 89)
- Delete a WorkSpace (p. 179)

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

Launch a WorkSpace using Simple AD

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

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 WorkSpaces (p. 103).

Tasks

- Before you begin (p. 107)
- Step 1: Create a Simple AD directory (p. 108)
- Step 2: Create a WorkSpace (p. 109)
- Step 3: Connect to the WorkSpace (p. 109)
- Next steps (p. 110)

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 for Simple AD, see Region Availability for AWS Directory Service.
- WorkSpaces is not available in every Region. Verify the supported Regions and select a Region for your WorkSpaces. For more information about the supported Regions, see WorkSpaces Pricing by AWS Region.
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.

**Note**
Simple AD is made available to you free of charge to use with WorkSpaces. If there are no WorkSpaces being used with your Simple AD directory for 30 consecutive days, this directory will be automatically deregistered for use with Amazon WorkSpaces, and you will be charged for this directory as per the AWS Directory Service pricing terms.

To delete empty directories, see Delete the directory for your WorkSpaces (p. 99). If you delete your Simple AD directory, you can always create a new one when you want to start using WorkSpaces again.

**To create a Simple AD directory**

2. In the navigation pane, choose **Directories**.
3. Choose **Set up Directory**, **Simple AD**, and **Next**.
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 name**, enter the fully-qualified name for the directory (for example, example.com).
      **Important**
      If you need to update your DNS server after launching your WorkSpaces, follow the procedure in Update DNS servers for Amazon WorkSpaces (p. 94) to ensure that your WorkSpaces get properly updated.
   c. For **NetBIOS name**, enter a short name for the directory (for example, example).
   d. For **Admin password** and **Confirm password**, enter a password for the directory administrator account. For more information about the password requirements, see How to Create a Microsoft AD Directory in the AWS Directory Service Administration Guide.
   e. (Optional) For **Description**, enter a description for the directory.
   f. For **Directory size**, choose **Small**.
   g. For **VPC**, select the VPC that you created.
   h. For **Subnets**, select the two private subnets (with the CIDR blocks 10.0.1.0/24 and 10.0.2.0/24).
   i. Choose **Next**.
5. Choose **Create directory**.
6. The initial status of the directory is **Requested** and then **Creating**. When directory creation is complete (this might take a few minutes), the status is **Active**.
What happens during directory creation

WorkSpaces completes the following tasks on your behalf:

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

Step 2: Create a WorkSpace

Now you are ready to launch the WorkSpace.

To create a WorkSpace for a user

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 Self Service Permissions, choose Yes or No and enter a description.
   c. For Enable Amazon WorkDocs, choose Yes.
      
     Note
     This option is available only if Amazon WorkDocs is available in the selected Region.
   d. Choose Next Step. 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.
   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 (this can take up to 20 minutes), the status is AVAILABLE and an invitation is sent to the email address that you specified for the user.

   Note
   Invitation emails aren't sent if the user already exists in Active Directory. Instead, make sure you manually send the user an invitation email. For more information, see Send an invitation email (p. 118).

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 each of the following categories: lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9), and ~!@#$%^&*_-+=`\|{}[]:;'",<>,.?/.

2. Review WorkSpaces Clients in the Amazon WorkSpaces User Guide for more information about the requirements for each client, and then do one of the following:
   
   • When prompted, download one of the client applications or launch Web Access.
   • If you aren’t prompted and you haven’t installed a client application already, open https://clients.amazonworkspaces.com/ and download one of the client applications or launch Web Access.
   
   **Note**
   
   You cannot use a web browser (Web Access) to connect to Amazon Linux WorkSpaces.

3. Start the client, enter the registration code from the invitation email, and choose Register.
4. When prompted to sign in, enter the 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. You can also perform various administrative tasks for your WorkSpaces and your WorkSpaces directory. If you are finished with your WorkSpace, you can delete it. For more information, see the following documentation.

- Create a custom WorkSpaces image and bundle (p. 181)
- Administer your WorkSpaces (p. 125)
- Manage directories for WorkSpaces (p. 89)
- Delete a WorkSpace (p. 179)

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

**Launch a WorkSpace using AD Connector**

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

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 WorkSpaces (p. 103).
Before you begin

- WorkSpaces is not available in every Region. Verify the supported Regions and select a Region for your WorkSpaces. For more information about the supported Regions, see WorkSpaces Pricing by AWS Region.
- 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. For more information, see Configure a VPC for WorkSpaces. 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.

Step 1: Create an AD Connector

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

To create an AD Connector

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.
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

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 about Amazon WorkDocs, see Amazon WorkDocs Drive in the Amazon WorkDocs Administration Guide.
6. Choose Next. 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 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. 147).
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. (These invitations aren't sent automatically if you're using AD Connector.) For more information, see Send an invitation email (p. 118).

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. Review WorkSpaces Clients in the Amazon WorkSpaces User Guide for more information about the requirements for each client, and then do one of the following:
   - When prompted, download one of the client applications or launch Web Access.
   - If you aren't prompted and you haven't installed a client application already, open https://clients.amazonworkspaces.com/ and download one of the client applications or launch Web Access.

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

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

   **Note**
   Because you're using AD Connector, your users won't be able to reset their own passwords. (The Forgot password? option on the WorkSpaces client application login screen won't be available.) For information about how to reset user passwords, see Set up Active Directory Administration Tools for WorkSpaces (p. 101).

Next steps

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

- Create a custom WorkSpaces image and bundle (p. 181)
- Administer your WorkSpaces (p. 125)
- Manage directories for WorkSpaces (p. 89)
- Delete a WorkSpace (p. 179)

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

Launch a WorkSpace using a trusted domain

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

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 WorkSpaces (p. 103).
Before you begin

Tasks

- Before you begin (p. 114)
- Step 1: Establish a trust relationship (p. 114)
- Step 2: Create a WorkSpace (p. 114)
- Step 3: Connect to the WorkSpace (p. 115)
- Next steps (p. 116)

Before you begin

- Launching WorkSpaces with user accounts in a separate trusted domain works with AWS Managed Microsoft AD when it is configured with a trust relationship to your on-premises directory. However, WorkSpaces using Simple AD or AD Connector cannot launch WorkSpaces for users from a trusted domain.

- WorkSpaces is not available in every Region. Verify the supported Regions and select a Region for your WorkSpaces. For more information about the supported Regions, see WorkSpaces Pricing by AWS Region.

- 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.

- 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 WorkSpaces (p. 10).

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.

   Note

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

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

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

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 WorkSpaces.

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

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. (These invitations aren't sent automatically if you're using a trust relationship.) For more information, see Send an invitation email (p. 118).

**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 each of the following categories: lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9), and ~!@#$%^&*_-+=`|{}\[]":;"'<>,.?/.

2. Review WorkSpaces Clients in the Amazon WorkSpaces User Guide for more information about the requirements for each client, and then do one of the following:
   - When prompted, download one of the client applications or launch Web Access.
   - If you aren't prompted and you haven't installed a client application already, open https://clients.amazonworkspaces.com/ and download one of the client applications or launch Web Access.

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

3. Start the client, enter the registration code from the invitation email, and choose Register.
4. When prompted to sign in, enter the 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. You can also perform various administrative tasks for your WorkSpaces and your WorkSpaces directory. If you are finished with your WorkSpace, you can delete it. For more information, see the following documentation.

- Create a custom WorkSpaces image and bundle (p. 181)
- Administer your WorkSpaces (p. 125)
- Manage directories for WorkSpaces (p. 89)
- Delete a WorkSpace (p. 179)

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

Each WorkSpace is assigned to a single user and cannot be shared by multiple users. By default, only one WorkSpace per user per directory is allowed.

Contents
- Manage WorkSpaces users (p. 117)
- Create multiple WorkSpaces for a user (p. 118)
- Customize how users log in to their WorkSpaces (p. 119)
- Enable self-service WorkSpace management capabilities for your users (p. 120)
- Enable Amazon Connect audio optimization for your users (p. 122)

Manage WorkSpaces users

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

Edit user information

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

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

To edit user information
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.

Add or delete users

You can create new users from the Amazon WorkSpaces console only during the process of launching a WorkSpace, and you cannot delete users through the Amazon WorkSpaces console. Most user management tasks, including managing user groups, must be performed through your directory.

To add or delete users and groups

To add, delete, or otherwise manage users and groups, you must do this through your directory. You'll perform most administrative tasks for your WorkSpaces directory using directory management tools, such as the Active Directory Administration Tools. For more information, see Set up Active Directory Administration Tools for WorkSpaces (p. 101).
Important
Before you can remove a user, you must delete the WorkSpace assigned to that user. For more information, see Delete a WorkSpace (p. 179).

The process you use for managing users and groups depends on which type of directory you're using.

- If you're using AWS Managed Microsoft AD, see Manage Users and Groups in AWS Managed Microsoft AD in the AWS Directory Service Administration Guide.
- If you're using Simple AD, see Manage Users and Groups in Simple AD in the AWS Directory Service Administration Guide.
- If you use Microsoft Active Directory through AD Connector or a trust relationship, you can manage users and groups by using the Active Directory module.

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

Note
If you're using AD Connector or a trusted domain, invitation emails aren't automatically sent to your users, so you must send them manually. Invitation emails also aren't sent automatically if the user already exists in Active Directory.

To resend an invitation email
2. In the navigation pane, choose WorkSpaces.
3. On the WorkSpaces page, use the search box to search for the user you want to send an invitation to, and then select the corresponding WorkSpace from the search results. You can select only one WorkSpace at a time.
5. 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.

Create multiple WorkSpaces for a user
By default, you can create only one WorkSpace per user per directory. However, if needed, you can create more than one WorkSpace for a user, depending on your directory setup.

- If you have only one directory for your WorkSpaces, create multiple usernames for the user. For example, a user named Mary Major can have mmajor1, mmajor2, and so on as usernames. Each username is associated with a different WorkSpace in the same directory, but the WorkSpaces have the same registration code, as long as the WorkSpaces are all created in the same directory in the same AWS Region.
- If you have multiple directories for your WorkSpaces, create the WorkSpaces for the user in separate directories. You can use the same username in the directories, or you can use different usernames in the directories. The WorkSpaces will have different registration codes.

Tip
So that you can easily locate all the WorkSpaces that you've created for a user, use the same base username for each WorkSpace. For example, if you have a user named Mary Major with the Active Directory username mmajor, create WorkSpaces for her with usernames such as mmajor, mmajor1, mmajor2, mmajor3, or other variants, such as mmajor_windows or mmajor_linux. As long as all the WorkSpaces have
the same starting base username (mmajor), you can sort on the username in your WorkSpaces console to group all of the WorkSpaces for that user together.

**Important**

- A user can have both a PCoIP and a WSP WorkSpace as long as the two WorkSpaces are located in separate directories. The same user cannot have a PCoIP and a WSP WorkSpace in the same directory.
- If you are setting up multiple WorkSpaces for use with cross-Region redirection, you must set up the WorkSpaces in different directories in different AWS Regions, and you must use the same usernames in each directory. For more information about cross-Region redirection, see Cross-region redirection for Amazon WorkSpaces (p. 222).

To switch between the WorkSpaces, the user logs in with the username and registration code associated with a particular Workspace. If the user is using a 3.0+ version of the WorkSpaces client applications for Windows, macOS, or Linux, the user can assign different names to the WorkSpaces by going to **Settings, Manage Login Information** in the client application.

**Customize how users log in to their WorkSpaces**

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.

URI access works with both Region-based registration codes (for example, WSpdx+ABC12D) and fully qualified domain name (FQDN) based registration codes (for example, desktop.example.com). For more information about creating and using FQDN-based registration codes, see Cross-region redirection for Amazon WorkSpaces (p. 222).

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 devices

To use URIs to access their WorkSpaces, users must first install the client application for their device by opening https://clients.amazonworkspaces.com/ and following the directions.

URI access is supported on the Firefox and Chrome browsers on Windows and macOS computers, on the Firefox browser on Ubuntu Linux 18.04 computers, and on the Internet Explorer and Microsoft Edge browsers on Windows computers. For more information about WorkSpaces clients, see WorkSpaces Clients in the Amazon WorkSpaces User Guide.

**Note**

On Android devices, URI access works only with the Firefox browser, not with the Google Chrome browser.
To configure URI access to WorkSpaces, use any of the URI formats described in the following table.

**Note**
If the data component of your URI includes any of the following reserved characters, we recommend that you use percent-encoding in the data component to avoid ambiguity:
- @
- :
- /?
- &
- =

For example, if you have 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>
<tr>
<td>workspaces:///username@registrationcode</td>
<td>Registers a user by using their WorkSpaces registration code. Also automatically enters the user name in the <code>username</code> field on the client login page.</td>
</tr>
<tr>
<td>workspaces:///username@registrationcode?MFACode=mfa</td>
<td>Registers a user by using their WorkSpaces registration code. Also automatically enters the user name in the <code>username</code> field and the multi-factor authentication (MFA) code in the <code>MFA code</code> field on the client login page.</td>
</tr>
<tr>
<td>workspaces:///@registrationcode?MFACode=mfa</td>
<td>Registers a user by using their WorkSpaces registration code. Also automatically enters the multi-factor authentication (MFA) code in the <code>MFA code</code> field on the client login page.</td>
</tr>
</tbody>
</table>

**Note**
If users open a URI link when they are already connected to a WorkSpace from a Windows client, a new WorkSpaces session opens and their original WorkSpaces session remains open. If users open a URI link when they are connected to a WorkSpace from a macOS, iPad, or Android client, no new session opens; only their original WorkSpaces session remains open.

## Enable self-service WorkSpace management capabilities for your users

In WorkSpaces, you can enable self-service WorkSpace management capabilities for your users to provide them with more control over their experience. It can also reduce your IT support staff workload for WorkSpaces. When you enable self-service capabilities, users can perform one or more of the following tasks directly from their WorkSpaces client:

- Cache their credentials on their client. This lets them reconnect to their WorkSpace without re-entering their credentials.
- Restart (reboot) their WorkSpace.
- Increase the size of the root and user volumes on their WorkSpace.
- Change the compute type (bundle) for their WorkSpace.
- Switch the running mode of their WorkSpace.
- Rebuild their WorkSpace.

**Supported clients**
- Android, running on Android or Android-compatible Chrome OS systems
- Linux
- macOS
- Windows

**To enable self-service management capabilities for your users**

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. 142).

   - **Restart WorkSpace from client** — Users can restart (reboot) their WorkSpace. Restarting disconnects the user from their WorkSpace, shuts it down, and reboots it. The user data, operating system, and system settings are not affected.

   - **Increase volume size** — Users can expand the root and user volumes on their WorkSpace to a specified size without contacting IT support. Users can increase the size of the root volume (for Windows, the C: drive; for Linux, /) up to 175 GB, and the size of the user volume (for Windows, the D: drive; for Linux, /home) up to 100 GB. WorkSpace root and user volumes come in set groups that can't be changed. The available groups are [Root(GB), User(GB)]: [80, 10], [80, 50], [80, 100], [175 to 2000, 100 to 2000]. For more information, see **Modify a WorkSpace** (p. 149).

   For a newly created WorkSpace, users must wait 6 hours before they can increase the size of these drives. After that, they can do so only once in a 6-hour period. While a volume size increase is in progress, users can perform most tasks on their WorkSpace. The tasks that they can't perform are: changing their WorkSpace compute type, switching their WorkSpace running mode, restarting their WorkSpace, or rebuilding their WorkSpace. When the process is finished, the WorkSpace must be rebooted for the changes to take effect. This process might take up to an hour.

   **Note**
   If users increase the volume size on their WorkSpace, this increases the billing rate for their WorkSpace.

   - **Change compute type** — Users can switch their WorkSpace between compute types (bundles). For a newly created WorkSpace, users must wait 6 hours before they can switch to a different bundle. After that, they can switch to a larger bundle only once in a 6-hour period, or to a smaller bundle once in a 30-day period. When a WorkSpace compute type change is in progress, users are disconnected from their WorkSpace, and they can't use or change the WorkSpace. The WorkSpace is automatically rebooted during the compute type change process. This process might take up to an hour.

   **Note**
   If users change their WorkSpace compute type, this changes the billing rate for their WorkSpace.

   - **Switch running mode** — Users can switch their WorkSpace between the **AlwaysOn** and **AutoStop** running modes. For more information, see **Manage the WorkSpace running mode** (p. 147).
Enable Amazon Connect audio optimization for your users

In the WorkSpaces management console, you can enable Amazon Connect Contact Control Panel (CCP) audio optimization for your WorkSpaces fleets to enhance security and to enable native-quality audio. After enabling CCP audio optimization, the CCP audio will be processed by the client endpoints, while WorkSpaces users can interact with the CCP from within their WorkSpaces.

Amazon Connect Contact Control Panel (CCP) audio optimization works with:

- The WorkSpaces Windows client.
- Amazon Linux and Windows WorkSpaces.
- WorkSpaces using PCoIP or WSP.

Requirements

- You must be set up with Amazon Connect.
- You must build a custom CCP with the Amazon Connect Stream API by creating a CCP with no media for call signaling. This way, the media is handled on the local desktop using standard CCP, and the signaling and call controls are handled on the remote connection with the CCP with no media. For more information about the Amazon Connect streams API, see the GitHub repository at https://github.com/aws/amazon-connect-streams. The custom CCP that you build is the CCP your Amazon Connect agents will use within their WorkSpaces.
- You must have a web browser installed onto WorkSpaces client endpoints that's supported by Amazon Connect. For the list of supported browsers, see Browsers supported by Amazon Connect.

Note

If your users use browsers that are not supported, they will be asked to download a supported browser when they attempt to log in to the CCP.

Enable Amazon Connect audio optimization

To enable Amazon Connect audio optimization for your users:

2. In the navigation pane, choose Directories.
3. Select your directory, and choose Actions, Update Details.
4. Expand Amazon Connect Audio Optimization.
   
   **Note**
   Before configuring with Amazon Connect, choose Update to save any unsaved changes made previously in the management console.

5. Choose Configure Amazon Connect.

6. Enter an Amazon Connect Contact Control Panel (CCP) name.
   
   **Note**
   The name that you give your CCP will be used in the user add-in menu. Choose a name that will be meaningful to your users.

7. Enter the Amazon Connect Contact Control Panel URL that’s generated by Amazon Connect. See Provide access to the Contact Control Panel for more information on getting the URL.

8. Choose Create Amazon Connect.

### Update directory's Amazon Connect audio optimization details

To update a directory's Amazon Connect audio optimization details:

2. In the navigation pane, choose Directories.
3. Select your directory, and choose Actions, Update Details.
4. Expand Amazon Connect Audio Optimization.
   
   **Note**
   Before configuring with Amazon Connect, choose Update to save any unsaved changes made previously in the management console.

5. Choose Configure Amazon Connect.

6. Choose Edit.

7. Select your directory, and choose Actions, Update Details.

8. Update the Amazon Connect Contact Control Panel name and URL.

9. Choose Save.

### Delete directory's Amazon Connect audio optimization

To delete a directory’s Amazon Connect audio optimization:

2. In the navigation pane, choose Directories.
3. Select your directory, and choose Actions, Update Details.
4. Expand Amazon Connect Audio Optimization.
   
   **Note**
   Before configuring with Amazon Connect, choose Update to save any unsaved changes made previously in the management console.

5. Choose Configure Amazon Connect.

6. Choose Delete Amazon Connect.
See the Agent training guide for more information.
Administer your WorkSpaces

You can administer your WorkSpaces using the WorkSpaces console.

To perform directory administration tasks, see the section called “Set up Directory Administration” (p. 101).

Contents
- Manage your Windows WorkSpaces (p. 125)
- Manage your Amazon Linux WorkSpaces (p. 143)
- Manage the WorkSpace running mode (p. 147)
- Modify a WorkSpace (p. 149)
- Customize WorkSpace branding (p. 152)
- Tag WorkSpaces resources (p. 157)
- WorkSpace maintenance (p. 159)
- Encrypted WorkSpaces (p. 160)
- Reboot a WorkSpace (p. 166)
- Rebuild a WorkSpace (p. 167)
- Restore a WorkSpace (p. 168)
- Upgrade Windows 10 BYOL WorkSpaces (p. 169)
- Migrate a WorkSpace (p. 175)
- Delete a WorkSpace (p. 179)

Manage your Windows WorkSpaces

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

Note
Linux instances do not adhere to Group Policy. For information about managing Amazon Linux WorkSpaces, see Manage your Amazon Linux WorkSpaces (p. 143).

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

To use the Group Policy settings that are specific to Amazon WorkSpaces, you must install the Group Policy administrative template for the protocol or protocols that you are using, either PCoIP or WorkSpaces Streaming Protocol (WSP).

Warning
Group Policy settings can affect the experience of your WorkSpace users as follows:

- Implementing an interactive logon message to display a logon banner prevents users from being able to access their WorkSpaces. The interactive logon message Group Policy setting is not currently supported by WorkSpaces.
- Disabling removable storage through Group Policy settings causes a login failure that results in users being logged in to temporary user profiles with no access to drive D.
- **Removing users from the Remote Desktop Users local group through Group Policy settings prevents those users from being able to authenticate** through the WorkSpaces client applications. For more information about this Group Policy setting, see Allow log on through Remote Desktop Services in the Microsoft documentation.

- **If you remove the built-in Users group from the Allow log on locally security policy,** your PCoIP WorkSpaces users won't be able to connect to their WorkSpaces through the WorkSpaces client applications. Your PCoIP WorkSpaces also won't receive updates to the PCoIP agent software. PCoIP agent updates might contain security and other fixes, or they might enable new features for your WorkSpaces. For more information about working with this security policy, see Allow log on locally in the Microsoft documentation.

- **Group Policy settings can be used to restrict drive access.** If you configure Group Policy settings to restrict access to drive C or to drive D, users can't access their WorkSpaces. To prevent this issue from occurring, make sure that your users can access drive C and drive D.

- **The WorkSpaces audio-in feature requires local logon access inside the WorkSpace.** The audio-in feature is enabled by default for Windows WorkSpaces. However, if you have a Group Policy setting that restricts users' local logon in their WorkSpaces, audio-in won't work on your WorkSpaces. If you remove that Group Policy setting, the audio-in feature is enabled after the next reboot of the WorkSpace. For more information about this Group Policy setting, see Allow log on locally in the Microsoft documentation.

For more information about enabling or disabling audio-in redirection, see Enable or disable audio-in redirection for PCoIP (p. 132) or Enable or disable audio-in redirection for WSP (p. 139).

- **Using Group Policy to set the Windows power plan to Balanced or Power saver might cause your WorkSpaces to sleep when they're left idle.** We strongly recommend using Group Policy to set the Windows power plan to High performance. For more information, see My Windows WorkSpace goes to sleep when it's left idle (p. 263).

- Some Group Policy settings force users to log off when they are disconnected from a session. Any applications that users have open on their WorkSpaces are closed.

- "Set time limit for active but idle Remote Desktop Services sessions" is currently not supported on WSP WorkSpaces. Avoid using it during WSP sessions as it causes a disconnect even when there is activity and the session is not idle.

For information about using the Active Directory administration tools to work with GPOs, see Set up Active Directory Administration Tools for WorkSpaces (p. 101).

**Contents**

- Install the Group Policy administrative template for PCoIP (p. 127)
  - Configure printer support for PCoIP (p. 129)
  - Enable or disable clipboard redirection for PCoIP (p. 130)
  - Set the session resume timeout for PCoIP (p. 131)
  - Enable or disable audio-in redirection for PCoIP (p. 132)
  - Disable time zone redirection for PCoIP (p. 132)
  - Configure PCoIP security settings (p. 133)
  - Enable USB redirection for YubiKey U2F (p. 134)

- Install the Group Policy administrative template files for the WorkSpaces Streaming Protocol (WSP) (p. 134)
  - Configure printer support for WSP (p. 136)
  - Enable or disable clipboard redirection for WSP (p. 136)
  - Set the session resume timeout for WSP (p. 137)
  - Enable or disable video-in redirection for WSP (p. 138)
  - Enable or disable audio-in redirection for WSP (p. 139)
Install the Group Policy administrative template for PCoIP

To use the Group Policy settings that are specific to Amazon WorkSpaces when using the PCoIP protocol, you must add the Group Policy administrative template that is appropriate to the version of the PCoIP agent (either 32-bit or 64-bit) that is being used for your WorkSpaces.

**Note**
If you have a mix of WorkSpaces with 32-bit and 64-bit agents, you can use the Group Policy administrative templates for 32-bit agents, and your Group Policy settings will be applied to both 32-bit and 64-bit agents. When all of your WorkSpaces are using the 64-bit agent, you can switch to using the administrative template for 64-bit agents.

**To determine whether your WorkSpaces have the 32-bit agent or the 64-bit agent**

1. Log in to a WorkSpace, and then open the Task Manager by choosing View, Send Ctrl + Alt + Delete or by right-clicking the taskbar and choosing Task Manager.
2. In the Task Manager, go to the Details tab, right-click the column headers, and choose Select Columns.
3. In the Select Columns dialog box, select Platform, and then choose OK.
4. On the Details tab, find pcoip_agent.exe, and then check its value in the Platform column to determine if the PCoIP agent is 32-bit or 64-bit. (You might see a mix of 32-bit and 64-bit WorkSpaces components; this is normal.)

**Install the Group Policy administrative template for PCoIP (32-Bit)**

To use the Group Policy settings that are specific to WorkSpaces when using the PCoIP protocol with the 32-bit PCoIP agent, you must install the Group Policy administrative template for PCoIP. Perform the following procedure on a directory administration WorkSpace or Amazon EC2 instance that is joined to your directory.

For more information about working with .adm files, see Recommendations for managing Group Policy administrative template (.adm) files in the Microsoft documentation.

**To install the Group Policy administrative template for PCoIP**

1. From a running Windows WorkSpace, make a copy of the pcoip.adm file in the C:\Program Files (x86)\Teradici\PCoIP Agent\configuration directory.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (gpmc.msc) and navigate to the organizational unit in your domain that contains your WorkSpaces machine accounts.
3. Open the context (right-click) menu for the machine account organizational unit and choose Create a GPO in this domain, and link it here.
4. In the New GPO dialog box, enter a descriptive name for the GPO, such as WorkSpaces Machine Policies, and leave Source Starter GPO set to (none). Choose OK.
5. Open the context (right-click) menu for the new GPO and choose Edit.
6. In the Group Policy Management Editor, choose **Computer Configuration, Policies, and Administrative Templates**. Choose **Action, Add/Remove Templates** from the main menu.

7. In the **Add/Remove Templates** dialog box, choose **Add**, select the `pcoip.adm` file copied previously, and then choose **Open, Close**.

8. Close the Group Policy Management Editor. You can now use this GPO to modify the Group Policy settings that are specific to WorkSpaces.

**To verify that the administrative template file is correctly installed**

1. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (`gpmc.msc`) and navigate to and select the WorkSpaces GPO for your WorkSpaces machine accounts. Choose **Action, Edit** in the main menu.

2. In the Group Policy Management Editor, choose **Computer Configuration, Policies, Administrative Templates, Classic Administrative Templates**, and **PCoIP Session Variables**.

3. You can now use this **PCoIP Session Variables** Group Policy object to modify the Group Policy settings that are specific to Amazon WorkSpaces when using PCoIP.

   **Note**
   To allow the user to override your settings, choose **Overridable Administrator Settings**; otherwise, choose **Not Overridable Administrator Settings**.

**Install the Group Policy administrative template for PCoIP (64-Bit)**

To use the Group Policy settings that are specific to WorkSpaces when using the PCoIP protocol, you must add the Group Policy administrative template `PCoIP.admx` and `PCoIP.adml` files for PCoIP to the Central Store of the domain controller for your WorkSpaces directory. For more information about `.admx` and `.adml` files, see [How to create and manage the Central Store for Group Policy Administrative Templates in Windows](#).

The following procedure describes how to create the Central Store and add the administrative template files to it. Perform the following procedure on a directory administration WorkSpace or Amazon EC2 instance that is joined to your WorkSpaces directory.

**To install the Group Policy administrative template files for PCoIP**

1. From a running Windows WorkSpace, make a copy of the `PCoIP.admx` and `PCoIP.adml` files in the `C:\Program Files\Teradici\PCoIP Agent\configuration\policyDefinitions` directory. The `PCoIP.adml` file is in the `en-US` subfolder of that directory.

2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open Windows File Explorer, and in the address bar, enter your organization's fully qualified domain name (FQDN), such as `\example.com`.

3. Open the `sysvol` folder.

4. Open the folder with the **FQDN** name.

5. Open the `Policies` folder. You should now be in `\FQDN\sysvol\FQDN\Policies`.

6. If it doesn't already exist, create a folder named `PolicyDefinitions`.

7. Open the `PolicyDefinitions` folder.

8. Copy the `PCoIP.admx` file into the `\FQDN\sysvol\FQDN\Policies\PolicyDefinitions` folder.


10. Open the `en-US` folder.

11. Copy the `PCoIP.adml` file into the `\FQDN\sysvol\FQDN\Policies\PolicyDefinitions\en-US` folder.
To verify that the administrative template files are correctly installed

1. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (gpmc.msc).
2. Expand the forest (Forest: FQDN).
3. Expand Domains.
4. Expand your FQDN (for example, example.com).
5. Expand Group Policy Objects.
6. Select Default Domain Policy, open the context (right-click) menu, and choose Edit.

   Note
   If the domain backing the WorkSpaces is an AWS Managed Microsoft AD directory, you cannot use the Default Domain Policy to create your GPO. Instead, you must create and link the GPO under the domain container that has delegated privileges. When you create a directory with AWS Managed Microsoft AD, AWS Directory Service creates a yourdomainname organizational unit (OU) under the domain root. The name of this OU is based on the NetBIOS name that you typed when you created your directory. If you didn't specify a NetBIOS name, it will default to the first part of your Directory DNS name (for example, in the case of corp.example.com, the NetBIOS name is corp). To create your GPO, instead of selecting Default Domain Policy, select the yourdomainname OU (or any OU under that one), open the context (right-click) menu, and choose Create a GPO in this domain, and Link it here.
   For more information about the yourdomainname OU, see What Gets Created in the AWS Directory Service Administration Guide.

7. In the Group Policy Management Editor, choose Computer Configuration, Policies, Administrative Templates, and PCoIP Session Variables.
8. You can now use this PCoIP Session Variables Group Policy object to modify the Group Policy settings that are specific to WorkSpaces when using PCoIP.

   Note
   To allow the user to override your settings, choose Overridable Administrator Settings; otherwise, choose Not Overridable Administrator Settings.

Configure printer support for PCoIP

By default, WorkSpaces enables Basic remote printing, which offers limited printing capabilities because it uses a generic printer driver on the host side to ensure compatible printing.

Advanced remote printing for Windows clients lets you use specific features of your printer, such as double-sided printing, but it requires installation of the matching printer driver on the host side.

Remote printing is implemented as a virtual channel. If virtual channels are disabled, remote printing does not function.

For Windows WorkSpaces, you can use Group Policy settings to configure printer support as needed.

To configure printer support

1. Make sure that you've installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) (p. 127) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit) (p. 128).
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (gpmc.msc) and navigate to PCoIP Session Variables.
3. Open the Configure remote printing setting.
4. In the **Configure remote printing** dialog box, do one of the following:
   - To enable Advanced remote printing, choose **Enabled**, and then under **Options, Configure remote printing**, choose **Basic and Advanced printing for Windows clients**. To automatically use the client computer's current default printer, select **Automatically set default printer**.
   - To disable printing, choose **Enabled**, and then under **Options, Configure remote printing**, choose **Printing disabled**.

5. Choose **OK**.

6. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions, Reboot WorkSpaces**).
   - In an administrative command prompt, enter `gpupdate /force`.

By default, local printer auto-redirection is disabled. You can use Group Policy settings to enable this feature so that your local printer is set as the default printer every time that you connect to your WorkSpace.

**Note**

Local printer redirection is not available for Amazon Linux WorkSpaces.

### To enable local printer auto-redirection

1. Make sure that you've installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) (p. 127) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit) (p. 128).

2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**) and navigate to **PCoIP Session Variables**.

3. Open the **Configure remote printing** setting.

4. Choose **Enabled**, and then under **Options, Configure remote printing**, choose one of the following:
   - **Basic and Advanced printing for Windows clients**
   - **Basic printing**

5. Select **Automatically set default printer**, and then choose **OK**.

6. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions, Reboot WorkSpaces**).
   - In an administrative command prompt, enter `gpupdate /force`.

### Enable or disable clipboard redirection for PCoIP

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

### To enable or disable clipboard redirection

1. Make sure that you've installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) (p. 127) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit) (p. 128).
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (\gpmc.msc\) and navigate to **PCoIP Session Variables**.

3. Open the **Configure clipboard redirection** setting.

4. In the **Configure clipboard redirection** dialog box, choose **Enabled** and then choose one of the following settings to determine the direction in which clipboard redirection is allowed. When you're done, choose **OK**.
   - Disabled in both directions
   - Enabled agent to client only (WorkSpace to local computer)
   - Enabled client to agent only (local computer to WorkSpace)
   - Enabled in both directions

5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter `gpupdate /force`.

**Known limitation**

With clipboard redirection enabled on the WorkSpace, if you copy content that is larger than 890 KB from a Microsoft Office application, the application might become slow or unresponsive for up to 5 seconds.

### Set the session resume timeout for PCoIP

When using the 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 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.

#### To set the automatic session resume timeout value

1. Make sure that you've installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) (p. 127) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit) (p. 128).

2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (\gpmc.msc\) and navigate to **PCoIP Session Variables**.

3. Open the **Configure Session Automatic Reconnection Policy** setting.

4. In the **Configure Session Automatic Reconnection Policy** dialog box, choose **Enabled**, set the **Configure Session Automatic Reconnection Policy** option to the desired timeout, in minutes, and choose **OK**.

5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
install the Group Policy administrative template for PCoIP

• In an administrative command prompt, enter `gpupdate /force`.

Enable or disable audio-in redirection for PCoIP

By default, Amazon WorkSpaces supports redirecting data from a local microphone. If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

**Note**
If you have a Group Policy setting that restricts users' local logon in their WorkSpaces, audio-in won't work on your WorkSpaces. If you remove that Group Policy setting, the audio-in feature is enabled after the next reboot of the WorkSpace. For more information about this Group Policy setting, see Allow logon locally in the Microsoft documentation.

To enable or disable audio-in redirection

1. Make sure that you’ve installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) (p. 127) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit) (p. 128).
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (`gpmc.msc`) and navigate to PCoIP Session Variables.
3. Open the Enable/disable audio in the PCoIP session setting.
4. In the Enable/disable audio in the PCoIP session dialog box, choose Enabled or Disabled.
5. Choose OK.
6. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   • Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose Actions, Reboot WorkSpaces).
   • In an administrative command prompt, enter `gpupdate /force`.

Disable time zone redirection for PCoIP

By default, the time within a Workspace is set to mirror the time zone of the client that is being used to connect to the WorkSpace. This behavior is controlled through time zone redirection. You might want to turn off time zone direction for various reasons:

• Your company wants all employees to work in a certain time zone (even if some employees are in other time zones).
• You have scheduled tasks in a WorkSpace that are meant to run at a certain time in a specific time zone.
• Your users who travel a lot want to keep their WorkSpaces in one time zone for consistency and personal preference.

If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

To disable time zone redirection

1. Make sure that you’ve installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) (p. 127) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit) (p. 128).
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (gpmc.msc) and navigate to PCoIP Session Variables.

3. Open the **Configure timezone redirection** setting.

4. In the **Configure timezone redirection** dialog box, choose **Disabled**.

5. Choose **OK**.

6. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

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

7. Set the time zone for the WorkSpaces to the desired time zone.

The time zone of the WorkSpaces is now static and no longer mirrors the time zone of the client machines.

**Configure PCoIP security settings**

For PCoIP, data in transit is encrypted using TLS 1.2 encryption and SigV4 request signing. The PCoIP protocol uses encrypted UDP traffic, with AES encryption, for streaming pixels. The streaming connection, using port 4172 (TCP and UDP), is encrypted by using AES-128 and AES-256 ciphers, but the encryption defaults to 128-bit. You can change this default to 256-bit by using the **Configure PCoIP Security Settings** Group Policy setting.

You can also use this Group Policy setting to modify the TLS Security Mode and to block certain cipher suites. A detailed explanation of these settings and the supported cipher suites is provided in the **Configure PCoIP Security Settings** Group Policy dialog box.

**To configure PCoIP security settings**

1. Make sure that you've installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) (p. 127) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit) (p. 128).

2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (gpmc.msc) and navigate to PCoIP Session Variables.

3. Open the **Configure PCoIP Security Settings** setting.

4. In the **Configure PCoIP Security Settings** dialog box, choose **Enabled**. To set the default encryption for streaming traffic to 256-bit, go to the **PCoIP Data Encryption Ciphers** option, and select AES-256-GCM only.

5. (Optional) Adjust the **TLS Security Mode** setting, and then list any cipher suites that you want to block. For more information about these settings, see the descriptions provided in the **Configure PCoIP Security Settings** dialog box.

6. Choose **OK**.

7. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter `gpupdate /force`. 
Enable USB redirection for YubiKey U2F

**Note**
Amazon WorkSpaces currently supports USB redirection only for YubiKey U2F. Other types of USB devices might be redirected but they are not supported and might not work properly.

**To enable USB redirection for YubiKey U2F**

1. Make sure that you’ve installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) (p. 127) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit) (p. 128).
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (\gpmc.msc\) and navigate to PCoIP Session Variables.
3. Open the Enable/disable USB in the PCOIP session setting.
4. Choose Enabled, and then choose OK.
5. Open the Configure PCoIP USB allowed and unallowed device rules setting.
6. Choose Enabled, and under Enter the USB authorization table (maximum ten rules), configure your USB device allowlist rules.
   - Authorization rule - 110500407. This value is a combination of a Vendor ID (VID) and a Product ID (PID). The format for a VID/PID combination is 1xxxxyyyy, where xxxx is the VID in hexadecimal format and yyyy is the PID in hexadecimal format. For this example, 1050 is the VID, and 0407 is the PID. For more YubiKey USB values, see YubiKey USB ID Values.
7. Under Enter the USB authorization table (maximum ten rules), configure your USB device blocklist rules.
   - For Unauthorization Rule, set an empty string. This means that only USB devices in the authorization list are allowed.
   - Note
      You can define a maximum of 10 USB authorization rules and a maximum of 10 USB unauthorization rules. Use the vertical bar (|) character to separate multiple rules. For detailed information about the authorization/unauthorization rules, see Teradici PCoIP Standard Agent for Windows.
8. Choose OK.
9. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose Actions, Reboot WorkSpaces).
   - In an administrative command prompt, enter `gpupdate /force`.

After the setting takes effect, all supported USB devices will be able to be redirected to WorkSpaces unless restrictions are configured through the USB device rules setting.

Install the Group Policy administrative template files for the WorkSpaces Streaming Protocol (WSP)

To use the Group Policy settings that are specific to WorkSpaces when using the WorkSpaces Streaming Protocol (WSP), you must add the Group Policy administrative template `wsp.admx` and `wsp.adml` files for WSP to the Central Store of the domain controller for your WorkSpaces directory. For more
information about .admx and .adml files, see How to create and manage the Central Store for Group Policy Administrative Templates in Windows.

The following procedure describes how to create the Central Store and add the administrative template files to it. Perform the following procedure on a directory administration WorkSpace or Amazon EC2 instance that is joined to your WorkSpaces directory.

**To install the Group Policy administrative template files for WSP**

1. From a running Windows WorkSpace, make a copy of the wsp.admx and wsp.adml files in the C:\Program Files\Amazon\WSP directory.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open Windows File Explorer, and in the address bar, enter your organization's fully qualified domain name (FQDN), such as \example.com.
3. Open the sysvol folder.
4. Open the folder with the FQDN name.
5. Open the Policies folder. You should now be in \FQDN\sysvol\FQDN\Policies.
6. If it doesn’t already exist, create a folder named PolicyDefinitions.
7. Open the PolicyDefinitions folder.
8. Copy the wsp.admx file into the \FQDN\sysvol\FQDN\Policies\PolicyDefinitions folder.
10. Open the en-US folder.
11. Copy the wsp.adml file into the \FQDN\sysvol\FQDN\Policies\PolicyDefinitions\en-US folder.

**To verify that the administrative template files are correctly installed**

1. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (gpmc.msc).
2. Expand the forest (Forest:FQDN).
3. Expand Domains.
4. Expand your FQDN (for example, example.com).
5. Expand Group Policy Objects.
6. Select Default Domain Policy, open the context (right-click) menu, and choose Edit.

   **Note**
   
   If the domain backing the WorkSpaces is an AWS Managed Microsoft AD directory, you cannot use the Default Domain Policy to create your GPO. Instead, you must create and link the GPO under the domain container that has delegated privileges.

   When you create a directory with AWS Managed Microsoft AD, AWS Directory Service creates a yourdomainname organizational unit (OU) under the domain root. The name of this OU is based on the NetBIOS name that you typed when you created your directory. If you didn’t specify a NetBIOS name, it will default to the first part of your Directory DNS name (for example, in the case of corp.example.com, the NetBIOS name is corp). To create your GPO, instead of selecting Default Domain Policy, select the yourdomainname OU (or any OU under that one), open the context (right-click) menu, and choose Create a GPO in this domain, and Link it here.

   For more information about the yourdomainname OU, see What Gets Created in the AWS Directory Service Administration Guide.

7. In the Group Policy Management Editor, choose Computer Configuration, Policies, Administrative Templates, Amazon, and WSP.
8. You can now use this WSP Group Policy object to modify the Group Policy settings that are specific to WorkSpaces when using WSP.
Configure printer support for WSP

By default, WorkSpaces enables Basic remote printing, which offers limited printing capabilities because it uses a generic printer driver on the host side to ensure compatible printing.

Advanced remote printing for Windows clients (not available for WSP) lets you use specific features of your printer, such as double-sided printing, but it requires installation of the matching printer driver on the host side.

Remote printing is implemented as a virtual channel. If virtual channels are disabled, remote printing does not function.

For Windows WorkSpaces, you can use Group Policy settings to configure printer support as needed.

To configure printer support

1. Make sure that the most recent WorkSpaces Group Policy administrative template for WSP (p. 134) is installed in the Central Store of the domain controller for your WorkSpaces directory.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (gpmc.msc).
3. Expand the forest (Forest: FQDN).
4. Expand Domains.
5. Expand your FQDN (for example, example.com).
7. Select Default Domain Policy, open the context (right-click) menu, and choose Edit.
   
   Note
   If the domain backing the WorkSpaces is an AWS Managed Microsoft AD directory, you cannot use the Default Domain Policy to create your GPO. Instead, select the yourdomainname OU (or any OU under that one), open the context (right-click) menu, and choose Create a GPO in this domain, and Link it here. For more information about the yourdomainname OU, see What Gets Created in the AWS Directory Service Administration Guide.
8. In the Group Policy Management Editor, choose Computer Configuration, Policies, Administrative Templates, Amazon, and WSP.
9. Open the Configure remote printing setting.
10. In the Configure remote printing dialog box, do one of the following:
    • To enable local printer redirection, choose Enabled, and then for Printing options, choose Basic. To automatically use the client computer's current default printer, select Map local default printer to the remote host.
    • To disable printing, choose Disabled.
11. Choose OK.
12. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
    • Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose Actions, Reboot WorkSpaces).
    • In an administrative command prompt, enter gpupdate /force.

Enable or disable clipboard redirection for WSP

By default, WorkSpaces supports two-way (copy/paste) clipboard redirection. If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.
To enable or disable clipboard redirection for Windows WorkSpaces

1. Make sure that the most recent WorkSpaces Group Policy administrative template for WSP (p. 134) is installed in the Central Store of the domain controller for your WorkSpaces directory.

2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (gpmc.msc).

3. Expand the forest (Forest:FQDN).

4. Expand Domains.

5. Expand your FQDN (for example, example.com).


7. Select Default Domain Policy, open the context (right-click) menu, and choose Edit.

   **Note**
   If the domain backing the WorkSpaces is an AWS Managed Microsoft AD directory, you cannot use the Default Domain Policy to create your GPO. Instead, select the yourdomainname OU (or any OU under that one), open the context (right-click) menu, and choose Create a GPO in this domain, and Link it here. For more information about the yourdomainname OU, see What Gets Created in the AWS Directory Service Administration Guide.

8. In the Group Policy Management Editor, choose Computer Configuration, Policies, Administrative Templates, Amazon, and WSP.

9. Open the Enable/disable clipboard redirection setting.

10. In the Enable/disable clipboard redirection dialog box, choose Enabled or Disabled.

11. Choose OK.

12. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

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

**Known limitation**

With clipboard redirection enabled on the WorkSpace, if you copy content that is larger than 890 KB from a Microsoft Office application, the application might become slow or unresponsive for up to 5 seconds.

**Set the session resume timeout for WSP**

When using the 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 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 (1200 seconds), but you can modify that value for WorkSpaces that are controlled by your domain’s Group Policy settings.

**To set the automatic session resume timeout value**

1. Make sure that the most recent WorkSpaces Group Policy administrative template for WSP (p. 134) is installed in the Central Store of the domain controller for your WorkSpaces directory.

2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (gpmc.msc).

3. Expand the forest (Forest:FQDN).
4. Expand **Domains**.
5. Expand your FQDN (for example, `example.com`).
6. Expand **Group Policy Objects**.
7. Select **Default Domain Policy**, open the context (right-click) menu, and choose **Edit**.

**Note**
If the domain backing the WorkSpaces is an AWS Managed Microsoft AD directory, you cannot use the Default Domain Policy to create your GPO. Instead, select the `yourdomainname` OU (or any OU under that one), open the context (right-click) menu, and choose **Create a GPO in this domain, and Link it here**. For more information about the `yourdomainname` OU, see **What Gets Created** in the *AWS Directory Service Administration Guide*.

8. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
9. Open the **Enable/disable automatic reconnect** setting.
10. In the **Enable/disable automatic reconnect** dialog box, choose **Enabled**, and then set **Reconnect timeout (seconds)** to the desired timeout in seconds.
11. Choose **OK**.

The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

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

### Enable or disable video-in redirection for WSP

By default, WorkSpaces supports redirecting data from a local camera. If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

**To enable or disable video-in redirection for Windows WorkSpaces**

1. Make sure that the most recent *WorkSpaces Group Policy administrative template for WSP* (p. 134) is installed in the Central Store of the domain controller for your WorkSpaces directory.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (`gpmc.msc`).
3. Expand the forest (**Forest:** `FQDN`).
4. Expand **Domains**.
5. Expand your FQDN (for example, `example.com`).
6. Expand **Group Policy Objects**.
7. Select **Default Domain Policy**, open the context (right-click) menu, and choose **Edit**.

**Note**
If the domain backing the WorkSpaces is an AWS Managed Microsoft AD directory, you cannot use the Default Domain Policy to create your GPO. Instead, select the `yourdomainname` OU (or any OU under that one), open the context (right-click) menu, and choose **Create a GPO in this domain, and Link it here**. For more information about the `yourdomainname` OU, see **What Gets Created** in the *AWS Directory Service Administration Guide*.

8. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Amazon**, and **WSP**.
9. Open the **Enable/disable video-in redirection** setting.
10. In the **Enable/disable video-in redirection** dialog box, choose **Enabled** or **Disabled**.
11. Choose **OK**.
12. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions, Reboot WorkSpaces**).
   - In an administrative command prompt, enter `gpupdate /force`.

### Enable or disable audio-in redirection for WSP

By default, WorkSpaces supports redirecting data from a local microphone. If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

**To enable or disable audio-in redirection for Windows WorkSpaces**

1. Make sure that the most recent WorkSpaces Group Policy administrative template for WSP (p. 134) is installed in the Central Store of the domain controller for your WorkSpaces directory.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**).
3. Expand the forest (**Forest:FQDN**).
4. Expand **Domains**.
5. Expand your FQDN (for example, **example.com**).
6. Expand **Group Policy Objects**.
7. Select **Default Domain Policy**, open the context (right-click) menu, and choose **Edit**.
   
   **Note**
   If the domain backing the WorkSpaces is an AWS Managed Microsoft AD directory, you cannot use the Default Domain Policy to create your GPO. Instead, select the **yourdomainname** OU (or any OU under that one), open the context (right-click) menu, and choose **Create a GPO in this domain, and Link it here**. For more information about the **yourdomainname** OU, see What Gets Created in the AWS Directory Service Administration Guide.
8. In the Group Policy Management Editor, choose **Computer Configuration, Policies, Administrative Templates, Amazon, and WSP**.
9. Open the **Enable/disable audio-in redirection** setting.
10. In the **Enable/disable audio-in redirection** dialog box, choose **Enabled** or **Disabled**.
11. Choose **OK**.
12. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions, Reboot WorkSpaces**).
   - In an administrative command prompt, enter `gpupdate /force`.

### Disable time zone redirection for WSP

By default, the time within a Workspace is set to mirror the time zone of the client that is being used to connect to the WorkSpace. This behavior is controlled through time zone redirection. You might want to turn off time zone direction for various reasons:
• Your company wants all employees to work in a certain time zone (even if some employees are in other time zones).
• You have scheduled tasks in a WorkSpace that are meant to run at a certain time in a specific time zone.
• Your users who travel a lot want to keep their WorkSpaces in one time zone for consistency and personal preference.

If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

To disable time zone redirection for Windows WorkSpaces

1. Make sure that the most recent WorkSpaces Group Policy administrative template for WSP (p. 134) is installed in the Central Store of the domain controller for your WorkSpaces directory.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (gpmc.msc).
3. Expand the forest (Forest: FQDN).
4. Expand Domains.
5. Expand your FQDN (for example, example.com).
7. Select Default Domain Policy, open the context (right-click) menu, and choose Edit.
   
   Note
   If the domain backing the WorkSpaces is an AWS Managed Microsoft AD directory, you cannot use the Default Domain Policy to create your GPO. Instead, select the yourdomainname OU (or any OU under that one), open the context (right-click) menu, and choose Create a GPO in this domain, and Link it here. For more information about the yourdomainname OU, see What Gets Created in the AWS Directory Service Administration Guide.
8. In the Group Policy Management Editor, choose Computer Configuration, Policies, Administrative Templates, Amazon, and WSP.
9. Open the Enable/disable time zone redirection setting.
10. In the Enable/disable time zone redirection dialog box, choose Disabled.
11. Choose OK.
12. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   • Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose Actions, Reboot WorkSpaces).
   • In an administrative command prompt, enter gpupdate /force.
13. Set the time zone for the WorkSpaces to the desired time zone.

The time zone of the WorkSpaces is now static and no longer mirrors the time zone of the client machines.

Enable or disable smart card redirection for WSP

By default, Amazon WorkSpaces are not enabled to support the use of smart cards for either pre-session authentication or in-session authentication. Pre-session authentication refers to smart card authentication that’s performed while users are logging in to their WorkSpaces. In-session authentication refers to authentication that’s performed after logging in.
If needed, you can enable pre-session and in-session authentication for Windows WorkSpaces by using Group Policy settings. Pre-session authentication must also be enabled through your AD Connector directory settings by using the `EnableClientAuthentication` API action or the `enable-client-authentication` AWS CLI command. For more information, see Enable Smart Card Authentication for AD Connector in the AWS Directory Service Administration Guide.

**Note**
To enable the use of smart cards with Windows WorkSpaces, additional steps are required. For more information, see Use smart cards for authentication (p. 66).

### To enable or disable smart card redirection for Windows WorkSpaces

1. Make sure that the most recent WorkSpaces Group Policy administrative template for WSP (p. 134) is installed in the Central Store of the domain controller for your WorkSpaces directory.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (`gpmc.msc`).
3. Expand the forest (`Forest: FQDN`).
4. Expand Domains.
5. Expand your FQDN (for example, `example.com`).
7. Select Default Domain Policy, open the context (right-click) menu, and choose Edit.

   **Note**
   If the domain backing the WorkSpaces is an AWS Managed Microsoft AD directory, you cannot use the Default Domain Policy to create your GPO. Instead, select the `yourdomainname` OU (or any OU under that one), open the context (right-click) menu, and choose Create a GPO in this domain, and Link it here. For more information about the `yourdomainname` OU, see What Gets Created in the AWS Directory Service Administration Guide.

8. In the Group Policy Management Editor, choose Computer Configuration, Policies, Administrative Templates, Amazon, and WSP.
9. Open the Enable/disable smart card redirection setting.
10. In the Enable/disable smart card redirection dialog box, choose Enabled or Disabled.
11. Choose OK.
12. The Group Policy setting change takes effect after the WorkSpace session is restarted. To apply the Group Policy change, reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose Actions, Reboot WorkSpaces).

### Enable or disable disconnect session on screen lock for WSP

If needed, you can disconnect users' WorkSpaces sessions when the Windows lock screen is detected. To reconnect from the WorkSpaces client, users can use their passwords or their smart cards to authenticate themselves, depending on which type of authentication has been enabled for their WorkSpaces.

This Group Policy setting is disabled by default. If needed, you can enable disconnecting the session when the Windows lock screen is detected for Windows WorkSpaces by using Group Policy settings.

**Note**

- This Group Policy setting is available only in the AWS GovCloud (US-West) Region at this time.
- This Group Policy setting applies to both password-authenticated and smart card-authenticated sessions.
- To enable the use of smart cards with Windows WorkSpaces, additional steps are required. For more information, see Use smart cards for authentication (p. 66).
To enable or disable disconnect session on screen lock for Windows WorkSpaces

1. Make sure that the most recent WorkSpaces Group Policy administrative template for WSP (p. 134) is installed in the Central Store of the domain controller for your WorkSpaces directory.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (gpmc.msc).
3. Expand the forest (Forest: FQDN).
4. Expand Domains.
5. Expand your FQDN (for example, example.com).
7. Select Default Domain Policy, open the context (right-click) menu, and choose Edit.
   
   Note
   If the domain backing the WorkSpaces is an AWS Managed Microsoft AD directory, you cannot use the Default Domain Policy to create your GPO. Instead, select the yourdomainname OU (or any OU under that one), open the context (right-click) menu, and choose Create a GPO in this domain, and Link it here. For more information about the yourdomainname OU, see What Gets Created in the AWS Directory Service Administration Guide.

8. In the Group Policy Management Editor, choose Computer Configuration, Policies, Administrative Templates, Amazon, and WSP.
9. Open the Enable/disable disconnect session on screen lock setting.
10. In the Enable/disable disconnect session on screen lock dialog box, choose Enabled or Disabled.
11. Choose OK.
12. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose Actions, Reboot WorkSpaces).
   - In an administrative command prompt, enter gpupdate /force.

Set the maximum lifetime for a Kerberos ticket

If you have not disabled the Remember Me feature of your Windows WorkSpaces, your WorkSpace users can use the Remember Me or Keep me logged in check box in their WorkSpaces client application to save their credentials. This feature allows users to easily connect to their WorkSpaces while the client application remains running. Their credentials are securely cached up to the maximum lifetime of their Kerberos tickets.

If your WorkSpace uses an AD Connector directory, you can modify the maximum lifetime of the Kerberos tickets for your WorkSpaces users through Group Policy by following the steps in Maximum Lifetime for a User Ticket in the Microsoft Windows documentation.

To enable or disable the Remember Me feature, see Enable self-service WorkSpace management capabilities for your users (p. 120).

Configure device proxy server settings for internet access

By default, the WorkSpaces Windows client application uses the proxy server that’s specified in the device operating system settings for HTTPS (port 443) traffic. The Amazon WorkSpaces client applications use the HTTPS port for updates, registration, and authentication.
Note

- The desktop streaming connections to the WorkSpace require ports 4172 and 4195 to be enabled, and do not go through the proxy server.
- Proxy servers that require authentication with a username and password are not supported.

You can configure the device proxy server settings for your Windows WorkSpaces through Group Policy by following the steps in Configure device proxy and internet connectivity settings in the Microsoft documentation.

For more information about configuring the proxy settings in the WorkSpaces Windows client application, see Proxy Server in the Amazon WorkSpaces User Guide.

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.

Note

Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) bundles are available only in the AWS GovCloud (US-West) Region at this time.

Linux WorkSpaces on WSP currently have the following limitations:

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

Control PCoIP Agent behavior on Amazon Linux WorkSpaces

The behavior of the PCoIP Agent is controlled by configuration settings in the `pcoip-agent.conf` file, which is located in the `/etc/pcoip-agent/` directory. To deploy and enforce changes to the policy, use a configuration management solution that supports Amazon Linux. Any changes take effect when the agent starts up. Restarting the agent ends any open connections and restarts the window manager. To apply any changes, we recommend rebooting the WorkSpace.

Note

If you make incorrect or unsupported changes to the `pcoip-agent.conf` file, you might cause your WorkSpace to stop working. If your WorkSpace stops working, you might need to either connect to your WorkSpace using SSH (p. 82) to roll back the changes, or you might have to rebuild the WorkSpace (p. 167).

The following sections describe how to enable or disable certain features. For a full listing of the available settings, run `man pcoip-agent.conf` from the terminal on any Amazon Linux WorkSpace.
Enable or disable clipboard redirection for Amazon Linux WorkSpaces

By default, WorkSpaces supports clipboard redirection. Use the PCoIP Agent conf to disable this feature, if needed. This setting takes effect when you reboot the WorkSpace.

**Note**
Clipboard redirection is not currently supported on Linux WorkSpaces using WSP.

**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.

   ```bash
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Add the following line to the end of the file.

   ```
pcoip.server_clipboard_state = X
   ```

   Where the possible values for `X` are:
   - 0 — Disabled in both directions
   - 1 — Enabled in both directions
   - 2 — Enabled client to agent only (allow copy and paste only from local client device to the remote host desktop)
   - 3 — Enabled agent to client only (allow copy and paste only from the remote host desktop to the local client device)

**Note**
Clipboard redirection is implemented as a virtual channel. If virtual channels are disabled, clipboard redirection doesn't work. To enable virtual channels, see [PCoIP Virtual Channels](#) in the Teradici documentation.

Enable or disable audio-in redirection for Amazon Linux WorkSpaces

By default, WorkSpaces supports audio-in redirection. Use the PCoIP Agent conf to disable this feature, if needed. This setting takes effect when you reboot the WorkSpace.

**Note**
Audio-in redirection is not currently supported on Linux WorkSpaces using WSP.

**To enable or disable audio-in redirection for Amazon Linux WorkSpaces**

1. Open the `pcoip-agent.conf` file in an editor with elevated rights by using the following command.

   ```bash
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```
2. Add the following line to the end of the file.

```
pcoip.enable_audio = x
```

Where the possible values for \(x\) are:

- \(0\) — Disabled
- \(1\) — Enabled

**Enable or disable time zone redirection for Amazon Linux WorkSpaces**

By default, the time within a Workspace is set to mirror the time zone of the client that is being used to connect to the WorkSpace. This behavior is controlled through time zone redirection. You might want to turn off time zone direction for various reasons:

- Your company wants all employees to work in a certain time zone (even if some employees are in other time zones).
- You have scheduled tasks in a WorkSpace that are meant to run at a certain time in a specific time zone.
- Your users who travel a lot want to keep their WorkSpaces in one time zone for consistency and personal preference.

If needed for Linux WorkSpaces, you can use the PCoIP Agent conf to disable this feature. This setting takes effect when you reboot the WorkSpace.

**Note**

Time zone redirection is not currently supported on Linux WorkSpaces using WSP.

**To enable or disable time zone 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.

```
pcoip.enable_timezone_redirect= x
```

Where the possible values for \(x\) are:

- \(0\) — Disabled
- \(1\) — Enabled

**Grant SSH access to Amazon Linux WorkSpaces administrators**

By default, only assigned users and accounts in the Domain Admins group can connect to Amazon Linux WorkSpaces by using SSH.
We recommend that you create a dedicated administrators group for your Amazon Linux WorkSpaces administrators in Active Directory.

To enable sudo access for members of the Linux_Workspaces_Admins Active Directory group

1. Edit the sudoers file by using visudo, as shown in the following example.

   ```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
   ```

For more information about enabling SSH connections, see Enable SSH connections for your Linux WorkSpaces (p. 82).

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`.

```bash
export SHELL=$(which zsh)
[ -n "#$SSH_TTY" ] && exec $SHELL
```

Note

After making this change, you must either reboot the WorkSpace or log out of the WorkSpace (not just disconnect) and then log back in for the change to take effect.

Protect custom repositories from unauthorized access

To control access to your custom repositories, we recommend using the security features built into Amazon Virtual Private Cloud (Amazon VPC) rather than using passwords. For example, use network access control lists (ACLs) and security groups. For more information about these features, see Security in the Amazon VPC User Guide.

If you must use passwords to protect your repositories, be sure to create your `yum` repository definition files as shown in Repository Definition Files in the Fedora documentation.
Use the Amazon Linux Extras Library repository

With Amazon Linux, you can use the Extras Library to install application and software updates on your instances. For information about using the Extras Library, see Extras Library (Amazon Linux) in the Amazon EC2 User Guide for Linux Instances.

**Note**
If you are using the Amazon Linux repository, your Amazon Linux WorkSpaces must have internet access, or you must configure virtual private cloud (VPC) endpoints to this repository and to the main Amazon Linux repository. For more information, see Provide internet access from your WorkSpace (p. 74).

Use smart cards for authentication on Linux WorkSpaces

Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) bundles allow the use of Common Access Card (CAC) and Personal Identity Verification (PIV) smart cards for authentication. For more information, see Use smart cards for authentication (p. 66).

Manage the WorkSpace running mode

The *running mode* of a WorkSpace determines its immediate availability and how you pay for it (monthly or hourly). You can choose between the following running modes when you create the WorkSpace:

- **AlwaysOn** — Use when paying a fixed monthly fee for unlimited usage of your WorkSpaces. This mode is best for users who use their WorkSpace full time as their primary desktop.
- **AutoStop** — Use when paying for your WorkSpaces by the hour. With this mode, your WorkSpaces stop after a specified period of disconnection, and the state of apps and data is saved.

For more information, see WorkSpaces Pricing.

**AutoStop WorkSpaces**

To set the automatic stop time, select the WorkSpace in the Amazon WorkSpaces console, choose **Actions, Modify Running Mode Properties**, and then set **AutoStop Time (hours)**. By default, **AutoStop Time (hours)** is set to 1 hour, which means that the WorkSpace is automatically stopped 1 hour after the WorkSpace has been disconnected.

After a WorkSpace is disconnected and the AutoStop Time period has expired, it might take several additional minutes for the WorkSpace to be automatically stopped. However, billing stops as soon as the AutoStop Time period expires, and you aren't charged for that additional time.

When possible, the state of the desktop is saved to the root volume of the WorkSpace. The WorkSpace resumes when a user logs in, and all open documents and running programs return to their saved state.

AutoStop Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro WorkSpaces do not preserve the state of data and programs when they stop. For these Autostop WorkSpaces, we recommend saving your work when you're done using them each time.

For Bring Your Own License (BYOL) AutoStop WorkSpaces, a large number of concurrent logins could result in significantly increased time for WorkSpaces to be available. If you expect many users to log into your BYOL AutoStop WorkSpaces at the same time, please consult your account manager for advice.
Important
AutoStop WorkSpaces are automatically stopped only if the WorkSpaces are disconnected.

A WorkSpace is disconnected only in the following circumstances:

- If the user manually disconnects from the WorkSpace or quits the Amazon WorkSpaces client application.
- If the client device is shut down.
- If there's no connection between the client device and the WorkSpace for more than 20 minutes.

As a best practice, AutoStop WorkSpace users should manually disconnect from their WorkSpaces when they're done using them each day. To manually disconnect, choose Disconnect WorkSpace or Quit Amazon WorkSpaces from the Amazon WorkSpaces menu in the WorkSpaces client applications for Linux, macOS, or Windows. For Android or iPad, choose Disconnect from the sidebar menu.

AutoStop WorkSpaces might not be automatically stopped in the following situations

- If the client device is only locked, sleeping, or otherwise inactive (for example, the laptop lid is closed) instead of shut down, the WorkSpaces application might still be running in the background. As long as the WorkSpaces application is still running, the WorkSpace might not be disconnected, and therefore the WorkSpace might not automatically stop.
- WorkSpaces can detect disconnection only when users are using WorkSpaces clients. If users are using third-party clients, WorkSpaces might not be able to detect disconnection, and therefore the WorkSpaces might not automatically stop and billing might not be suspended.

Modify the running mode

You can switch between running modes at any time.

To modify the running mode of a WorkSpace

2. In the navigation pane, choose WorkSpaces.
3. Select the WorkSpace to modify and choose Actions, Modify Running Mode Properties.
4. Select the new running mode, AlwaysOn or AutoStop, and then choose Modify.

To modify the running mode of a WorkSpace using the AWS CLI

Use the modify-workspace-properties command.

Stop and start an AutoStop WorkSpace

When your AutoStop WorkSpaces are disconnected, they are automatically stopped after a specified period of disconnection, and hourly billing is suspended. To further optimize costs, you can manually suspend the hourly charges associated with AutoStop WorkSpaces. The WorkSpace is stopped and all apps and data are saved for the next time a user logs in to the WorkSpace.

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

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

To stop an AutoStop WorkSpace

To modify a WorkSpace:

1. In the navigation pane, choose **WorkSpaces**.
2. Select the WorkSpace to be stopped and choose **Actions, Stop WorkSpaces**.
3. When prompted for confirmation, choose **Stop**.

To start an AutoStop WorkSpace:

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 that are associated with AutoStop WorkSpaces, remove the WorkSpace from your account. For more information, see [Delete a WorkSpace](#) (p. 179).

To stop and start an AutoStop WorkSpace using the AWS CLI

Use the `stop-WorkSpaces` and `start-WorkSpaces` commands.

### Modify a WorkSpace

After you launch a WorkSpace, you can modify its configuration in two ways:

- You can change the size of its root volume (for Windows, drive C; for Linux, /) and its user volume (for Windows, drive D; for Linux /home).
- You can change its compute type to select a new bundle.

To see the current modification state of a WorkSpace, select the arrow to show more details about that WorkSpace. The possible values for **State** are **Modifying Compute**, **Modifying Storage**, and **None**.

If you want to modify a WorkSpace, it must have a status of **AVAILABLE** or **STOPPED**. When you are modifying the volume size, you can't change the compute type at the same time, and vice versa.

Changing the volume size or compute type of a WorkSpace will change the billing rate for the WorkSpace.

To allow your users to modify their volumes and compute types themselves, see [Enable self-service WorkSpace management capabilities for your users](#) (p. 120).

### Change volume sizes

You can increase the size of the root and user volumes for a WorkSpace, up to 2000 GB each. WorkSpace root and user volumes come in set groups that can't be changed. The available groups are:

<table>
<thead>
<tr>
<th>[Root (GB), User (GB)]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[80, 10]</td>
</tr>
<tr>
<td>[80, 50]</td>
</tr>
<tr>
<td>[80, 100]</td>
</tr>
</tbody>
</table>
You can expand the root and user volumes whether they are encrypted or unencrypted, and you can expand both volumes once in a 6-hour period. However, you can't increase the size of the root and user volumes at the same time. For more information, see Limitations for Increasing Volumes (p. 150).

**Note**
When you expand a volume for a WorkSpace, WorkSpaces automatically extends the volume's partition within Windows or Linux. When the process is finished, you must reboot the WorkSpace for the changes to take effect.

To ensure that your data is preserved, you cannot decrease the size of the root or user volumes after you launch a WorkSpace. Instead, make sure that you specify the minimum sizes for these volumes when launching a WorkSpace. You can launch a Value, Standard, Performance, Power, or PowerPro WorkSpace with a minimum of 80 GB for the root volume and 10 GB for the user volume. You can launch a Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro WorkSpace with a minimum of 100 GB for the root volume and 100 GB for the user volume.

While a WorkSpace disk size increase is in progress, users can perform most tasks on their WorkSpace. However, they can't change their WorkSpace compute type, switch the WorkSpace running mode, rebuild their WorkSpace, or reboot (restart) their WorkSpace.

**Note**
If you want your users to be able to use their WorkSpaces while the disk size increase is in progress, make sure the WorkSpaces have a status of AVAILABLE instead of STOPPED before you resize the volumes of the WorkSpaces. If the WorkSpaces are STOPPED, they can't be started while the disk size increase is in progress.

In most cases, the disk size increase process might take up to two hours. However, if you're modifying the volume sizes for a large number of WorkSpaces, the process can take significantly longer. If you have a large number of WorkSpaces to modify, we recommend contacting AWS Support for assistance.

**Limitations for increasing volumes**

- You can resize only SSD volumes.
- When you launch a WorkSpace, you must wait 6 hours before you can modify the sizes of its volumes.
- You cannot increase the size of the root and user volumes at the same time. To increase the root volume, you must first change the user volume to 100 GB. After that change is made, you can then update the root volume to any value between 175 and 2000 GB. After the root volume has been changed to any value between 175 and 2000 GB, you can then update the user volume further, to any value between 100 and 2000 GB.

  **Note**
  If you want to increase both volumes, you must wait 20-30 minutes for the first operation to finish before you can start the second operation.

- Unless the WorkSpace is a Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro WorkSpace, the root volume cannot be less than 175 GB when the user volume is 100 GB. Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro WorkSpaces can have the root and user volumes both set to 100 GB minimum.
- If the user volume is 50 GB, you cannot update the root volume to anything other than 80 GB. If the root volume is 80 GB, the user volume can only be 10, 50, or 100 GB.

**To change the volume sizes of a WorkSpace**

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 value.
5. Choose **Modify**.
6. When the disk size increase is finished, you must **reboot the WorkSpace** (p. 166) for the changes to take effect. To avoid data loss, make sure the user saves any open files before you reboot the WorkSpace.

To change the volume sizes of a WorkSpace

Use the `modify-workspace-properties` command with the `RootVolumeSizeGib` or `UserVolumeSizeGib` property.

# Change bundle types

You can switch a WorkSpace between the Value, Standard, Performance, Power, and PowerPro bundles. For more information about these bundle types, see [Amazon WorkSpaces Bundles](https://aws.amazon.com/).  

**Note**

- You can change the compute type from `Graphics.g4dn` to `GraphicsPro.g4dn` and vice versa. You cannot change the compute type of `Graphics.g4dn` and `GraphicsPro.g4dn` to any other value.

- You cannot change the compute type of `Graphics` and `GraphicsPro` to any other value.

When you request a bundle change, WorkSpaces reboots the WorkSpace using the new bundle. 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.

When a WorkSpace compute type change is in progress, users are disconnected from their WorkSpace, and they can't use or change the WorkSpace. The WorkSpace is automatically rebooted during the compute type change process.

**Important**

To avoid data loss, make sure users save any open documents and other application files before you change the WorkSpace compute type.

The compute type change process might take up to an hour.

To change the bundle type of a WorkSpace

2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpace and choose **Actions, Modify WorkSpace**.
4. To change the bundle, choose **Change Compute Type** and select the new bundle type.
5. Choose **Modify**.

To change the bundle type of a WorkSpace
Use the `modify-workspace-properties` command with the `ComputeTypeName` property.

## Customize WorkSpace branding

Amazon WorkSpaces allows you to create a familiar WorkSpaces experience for your users by using APIs to customize the appearance of your WorkSpace's login page with your own branding logo, IT support information, forgot password link, and login message. Your branding will be displayed to your users in their WorkSpace login page rather than the default WorkSpaces branding.

The following clients are supported:

- Windows
- Linux
- Android
- MacOS
- iOS
- Web Access

**Note**

WorkSpaces custom branding is currently unavailable in the AWS GovCloud (US-West) Region.

### Import custom branding

To import your client branding customization, use the action `ImportClientBranding`, which includes the following elements. See [ImportClientBranding API reference](#) for more information.

**Important**

Client branding attributes are public facing. Ensure that you don't include sensitive information.
1. Support link
2. Logo
3. Forgot password link
4. Login message
### Custom branding elements

<table>
<thead>
<tr>
<th>Branding element</th>
<th>Description</th>
<th>Requirements and recommendations</th>
</tr>
</thead>
</table>
| **Support link** | Allows you to specify a support email link for users to contact for help with their WorkSpaces. You can use the SupportEmail attribute or provide a link to your support page using the SupportLink attribute. | • For each platform type, the SupportEmail and SupportLink parameters are mutually exclusive. You can specify a single parameter for each platform type, but not both.  
• The default email is workspaces-feedback@amazon.com.  
• Length constraints: Minimum length of 1. Maximum length of 200. |
| **Logo**         | Allows you to customize your organization's logo using the Logo attribute. | The only image format accepted is a binary data object that is converted from a .png file. |
| **Forgot password link** | Allows you to add a web address using the ForgotPasswordLink attribute that users can go to if they forget their password to their WorkSpace. | Length Constraints: Minimum length of 1. Maximum length of 200. |
| **Login message** | Allows you to customize a message using the LoginMessage attribute on the sign in screen. | • Length Constraints: Minimum length of 0. Maximum length of 2000 characters for integration with HTML tags and different font size. For default cases without HTML tags, it is recommended to keep the login message under 600 characters.  
• HTML tags supported: a, b, blockquote, br, cite, code, dd, dl, dt, div, em, i, li, ol, p, pre, q, small, span, strike, strong, sub, sup, u, ul |

The following are sample code snippets for using ImportClientBranding.

**AWS CLI Version 2**

**Warning**

Importing custom branding overwrites the attributes, within that platform, that you specify with your custom data. It also overwrites the attributes that you don't specify with default custom branding attribute values. You must include the data for any attribute that you don't want to overwrite.
aws workspaces import-client-branding
--cli-input-json file:///~/.Downloads/import-input.json
--region us-west-2

The import JSON file should look like the following sample code:

```
{
  "ResourceId": "<directory-id>",
  "DeviceTypeOsx": {
    "Logo": "iVBORw0KGgoAAAANSUhEUgAAAAIAAAACCAYAAABytg0kAAAAC0lEQVR42mNgQAcAABIAAeRVjecAAAAASUVORK5CYII=",
    "ForgotPasswordLink": "https://amazon.com/",
    "SupportLink": "https://amazon.com/",
    "LoginMessage": {
      "en_US": "Hello!!"
    }
  }
}
```

The follow sample Java code snippet converts the logo image into the base64bit binary format.

```
// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

//convert byte[] to base64 format and print it
String bytesBase64 = Base64.encodeBase64String(bytes);
System.out.println(bytesBase64);
```

The follow sample Python code snippet converts the logo image into the base64bit binary format.

```
# Read logo into 64bit based string
with open("~/Downloads/logo.png", "rb") as imageFile:
  f = imageFile.read()
  base64String = base64.b64encode(f)
  print(base64String)
```

**Java**

**Warning**
Importing custom branding overwrites the attributes, within that platform, that you specify with your custom data. It also overwrites the attributes that you don't specify with default custom branding attribute values. You must include the data for any attribute that you don't want to overwrite.

```java
// Create WS Client
WorkSpacesClient client = WorkSpacesClient.builder().build();

// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();
```
// Create import attributes for the platform
DefaultImportClientBrandingAttributes attributes =
    DefaultImportClientBrandingAttributes.builder()
    .logo(SdkBytes.fromByteArray(bytes))
    .forgotPasswordLink("https://aws.amazon.com/")
    .supportLink("https://aws.amazon.com/")
    .build();

// Create import request
ImportClientBrandingRequest request =
    ImportClientBrandingRequest.builder()
    .resourceId("<directory-id>")
    .deviceTypeOsx(attributes)
    .build();

// Call ImportClientBranding API
ImportClientBrandingResponse response = client.importClientBranding(request);

---

**Python**

**Warning**
Importing custom branding overwrites the attributes, within that platform, that you specify with your custom data. It also overwrites the attributes that you don't specify with default custom branding attribute values. You must include the data for any attribute that you don't want to overwrite.

```python
import boto3

# Read logo into bytearray
with open("~/Downloads/logo.png", "rb") as imageFile:
    f = imageFile.read()
    bytes = bytearray(f)

# Create workspaces client
client = boto3.client('workspaces')

# Call import API
response = client.import_client_branding(
    ResourceId='<directory-id>',
    DeviceTypeOsx={
        'Logo': bytes,
        'SupportLink': 'https://aws.amazon.com/',
        'ForgotPasswordLink': 'https://aws.amazon.com/',
        'LoginMessage': {
            'en_US': 'Hello!!'
        }
    }
)
```

---

**PowerShell**

```powershell
# This forces the latest version of Tools or newer. May want to just add a note incase the user don't have the full awspowershell module
#Requires -Modules @{ ModuleName="AWS.Tools.WorkSpaces"; ModuleVersion="4.1.56"}

# Specify Image Path
$imagePath = "~/Downloads/logo.png"

# Create Byte Array from image file
$imageByte = ($System.IO.File) ReadAllBytes($imagePath)
```
Describe custom branding

To see the details of the client branding customization you currently have, use the action DescribeCustomBranding. The following is the sample script for using DescribeClientBranding. See DescribeClientBranding API reference for more information.

```bash
aws workspaces describe-client-branding \
-resource-id directory-id \ 
-region us-west-2
```

Delete custom branding

To delete your client branding customization, use the action DeleteCustomBranding. The following is the sample script for using DeleteClientBranding. See DeleteClientBranding API reference for more information.

```bash
aws workspaces delete-client-branding \
-resource-id d-92677ad933 \ 
-platforms DeviceTypeAndroid DeviceTypeIos \ 
-region us-west-2
```

Note
Changes may take up to 1 minute to appear.

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 to organize data, including billing data.

When you add tags to an existing resource, those tags don’t appear in your cost allocation report until the first day of the following month. For example, if you add tags to an existing WorkSpace on July 15, the tags won’t appear in your cost allocation report until August 1. For more information, see Using Cost Allocation Tags in the AWS Billing User Guide.

Note
To view your WorkSpaces resource tags in the Cost Explorer, you must activate the tags that you have applied to your WorkSpaces resources by following the instructions in Activating User-Defined Cost Allocation Tags in the AWS Billing User Guide.

Although tags appear 24 hours after activation, it can take 4 to 5 days for values associated with those tags to appear in the Cost Explorer. Additionally, to appear and provide cost data in Cost
Explorer, WorkSpaces resources that have been tagged must incur charges during that time. Cost Explorer only shows cost data from the time when the tags were activated and onward. No historical data is available at this time.

Resources that you can tag

- You can add tags to the following resources when you create them—WorkSpaces, imported images, and IP access control groups.
- You can add tags to existing resources of the following types—WorkSpaces, registered directories, custom bundles, images, and IP access control groups.

Tag restrictions

- Maximum number of tags per resource—50
- Maximum key length—127 Unicode characters
- Maximum value length—255 Unicode characters
- Tag keys and values are case-sensitive. Allowed characters are letters, spaces, and numbers representable in UTF-8, plus the following special characters: + - = . _ : / @. Do not use leading or trailing spaces.
- Do not use the `aws:` or `aws:workspaces:` prefixes in your tag names or values because they are reserved for AWS use. You can't edit or delete tag names or values with these prefixes.

To update the tags for an existing resource using the console (directories, WorkSpaces, or IP access control groups)

2. In the navigation pane, choose one of the following resource types: Directories, WorkSpaces, or IP Access Controls.
3. Select the resource and choose Actions, Manage Tags.
4. Do one or more of the following:
   - To update a tag, edit the values of Key and Value.
   - To add a tag, choose Add Tag and then edit the values of Key and Value.
   - To delete a tag, choose the delete icon (X) next to the tag.
5. When you are finished updating tags, choose Save.

To update the tags for an existing resource using the console (images or bundles)

2. In the navigation pane, choose one of the following resource types: Bundles or Images.
3. Choose the resource to open its details page.
4. Under Tags, choose Manage tags.
5. Do one or more of the following:
   - To update a tag, edit the values of Key and Value.
   - To add a tag, choose Add new tag and then edit the values of Key and Value.
   - To delete a tag, choose Remove next to the tag.
6. When you are finished updating tags, choose Save changes.

To update the tags for an existing resource using the AWS CLI
Use the `create-tags` and `delete-tags` commands.

WorkSpace maintenance

We recommend that you maintain your WorkSpaces on a regular basis. WorkSpaces schedules default maintenance windows for your WorkSpaces. During the maintenance window, the WorkSpace installs important updates from Amazon WorkSpaces and reboots as necessary. If available, operating system updates are also installed from the OS update server that the WorkSpace is configured to use. During maintenance, your WorkSpaces might be unavailable.

By default, your Windows WorkSpaces are configured to receive updates from Windows Update. To configure your own automatic update mechanisms for Windows, see the documentation for Windows Server Update Services (WSUS) and Configuration Manager.

Requirement

Your WorkSpaces must have access to the internet so that you can install updates to the operating system and deploy applications. For more information, see the section called “Internet access” (p. 74).

Maintenance windows for AlwaysOn WorkSpaces

For AlwaysOn WorkSpaces, the maintenance window is determined by operating system settings. The default is a four-hour period from 00h00 to 04h00, in the time zone of the WorkSpace, each Sunday morning. By default, the time zone of an AlwaysOn WorkSpace is the time zone of the AWS Region for the WorkSpace. However, if you connect from another Region and time zone redirection is enabled, and then you disconnect, the time zone of the WorkSpace is updated to the time zone of the Region that you connected from.

You can disable time zone redirection for Windows WorkSpaces (p. 132) using Group Policy. You can disable time zone redirection for Linux WorkSpaces (p. 145) by using the PCoIP Agent conf.

For Windows WorkSpaces, you can configure the maintenance window using Group Policy; see Configure Group Policy Settings for Automatic Updates. You cannot configure the maintenance window for Linux WorkSpaces.

Maintenance windows for AutoStop WorkSpaces

AutoStop WorkSpaces are started automatically once a month in order to install important updates. Beginning on the third Monday of the month, and for up to two weeks, the maintenance window is open each day from about 00h00 to 05h00, in the time zone of the AWS Region for the WorkSpace. The WorkSpace can be maintained on any one day in the maintenance window.

During the time period when the WorkSpace is undergoing maintenance, the state of the WorkSpace is set to MAINTENANCE.

Although you cannot modify the time zone that is used for maintaining AutoStop WorkSpaces, you can disable the maintenance window for your AutoStop WorkSpaces as follows. If you disable maintenance mode, your WorkSpaces are not rebooted and do not enter the MAINTENANCE state.

To disable maintenance mode

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**.

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**

WorkSpaces is integrated with the AWS Key Management Service (AWS KMS). This enables you to encrypt storage volumes of WorkSpaces using AWS KMS Key. When you launch a WorkSpace, you can encrypt the root volume (for Microsoft Windows, the C drive; for Linux, `/`) and the user volume (for Windows, the D drive; for Linux, `/home`). Doing so ensures that the data stored at rest, disk I/O to the volume, and snapshots created from the volumes are all encrypted.

*Note*  
In addition to encrypting your WorkSpaces, you can also use FIPS endpoint encryption in certain AWS US Regions. For more information, see [Set up Amazon WorkSpaces for FedRAMP authorization or DoD SRG compliance](p. 81).

**Contents**

- Prerequisites (p. 161)
- Limits (p. 161)
- Overview of WorkSpaces encryption using AWS KMS (p. 162)
- WorkSpaces encryption context (p. 162)
- Grant WorkSpaces permission to use a KMS Key on your behalf (p. 163)
• Encrypt a WorkSpace (p. 166)
• View encrypted WorkSpaces (p. 166)

Prerequisites

You need an AWS KMS Key before you can begin the encryption process. This KMS Key can be either the
AWS managed KMS Key for Amazon WorkSpaces (aws/workspaces) or a symmetric customer managed
KMS Key.

• AWS managed KMS Keys – The first time that you launch an unencrypted WorkSpace from the
WorkSpaces console in a Region, Amazon WorkSpaces automatically creates an AWS managed KMS
Key (aws/workspaces) in your account. You can select this AWS managed KMS Key to encrypt the user
and root volumes of your WorkSpace. For details, see Overview of WorkSpaces encryption using AWS
KMS (p. 162).

You can view this AWS managed KMS Key, including its policies and grants, and can track its use in
AWS CloudTrail logs, but you cannot use or manage this KMS Key. Amazon WorkSpaces creates and
manages this KMS Key. Only Amazon WorkSpaces can use this KMS Key, and WorkSpaces can use it
only to encrypt WorkSpaces resources in your account.

AWS managed KMS Key, including the one that Amazon WorkSpaces supports, are rotated every three
years. For details, see Rotating AWS KMS Key in the AWS Key Management Service Developer Guide.

• Customer managed KMS Key – Alternatively, you can select a symmetric customer managed
KMS Key that you created using AWS KMS. You can view, use, and manage this KMS Key, including
setting its policies. For more information about creating KMS Keys, see Creating Keys in the AWS Key
Management Service Developer Guide. For more information about creating KMS Keys using the AWS
KMS API, see Working with Keys in the AWS Key Management Service Developer Guide.

Customer managed KMS Keys are not automatically rotated unless you decide to enable automatic key
rotation. For details, see Rotating AWS KMS Keys in the AWS Key Management Service Developer Guide.

Important
When you rotate KMS Keys, you must keep both the original KMS Key and the new KMS Key
enabled so that AWS KMS can decrypt the WorkSpaces that the original KMS Key encrypted. If
you don’t want to keep the original KMS Key enabled, you must recreate your WorkSpaces and
encrypt them using the new KMS Key.

You must meet the following requirements to use an AWS KMS Key to encrypt your WorkSpaces:

• The KMS Key must be symmetric. Amazon WorkSpaces does not support asymmetric KMS Keys.
For information about distinguishing between symmetric and asymmetric KMS Keys, see Identifying
Symmetric and Asymmetric KMS Keys in the AWS Key Management Service Developer Guide.

• The KMS Key must be enabled. To determine whether a KMS Key is enabled, see Displaying KMS Key
Details in the AWS Key Management Service Developer Guide.

• You must have the correct permissions and policies associated with the KMS Key. For more
information, see Part 2: Grant WorkSpaces administrators additional permissions using an IAM
policy (p. 164).

Limits

• You can’t encrypt an existing WorkSpace. You must encrypt a WorkSpace when you launch it.
• Creating a custom image from an encrypted WorkSpace is not supported.
• Disabling encryption for an encrypted WorkSpace is not currently supported.
• WorkSpaces launched with root volume encryption enabled might take up to an hour to provision.
• To reboot or rebuild an encrypted WorkSpace, first make sure that the AWS KMS KMS Key is enabled; otherwise, the WorkSpace becomes unusable. To determine whether a KMS Key is enabled, see Displaying KMS Key Details in the AWS Key Management Service Developer Guide.

Overview of WorkSpaces encryption using AWS KMS

When you create WorkSpaces with encrypted volumes, WorkSpaces uses Amazon Elastic Block Store (Amazon EBS) to create and manage those volumes. Amazon EBS encrypts your volumes with a data key using the industry-standard AES-256 algorithm. Both Amazon EBS and Amazon WorkSpaces use your KMS Key to work with the encrypted volumes. For more information about EBS volume encryption, see Amazon EBS Encryption in the Amazon EC2 User Guide for Windows Instances.

When you launch WorkSpaces with encrypted volumes, the end-to-end process works like this:

1. You specify the KMS Key to use for encryption as well as the user and directory for the WorkSpace. This action creates a grant that allows WorkSpaces to use your KMS Key only for this WorkSpace—that is, only for the WorkSpace associated with the specified user and directory.
2. WorkSpaces creates an encrypted EBS volume for the WorkSpace and specifies the KMS Key to use as well as the volume’s user and directory. This action creates a grant that allows Amazon EBS to use your KMS Key only for this WorkSpace and volume—that is, only for the WorkSpace associated with the specified user and directory, and only for the specified volume.
3. Amazon EBS requests a volume data key that is encrypted under your KMS Key and specifies the WorkSpace user’s Active Directory security identifier (SID) and AWS Directory Service directory ID as well as the Amazon EBS volume ID as the encryption context (p. 162).
4. AWS KMS creates a new data key, encrypts it under your KMS Key, and then sends the encrypted data key to Amazon EBS.
5. WorkSpaces uses Amazon EBS to attach the encrypted volume to your WorkSpace. Amazon EBS sends the encrypted data key to AWS KMS with a Decrypt request and specifies the WorkSpace user’s SID, the directory ID, and the volume ID, which is used as the encryption context.
6. AWS KMS uses your KMS Key to decrypt the data key, and then sends the plaintext data key to Amazon EBS.
7. Amazon EBS uses the plaintext data key to encrypt all data going to and from the encrypted volume. Amazon EBS keeps the plaintext data key in memory for as long as the volume is attached to the WorkSpace.
8. Amazon EBS stores the encrypted data key (received at Step 4 (p. 162)) with the volume metadata for future use in case you reboot or rebuild the WorkSpace.
9. When you use the AWS Management Console to remove a WorkSpace (or use the TerminateWorkspaces action in the WorkSpaces API), WorkSpaces and Amazon EBS retire the grants that allowed them to use your KMS Key for that WorkSpace.

WorkSpaces encryption context

WorkSpaces doesn’t use your KMS Key directly for cryptographic operations (such as Encrypt, Decrypt, GenerateDataKey, etc.), which means WorkSpaces doesn’t send requests to AWS KMS that include an encryption context. However, when Amazon EBS requests an encrypted data key for the encrypted volumes of your WorkSpaces (Step 3 (p. 162) in the Overview of WorkSpaces encryption using AWS KMS (p. 162)) and when it requests a plaintext copy of that data key (Step 5 (p. 162)), it includes encryption context in the request.

The encryption context provides additional authenticated data (AAD) that AWS KMS uses to ensure data integrity. The encryption context is also written to your AWS CloudTrail log files, which can help you understand why a given KMS Key was used. Amazon EBS uses the following for the encryption context:
Grant WorkSpaces permission to use a KMS Key on your behalf

You can protect your WorkSpace data under the AWS managed KMS Key for WorkSpaces (aws/workspaces) or a customer managed KMS Key. If you use a customer managed KMS Key, you need to grant WorkSpaces permission to use the KMS Key on behalf of the WorkSpaces administrators in your account. The AWS managed KMS Key for WorkSpaces has the required permissions by default.

To prepare your customer managed KMS Key for use with WorkSpaces, use the following procedure.

1. Add your WorkSpaces administrators to the list of key users in the KMS Key's key policy (p. 163)
2. Give your WorkSpaces administrators additional permissions with an IAM policy (p. 164)

Your WorkSpaces administrators also need permission to use WorkSpaces. For more information about these permissions, go to Identity and access management for WorkSpaces (p. 234).

Part 1: Add WorkSpaces administrators to as key users

To give WorkSpaces administrators the permissions that they require, you can use the AWS Management Console or the AWS KMS API.

To add WorkSpaces administrators as key users for a KMS Key (console)

1. Sign in to the AWS Management Console and open the AWS Key Management Service (AWS KMS) console at https://console.aws.amazon.com/kms.
2. To change the AWS Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose Customer managed keys.
4. Choose the key ID or alias of your preferred customer managed KMS Key.
5. Choose the Key policy tab. Under Key users, choose Add.
6. In the list of IAM users and roles, select the users and roles that correspond to your WorkSpaces administrators, and then choose Add.

To add WorkSpaces administrators as key users for a KMS Key (API)

1. Use the GetKeyPolicy operation to get the existing key policy, and then save the policy document to a file.
2. Open the policy document in your preferred text editor. Add the IAM users and roles that correspond to your WorkSpaces administrators to the policy statements that give permission to key users. Then save the file.
3. Use the `PutKeyPolicy` operation to apply the key policy to the KMS Key.

**Part 2: Grant WorkSpaces administrators additional permissions using an IAM policy**

If you select a customer managed KMS Key to use for encryption, you must establish IAM policies that allow Amazon WorkSpaces to use the KMS Key on behalf of an IAM user in your account who launches encrypted WorkSpaces. That user also needs permission to use Amazon WorkSpaces. For more information about creating and editing IAM user policies, see Managing IAM Policies in the IAM User Guide and Identity and access management for WorkSpaces (p. 234).

WorkSpaces encryption requires limited access to the KMS Key. The following is a sample key policy that you can use. This policy separates the principals who can manage the AWS KMS KMS Key from those who can use it. Before you use this sample key policy, replace the example account ID and IAM user name with actual values from your account.

The first statement matches the default AWS KMS key policy. It gives your account permission to use IAM policies to control access to the KMS Key. The second and third statements define which AWS principals can manage and use the key, respectively. The fourth statement enables AWS services that are integrated with AWS KMS to use the key on behalf of the specified principal. This statement enables AWS services to create and manage grants. The statement uses a condition element that limits grants on the KMS Key to those made by AWS services on behalf of users in your account.

Note

If your WorkSpaces administrators use the AWS Management Console to create WorkSpaces with encrypted volumes, the administrators need permission to list aliases and list keys (the "kms:ListAliases" and "kms:ListKeys" permissions). If your WorkSpaces administrators use only the Amazon WorkSpaces API (not the console), you can omit the "kms:ListAliases" and "kms:ListKeys" permissions.

```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"},
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
            "Resource": "*"
        }
    ]
}
```
The IAM policy for a user or role that is encrypting a WorkSpace must include usage permissions on the
customer managed KMS Key, as well as access to WorkSpaces. To give an IAM user or role WorkSpaces
permissions, you can attach the following sample policy to the IAM user or role.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:*",
        "ds:DescribeDirectories",
        "workspaces:*",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:CreateWorkspaces",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaces",
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
      ],
      "Resource": "*"
    }
  ]
}
```

The following IAM policy is required by the user for using AWS KMS. It gives the user read-only access to
the KMS Key along with the ability to create grants.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:Describe*",
        "kms:List*"
      ],
      "Resource": "*"
    }
  ]
}
```
Encrypt a WorkSpace

To encrypt a WorkSpace

2. Choose Launch WorkSpaces and complete the first three steps.
3. For the WorkSpaces Configuration step, do the following:
   a. Select the volumes to encrypt: Root Volume, User Volume, or both volumes.
   b. For Encryption Key, select an AWS KMS Key, either the AWS managed KMS Key created by Amazon WorkSpaces or a KMS Key that you created. The KMS Key that you select must be symmetric. Amazon WorkSpaces does not support asymmetric KMS Keys.
   c. Choose Next Step.

View encrypted WorkSpaces

To see which WorkSpaces and volumes have been encrypted from the WorkSpaces console, choose WorkSpaces from the navigation bar on the left. The Volume Encryption column shows whether each WorkSpace has encryption enabled or disabled. To see which specific volumes have been encrypted, expand the WorkSpace entry to see the Encrypted Volumes field.

Reboot a WorkSpace

Occasionally, you might need to reboot (restart) a WorkSpace manually. Rebooting a WorkSpace disconnects the user and then performs a shutdown and reboot of the WorkSpace. To avoid data loss, make sure the user saves any open documents and other application files before you reboot the WorkSpace. The user data, operating system, and system settings are not affected.
Warning
To reboot an encrypted WorkSpace, first make sure that the AWS KMS Key is enabled; otherwise, the WorkSpace becomes unusable. To determine whether a KMS Key is enabled, see Displaying KMS Key Details in the AWS Key Management Service Developer Guide.

To reboot a WorkSpace
2. In the navigation pane, choose WorkSpaces.
3. Select the WorkSpaces to be rebooted and choose Actions, Reboot WorkSpaces.
4. When prompted for confirmation, choose Reboot WorkSpaces.

To rebuild a WorkSpace
If needed, you can rebuild a WorkSpace. This recreates the root volume, the user volume, and the primary elastic network interface.

Rebuilding a WorkSpace causes the following to occur:

- The root volume (for Microsoft Windows, drive C; for Linux, /) is refreshed with the most recent image of the bundle that the WorkSpace was created from. Any applications that were installed, or system settings that were changed after the WorkSpace was created, are lost.
- The user volume (for Microsoft Windows, the D drive; for Linux, /home) is recreated from the most recent snapshot. The current contents of the user volume are overwritten.
- The primary elastic network interface is recreated. The WorkSpace receives a new private IP address.

Automatic snapshots for use when rebuilding a WorkSpace are scheduled every 12 hours. These snapshots of the user volume are taken regardless of the health of the WorkSpace. When you choose Actions, Rebuild / Restore WorkSpace, the date and time of the most recent snapshot is shown.

Important
After January 14, 2020, WorkSpaces created from a public Windows 7 bundle can no longer be rebuilt. You might want to consider migrating your Windows 7 WorkSpaces to Windows 10. For more information, see Migrate a WorkSpace (p. 175).

You can rebuild a WorkSpace only if the following conditions are met:

- The WorkSpace must have a state of AVAILABLE, ERROR, UNHEALTHY, STOPPED, or REBOOTING. To rebuild a WorkSpace in the REBOOTING state, you must use the RebuildWorkspaces API operation or the rebuild-workspaces AWS CLI command.
- A snapshot of the user volume must exist.

To rebuild a WorkSpace

Warning
To rebuild an encrypted WorkSpace, first make sure that the AWS KMS Key is enabled; otherwise, the WorkSpace becomes unusable. To determine whether a KMS Key is enabled, see Displaying KMS Key Details in the AWS Key Management Service Developer Guide.
2. In the navigation pane, choose WorkSpaces.
3. Select the WorkSpace to be rebuilt and choose Actions, Rebuild / Restore WorkSpace.
4. Select the Rebuild WorkSpace option.
5. Choose Rebuild / Restore WorkSpace.

To rebuild a WorkSpace using the AWS CLI

Use the rebuild-workspaces command.

Troubleshooting

If you rebuild a WorkSpace after changing the user’s sAMAccountName user naming attribute in Active Directory, you might receive the following error message:

```
"ErrorCode": "InvalidUserConfiguration.Workspace"
"ErrorMessage": "The user was either not found or is misconfigured."
```

To work around this issue, either revert to the original user naming attribute and then reinitiate the rebuild, or create a new WorkSpace for that user.

### Restore a WorkSpace

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 root volume (for Microsoft Windows, drive C; for Linux, /) is restored to the most recent snapshot. 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.

**When snapshots are taken**

Snapshots of the root and user volume are taken on the following basis. When you choose Actions, Rebuild / Restore WorkSpace, the date and time of the most recent snapshots are shown.

- **After a WorkSpace is first created** — Typically, the initial snapshots of the root and user volumes are taken soon after a WorkSpace is created (often within 30 minutes). In some AWS Regions, it might take several hours for the initial snapshots to be taken after a WorkSpace is created.

  If a WorkSpace becomes unhealthy before the initial snapshots are taken, the WorkSpace can't be restored. In that case, you can try rebuilding the WorkSpace (p. 167) or contact AWS Support for assistance.

- **During regular use** — Automatic snapshots for use when restoring a WorkSpace are scheduled every 12 hours. If the WorkSpace is healthy, snapshots of both the root volume and user volume are created around the same time. If the WorkSpace is unhealthy, snapshots are created only for the user volume.

- **After a WorkSpace has been restored** — When you restore a WorkSpace, new snapshots are taken soon after the restore is finished (often within 30 minutes). In some AWS Regions, it might take several hours for these snapshots to be taken after a WorkSpace is restored.
After a WorkSpace has been restored, if the WorkSpace becomes unhealthy before new snapshots can be taken, the WorkSpace can't be restored again. In that case, you can try rebuilding the WorkSpace (p. 167) or contact AWS Support for assistance.

You can restore a WorkSpace only if the following conditions are met:

- The WorkSpace must have a state of AVAILABLE, ERROR, UNHEALTHY, or STOPPED.
- Snapshots of the root and user volumes must exist.

**To restore a WorkSpace**

2. In the navigation pane, choose WorkSpaces.
3. Select the WorkSpace to be restored and choose Actions, Rebuild / Restore WorkSpace.
4. Select the Restore WorkSpace option.
5. Choose Rebuild / Restore WorkSpace.

**To restore a WorkSpace using the AWS CLI**

Use the `restore-workspace` command.

---

**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.

**Contents**

- Prerequisites (p. 169)
- Considerations (p. 170)
- Known limitations (p. 170)
- Summary of registry key settings (p. 170)
- Perform an in-place upgrade (p. 171)
- Troubleshooting (p. 173)
- Update your WorkSpace registry using a PowerShell script (p. 174)

**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
Considerations

The in-place upgrade process recreates the user profile by making a copy of a special profile named `Default User (C:\Users\Default)`. Do not use this default user profile to make customizations. We recommend making any customizations to the user profile through Group Policy Objects (GPOs) instead. Customizations made through GPOs can be easily modified or rolled back and are less prone to error.

- The in-place upgrade process can back up and recreate only one user profile. If you have multiple user profiles on drive D, delete all the profiles except for the one that you need.

### Known limitations

- The user profile location change from drive D to drive C does not happen during WorkSpace rebuilds or migrations. If you perform an in-place upgrade on a Windows 10 BYOL WorkSpace and then rebuild or migrate it, the new WorkSpace will have the user profile on drive D.

  **Warning**
  
  If you leave the user profile on drive C after the in-place upgrade, the user profile data stored on drive C will be lost during rebuilds or migrations unless you manually back up the user profile data prior to rebuilding or migrating, and then manually restore the user profile data after running the rebuild or migration process.

- If your default BYOL bundle contains an image that is based on an earlier release of Windows 10, you must perform the in-place upgrade again after the WorkSpace is rebuilt or migrated.

### Summary of registry key settings

To enable the in-place upgrade process and to specify where you would like the user profile to be located after the upgrade, you must set a number of registry keys.
To enable in-place Windows upgrades on your BYOL WorkSpaces, you must set certain registry keys, as described in the following procedure. You must also set certain registry keys to indicate the drive (C or D) where you want the user profiles to be located after the in-place upgrades are finished.

You can make these registry changes manually. If you have multiple WorkSpaces to update, you can use Group Policy or SCCM to push a PowerShell script. For a sample PowerShell script, see Update your WorkSpace registry using a PowerShell script (p. 174).
To perform an in-place upgrade of Windows 10

1. Make note of which version of Windows is 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.
   - HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1
   - HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\update-pvdrivers.ps1

   **Note**
   If these keys do not exist, reboot the WorkSpace. The keys should be added when the system is rebooted.

   (Optional) If you are using a managed workflow such as SCCM Task Sequences to perform the upgrade, set the following key value to 1 to prevent the computer from rebooting:
   - HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1\NoReboot

3. Decide which drive you want user profiles to be located on after the in-place upgrade process (for more information, see Considerations (p. 170)), and set the registry keys as follows:

   - Settings if you want the user profile on drive C after the upgrade:
     - HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1
     - Key name: PostUpgradeRestoreProfileOnD
     - Key value: 0
     - Key name: UserShellFoldersRedirection
     - Key value: 1

   - Settings if you want the user profile on drive D after the upgrade:
     - HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1
     - Key name: PostUpgradeRestoreProfileOnD
     - Key value: 1
     - Key name: UserShellFoldersRedirection
     - Key value: 0

4. After saving the changes to the registry, reboot the WorkSpace again so that the changes are applied.

   **Note**
   - After the reboot, logging in to the WorkSpace creates a new user profile. You might see placeholder icons in the Start menu. This behavior is automatically resolved after the in-place upgrade is complete.
   - Wait for 10 minutes to allow the WorkSpace to be unblocked.

   (Optional) Confirm that the following key value is set to 1, which unblocks the WorkSpace for updating:
HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1\profileImagePathDeleted

5. Perform the in-place upgrade. You can use whichever method you like, such as SCCM, ISO, or Windows Update (WU). Depending on your original Windows 10 version and how many apps were installed, this process can take from 40 to 120 minutes.

6. After the update process is finished, confirm that the Windows version has been updated.

   **Note**
   If the in-place upgrade fails, Windows automatically rolls back to use the Windows 10 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

7. If you modified the running mode of the WorkSpace by setting it to AlwaysOn or by changing the AutoStop time period so that the in-place upgrade process could run without interruption, set the running mode back to your original settings. For more information, see Modify the running mode (p. 148).

If you haven’t set the PostUpgradeRestoreProfileOnD registry key to 1, the user profile is regenerated by Windows and placed in C:\Users\%USERNAME% after the in-place upgrade, so that you do not have to go through the above steps again for future Windows 10 in-place upgrades. By default, the enable-inplace-upgrade.ps1 script redirects the following shell folders to drive D:

- D:\Users\%USERNAME%\Downloads
- D:\Users\%USERNAME%\Desktop
- D:\Users\%USERNAME%\Favorites
- D:\Users\%USERNAME%\Music
- D:\Users\%USERNAME%\Pictures
- D:\Users\%USERNAME%\Videos
- D:\Users\%USERNAME%\Documents
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Network Shortcuts
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\SendTo
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates

If you redirect the shell folders to other locations on your WorkSpaces, perform the necessary operations on the WorkSpaces after the in-place upgrades.

**Troubleshooting**

If you encounter any issues with the update, you can check the following items to assist with troubleshooting:
Update your WorkSpace registry using a PowerShell script

You can use the following sample PowerShell script to update the registry on your WorkSpaces to enable in-place upgrades. Follow the Perform an in-place upgrade (p. 171), but use this script to update the registry on each WorkSpace.

```
# AWS WorkSpaces 1.28.20
# Enable In-Place Update Sample Scripts
# These registry keys and values will enable scripts to execute on the next reboot of the WorkSpace.

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

foreach ($scriptName in $scriptlist) {
    $scriptRegKey = "$wsConfigRegistryRoot\$scriptName"
    try {
        if (-not(Test-Path $scriptRegKey)) {
            Write-Host "Registry key not found. Creating registry key '$scriptRegKey' with 'Update' enabled."
            New-Item -Path $wsConfigRegistryRoot -Name $scriptName | Out-Null
            New-ItemProperty -Path $scriptRegKey -Name Enabled -PropertyType DWord -Value $Enabled | Out-Null
            Write-Host "Value created. '$scriptRegKey' Enabled='$(Get-ItemProperty -Path $scriptRegKey).Enabled')'"
        } else {
            Write-Host "Registry key is already present with value '$scriptRegKey' Enabled='$(Get-ItemProperty -Path $scriptRegKey).Enabled')'"
            if((Get-ItemProperty -Path $scriptRegKey).Enabled -ne $Enabled) {
                Set-ItemProperty -Path $scriptRegKey -Name Enabled -Value $Enabled
                Write-Host "Value updated. '$scriptRegKey' Enabled='$(Get-ItemProperty -Path $scriptRegKey).Enabled')'"
            }
        }
    } catch 
        write-host "An error occurred: $exception"
}
```

Tip
During the in-place upgrade process, if you see that some icon shortcuts on the desktop no longer work, it's because WorkSpaces moves any user profiles located on drive D to drive C to prepare for the upgrade. After the upgrade is completed, the shortcuts will work as expected.
Migrate a WorkSpace

You can migrate a WorkSpace from one bundle to another, while retaining the data on the user volume. The following are example scenarios:

- You can migrate WorkSpaces from the Windows 7 desktop experience to the Windows 10 desktop experience.
- You can migrate WorkSpaces from the PCoIP protocol to the WorkSpaces Streaming Protocol (WSP).
- You can migrate WorkSpaces from one public or custom bundle to another. For example, you can migrate from GPU-enabled (Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro) bundles to non-GPU-enabled bundles, and vice versa.

For more information about Amazon WorkSpaces bundles, see WorkSpace bundles and images (p. 181).

The migration process recreates the WorkSpace by using a new root volume from the target bundle image and the user volume from the last available snapshot of the original WorkSpace. A new user profile is generated during migration for better compatibility. The old user profile is renamed, and then certain files in the old user profile are moved to the new user profile. (For details about what gets moved, see What happens during migration (p. 177).)

The migration process takes up to one hour per WorkSpace. When you initiate the migration process, a new WorkSpace is created. If an error occurs that prevents successful migration, the original WorkSpace is recovered and returned to its original state, and the new WorkSpace is terminated.

Contents
- Migration limits (p. 175)
- Migration scenarios (p. 176)
- What happens during migration (p. 177)
- Best practices (p. 177)
- Troubleshooting (p. 178)
- How billing is affected (p. 178)
- Migrating a WorkSpace (p. 178)

Migration limits

- You cannot migrate to a public or custom Windows 7 desktop experience bundle. You also cannot migrate to Bring Your Own License (BYOL) Windows 7 bundles.
- You can migrate BYOL WorkSpaces only to other BYOL bundles. To migrate a BYOL WorkSpace from PCoIP to WSP, you must first create a BYOL bundle with the WSP protocol. You can then migrate your PCoIP BYOL WorkSpaces to that WSP BYOL bundle.
- You cannot migrate a WorkSpace created from public or custom bundles to a BYOL bundle.
• Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro bundles are available for only the PCoIP protocol at this time, so Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro WorkSpaces can't be migrated to WSP yet.
• Migrating Linux WorkSpaces is not currently supported.
• In AWS Regions that support more than one language, you can migrate WorkSpaces between language bundles.
• The source and target bundles must be different. (However, in Regions that support more than one language, you can migrate to the same Windows 10 bundle as long as the languages differ.) If you want to refresh your WorkSpace using the same bundle, rebuild the WorkSpace (p. 167) instead.
• You cannot migrate WorkSpaces across Regions.
• In some cases, if migration is unable to finish successfully, you might not receive an error message, and it might appear that the migration process did not start. If the WorkSpace bundle remains the same one hour after attempting migration, the migration is unsuccessful. Contact the AWS Support Center for assistance.

Migration scenarios

The following table shows which migration scenarios are available:

<table>
<thead>
<tr>
<th>Source OS</th>
<th>Target OS</th>
<th>Available?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public or custom bundle Windows 7</td>
<td>Public or custom bundle Windows 10</td>
<td>Yes</td>
</tr>
<tr>
<td>Custom bundle Windows 7</td>
<td>Public bundle Windows 7</td>
<td>No</td>
</tr>
<tr>
<td>Custom bundle Windows 7</td>
<td>Custom bundle Windows 7</td>
<td>No</td>
</tr>
<tr>
<td>Public bundle Windows 7</td>
<td>Custom bundle Windows 7</td>
<td>No</td>
</tr>
<tr>
<td>Public or custom bundle Windows 10</td>
<td>Public or custom bundle Windows 7</td>
<td>No</td>
</tr>
<tr>
<td>Custom bundle Windows 10</td>
<td>Public bundle Windows 10</td>
<td>No</td>
</tr>
<tr>
<td>Public or custom bundle Windows 10</td>
<td>Custom bundle Windows 10</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows 7 BYOL bundle</td>
<td>Windows 7 BYOL bundle</td>
<td>No</td>
</tr>
<tr>
<td>Windows 7 BYOL bundle</td>
<td>Windows 10 BYOL bundle</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows 10 BYOL bundle</td>
<td>Windows 7 BYOL bundle</td>
<td>No</td>
</tr>
<tr>
<td>Windows 10 BYOL bundle</td>
<td>Windows 10 BYOL bundle</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note
Web access is not available for the Windows Server 2019-powered Public Windows 10 bundle PCoIP branch.
What happens during migration

During migration, the data on the user volume (drive D) is preserved, but all of the data on the root volume (drive C) is lost. This means that none of the installed applications, settings, and changes to the registry are preserved. The old user profile folder is renamed with the .NotMigrated suffix, and a new user profile is created.

The migration process recreates drive D based on the last snapshot of the original user volume. During the first boot of the new WorkSpace, the migration process moves the original D:\Users\%USERNAME% folder to a folder named D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated. A new D:\Users\%USERNAME% folder is generated by the new OS.

After the new user profile is created, the files in the following user shell folders are moved from the old .NotMigrated profile to the new profile:

- D:\Users\%USERNAME%\Desktop
- D:\Users\%USERNAME%\Documents
- D:\Users\%USERNAME%\Downloads
- D:\Users\%USERNAME%\Favorites
- D:\Users\%USERNAME%\Music
- D:\Users\%USERNAME%\Pictures
- D:\Users\%USERNAME%\Videos

Important
The migration process attempts to move the files from the old user profile to the new profile. Any files that weren't moved during migration remain in the D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated folder. If the migration is successful, you can see which files got moved in C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs. You can manually move any files that didn't get moved automatically.

By default, the public bundles have local search indexing disabled. If you were to enable it, the default is to search C:\Users and not D:\Users, so you need to adjust that as well. If you've set local search indexing specifically to D:\Users\username and not to D:\Users, then local search indexing might not work post-migration for any user files that are in the D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated folder.

Any tags assigned to the original WorkSpace are carried over during migration, and the running mode of the WorkSpace is preserved. However, the new WorkSpace gets a new WorkSpace ID, computer name, and IP address.

Best practices

Before you migrate a WorkSpace, do the following:

- Back up any important data on drive C to another location. All data on drive C is erased during migration.
- Make sure that the WorkSpace being migrated is at least 12 hours old, to ensure that a snapshot of the user volume has been created. On the Migrate WorkSpaces page in the Amazon WorkSpaces
console, you can see the time of the last snapshot. Any data created after the last snapshot is lost during migration.

- To avoid potential data loss, make sure that your users log out of their WorkSpaces and don't log back in until after the migration process is finished. Note that WorkSpaces cannot be migrated when they are in ADMIN_MAINTENANCE mode.
- Make sure that the WorkSpaces you want to migrate have a status of AVAILABLE, STOPPED, or ERROR.
- Make sure that you have enough IP addresses for the WorkSpaces you are migrating. During migration, new IP addresses will be allocated for the WorkSpaces.
- If you are using scripts to migrate WorkSpaces, migrate them in batches of no more than 25 WorkSpaces at a time.

Troubleshooting

- If your users report missing files after migration, check to see if their user profile files did not get moved during the migration process. You can see which files got moved in C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs. The files that didn't get moved will be located in the D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated folder. You can manually move any files that didn't get moved automatically.
- If you are using the API to migrate WorkSpaces and the migration does not succeed, the target WorkSpace ID returned by the API will not be used, and the WorkSpace will still have the original WorkSpace ID.
- If a migration does not successfully finish, check the Active Directory to see if it was cleaned up accordingly. You might need to manually remove WorkSpaces that you no longer need.

How billing is affected

During the month in which migration occurs, you are charged prorated amounts for both the new and the original WorkSpaces. For example, if you migrate WorkSpace A to WorkSpace B on May 10, you will be charged for WorkSpace A from May 1 to May 10, and you will be charged for WorkSpace B from May 11 to May 30.

**Note**

If you are migrating a WorkSpace to a different bundle type (for example, from Performance to Power, or Value to Standard), the size of the root volume (drive C) and the user volume (drive D) might increase during the migration process. If necessary, the root volume increases to match the default root volume size for the new bundle. However, if you had already specified a different size (higher or lower) for the user volume than the default for the original bundle, that same user volume size is retained during the migration process. Otherwise, the migration process uses the larger of the source WorkSpace user volume size and the default user volume size for the new bundle.

Migrating a WorkSpace

You can migrate WorkSpaces through the Amazon WorkSpaces console, the AWS CLI or the Amazon WorkSpaces API.

**To migrate a WorkSpace**

2. In the navigation pane, choose WorkSpaces.
3. Select your WorkSpace and choose Actions, Migrate WorkSpaces.
4. Under Select Target Bundle, select the bundle that you'd like to migrate your WorkSpace to.
To migrate a BYOL WorkSpace from PCoIP to WSP, you must first create a BYOL bundle with the WSP protocol. You can then migrate your PCoIP BYOL WorkSpaces to that WSP BYOL bundle.

5. Under **Assign WorkSpace Bundle**, choose the target bundle for each WorkSpace user.

**Warning**

For each WorkSpace, take note of the listed snapshot time. Any changes made to the user volume after the listed snapshot time are discarded during the migration process.

6. Choose **Migrate WorkSpaces**.

A new WorkSpace with a status of **PENDING** appears in the Amazon WorkSpaces console. When the migration is finished, the original WorkSpace is terminated, and the status of the new WorkSpace is set to **AVAILABLE**.

7. (Optional) To delete any custom bundles and images that you no longer need, see Delete a custom WorkSpaces bundle or image (p. 197).

To migrate WorkSpaces through the AWS CLI, use the `migrate-workspace` command. To migrate WorkSpaces through the Amazon WorkSpaces API, see MigrateWorkSpace in the Amazon WorkSpaces API Reference.

### Delete a WorkSpace

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

**Warning**

Deleting a WorkSpace is a permanent action and cannot be undone. The WorkSpace user’s data does not persist and is destroyed. For help with backing up user data, contact AWS Support.

**Note**

Simple AD and AD Connector are made available to you free of charge to use with WorkSpaces. If there are no WorkSpaces being used with your Simple AD or AD Connector directory for 30 consecutive days, this directory will be automatically deregistered for use with Amazon WorkSpaces, and you will be charged for this directory as per the AWS Directory Service pricing terms.

To delete empty directories, see Delete the directory for your WorkSpaces (p. 99). If you delete your Simple AD or AD Connector directory, you can always create a new one when you want to start using WorkSpaces again.

**To delete a WorkSpace**

You can delete a WorkSpace that is in any state except **SUSPENDED**.

2. In the navigation pane, choose **WorkSpaces**.
3. Select your WorkSpace and choose **Actions**, **Remove WorkSpaces**.
4. When prompted for confirmation, choose **Remove WorkSpaces**. It takes approximately 5 minutes for a WorkSpace to be deleted. During deletion, the status of the WorkSpace is set to **TERMINATING**. When the deletion is complete, the status is very briefly set to **TERMINATED** before the WorkSpace disappears from the console.
5. (Optional) To delete any custom bundles and images that you are finished with, see Delete a custom WorkSpaces bundle or image (p. 197).
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. 99).
7. (Optional) After you delete all resources in the virtual private cloud (VPC) for your directory, you can delete the VPC and release the Elastic IP address used for the NAT gateway. For more information, see Deleting your VPC and Working with Elastic IP addresses in the Amazon VPC User Guide.

To delete a WorkSpace using the AWS CLI

Use the terminate-workspaces command.
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. The default bundles available for WorkSpaces are called public bundles. For more information about the various public bundles available for WorkSpaces, see Amazon WorkSpaces Bundles.

If you've launched a Windows or Amazon Linux WorkSpace and have customized it, you can create a custom image from that WorkSpace.

A custom image contains only the OS, software, and settings for the WorkSpace. A custom bundle is a combination of both that custom image and the hardware from which a WorkSpace can be launched.

After you create a custom image, you can build a custom bundle that combines the custom WorkSpace image and the underlying compute and storage configuration that you select. You can then specify this custom bundle when you launch new WorkSpaces to ensure that the new WorkSpaces have the same consistent configuration (hardware and software).

If you need to perform software updates or to install additional software on your WorkSpaces, you can update your custom bundle and use it to rebuild your WorkSpaces.

Contents
- Create a custom WorkSpaces image and bundle (p. 181)
- Update a custom WorkSpaces bundle (p. 194)
- Copy a custom WorkSpaces image (p. 194)
- Share or unshare a custom WorkSpaces image (p. 196)
- Delete a custom WorkSpaces bundle or image (p. 197)
- Bring Your Own Windows desktop licenses (p. 198)

Create a custom WorkSpaces image and bundle

If you've launched a Windows or Amazon Linux WorkSpace and have customized it, you can create a custom image and custom bundles from that WorkSpace.

A custom image contains only the OS, software, and settings for the WorkSpace. A custom bundle is a combination of both that custom image and the hardware from which a WorkSpace can be launched.

After you create a custom image, you can build a custom bundle that combines the custom image and the underlying compute and storage configuration that you select. You can then specify this custom bundle when you launch new WorkSpaces to ensure that the new WorkSpaces have the same consistent configuration (hardware and software).

You can use the same custom image to create various custom bundles by selecting different compute and storage options for each bundle.

Important

- If you plan to create an image from a Windows 10 WorkSpace, note that image creation is not supported on Windows 10 systems that have been upgraded from one version of Windows 10 to a newer version of Windows 10 (a Windows feature/version upgrade). However, Windows cumulative or security updates are supported by the WorkSpaces image-creation process.
- After January 14, 2020, images cannot be created from public Windows 7 bundles. You might want to consider migrating your Windows 7 WorkSpaces to Windows 10. For more information, see Migrate a WorkSpace (p. 175).
Custom bundles cost as same as the public bundles they are created from. For more information about pricing, see Amazon WorkSpaces Pricing.

Contents

- Requirements to create Windows custom images (p. 182)
- Requirements to create Amazon Linux custom images (p. 182)
- Best practices (p. 183)
- (Optional) Step 1: Specify a custom computer name format for your image (p. 184)
- Step 2: Run the Image Checker (p. 185)
- Step 3: Create a custom image and custom bundle (p. 191)
- What's included with Windows WorkSpaces custom images (p. 192)
- What's included with Amazon Linux WorkSpace custom images (p. 193)

Requirements to create Windows custom images

- The status of the WorkSpace must be Available and its modification state must be None.
- All applications and user profiles on WorkSpaces images must be compatible with Microsoft Sysprep.
- All applications to be included in the image must be installed on the C drive.
- For Windows 7 WorkSpaces, and its total size (files and data) must be less than 10 GB.
- For Windows 7 WorkSpaces, the C drive must have at least 12 GB of available space.
- All application services running on the WorkSpace must use a local system account instead of domain user credentials. For example, you cannot have a Microsoft SQL Server Express installation running with a domain user's credentials.
- The WorkSpace must not be encrypted. Image creation from an encrypted WorkSpace is not currently supported.
- The following components are required in an image. Without these components, the WorkSpaces that you launch from the image will not function correctly. For more information, see the section called “Required configuration” (p. 86).
  - Windows PowerShell version 3.0 or later
  - Remote Desktop Services
  - AWS PV drivers
  - Windows Remote Management (WinRM)
  - Teradici PCoIP agents and drivers
  - STXHD agents and drivers
  - AWS and WorkSpaces certificates
  - Skylight agent

Requirements to create Amazon Linux custom images

- The status of the WorkSpace must be Available and its modification state must be None.
- All applications to be included in the image must be installed outside of the user volume (the /home directory).
- The root volume (/) should be less than 97% full.
• The WorkSpace must not be encrypted. Image creation from an encrypted WorkSpace is not currently supported.

• The following components are required in an image. Without these components, the WorkSpaces that you launch from the image will not function correctly:
  • Cloud-init
  • Teradici PCoIP agents and drivers
  • Skylight agent

Best practices

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

• Use a separate VPC that is not connected to your production environment.
• Deploy the WorkSpace in a private subnet and use a NAT instance for outbound traffic.
• Use a small Simple AD directory.
• Use the smallest volume size for the source WorkSpace, and then adjust the volume size as needed when creating the custom bundle.
• Install all operating system updates (except Windows feature/version updates) and all application updates on the WorkSpace. For more information, see the Important note (p. 181) at the start of this topic.
• Delete cached data from the WorkSpace that shouldn't be included in the bundle (for example, browser history, cached files, and browser cookies).
• Delete configuration settings from the WorkSpace that shouldn't be included in the bundle (for example, email profiles).
• Switch to dynamic IP address settings using DHCP.
• Make sure that you haven't exceeded your quota for WorkSpace images allowed in a Region. By default, you're allowed 40 WorkSpace images per Region. If you've reached this quota, new attempts to create an image will fail. To request a quota increase, use the WorkSpaces Limits form.
• Make sure that you aren't trying to create an image from an encrypted WorkSpace. Image creation from an encrypted WorkSpace is not currently supported.
• If you're running any antivirus software on the WorkSpace, disable it while you're attempting to create an image.
• If you have a firewall enabled on your WorkSpace, make sure that it isn't blocking any necessary ports. For more information, see IP address and port requirements for WorkSpaces (p. 14).
• For Windows WorkSpaces, don't configure any Group Policy Objects (GPOs) before image creation.
• For Windows WorkSpaces, do not customize the default user profile (C:\Users\Default) before creating an image. We recommend making any customizations to the user profile through GPOs, and applying them after image creation. GPOs can be easily modified or rolled back, and are therefore less prone to error than customizations made to the default user profile.
• For Linux WorkSpaces, see also the "Best Practices to Prepare Your Amazon WorkSpaces for Linux Images" whitepaper.
• If you want to use smart cards on Linux WorkSpaces with WorkSpaces Streaming Protocol (WSP) enabled, see Use smart cards for authentication (p. 66) for the customizations that you must make to your Linux WorkSpace before creating your image.
(Optional) Step 1: Specify a custom computer name format for your image

For the WorkSpaces launched from your custom or Bring Your Own License (BYOL) images, you can specify a custom prefix for the computer name format instead of using the default computer name format (p. 103). To specify a custom prefix, follow the appropriate procedure for your image type.

To specify a custom computer name format for custom images

1. On the WorkSpace that you're using to create your custom image, open C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml in Notepad or another text editor. For more information about working with the Unattend.xml file, see Answer files (unattend.xml) in the Microsoft documentation.

   **Note**
   To access the C: drive from the Windows File Explorer on your WorkSpace, enter C: in the address bar.

2. In the `<settings pass="specialize">` section, make sure that `<ComputerName>` is set to an asterisk (*). If `<ComputerName>` is set to any other value, your custom computer name settings will be ignored. For more information about the `<ComputerName>` setting, see ComputerName in the Microsoft documentation.

3. In the `<settings pass="specialize">` section, set `<RegisteredOrganization>` and `<RegisteredOwner>` to your preferred values.

   During Sysprep, the values that you specify for `<RegisteredOwner>` and `<RegisteredOrganization>` are concatenated together, and the first 7 characters of the combined string are used to create the computer name. For example, if you specify `Amazon.com` for `<RegisteredOrganization>` and `EC2` for `<RegisteredOwner>`, the computer names for the WorkSpaces created from your custom bundle will start with EC2AMAZ-xxxxxxx.

   **Note**
   The `<RegisteredOrganization>` and `<RegisteredOwner>` values in the `<settings pass="oobeSystem">` section are ignored by Sysprep.

4. Save your changes to the Unattend.xml file.

To specify a custom computer name format for BYOL images

1. Open C:\Program Files\Amazon\Ec2ConfigService\Sysprep2008.xml in Notepad or another text editor.

2. In the `<settings pass="specialize">` section, uncomment `<ComputerName>*</ComputerName>`, and make sure that `<ComputerName>` is set to an asterisk (*). If `<ComputerName>` is set to any other value, your custom computer name settings will be ignored. For more information about the `<ComputerName>` setting, see ComputerName in the Microsoft documentation.

3. In the `<settings pass="specialize">` section, set `<RegisteredOrganization>` and `<RegisteredOwner>` to your preferred values.

   During Sysprep, the values that you specify for `<RegisteredOwner>` and `<RegisteredOrganization>` are concatenated together, and the first 7 characters of the combined string are used to create the computer name. For example, if you specify `Amazon.com` for `<RegisteredOrganization>` and `EC2` for `<RegisteredOwner>`, the computer names for the WorkSpaces created from your custom bundle will start with EC2AMAZ-xxxxxxx.
Step 2: Run the Image Checker

Note
The Image Checker is available only for Windows WorkSpaces. If you are creating an image from a Linux WorkSpace, skip to Step 3: Create a custom image and custom bundle (p. 191).

To confirm that your Windows WorkSpace meets the requirements for image creation, we recommend running the Image Checker. The Image Checker performs a series of tests on the WorkSpace that you want to use to create your image, and provides guidance on how to resolve any issues it finds.

Important
• The WorkSpace must pass all of the tests run by the Image Checker before you can use it for image creation.
• Before you run the Image Checker, verify that the latest Windows security and cumulative updates are installed on your WorkSpace.
• The Image Checker does not check the user profile size for Windows 10 WorkSpaces. If you have a Windows 10 WorkSpace, make sure that the user profile size is less than 10 GB.

To get the Image Checker, do one of the following:
• Reboot your WorkSpace (p. 166). The Image Checker is downloaded automatically during the reboot and installed at C:\Program Files\Amazon\ImageChecker.exe.
• Download the Amazon WorkSpaces Image Checker from https://tools.amazonworkspaces.com/ImageChecker.zip and extract the ImageChecker.exe file. Copy this file to C:\Program Files\Amazon\.

To run the Image Checker
1. Open the C:\Program Files\Amazon\ImageChecker.exe file.
2. In the Amazon WorkSpaces Image Checker dialog box, choose Run.
3. After each test is completed, you can view the status of the test.
   For any test with a status of FAILED, choose Info to display information about how to resolve the issue that caused the failure. For more information about how to resolve these issues, see Tips for resolving issues detected by the Image Checker (p. 186).
   If any tests display a status of WARNING, choose the Fix All Warnings button.

The tool generates an output log file in the same directory where the Image Checker is located. By default, this file is located at C:\Program Files\Amazon\ImageChecker_yyyymmddhhmss.log.

Tip
Do not delete this log file. If an issue occurs, this log file might be helpful in troubleshooting.

4. If applicable, resolve any issues that cause test failures and warnings, and repeat the process of running the Image Checker until the WorkSpace passes all tests. All failures and warnings must be resolved before you can create an image.
5. After your WorkSpace passes all tests, you see a **Validation Successful** message. You are now ready to create a custom bundle.

### Tips for resolving issues detected by the Image Checker

In addition to consulting the following tips for resolving issues that are detected by the Image Checker, be sure to review the Image Checker log file at `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`.

**PowerShell version 3.0 or later must be installed**

Install the latest version of Microsoft Windows PowerShell.

**Important**
The PowerShell execution policy for a WorkSpace must be set to allow **RemoteSigned** scripts. To check the execution policy, run the `Get-ExecutionPolicy` PowerShell command. If the execution policy is not set to **Unrestricted** or **RemoteSigned**, run the `Set-ExecutionPolicy –ExecutionPolicy RemoteSigned` command to change the value of the execution policy. The **RemoteSigned** setting allows the execution of scripts on Amazon WorkSpaces, which is required to create an image.

**Only the C and D drives can be present**

Only the C and D drives can be present on a WorkSpace that's used for imaging. Remove all other drives, including virtual drives.

**No pending reboot due to Windows Updates can be detected**

- The Create Image process can't be run until Windows has been rebooted to finish installing security or cumulative updates. Reboot Windows to apply these updates, and make sure that no other pending Windows security or cumulative updates need to be installed.
- Image creation is not supported on Windows 10 systems that have been upgraded from one version of Windows 10 to a newer version of Windows 10 (a Windows feature/version upgrade). However, Windows cumulative or security updates are supported by the WorkSpaces image-creation process.

**The Sysprep file must exist and can't be blank**

If there are problems with your Sysprep file, contact the AWS Support Center to get your EC2Config or EC2Launch repaired.

**The user profile size must be less than 10 GB**

For Windows 7 WorkSpaces, the user profile (`D:\Users\username`) must be less than 10 GB total. Remove files as needed to reduce the size of the user profile.

**Drive C must have enough free space**

For Windows 7 WorkSpaces, you must have at least 12 GB of free space on drive C. Remove files as needed to free up space on drive C. For Windows 10 WorkSpaces, ignore if you receive a **FAILED** message and the disk space is above 2GB.

**No services can be running under a domain account**

To run the Create Image process, no services on the WorkSpace can be running under a domain account. All services must be running under a local account.

**To run services under a local account**

1. Open `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log` and find the list of services that are running under a domain account.
Step 2: Run the Image Checker

2. In the Windows search box, enter `services.msc` to open the Windows Services Manager.
3. Under **Log On As**, look for the services that are running under domain accounts. (Services running as **Local System**, **Local Service**, or **Network Service** do not interfere with image creation.)
4. Select a service that is running under a domain account, and then choose **Action, Properties**.
5. Open the **Log On** tab. Under **Log on as**, choose **Local System account**.
6. Choose **OK**.

**Amazon WorkSpaces Application Manager (Amazon WAM) must be installed**

If you have used Amazon WAM to assign applications to your users, you must set up the Amazon WAM installer on your WorkSpace. When you are finished, the **Amazon WAM** shortcut will appear on your WorkSpace desktop.

**The WorkSpace must be configured to use DHCP**

You must configure all network adapters on the WorkSpace to use DHCP instead of static IP addresses.

**To set all network adapters to use DHCP**

1. In the Windows search box, enter `control panel` to open the Control Panel.
2. Choose **Network and Internet**.
3. Choose **Network and Sharing Center**.
4. Choose **Change adapter settings**, and select an adapter.
5. Choose **Change settings of this connection**.
6. On the **Networking** tab, select **Internet Protocol Version 4 (TCP/IPv4)**, and then choose **Properties**.
7. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select **Obtain an IP address automatically**.
8. Choose **OK**.
9. Repeat this process for all network adapters on the WorkSpace.

**Remote Desktop Services must be enabled**

The Create Image process requires Remote Desktop Services to be enabled.

**To enable Remote Desktop Services**

1. In the Windows search box, enter `services.msc` to open the Windows Services Manager.
2. In the **Name** column, find **Remote Desktop Services**.
3. Select **Remote Desktop Services**, and then choose **Action, Properties**.
4. On the **General** tab, for **Startup type**, choose **Manual** or **Automatic**.
5. Choose **OK**.

**A user profile must exist**

The WorkSpace that you're using to create images must have a user profile (`D:\Users\username`). If this test fails, contact the **AWS Support Center** for assistance.

**The environment variable path must be properly configured**

The environment variable path for the local machine is missing entries for System32 and for Windows PowerShell. These entries are required for Create Image to run.
To configure your environment variable path

1. In the Windows search box, enter `environment variables` and then choose `Edit the system environment variables`.
2. In the `System Properties` dialog box, open the `Advanced` tab, and choose `Environment Variables`.
3. In the `Environment Variables` dialog box, under `System variables`, select the `Path` entry and then choose `Edit`.
4. Choose `New`, and add the following path:
   
   `C:\Windows\System32`

5. Choose `New` again, and add the following path:

   `C:\Windows\System32\WindowsPowerShell\v1.0`  

6. Choose `OK`.
7. Restart the WorkSpace.

**Tip**
The order in which items appear in the environment variable path matters. To determine the correct order, you might want to compare the environment variable path of your WorkSpace with one from a newly created WorkSpace or a new Windows instance.

Windows Modules Installer must be enabled

The Create Image process requires the Windows Modules Installer service to be enabled.

**To enable the Windows Modules Installer service**

1. In the Windows search box, enter `services.msc` to open the Windows Services Manager.
2. In the `Name` column, find `Windows Modules Installer`.
3. Select `Windows Modules Installer`, and then choose `Action, Properties`.
4. On the `General` tab, for `Startup type`, choose `Manual` or `Automatic`.
5. Choose `OK`.

Amazon SSM Agent must be disabled

The Create Image process requires the Amazon SSM Agent service to be disabled.

**To disable the Amazon SSM Agent service**

1. In the Windows search box, enter `services.msc` to open the Windows Services Manager.
2. In the `Name` column, find `Amazon SSM Agent`.
3. Select `Amazon SSM Agent`, and then choose `Action, Properties`.
4. On the `General` tab, for `Startup type`, choose `Disabled`.
5. Choose `OK`.

SSL3 and TLS version 1.2 must be enabled

To configure SSL/TLS for Windows, see How to Enable TLS 1.2 in the Microsoft Windows documentation.

Only one user profile can exist on the WorkSpace

There can be only one WorkSpaces user profile (`D:\Users\username`) on the WorkSpace that you're using to create images. Delete any user profiles that don't belong to the intended user of the WorkSpace.
For image creation to work, your WorkSpace can have only three user profiles on it:

- The user profile of the intended user of the WorkSpace (D:\Users\username)
- The default user profile (also known as Default Profile)
- The Administrator user profile

If there are additional user profiles, you can delete them through the advanced system properties in the Windows Control Panel.

**To delete a user profile**

1. To access the advanced system properties, do one of the following:
   - Press the **Windows key+Pause Break**, and then choose **Advanced system settings** in the left pane of the **Control Panel > System and Security > System** dialog box.
   - In the Windows search box, enter **control panel**. In the Control Panel, choose **System and Security**, then choose System, and then choose **Advanced system settings** in the left pane of the **Control Panel > System and Security > System** dialog box.
2. In the **System Properties** dialog box, on the **Advanced** tab, choose **Settings** under **User Profiles**.
3. If any profile is listed other than the Administrator profile, the Default Profile, and the profile of the intended WorkSpaces user, select that additional profile and choose **Delete**.
4. When asked if you want to delete the profile, choose **Yes**.
5. If necessary, repeat Steps 3 and 4 to remove any other profiles that don't belong on the WorkSpace.
6. Choose **OK** twice and close the Control Panel.
7. Restart the WorkSpace.

**No AppX packages can be in a staged state**

One or more AppX packages are in a staged state. This might cause a Sysprep error during image creation.

**To remove all staged AppX packages**

1. In the Windows search box, enter **powershell**. Choose **Run as Administrator**.
2. When asked “Do you want to allow this app to make changes to your device?”, choose **Yes**.
3. In the Windows PowerShell window, enter the following commands to list all staged AppX packages, and press Enter after each one.

   ```powershell
   $workSpaceUserName = $env:username
   $allAppxPackages = Get-AppxPackage -AllUsers
   $packages = $allAppxPackages | Where-Object { `n   ($_.PackageUserInformation -like "*S-1-5-18*" -and ! ($_.PackageUserInformation -like "$workSpaceUserName*)) -and `n   ($_.PackageUserInformation -like "*Installed*")) -or `n   ($_.PackageUserInformation -like "*Staged*" -or `n   ($_.PackageUserInformation -like "*S-1-5-18*" -and `n   ($_.PackageUserInformation -like "$workSpaceUserName*)) -and `n   ($_.PackageUserInformation -like "*Staged*"))
   ```
4. Enter the following command to remove all staged AppX packages, and press Enter.
5. Run the Image Checker again. If this test still fails, enter the following commands to remove all AppX packages, and press Enter after each one.

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -ErrorAction SilentlyContinue
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

**Windows must not have been upgraded from a previous version**

Image creation is not supported on Windows systems that have been upgraded from one version of Windows 10 to a newer version of Windows 10 (a Windows feature/version upgrade).

To create images, use a WorkSpace that has not undergone a Windows feature/version upgrade.

**The Windows rearm count must not be 0**

The rearm feature allows you to extend the activation period for the trial version of Windows. The Create Image process requires that the rearm count be a value other than 0.

**To check the Windows rearm count**

1. On the Windows Start menu, choose Windows System, then choose Command Prompt.
2. In the Command Prompt window, enter the following command, and then press Enter.

```
cscript C:\Windows\System32\slmgr.vbs /dlv
```

To reset the rearm count to a value other than 0, see Sysprep (Generalize) a Windows installation in the Microsoft Windows documentation.

**Other troubleshooting tips**

If your WorkSpace passes all of the tests run by the Image Checker, but you are still unable to create an image from the WorkSpace, check for the following issues:

- Make sure that the WorkSpace isn’t assigned to a user within a Domain Guests group. To check if there are any domain accounts, run the following PowerShell command.

```
Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*\$env:USERDOMAIN*" }
```

- For Windows 7 WorkSpaces only: If problems occur while the user profile is being copied during image creation, check for the following issues:
  - Long profile paths can cause image creation errors. Make sure that the paths of all folders within the user profile are less than 261 characters.
  - Make sure to grant full permissions on the profile folder to the system and all application packages.
  - If any files in the user profile are locked by a process or are in use during image creation, copying the profile might fail.
  - Some Group Policy Objects (GPOs) restrict access to the RDP certificate thumbprint when it is requested by the EC2Config service or the EC2Launch scripts during Windows instance configuration. Before you try to create an image, move the WorkSpace to a new organizational unit (OU) with blocked inheritance and no GPOs applied.
Step 3: Create a custom image and custom bundle

After you have validated your WorkSpace image, you can proceed with creating your custom image and custom bundle.

To create a custom image and custom bundle

1. If you are still connected to the WorkSpace, disconnect by choosing Amazon Workspaces and Disconnect in the WorkSpaces client application.
3. In the navigation pane, choose WorkSpaces.
4. Select the WorkSpace and choose Actions, Create Image. If the status of the WorkSpace is STOPPED, you must start it first (choose Actions, Start WorkSpaces) before you can choose Actions, Create Image.
5. A message displays, prompting you to reboot (restart) your WorkSpace before continuing. Rebooting your WorkSpace updates your Amazon WorkSpaces software to the latest version. Reboot your WorkSpace by closing the message and following the steps in Reboot a WorkSpace (p. 166). When you're done, repeat Step 4 (p. 191) of this procedure, but this time choose Next when the reboot message appears. To create an image, the status of the WorkSpace must be AVAILABLE and its modification state must be None.
6. Enter an image name and a description that will help you identify the image, and then choose Create Image. While the image is being created, the status of the WorkSpace is SUSPENDED and the WorkSpace is unavailable.
7. In the navigation pane, choose Images. The image is complete when the status of the WorkSpace changes to Available (this can take up to 45 minutes).
8. Select the image and choose Actions, Create bundle.

   Note
   To create a bundle programmatically, use the CreateWorkspaceBundle API action. For more information, see CreateWorkspaceBundle in the Amazon WorkSpaces API Reference.

9. Enter a bundle name and a description, and then do the following:
   • For Bundle hardware type, choose the hardware to use when launching WorkSpaces from this custom bundle.
   • For Storage settings, select one of the default combinations for the root volume and user volume size, or select Custom, and then enter values (up to 2000 GB) for Root volume size and User volume size.

   The default available size combinations for the root volume (for Microsoft Windows, the C drive, for Linux, /) and the user volume (for Windows, the D drive; for Linux, /home) are as follows:
   • Root: 80 GB, User: 10 GB, 50 GB, or 100 GB
   • Root: 175 GB, User: 100 GB
   • For Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro WorkSpaces only: Root: 100 GB, User: 100 GB
Alternatively, you can expand the root and user volumes up to 2000 GB each.

**Note**
To ensure that your data is preserved, you cannot decrease the size of the root or user volumes after you launch a WorkSpace. Instead, make sure that you specify the minimum sizes for these volumes when launching a WorkSpace. You can launch a Value, Standard, Performance, Power, or PowerPro WorkSpace with a minimum of 80 GB for the root volume and 10 GB for the user volume. You can launch a Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro WorkSpace with a minimum of 100 GB for the root volume and 100 GB for the user volume.

10. Choose **Create bundle**.
11. To confirm that your bundle has been created, choose **Bundles** and verify that the bundle is listed.

### What's included with Windows WorkSpaces custom images

When you create an image from a Windows 7 or 10 WorkSpace, the entire contents of the *C* drive are included.

For Windows 10 WorkSpaces, the user profile in *D:\Users\username* is not included in the custom image.

For Windows 7 WorkSpaces, the entire contents of the user profile in *D:\Users\username* are included, except for the following:

- Contacts
- Downloads
- Music
- Pictures
- Saved games
- Videos
- Podcasts
- Virtual machines
- `.virtualbox`
- Tracing
- `appdata\local\temp`
- `appdata\roaming\apple computer\mobilesync\`
- `appdata\roaming\apple computer\logs\`
- `appdata\roaming\apple computer\itunes\iphone software updates\`
- `appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\`
- `appdata\roaming\macromedia\flash player\#sharedobjects\`
- `appdata\roaming\adobe\flash player\assetcache\`
- `appdata\roaming\microsoft\windows\recent\`
- `appdata\roaming\microsoft\office\recent\`
- `appdata\roaming\microsoft\office\live meeting`
- `appdata\roaming\microsoft shared\livemeeting shared\`
- `appdata\roaming\mozilla\firefox\crash reports\`
- `appdata\roaming\mcafee\common framework\`
What's included with Amazon Linux WorkSpace custom images

When you create an image from an Amazon Linux WorkSpace, the entire contents of the user volume (/home) are removed. The contents of the root volume (/) are included, except the following 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
Update a custom WorkSpaces bundle

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

Important
Existing WorkSpaces aren't automatically updated when you update the bundle that they're based on. To update existing WorkSpaces that are based on a bundle that you've updated, you must either rebuild the WorkSpaces or delete and recreate them.

To update a bundle using the console

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

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

2. If you are still connected to the WorkSpace, disconnect by choosing Amazon WorkSpaces and Disconnect in the WorkSpaces client application.


4. In the navigation pane, choose WorkSpaces.

5. Select the WorkSpace and choose Actions, Create Image. If the status of the WorkSpace is STOPPED, you must start it first (choose Actions, Start WorkSpaces) before you can choose Actions, Create Image.

6. Enter an image name and a description, and then choose Create Image. The WorkSpace is unavailable while the image is being created. For detailed information about the image creation process, see Create a custom WorkSpaces image and bundle (p. 181).

7. In the navigation pane, choose Bundles.

8. Choose the bundle to open its details page, and then under Source image, choose Edit.

9. On the Update source image page, select the image that you created and choose Update bundle.

10. As needed, update any existing WorkSpaces that are based on the bundle by rebuilding the WorkSpaces or deleting and recreating them. For more information, see Rebuild a WorkSpace (p. 167).

To update a bundle programmatically

To update a bundle programmatically, use the UpdateWorkspaceBundle API action. For more information, see UpdateWorkspaceBundle in the Amazon WorkSpaces API Reference.

Copy a custom WorkSpaces image

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

You can copy a Bring Your Own License (BYOL) image to another Region as long as the destination Region is enabled for BYOL.

Note
In the China (Ningxia) Region, you can copy images only within the same Region.
In the AWS GovCloud (US-West) Region, to copy images to and from other AWS Regions, contact AWS Support.
You can also copy an image that has been shared with you by another AWS account. For more information about shared images, see Share or unshare a custom WorkSpaces image (p. 196).

There are no additional charges for copying an image within or across Regions. However, the quota for the number of images in the destination Region applies. For more information about Amazon WorkSpaces quotas, see Amazon WorkSpaces quotas (p. 271).

**IAM Permissions to copy an image**

If you use an IAM user to copy an image, the user must have permissions for `workspaces:DescribeWorkspaceImages` and `workspaces:CopyWorkspaceImage`.

The following example policy allows the user to copy the specified image to the specified account in the specified Region.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
        "arn:aws:workspaces:us-east-1:123456789012:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

**Important**

If you are creating an IAM policy for copying shared images for accounts that don't own the images, you cannot specify an account ID in the ARN. Instead, you must use `*` for the account ID, as shown in the following example policy.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
        "arn:aws:workspaces:us-east-1:*:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

You can specify an account ID in the ARN only when that account owns the images to be copied.

For more information about working with IAM, see Identity and access management for WorkSpaces (p. 234).

**Bulk copy images**

You can copy images one by one using the console. To bulk copy images, use the `CopyWorkspaceImage` API operation or the `copy-workspace-image` command in the AWS Command Line Interface (AWS CLI).
For more information, see `CopyWorkspaceImage` in the *Amazon WorkSpaces API Reference* or see `copy-workspace-image` in the *AWS CLI Command Reference*.

**Important**
Before copying a shared image, be sure to verify that it has been shared from the correct AWS account. To determine if an image has been shared and to see the AWS account ID that owns an image, use the `DescribeWorkspaceImages` and `DescribeWorkspaceImagePermissions` API operations or the `describe-workspace-images` and `describe-workspace-image-permissions` commands in the AWS CLI.

**To copy an image using the console**
2. In the navigation pane, choose **Images**.
3. Select the image and choose **Actions**, **Copy image**.
4. For **Select destination**, select the AWS Region that you want to copy the image to.
5. For **Name of the copy**, enter the new name for the copied image, and for **Description**, enter a description for the copied image.
6. (Optional) Under **Tags**, enter tags for the copied image. For more information, see *Tag WorkSpaces resources* (p. 157).
7. Choose **Copy image**.

**Share or unshare a custom WorkSpaces image**

You can share custom WorkSpaces images across AWS accounts within the same AWS Region. After an image has been shared, the recipient account can copy the image to other AWS Regions as needed. For more information about copying images, see *Copy a custom WorkSpaces image* (p. 194).

**Note**
In the China (Ningxia) Region, you can copy images only within the same Region.
In the AWS GovCloud (US-West) Region, to copy images to and from other AWS Regions, contact AWS Support.

There are no additional charges for sharing an image. However, the quota for the number of images in the AWS Region applies. A shared image doesn’t count against the recipient account’s quota until the recipient copies the image. For more information about Amazon WorkSpaces quotas, see *Amazon WorkSpaces quotas* (p. 271).

To delete a shared image, you must unshare the image before you can delete it.

**Share Bring Your Own License images**

You can share Bring Your Own License (BYOL) images only with AWS accounts that are enabled for BYOL. The AWS account that you want to share BYOL images with must also be part of your organization (under the same payer account).

**Note**
Sharing BYOL images across AWS accounts isn't supported at this time in the AWS GovCloud (US-West) Region. To share BYOL images across accounts in the AWS GovCloud (US-West) Region, contact AWS Support.

**Images shared with you**

If images are shared with you, you can copy them. You can then use your copies of the shared images to create bundles for launching new WorkSpaces.

**Important**
Before copying a shared image, be sure to verify that it has been shared from the correct AWS account. To programmatically determine if an image has been shared, use the
Delete a custom bundle or image

You can delete unused custom bundles or custom images as needed.
Delete a bundle

To delete a bundle, you must first delete all of the WorkSpaces that are based on the bundle.

To delete a bundle using the console

2. In the navigation pane, choose Bundles.
3. Select the bundle and choose Delete.
4. When prompted for confirmation, choose Delete.

To delete a bundle programmatically

To delete a bundle programmatically, use the DeleteWorkspaceBundle API action. For more information, see DeleteWorkspaceBundle in the Amazon WorkSpaces API Reference.

Delete an image

After you delete a custom bundle, you can delete the image that you used to create or update the bundle.

To delete an image, you must first either delete any bundles that are associated with the image, or you must update those bundles to use another source image. You must also unshare the image if it is shared with other accounts. The image also can't be in the Pending or Validating state.

To delete an image using the console

2. In the navigation pane, choose Images.
3. Select the image and choose Delete.
4. When prompted for confirmation, choose Delete.

To delete an image programmatically

To delete an image programmatically, use the DeleteWorkspaceImage API action. For more information, see DeleteWorkspaceImage in the Amazon WorkSpaces API Reference.

Bring Your Own Windows desktop licenses

If your licensing agreement with Microsoft allows it, you can use your Windows 10 Enterprise or Windows 10 Pro desktop licenses for your WorkSpaces. To do this, you must Bring Your Own License (BYOL) and provide a Windows 10 license that meets the following requirements. For more information about using Microsoft software on AWS, see Amazon Web Services and Microsoft.

To stay compliant with Microsoft licensing terms, AWS runs your BYOL WorkSpaces on hardware that is dedicated to you in the AWS Cloud. By bringing your own license, you can provide a consistent experience for your users. For more information, see WorkSpaces Pricing.

Important

Image creation is not supported on Windows 10 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.
Contents

- Requirements (p. 199)
- Windows versions supported for BYOL (p. 200)
- Add Microsoft Office to Your BYOL image (p. 200)
- Step 1: Check the eligibility of your account for BYOL using the Amazon WorkSpaces console (p. 204)
- Step 2: Enable BYOL for your account for BYOL using the Amazon WorkSpaces console (p. 204)
- Step 3: Run the BYOL Checker PowerShell script on a Windows VM (p. 205)
- Step 4: Export the VM from your virtualization environment (p. 206)
- Step 5: Import the VM as an image into Amazon EC2 (p. 207)
- Step 6: Create a BYOL image using the WorkSpaces console (p. 207)
- Step 7: Create a custom bundle from the BYOL image (p. 208)
- Step 8: Register a dedicated directory for WorkSpaces (p. 208)
- Step 9: Launch your BYOL WorkSpaces (p. 209)

Requirements

Before you begin, verify the following:

- Your Microsoft licensing agreement allows Windows to be run in a virtual hosted environment.
- If you will be using non-GPU-enabled bundles (bundles other than Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro), verify that you will use a minimum of 100 WorkSpaces per Region. These 100 WorkSpaces can be any mix of AlwaysOn and AutoStop WorkSpaces. Using a minimum of 100 WorkSpaces per Region is a requirement for running your WorkSpaces on dedicated hardware. Running your WorkSpaces on dedicated hardware is necessary to comply with Microsoft licensing requirements. The dedicated hardware is provisioned on the AWS side, so your VPC can stay on default tenancy.

If you plan to use GPU-enabled (Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro) bundles, verify that you will run a minimum of 4 AlwaysOn or 20 AutoStop GPU-enabled WorkSpaces in a Region per month on dedicated hardware.

Note
- Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro bundles can be created only for the PCoIP protocol at this time.
- Graphics and GraphicsPro bundles aren't currently available in the Asia Pacific (Mumbai) Region.

WorkSpaces can use a management interface in the /16 IP address range. The management interface is connected to a secure WorkSpaces management network used for interactive streaming. This allows WorkSpaces to manage your WorkSpaces. For more information, see Network interfaces (p. 26). You must reserve a /16 netmask from at least one of the following IP address ranges for this purpose:

- 10.0.0.0/8
- 100.64.0.0/10
- 172.16.0.0/12
- 192.168.0.0/16
- 198.18.0.0/15

Note
- As you adopt the WorkSpaces service, the available management interface IP address ranges frequently change. To determine which ranges are currently available, run the list-available-management-cidr-ranges AWS Command Line Interface (AWS CLI) command.
Windows versions supported for BYOL

Your VM must run one of the following Windows versions:

- Windows 10 Version 2004 (May 2020 Update)
- Windows 10 Version 20H2 (October 2020 Update)
- Windows 10 Version 21H1 (May 2021 Update)
- Windows 10 Version 21H2 (December 2021 Update)

All supported OS versions support all of the compute types available in the AWS Region where you're using WorkSpaces. Versions of Windows that are no longer supported by Microsoft are not guaranteed to work and are not supported by AWS Support.

Note
Windows 10 N versions are not supported for BYOL at this time.

Add Microsoft Office to Your BYOL image

During the BYOL image ingestion process, if you are using Windows 10, you have the option to subscribe to Microsoft Office Professional 2016 (32-bit) or 2019 (64-bit) through AWS. If you choose this option,
Office is pre-installed in your BYOL image and included on any WorkSpaces that you launch from this image.

If you choose to subscribe to Office through AWS, additional charges will apply. For more information, see WorkSpaces Pricing.

**Important**

- If Microsoft Office is already installed on the VM that you are using to create your BYOL image, you must uninstall it from the VM if you want to subscribe to Office through AWS.
- If you plan to subscribe to Office through AWS, make sure that your VM has at least 20 GB of free disk space.

**Note**

Graphics.g4dn and GraphicsPro.g4dn BYOL images only support Office 2019 and do not support Office 2016.

If you choose to subscribe to Office, the BYOL image ingestion process takes a minimum of 3 hours.

For details about subscribing to Office during the BYOL ingestion process, see Step 6: Create a BYOL image using the WorkSpaces console (p. 207).

**Office language settings**

We choose the language used for your Office subscription based on the AWS Region where you’re performing your BYOL image ingestion. For example, if you’re performing your BYOL image ingestion in the Asia Pacific (Tokyo) Region, your Office subscription has Japanese as its language.

By default, we install a number of frequently used Office language packs on your WorkSpaces. If the language pack that you want isn’t installed, you can download additional language packs from Microsoft. For more information, see Language Accessory Pack for Office in the Microsoft documentation.

To change the language for Office, you have several options:

**Option 1: Allow individual users to customize their Office language settings**

Individual users can adjust the Office language settings on their WorkSpaces. For more information, see Add an editing or authoring language or set language preferences in Office in the Microsoft documentation.

**Option 2: Use GPO administrative templates (.admx/.adml) to enforce default Office language settings for all of your WorkSpaces users**

You can use Group Policy Object (GPO) settings to enforce default Office language settings for your WorkSpaces users.

**Note**

Your WorkSpaces users will not be able to override language settings enforced through GPO.

For more information about using GPO to set the language for Office, see Customize language setup and settings for Office in the Microsoft documentation. Office 2016 and Office 2019 use the same GPO settings (labeled with Office 2016).

To work with GPOs, you must install the Active Directory administration tools. For information about using the Active Directory administration tools to work with GPOs, see Set up Active Directory Administration Tools for WorkSpaces (p. 101).

Before you can configure Office 2016 or Office 2019 policy settings, you must download the administrative template files (.admx/.adml) for Office from the Microsoft Download Center. After you
download the administrative template files, you must add the office16.admx and office16.adml files to the Central Store of the domain controller for your WorkSpaces directory. (The office16.admx and office16.adml files apply to both Office 2016 and Office 2019.) For more information about working with .admx and .adml files, see How to create and manage the Central Store for Group Policy Administrative Templates in Windows in the Microsoft documentation.

The following procedure describes how to create the Central Store and add the administrative template files to it. Perform the following procedure on a directory administration WorkSpace or Amazon EC2 instance that is joined to your WorkSpaces directory.

To install the Group Policy administrative template files for Office

1. Download the administrative template files (.admx/.adml) for Office from the Microsoft Download Center.
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open Windows File Explorer, and in the address bar, enter your organization’s fully qualified domain name (FQDN), such as \example.com.
3. Open the SYSVOL folder.
4. Open the folder with the FQDN name.
5. Open the Policies folder. You should now be in \FQDN\SYSVOL\FQDN\Policies.
6. If it doesn’t already exist, create a folder named PolicyDefinitions.
7. Open the PolicyDefinitions folder.
8. Copy the office16.admx file into the \FQDN\SYSVOL\FQDN\Policies\PolicyDefinitions folder.
10. Open the en-US folder.
11. Copy the office16.adml file into the \FQDN\SYSVOL\FQDN\Policies\PolicyDefinitions\en-US folder.

To configure the GPO language settings for Office

1. On your directory administration WorkSpace or Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (gpmc.msc).
2. Expand the forest (Forest:FQDN).
3. Expand Domains.
4. Expand your FQDN (for example, example.com).
5. Select your FQDN, open the context (right-click) menu or open the Action menu, and choose Create a GPO in this domain, and Link it here.
6. Name your GPO (for example, Office).
7. Select your GPO, open the context (right-click) menu or open the Action menu, and choose Edit.
8. In the Group Policy Management Editor, choose User Configuration, Policies, Administrative Template Policy definitions (ADMX files) retrieved from the local computer, Microsoft Office 2016, and Language Preferences.

Note
Office 2016 and Office 2019 use the same GPO settings (labeled with Office 2016). If you don’t see Administrative Template Policy definitions (ADMX files) retrieved from the local computer under User Configuration, Policies, the office16.admx and office16.adml files aren’t correctly installed on your domain controller.

9. Under Language Preferences, specify the language that you want for the following settings. Be sure to set each setting to Enabled, and then under Options, select the language you want. Choose OK to save each setting.
Add Microsoft Office to Your BYOL image

• Display Language > Display help in
• Display Language > Display menus and dialog boxes in
• Editing languages > Primary Editing Language

10. Close the Group Policy Management tool when you’re finished.

11. Group Policy setting changes take effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

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

Option 3: Update the Office language registry settings on your WorkSpaces

To set the Office language settings through the registry, update the following registry settings:

• HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources \UILanguage
• HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources \HelpLanguage

For these settings, add a DWORD key value with the appropriate Office locale ID (LCID). For example, the LCID for English (US) is 1033. Because LCIDs are decimal values, you must set the Base option for the DWORD value to Decimal. For a list of the Office LCIDs, see Language identifiers and OptionState Id values in Office 2016 in the Microsoft documentation.

You can apply these registry settings to your WorkSpaces through GPO settings or a logon script.

For more information about working with the language settings for Office, see Customize language setup and settings for Office in the Microsoft documentation.

Add Office to your existing BYOL WorkSpaces

You can also add a subscription to Office to your existing BYOL WorkSpaces. After you have created a BYOL bundle with Office installed, you can use the WorkSpaces migration feature to migrate your existing BYOL WorkSpaces to the BYOL bundle that is subscribed to Office. For more information, see Migrate a WorkSpace (p. 175).

Migrate between versions of Microsoft Office

To migrate from Office 2016 to Office 2019 or from Office 2019 to Office 2016, you must create a BYOL bundle that is subscribed to the version of Office that you want to migrate to. Then, you use the WorkSpaces migration feature to migrate your existing BYOL WorkSpaces that are subscribed to Office to the BYOL bundle that is subscribed to the version of Office that you want to migrate to.

For example, to migrate from Office 2016 to Office 2019, create a BYOL bundle that is subscribed to Office 2019. Then use the WorkSpaces migration feature to migrate your existing BYOL WorkSpaces that are subscribed to Office 2016 to the BYOL bundle that is subscribed to Office 2019.

For more information about the migration process, see Migrate a WorkSpace (p. 175).

Unsubscribe from Office

To unsubscribe from Office, you must create a BYOL bundle that is not subscribed to Office. Then use the WorkSpaces migration feature to migrate your existing BYOL WorkSpaces to the BYOL bundle that is not subscribed to Office. For more information, see Migrate a WorkSpace (p. 175).
Office updates

If you have subscribed to Office through AWS, Office updates are included as part of your regular Windows updates. To stay current on all security patches and updates, we recommend that you periodically update your BYOL base images.

Step 1: Check the eligibility of your account for BYOL using the Amazon WorkSpaces console

Before you can enable your account for BYOL, you must go through a verification process to confirm your eligibility for BYOL. Until you go through this process, the Enable BYOL option will not be available in your Amazon WorkSpaces console.

Note
The verification process takes at least one business day and can take longer if you want to link two or more BYOL-enabled AWS accounts together so that they use the same underlying hardware.

To check the eligibility of your account for BYOL by using the Amazon WorkSpaces console

2. In the navigation pane, choose Account Settings, and then under Bring your own license (BYOL), choose View WorkSpaces BYOL settings. If your account is not currently eligible for BYOL, a message provides guidance for next steps. To get started, contact your AWS account manager or sales representative, or contact the AWS Support Center. Your contact will verify your eligibility for BYOL.

To determine your eligibility for BYOL, your contact will need certain information from you. For example, you might be asked to answer the following questions.

- Have you reviewed and accepted the BYOL requirements (p. 199) listed earlier?
- In which AWS Regions do you need your account enabled for BYOL?
- How many BYOL WorkSpaces do you plan to deploy per AWS Region?
- What is your ramp-up plan?
- Are you purchasing WorkSpaces from a reseller?
- What bundle types do you need for BYOL?
- Does your organization have any other AWS accounts enabled for BYOL in the same Region? If yes, do you want to link these accounts so that they use the same underlying hardware?

If the accounts are linked, the total number of WorkSpaces deployed in these accounts is aggregated together for the purposes of determining your eligibility for BYOL. Be aware that linking the accounts will take additional time. If you want to link the accounts, be ready to provide the account numbers to your contact.

3. After your eligibility is confirmed for BYOL, you can proceed to the next step, where you enable BYOL for your account in the Amazon WorkSpaces console.

Step 2: Enable BYOL for your account for BYOL using the Amazon WorkSpaces console

To enable BYOL for your account, you must specify a management network interface. This interface is connected to a secure Amazon WorkSpaces management network. It is used for interactive streaming of the WorkSpace desktop to Amazon WorkSpaces clients, and to allow Amazon WorkSpaces to manage the WorkSpace.
**Note**
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**
2. In the navigation pane, choose Account Settings, and then under Bring your own license (BYOL), choose View WorkSpaces BYOL settings.
3. On the Account Settings page, under Bring Your Own License (BYOL), choose Enable BYOL.
   
   If you don't see the Enable BYOL option, this means that your account is not currently eligible for BYOL. For more information, see Step 1: Check the eligibility of your account for BYOL using the Amazon WorkSpaces console (p. 204).
4. Under Bring Your Own License (BYOL), in the Management network interface IP address range area, choose an IP address range, and then choose Display available CIDR blocks.

   Amazon WorkSpaces searches for and displays available IP address ranges as IPv4 Classless Inter-Domain Routing (CIDR) blocks, within the range that you specify. If you require a specific IP address range, you can edit the search range.

   **Important**
   After you specify an IP address range, you cannot modify it. Make sure to specify an IP address range that doesn't conflict with the ranges used by your internal network. If you have any questions about which range to specify, contact your AWS account manager or sales representative, or contact the AWS Support Center before proceeding.
5. Choose the CIDR block that you want from the list of results, and then choose Enable BYOL.

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

**Step 3: Run the BYOL Checker PowerShell script on a Windows VM**

After you enable BYOL for your account, you must confirm that your VM meets the requirements for BYOL. To do so, perform these steps to download and run the WorkSpaces BYOL Checker PowerShell script. The script performs a series of tests on the VM that you plan to use to create your image.

**Important**
The VM must pass all tests before you can use it for BYOL.

**To download the BYOL Checker script**

Before you download and run the BYOL Checker script, verify that the latest Windows security updates are installed on your VM. While this script runs, it disables the Windows Update service.

1. Download the BYOL Checker script .zip file from https://tools.amazonworkspaces.com/ BYOLChecker.zip to your Downloads folder.
2. In your Downloads folder, create a BYOL folder.
3. Extract the files from BYOLChecker.zip and copy them to the Downloads\BYOL folder.
4. Delete the Downloads\BYOLChecker.zip folder so that only the extracted files remain.

Perform these steps to run the BYOL Checker script.
To run the BYOL Checker script

1. From the Windows desktop, open Windows PowerShell. Choose the Windows Start button, right-click Windows PowerShell, and choose Run as administrator. If you are prompted by User Account Control to choose whether you want PowerShell to make changes to your device, choose Yes.
2. At the PowerShell command prompt, change to the directory where the BYOL Checker script is located. For example, if the script is located in the Downloads\BYOL directory, enter the following command and press Enter:
   
   ```
   cd C:\Users\username\Downloads\BYOL
   ```
3. Enter the following command to update the PowerShell execution policy on the computer. Doing so allows the BYOL Checker script to run:
   
   ```
   Set-ExecutionPolicy Unrestricted
   ```
4. When prompted to confirm whether to change the PowerShell execution policy, enter A to specify Yes to All.
5. Enter the following command to run the BYOL Checker script:
   
   ```
   .\BYOLChecker.ps1
   ```
6. If a security notification appears, press the R key to Run Once.
7. In the WorkSpaces Image Validation dialog box, choose Begin Tests.
8. After each test is completed, you can view the status of the test. For any test with a status of FAILED, choose Info to display information about how to resolve the issue that caused the failure. If any tests display a status of WARNING, choose the Fix All Warnings button.
9. If applicable, resolve any issues that cause test failures and warnings, and repeat Step 7 (p. 206) and Step 8 (p. 206) 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, BYOLPrevalidationlogYYYY-MM-DD_HHmmss.txt and ImageInfo.text. These files are located in the directory that contains the BYOL Checker script files.
    
    **Tip**
    
    Do not delete these files. If an issue occurs, they might be helpful in troubleshooting.
11. After your VM passes all tests, you get a Validation Successful message. 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. Shut down the VM and create a snapshot of it.
13. Start the VM again. Choose Run Sysprep. If Sysprep is successful, your VM that you exported after Step 12 (p. 206) can be imported into Amazon Elastic Compute Cloud (Amazon EC2). Otherwise, review the Sysprep logs, roll back to the snapshot taken at Step 12 (p. 206), resolve the reported issues, take a new snapshot, and run the BYOL Checker script again.

    The most common reason that Sysprep fails is that the Modern AppX Packages are not uninstalled for all users. Use the Remove-AppxPackage PowerShell cmdlet to remove the AppX Packages.
14. After you have successfully created your image, you can remove the WorkSpaces_BYOL account.

Step 4: Export the VM from your virtualization environment

To create an image for BYOL, you must first export the VM from your virtualization environment. The VM must be on a single volume with a maximum size of 70 GB and at least 10 GB of free space. For more information, see the documentation for your virtualization environment and Export Your VM from its Virtualization Environment in the VM Import/Export User Guide.
Step 5: Import the VM as an image into Amazon EC2

After you export your VM, review the requirements for importing Windows operating systems from a VM. Take action as needed. For more information, see VM Import/Export Requirements.

Note
Importing a VM with an encrypted disk is not supported. If you've opted in to default encryption for Amazon Elastic Block Store (Amazon EBS) volumes, you must deselect that option before importing your VM.

Import your VM into Amazon EC2 as an Amazon Machine Image (AMI). Use one of the following methods:

- Use the `import-image` command with the AWS CLI. For more information, see `import-image` in the AWS CLI Command Reference.
- Use the ImportImage API operation. For more information, see ImportImage in the Amazon EC2 API Reference.

For more information, see Importing a VM as an Image in the VM Import/Export User Guide.

Step 6: Create a BYOL image using the WorkSpaces console

Perform these steps to create a WorkSpaces BYOL image.

Note
To perform this procedure, verify that you have AWS Identity and Access Management (IAM) permissions to:

- Call WorkSpaces `ImportWorkspaceImage`.
- Call Amazon EC2 `DescribeImages` on the Amazon EC2 image that you want to use to create the BYOL image.
- Call Amazon EC2 `ModifyImageAttribute` on the Amazon EC2 image that you want to use to create the BYOL image. Make sure that the launch permissions on the Amazon EC2 image are not restricted. The image must be shareable throughout the BYOL image creation process.

For an example IAM policy specific to BYOL WorkSpaces, see Identity and access management for WorkSpaces (p. 234). For more information about working with IAM permissions, see Changing Permissions for an IAM User in the IAM User Guide.

To create a Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro bundle from your image, contact the AWS Support Center to get your account added to the allow list. After your account is on the allow list, you can use the AWS CLI `import-workspace-image` command to ingest the Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro image. For more information, see `import-workspace-image` in the AWS CLI Command Reference.

To create an image from the Windows VM

2. In the navigation pane, choose Images.
3. Choose Create BYOL image.
4. On the Create BYOL image page, do the following:
   - For AMI ID, choose the EC2 Console link, and choose the Amazon EC2 image that you imported as described in the previous section (Step 5: Import the VM as an image into Amazon EC2 (p. 207)).
The image name must begin with `ami-` and be followed by the identifier for the AMI (for example, `ami-1234567e`).

- For **Image name**, enter a unique name for the image.
- For **Description**, enter a description to help you quickly identify the image.
- For **Instance type**, choose the appropriate bundle type (either **Regular**, **Graphics.g4dn**, **GraphicsPro.g4dn**, **Graphics**, or **GraphicsPro**), depending on which protocol you want to use for your image, either PCoIP or WorkSpaces Streaming Protocol (WSP). For non-GPU-enabled bundles (bundles other than Graphics.g4dn, GraphicsPro.g4dn, Graphics, or GraphicsPro), choose **Regular**.

  **Note**
  Graphics.g4dn, GraphicsPro.g4dn, Graphics, and GraphicsPro images can be created only for the PCoIP protocol at this time.

  - (Optional) For **Select applications**, choose which version of Microsoft Office you want to subscribe to. For more information, see **Add Microsoft Office to Your BYOL image** (p. 200).
  - (Optional) For **Tags**, choose **Add new tag** to associate tags with this image. For more information, see **Tag WorkSpaces resources** (p. 157).

5. Choose **Create BYOL image**.

While your image is being created, the image's status on the **Images** page of the console appears as **Pending**. The BYOL ingestion process takes a minimum of 90 minutes. If you have subscribed to Office as well, expect the process to take a minimum of 3 hours.

If the image validation does not succeed, the console displays an error code. When the image creation is complete, the status changes to **Available**.

### Step 7: Create a custom bundle from the BYOL image

After your BYOL image is created, you can use the image to create a custom bundle. For information, see **Create a custom WorkSpaces image and bundle** (p. 181).

### Step 8: Register a dedicated directory for WorkSpaces

To use BYOL images for WorkSpaces, you must register a directory for this purpose.

**To register a directory for 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 an AWS Managed Microsoft AD directory or an AD Connector directory for WorkSpaces that does not run on dedicated hardware, you can set up a new AWS Managed Microsoft AD directory or AD Connector directory for this purpose. You can also deregister the directory and then 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**

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 9: 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 WorkSpaces (p. 103)**.
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. 210).

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. 214).

CloudTrail logs

AWS CloudTrail provides a record of actions taken by a user, role, or an AWS service in WorkSpaces. Using the information collected by CloudTrail, you can determine the request that was made to WorkSpaces, the IP address from which the request was made, who made the request, when it was made, and additional details. For more information, see Logging WorkSpaces API Calls by Using CloudTrail. AWS CloudTrail logs successful and unsuccessful sign-in events for smart card users. For more information, see Understanding AWS sign-in events for smart card users (p. 217).

Monitor your WorkSpaces using CloudWatch metrics

WorkSpaces and Amazon CloudWatch are integrated, so you can gather and analyze performance metrics. You can monitor these metrics using the CloudWatch console, the CloudWatch command line interface, or programmatically using the CloudWatch API. CloudWatch also allows you to set alarms when you reach a specified threshold for a metric.

For more information about using CloudWatch and alarms, see the Amazon CloudWatch User Guide.

Prerequisites

To get CloudWatch metrics, enable access on port 443 on the AMAZON subset in the us-east-1 Region. For more information, see IP address and port requirements for WorkSpaces (p. 14).

Contents

- WorkSpaces metrics (p. 210)
- Dimensions for WorkSpaces metrics (p. 213)
- Monitoring example (p. 213)

WorkSpaces metrics

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

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Dimensions</th>
<th>Statistics</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>that are under maintenance.</td>
<td>WorkspaceId</td>
<td>Minimum, Data Samples</td>
<td></td>
</tr>
<tr>
<td>TrustedDeviceValidationAttempt</td>
<td>The number of device authentication signature validation attempts.</td>
<td>DirectoryId</td>
<td>Average, Sum, Maximum, Minimum, Data Samples</td>
<td>Count</td>
</tr>
<tr>
<td>TrustedDeviceValidationSuccess</td>
<td>The number of successful device authentication signature validations.</td>
<td>DirectoryId</td>
<td>Average, Sum, Maximum, Minimum, Data Samples</td>
<td>Count</td>
</tr>
<tr>
<td>TrustedDeviceValidationFailure</td>
<td>The number of failed device authentication signature validations.</td>
<td>DirectoryId</td>
<td>Average, Sum, Maximum, Minimum, Data Samples</td>
<td>Count</td>
</tr>
<tr>
<td>TrustedDeviceCertificateDaysBeforeExpiration</td>
<td>Days left before the root certificate associated with the directory is expired.</td>
<td>CertificateId</td>
<td>Average, Sum, Maximum, Minimum, Data Samples</td>
<td>Count</td>
</tr>
</tbody>
</table>

1 WorkSpaces periodically sends status requests to a WorkSpace. A WorkSpace is marked Available when it responds to these requests, and Unhealthy when it fails to respond to these requests. These metrics are available at a per-WorkSpace level of granularity, and also aggregated for all WorkSpaces in an organization.

2 WorkSpaces records metrics on connections made to each WorkSpace. These metrics are emitted after a user has successfully authenticated via the WorkSpaces client and the client then initiates a session. The metrics are available at a per-WorkSpace level of granularity, and also aggregated for all WorkSpaces in a directory.

3 WorkSpaces periodically sends connection status requests to a WorkSpace. Users are reported as connected when they are actively using their sessions. This metric is available at a per-WorkSpace level of granularity, and is also aggregated for all WorkSpaces in an organization.

4 This metric applies to WorkSpaces that are configured with an AutoStop running mode. If you have maintenance enabled for your WorkSpaces, this metric captures the number of WorkSpaces that are currently under maintenance. This metric is available at a per-WorkSpace level of granularity, which describes when a WorkSpace went into maintenance and when it was removed.

5 This metric is currently emitted only for PCoIP WorkSpaces.

6 If the trusted devices feature is enabled for the directory, Amazon WorkSpaces uses certificate-based authentication to determine whether a device is trusted. When users attempt to access their WorkSpaces, these metrics are emitted to indicate successful or failed trusted device authentication. These metrics are available at a per-directory level of granularity, and only for the Amazon WorkSpaces Windows and macOS client applications.
Dimensions for 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>
<tr>
<td>CertificateId</td>
<td>Filters the metric data to the specified root certificate associated with the directory. The form of the certificate ID is wsc-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.

   ```
   aws cloudwatch describe-alarms --state-value "ALARM"
   {
     "MetricAlarms": [
       {
         "Dimensions": [
           {
             "Name": "DirectoryId",
             "Value": "directory_id"
           }
         ]
       }
     }
   }
   ```

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

   ```
   aws workspaces describe-workspaces --directory-id directory_id
   {
     "Workspaces": [
       {
         "WorkspaceId": "workspace1_id",
         ...
       },
       {
         "WorkspaceId": "workspace2_id",
         ...
       }
     ]
   }
   ```
Monitor your WorkSpaces using CloudWatch Events

You can use events from Amazon WorkSpaces to view, search, download, archive, analyze, and respond to successful logins to your WorkSpaces. For example, you can use events for the following purposes:

- Store or archive WorkSpaces login events as logs for future reference, analyze the logs to look for patterns, and take action based on those patterns.
- Use the WAN IP address to determine where users are logged in from, and then use policies to allow users access only to files or data from WorkSpaces that meet the access criteria found in the event type of WorkSpaces Access.
- Analyze login data and perform automated actions using AWS Lambda.
- Use policy controls to block access to files and applications from unauthorized IP addresses.

Amazon WorkSpaces emits these events on a best-effort basis. Events are delivered to EventBridge in near real time. With EventBridge, you can create rules that trigger programmatic actions in response to an event. For example, you can configure a rule that invokes an SNS topic to send an email notification or invokes a Lambda function to take some action. For more information, see the Amazon EventBridge User Guide.
WorkSpaces Access events

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

Events emitted for WorkSpaces using the WorkSpaces Streaming Protocol (WSP) require the WorkSpaces client application version 4.0.1 or later.

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

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

**workspacesClientProductName**

The following values are case-sensitive.

- WorkSpaces Desktop client — Windows, macOS, and Linux clients
- Amazon WorkSpaces Mobile client — iOS client
- WorkSpaces Mobile Client — Android clients
- WorkSpaces Chrome Client — Chromebook client
- WorkSpaces Web Client — Web Access client
- Teradici PCoIP Zero Client, Teradici PCoIP Desktop Client, or Dell Wyse PCoIP Client — Zero Client

**loginTime**

The time at which the user logged in to the WorkSpace.

**clientPlatform**

- Android
Create a rule to handle WorkSpaces events

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

**Prerequisite**

To receive email notifications, create an Amazon Simple Notification Service topic.

2. In the navigation pane, choose Topics.
3. Choose Create topic.
4. For Type, choose Standard.
5. For Name, enter a name for your topic.
6. Choose Create topic.
7. Choose Create subscription.
8. For Protocol, choose Email.
9. For Endpoint, enter the email address that receives the notifications.
10. Choose Create subscription.
11. You'll receive an email message with the following subject line: AWS Notification - Subscription Confirmation. Follow the directions to confirm your subscription.

**To create a rule to handle WorkSpaces events**

1. Open the Amazon EventBridge console at https://console.aws.amazon.com/events/.
2. Choose Create rule.
3. For Name, enter a name for your rule.
4. For Rule type, choose Rule with an event pattern.
5. Choose Next.
6. For Event pattern, do the following:
   a. For Event source, choose AWS services.
   b. For AWS service, choose WorkSpaces.
   c. For Event type, choose WorkSpaces Access.
Understanding AWS sign-in events for smart card users

AWS CloudTrail logs successful and unsuccessful sign-in events for smart card users. This includes sign-in events that are captured each time a user is prompted to solve a specific credential challenge or factor, as well as the status of that particular credential verification request. A user is signed in only after completing all required credential challenges, which results in a `UserAuthentication` event being logged.

The following table captures each of the sign-in CloudTrail event names and their purposes.

<table>
<thead>
<tr>
<th>Event name</th>
<th>Event purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>CredentialChallenge</td>
<td>Notifies that AWS sign-in has requested that the user solve a specific credential challenge and specifies the <code>CredentialType</code> that is required (for example, SMARTCARD).</td>
</tr>
<tr>
<td>CredentialVerification</td>
<td>Notifies that the user has attempted to solve a specific <code>CredentialChallenge</code> request, and specifies whether that credential has succeeded or failed.</td>
</tr>
<tr>
<td>UserAuthentication</td>
<td>Notifies that all authentication requirements that the user was challenged with have been successfully completed and that the user was successfully signed in. When users fail to successfully complete the required credential challenges, no <code>UserAuthentication</code> event is logged.</td>
</tr>
</tbody>
</table>

The following table captures additional useful event data fields contained within specific sign-in CloudTrail events.

<table>
<thead>
<tr>
<th>Event name</th>
<th>Event purpose</th>
<th>Sign-in event applicability</th>
<th>Example values</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthWorkflowID</td>
<td>Correlates all events emitted across an entire sign-in sequence. For each user sign-in, multiple events can be emitted by AWS sign-in.</td>
<td>CredentialChallenge, CredentialVerification, UserAuthentication</td>
<td>&quot;AuthWorkflowID&quot;: &quot;9de74b32-8362-4a01-a524-de21df59fd83&quot;</td>
</tr>
<tr>
<td>Event name</td>
<td>Event purpose</td>
<td>Sign-in event applicability</td>
<td>Example values</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>CredentialChallenge</td>
<td>Notifies that the user has attempted to solve a specific CredentialChallenge request and specifies whether that credential has succeeded or failed.</td>
<td>CredentialChallenge, CredentialVerification, UserAuthentication</td>
<td>CredentialType&quot;: &quot;SMARTCARD&quot; (possible values today: SMARTCARD)</td>
</tr>
<tr>
<td>LoginTo</td>
<td>Notifies that all authentication requirements that the user was challenged with have been successfully completed and that the user was successfully signed in. When users fail to successfully complete the required credential challenges, no UserAuthentication event is logged.</td>
<td>UserAuthentication</td>
<td>&quot;LoginTo&quot;: &quot;<a href="https://skylight.local">https://skylight.local</a>&quot;</td>
</tr>
</tbody>
</table>

Example events for AWS sign-in scenarios

The following examples show the expected sequence of CloudTrail events for different sign-in scenarios.

Contents

- Successful sign-in when authenticating with smart card (p. 218)
- Failed sign-in when authenticating with only a smart card (p. 220)

Successful sign-in when authenticating with smart card

The following sequence of events captures an example of a successful smart card sign-in.

CredentialChallenge

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:29Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awsRegion": "us-east-1",
    "sourceIPaddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
```
Successful Credential Verification

```json
{
   "eventVersion": "1.08",
   "userIdentity": {
      "type": "Unknown",
      "principalId": "509318101470",
      "arn": "",
      "accountId": "509318101470",
      "accessKeyId": ""
   },
   "eventTime": "2021-07-30T17:23:39Z",
   "eventSource": "signin.amazonaws.com",
   "eventName": "CredentialVerification",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "AWS Internal",
   "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
   "requestParameters": null,
   "responseElements": null,
   "additionalEventData": {
      "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
      "CredentialType": "SMARTCARD"
   },
   "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
   "eventID": "84c0a2ff-413f-4d0f-9108-f72c90a41b6c",
   "readOnly": false,
   "eventType": "AwsServiceEvent",
   "managementEvent": true,
   "eventCategory": "Management",
   "recipientAccountId": "509318101470",
   "serviceEventDetails": {
      "CredentialVerification": "Success"
   }
}
```

Successful User Authentication

```json
{
   "eventVersion": "1.08",
   "userIdentity": {
      "type": "Unknown",
      "principalId": "509318101470",
      "arn": "",
      "accountId": "509318101470",
      "accessKeyId": ""
   },
   "eventTime": "2021-07-30T17:23:39Z",
   "eventSource": "signin.amazonaws.com",
   "eventName": "UserAuthentication",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "AWS Internal",
   "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
   "requestParameters": null,
   "responseElements": null,
   "additionalEventData": {
      "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
      "CredentialType": "SMARTCARD"
   },
   "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
   "eventID": "84c0a2ff-413f-4d0f-9108-f72c90a41b6c",
   "readOnly": false,
   "eventType": "AwsServiceEvent",
   "managementEvent": true,
   "eventCategory": "Management",
   "recipientAccountId": "509318101470",
   "serviceEventDetails": {
      "UserAuthentication": "Success"
   }
}
```
Failed sign-in when authenticating with only a smart card

The following sequence of events captures an example of failed smart card sign-in.

CredentialChallenge

```json
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "509318101470",
    "arn": "",
    "accountId": "509318101470",
    "accessKeyId": ""
  },
  "eventTime": "2021-07-30T17:23:06Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialChallenge",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "73df266f-f812-4bd2-8e29-0b2abb358cdb",
    "CredentialType": "SMARTCARD"
  },
  "requestID": "73eb499d-91a8-4c18-9c5d-281fd45ab50a",
  "eventID": "f30a50ec-71cf-415a-a5ab-e287edc800da",
  "readOnly": false
}
```
Example events for AWS sign-in scenarios

Failed CredentialVerification

```json
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "509318101470",
    "arn": "",
    "accountId": "509318101470",
    "accessKeyId": ""
  },
  "eventTime": "2021-07-30T17:23:13Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialVerification",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userIdentity": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b358c358c35",
    "CredentialType": "SMARTCARD"
  },
  "requestID": "051ca316-0b0d-4d38-940b-5fe5794fda03",
  "eventID": "4e6fbfc7-0479-48da-b7dc-e875155a8177",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "509318101470",
  "serviceEventDetails": {
    "CredentialVerification": "Failure"
  }
}
```
Business continuity for Amazon WorkSpaces

Amazon WorkSpaces is built on the AWS global infrastructure, which is organized into AWS Regions and Availability Zones. These Regions and Availability Zones provide resiliency in terms of both physical isolation and data redundancy. For more information, see Resilience in Amazon WorkSpaces (p. 245).

Amazon WorkSpaces also provides cross-Region redirection, a feature that works with your Domain Name System (DNS) routing policies to redirect your WorkSpaces users to alternative WorkSpaces when their primary WorkSpaces aren't available. For example, by using DNS failover routing policies, you can connect your users to WorkSpaces in your specified failover Region when they can't access their WorkSpaces in the primary Region.

You can use cross-Region redirection to achieve regional resiliency and high availability. You can also use it for other purposes, such as traffic distribution or providing alternative WorkSpaces during maintenance periods. If you use Amazon Route 53 for your DNS configuration, you can take advantage of health checks that monitor Amazon CloudWatch alarms.

Contents
- Cross-region redirection for Amazon WorkSpaces (p. 222)

Cross-region redirection for Amazon WorkSpaces

With the cross-Region redirection feature in Amazon WorkSpaces, you can use a fully qualified domain name (FQDN) as the registration code for your WorkSpaces. Cross-Region redirection works with your Domain Name System (DNS) routing policies to redirect your WorkSpaces users to alternative WorkSpaces when their primary WorkSpaces aren't available. For example, by using DNS failover routing policies, you can connect your users to WorkSpaces in your specified failover AWS Region when they can't access their WorkSpaces in the primary Region.

You can use cross-Region redirection along with your DNS failover routing policies to achieve regional resiliency and high availability. You can also use this feature for other purposes, such as traffic distribution or providing alternative WorkSpaces during maintenance periods. If you use Amazon Route 53 for your DNS configuration, you can take advantage of health checks that monitor Amazon CloudWatch alarms.

To use this feature, you must set up WorkSpaces for your users in two (or more) AWS Regions. You must also create special FQDN-based registration codes called connection aliases. These connection aliases replace Region-specific registration codes for your WorkSpaces users. (The Region-specific registration codes remain valid; however, for cross-Region redirection to work, your users must use the FQDN instead as their registration code.)

To create a connection alias, you specify a connection string, which is your FQDN, such as www.example.com or desktop.example.com. To use this domain for cross-Region redirection, you must register it with a domain registrar and configure the DNS service for your domain.

After you've created your connection aliases, you associate them with your WorkSpaces directories in different Regions to create association pairs. Each association pair has a primary Region and one or more failover Regions. If an outage occurs in the primary Region, your DNS failover routing policies redirect your WorkSpaces users to the WorkSpaces that you've set up for them in the failover Region.

To designate your primary and failover Regions, you define the Region priority (either primary or secondary) when configuring your DNS failover routing policies.
Prerequisites

- You must own and register the domain that you want to use as the FQDN in your connection aliases. If you're not already using another domain registrar, you can use Amazon Route 53 to register your domain. For more information, see Registering domain names using Amazon Route 53 in the Amazon Route 53 Developer Guide.

  Important
  You must have all necessary rights to use any domain name that you use in conjunction with Amazon WorkSpaces. You agree that the domain name does not violate or infringe on the legal rights of any third party or otherwise violate applicable law.

  The total length of your domain name can't exceed 255 characters. For more information about domain names, see DNS domain name format in the Amazon Route 53 Developer Guide.

  Cross-Region redirection works with both public domain names and domain names in private DNS zones. If you're using a private DNS zone, you must provide a virtual private network (VPN) connection to the virtual private cloud (VPC) that contains your WorkSpaces. If your WorkSpaces users attempt to use a private FQDN from the public internet, the WorkSpaces client applications return the following error message:

  "We're unable to register the WorkSpace because of a DNS server issue. Contact your administrator for help."

- You must set up your DNS service and configure the necessary DNS routing policies. Cross-Region redirection works in conjunction with your DNS routing policies to redirect your WorkSpaces users as needed.

- In each primary and failover Region where you want to set up cross-Region redirection, create WorkSpaces for your users. Make sure that you use the same usernames in each WorkSpaces directory in each Region. To keep your Active Directory user data in sync, we recommend using AD Connector to point to the same Active Directory in each Region where you've set up WorkSpaces for your users. For more information about creating WorkSpaces, see Launch WorkSpaces (p. 103).

  Important
  If you configure your AWS Managed Microsoft AD directory for multi-Region replication, only the directory in the primary Region can be registered for use with Amazon WorkSpaces. Attempts to register the directory in a replicated Region for use with Amazon WorkSpaces will fail. Multi-Region replication with AWS Managed Microsoft AD isn't supported for use with Amazon WorkSpaces within replicated Regions.
When you've finished setting up cross-Region redirection, you must make sure your WorkSpaces users are using the FQDN-based registration code instead of the Region-based registration code (for example, WSpdx+ABC12D) for their primary Region. To do this, you must send them an email with the FQDN connection string by using the procedure in Step 5: Send the connection string to your WorkSpaces users (p. 229).

**Note**
If you create your users in the WorkSpaces console instead of creating them in Active Directory, WorkSpaces automatically sends an invitation email to your users with a Region-based registration code whenever you launch a new WorkSpace. This means that when you set up WorkSpaces for your users in the failover Region, your users will also automatically receive emails for these failover WorkSpaces. You will need to instruct your users to ignore emails with Region-based registration codes.

**Limitations**

- Cross-Region redirection doesn't automatically check whether connections to the primary Region have failed and then fails your WorkSpaces over to another Region. In other words, automatic failover doesn't occur.

To implement an automatic failover scenario, you must use some other mechanism in conjunction with cross-Region redirection. For example, you can use an Amazon Route 53 failover DNS routing policy paired with a Route 53 health check that monitors a CloudWatch alarm in the primary Region. If the CloudWatch alarm in the primary Region is triggered, your DNS failover routing policy then redirects your WorkSpaces users to the WorkSpaces that you've set up for them in the failover Region.

- When you're using cross-Region redirection, user data isn't persisted between WorkSpaces in different Regions. To ensure that users can access their files from different Regions, we recommend that you set up Amazon WorkDocs for your WorkSpaces users, if Amazon WorkDocs is supported in your primary and failover Regions. For more information about Amazon WorkDocs, see Amazon WorkDocs Drive in the Amazon WorkDocs Administration Guide. For more information about enabling Amazon WorkDocs for your WorkSpace users, see Register a directory with WorkSpaces (p. 90) and Enable Amazon WorkDocs for AWS Managed Microsoft AD (p. 100). For information about how WorkSpaces users can set up Amazon WorkDocs on their WorkSpaces, see Integrate with WorkDocs in the Amazon WorkSpaces User Guide.

- Cross-Region redirection is supported only on version 3.0.9 or later of the Linux, macOS, and Windows WorkSpaces client applications.

- Cross-Region redirection is available in all AWS Regions where Amazon WorkSpaces is available, except for the AWS GovCloud (US-West) Region and the China (Ningxia) Region.

**Step 1: Create connection aliases**

Using the same AWS account, create connection aliases in each primary and failover Region where you want to set up cross-Region redirection.

**To create a connection alias**

2. In the upper-right corner of the console, select the primary AWS Region for your WorkSpaces.
3. In the navigation pane, choose Account Settings.
4. Under Cross-Region redirection, choose Create connection alias.
5. For **Connection string**, enter an FQDN, such as www.example.com or desktop.example.com. A connection string can be a maximum of 255 characters. It can include only letters (A-Z and a-z), numbers (0-9), and the following characters: .-
Important
After you create a connection string, it is always associated with your AWS account. You cannot recreate the same connection string with a different account, even if you delete all instances of it from the original account. The connection string is globally reserved for your account.

6. (Optional) Under Tags, specify any tags that you want to associate with your connection alias.
7. Choose Create connection alias.
8. Repeat these steps, but in Step 2 (p. 224), be sure to select the failover Region for your WorkSpaces. If you have more than one failover Region, repeat these steps for each failover Region. Be sure to use the same AWS account to create the connection alias in each failover Region.

(Optional) Step 2: Share a connection alias with another account

You can share a connection alias with one other AWS account in the same AWS Region. Sharing a connection alias with another account gives that account permission to associate or disassociate that alias with a directory owned by that account in the same Region only. Only the account that owns a connection alias can delete the alias.

Note
A connection alias can be associated with only one directory per AWS Region. If you share a connection alias with another AWS account, only one account (your account or the shared account) can associate the alias with a directory in that Region.

To share a connection alias with another AWS account

2. In the upper-right corner of the console, select the AWS Region where you want to share the connection alias with another AWS account.
3. In the navigation pane, choose Account Settings.
4. Under Cross-Region redirection associations, select the connection string, and then choose Actions, Share/unshare connection alias.

   You can also share an alias from the details page for your connection alias. To do so, under Shared account, choose Share connection alias.

5. On the Share/unshare connection alias page, under Share with an account, enter the AWS account ID that you want to share your connection alias with in this AWS Region.
6. Choose Share.

Step 3: Associate connection aliases with directories in each Region

Associating the same connection alias with a WorkSpaces directory in two or more Regions creates an association pair between the directories. Each association pair has a primary Region and one or more failover Regions.

For example, if your primary Region is the US West (Oregon) Region, you can pair your WorkSpaces directory in the US West (Oregon) Region with a WorkSpaces directory in the US East (N. Virginia) Region. If an outage occurs in the primary Region, cross-Region redirection works in conjunction with your DNS failover routing policies and any health checks that you've put in place on the US West (Oregon) Region.
Step 4: Configure your DNS service and set up DNS routing policies

After you've created your connection aliases and your connection alias association pairs, you can then configure the DNS service for the domain that you've used in your connection strings. You can use any DNS service provider for this purpose. If you don’t already have a preferred DNS service provider, you can use Amazon Route 53. For more information, see Configuring Amazon Route 53 as your DNS service in the Amazon Route 53 Developer Guide.

After you've configured the DNS service for your domain, you must set up the DNS routing policies that you want to use for cross-Region redirection. For example, you can use Amazon Route 53 health checks to determine whether your users can connect to their WorkSpaces in a particular Region. If your users can't connect, you can use a DNS failover policy to route your DNS traffic from one Region to another.

For more information about choosing your DNS routing policy, see Choosing a routing policy in the Amazon Route 53 Developer Guide. For more information about Amazon Route 53 health checks, see How Amazon Route 53 checks the health of your resources in the Amazon Route 53 Developer Guide.
When you're setting up your DNS routing policies, you will need the connection identifier for the association between the connection alias and the WorkSpaces directory in the primary Region. You will also need the connection identifier for the association between the connection alias and the WorkSpaces directory in your failover Region or Regions.

**Note**
The connection identifier is **not** the same as the connection alias ID. The connection alias ID starts with `wsca-`.

**To find the connection identifier for a connection alias association**

2. In the upper-right corner of the console, select the primary AWS Region for your WorkSpaces.
3. In the navigation pane, choose **Account Settings**.
4. Under **Cross-Region redirection associations**, select the connection string text (the FQDN) to view the connection alias details page.
5. On the details page for your connection alias, under **Associated directory**, make note of the value that's displayed for **Connection identifier**.
6. Repeat these steps, but in Step 2 (p. 227), be sure to select the failover Region for your WorkSpaces. If you have more than one failover Region, repeat these steps to find the connection identifier for each failover Region.

**Example: To set up a DNS failover routing policy using Route 53**

The following example sets up a public hosted zone for your domain. However, you can set up a public or a private hosted zone. For more information about setting up a hosted zone, see [Working with hosted zones in the Amazon Route 53 Developer Guide](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/creating-hosted-zone.html).

This example also uses a failover routing policy. You can use other routing policy types for your cross-Region redirection strategy. For more information about choosing your DNS routing policy, see [Choosing a routing policy in the Amazon Route 53 Developer Guide](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/choose-routing-policy.html).

When you're setting up a failover routing policy in Route 53, a health check is required for the primary Region. For more information about creating a health check in Route 53, see [Creating Amazon Route 53 health checks and configuring DNS failover](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-health-checks.html) and [Creating, updating, and deleting health checks](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-health-checks.html).

If you want to use an Amazon CloudWatch alarm with your Route 53 health check, you'll also need to set up a CloudWatch alarm to monitor the resources in your primary Region. For more information about CloudWatch, see [What Is Amazon CloudWatch? in the Amazon CloudWatch User Guide](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-overview.html). For more information about how Route 53 uses CloudWatch alarms in its health checks, see [How Route 53 determines the status of health checks that monitor CloudWatch alarms](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/how-route-53-monitors-cloudwatch-alarm.html) and [Monitoring a CloudWatch alarm in the Amazon Route 53 Developer Guide](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/how-route-53-monitors-cloudwatch-alarm.html).

To set up a DNS failover routing policy in Route 53, you first need to create a hosted zone for your domain.

2. In the navigation pane, choose **Hosted zones**, and then choose **Create hosted zone**.
3. On the **Created hosted zone** page, enter your domain name (such as `example.com`) under **Domain name**.
4. Under **Type**, choose **Public hosted zone**.
5. Choose **Create hosted zone**.

Then create a health check for your primary Region.
Step 4: Configure your DNS service and set up DNS routing policies

2. In the navigation pane, choose Health checks, and then choose Create health check.
3. On the Configure health check page, enter a name for your health check.
4. For What to monitor, select either Endpoint, Status of other health checks (calculated health check), or State of CloudWatch alarm.
5. Depending on what you’ve selected in the prior step, configure your health check, and then choose Next.
6. On the Get notified when health check fails page, for Create alarm, choose Yes or No.
7. Choose Create health check.

After you’ve created your health check, you can create the DNS failover records.

2. In the navigation pane, choose Hosted zones.
3. On the Hosted zones page, select your domain name.
4. On the details page for your domain name, choose Create record.
5. On the Choose routing policy page, select Failover, and then choose Next.
6. On the Configure records page, under Basic configuration, for Record name, enter your subdomain name. For example, if your FQDN is desktop.example.com, enter desktop.
   
   **Note**
   If you want to use the root domain, leave Record name blank. However, we recommend using a subdomain, such as desktop or workspaces, unless you’ve set up the domain solely for use with your WorkSpaces.
7. For Record type, select TXT – Used to verify email senders and for application-specific values.
8. Leave the TTL seconds settings at the default.
9. Under Failover records to add to your_domain_name, choose Define failover record.

Now you need to set up the failover records for your primary and failover Regions.

**Example: To set up the failover record for your primary Region**

1. In the Define failover record dialog box, for Value/route traffic to, select IP address or another value depending on the record type.
2. A box opens for you to enter your sample text entries. Enter the connection identifier for the connection alias association for your primary Region.
3. For Failover record type, choose Primary.
4. For Health check, select a health check that you’ve created for your primary Region.
5. For Record ID, enter a description to identify this record.
6. Choose Define failover record. Your new failover record appears under Failover records to add to your_domain_name.

**Example: To set up the failover record for your failover Region**

1. Under Failover records to add to your_domain_name, choose Define failover record.
2. In the Define failover record dialog box, for Value/route traffic to, select IP address or another value depending on the record type.
3. A box opens for you to enter your sample text entries. Enter the connection identifier for the connection alias association for your failover Region.
4. For Failover record type, choose Secondary.
5. (Optional) For Health check, enter a health check that you've created for your failover Region.
6. For Record ID, enter a description to identify this record.
7. Choose Define failover record. Your new failover record appears under Failover records to add to your_domain_name.

If the health check that you've set up for your primary Region fails, your DNS failover routing policy redirects your WorkSpaces users to your failover Region. Route 53 continues to monitor the health check for your primary Region, and when the health check for your primary Region no longer fails, Route 53 automatically redirects your WorkSpaces users back to their WorkSpaces in the primary Region.

For more information about creating DNS records, see Creating records by using the Amazon Route 53 console in the Amazon Route 53 Developer Guide. For more information about configuring DNS TXT records, see TXT record type in the Amazon Route 53 Developer Guide.

Step 5: Send the connection string to your WorkSpaces users

To make sure your users' WorkSpaces will be redirected as needed during an outage, you must send the connection string (FQDN) to your users. If you've already issued Region-based registration codes (for example, WSpdx+ABC12D) to your WorkSpaces users, those codes remain valid. However, for cross-Region redirection to work, your WorkSpaces users must use the connection string as their registration code when registering their WorkSpaces in the WorkSpaces client application.

Important
If you create your users in the WorkSpaces console instead of creating them in Active Directory, WorkSpaces automatically sends an invitation email to your users with a Region-based registration code (for example, WSpdx+ABC12D) whenever you launch a new WorkSpace. Even if you've already set up cross-Region redirection to work, your WorkSpaces users must use the connection string as their registration code when registering their WorkSpaces in the WorkSpaces client application.

To send the connection string to your WorkSpaces users

2. In the upper-right corner of the console, select the primary AWS Region for your WorkSpaces.
3. In the navigation pane, choose WorkSpaces.
4. On the WorkSpaces page, use the search box to search for a user that you want to send an invitation to, and then select the corresponding WorkSpace from the search results. You can select only one WorkSpace at a time.
5. Choose Actions, Invite User.
6. On the Invite Users to Their WorkSpaces page, you will see an email template to send to your users.
7. (Optional) If there is more than one connection alias associated with your WorkSpaces directory, select the connection string that you want your users to use from the Connection alias string list. The email template updates to display the string that you've chosen.
8. Copy the email template text and paste it into an email to the users using your own email application. In your email application, you can modify the text as needed. When the invitation email is ready, send it to your users.
What happens during cross-Region redirection

In the event of an outage, your WorkSpaces users are disconnected from their WorkSpaces in the primary Region. When they attempt to reconnect, they receive the following error message:

We can't connect to your WorkSpace. Check your network connection, and then try again.

Your users are then prompted to log in again. If they're using the FQDN as their registration code, when they log in again, your DNS failover routing policies redirect them to the WorkSpaces that you’ve set up for them in the failover Region.

**Note**

In some cases, users might be unable to reconnect when they log in again. If this behavior occurs, they must close and restart the WorkSpaces client application, and then try to log in again.

Disassociate a connection alias from a directory

Only the account that owns a directory can disassociate a connection alias from the directory.

If you've shared a connection alias with another account and that account has associated the connection alias with a directory owned by that account, that account must be used to disassociate the connection alias from the directory.

**To disassociate a connection alias from a directory**

2. In the upper-right corner of the console, select the AWS Region that contains the connection alias that you want to disassociate.
3. In the navigation pane, choose Account Settings.
4. Under Cross-Region redirection associations, select the connection string, and then choose Actions, Associate/disassociate.
   
   You can also dissociate a connection alias from the connection alias details page. To do so, under Associated directory, choose Disassociate.
5. On the Associate/disassociate page, choose Disassociate.
6. In the dialog box that asks you to confirm the disassociation, choose Disassociate.

Unshare a connection alias

Only the owner of a connection alias can unshare the alias. If you unshare a connection alias with an account, that account can no longer associate the connection alias with a directory.

**To unshare a connection alias**

2. In the upper-right corner of the console, select the AWS Region that contains the connection alias that you want to unshare.
3. In the navigation pane, choose Account Settings.
4. Under Cross-Region redirection associations, select the connection string, and then choose Actions, Share/unshare connection alias.
   
   You can also unshare a connection alias from the connection alias details page. To do so, under Shared account, choose Unshare.
5. On the **Share/unshare connection alias** page, choose **Unshare**.
6. In the dialog box that asks you to confirm unsharing the connection alias, choose **Unshare**.

## Delete a connection alias

You can delete a connection alias only if it is owned by your account and if it isn't associated with a directory.

If you've shared a connection alias with another account and that account has associated the connection alias with a directory owned by that account, that account must first disassociate the connection alias from the directory before you can delete the connection alias.

**Important**

After you create a connection string, it is always associated to your AWS account. You cannot recreate the same connection string with a different account, even if you delete all instances of it from the original account. The connection string is globally reserved for your account.

**Warning**

If you will no longer be using an FQDN as the registration code for your WorkSpaces users, you must take certain precautions to prevent potential security issues. For more information, see [Security considerations if you stop using cross-Region redirection (p. 232)](https://console.aws.amazon.com/workspaces/).

### To delete a connection alias

2. In the upper-right corner of the console, select the AWS Region that contains the connection alias that you want to delete.
3. In the navigation pane, choose **Account Settings**.
4. Under **Cross-Region redirection associations**, select the connection string, and then choose **Delete**.

You can also delete a connection alias from the connection alias details page. To do so, choose **Delete** in the upper-right corner of the page.

**Note**

If the **Delete** button is disabled, make sure that you are the owner of the alias, and make sure that the alias isn't associated with a directory.

5. In the dialog box that asks you to confirm deletion, choose **Delete**.

## IAM permissions to associate and disassociate connection aliases

If you use an IAM user to associate or disassociate connection aliases, the user must have permissions for `workspaces:AssociateConnectionAlias` and `workspaces:DisassociateConnectionAlias`.

```json
{
   "Version": "2012-10-17",
   "Statement": [
    {
       "Effect": "Allow",
       "Action": [
         "workspaces:AssociateConnectionAlias",
         "workspaces:DisassociateConnectionAlias"
       ],
       "Resource": [
         "arn:aws:workspaces:us-east-1:123456789012:connectionalias/wsca-a1bcd2efg"
       ]
    }
   ]
}
```
Important
If you are creating an IAM policy for associating or disassociating connection aliases for accounts that don’t own the connection aliases, you cannot specify an account ID in the ARN. Instead, you must use * for the account ID, as shown in the following example policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
        "arn:aws:workspaces:us-east-1:*:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

You can specify an account ID in the ARN only when that account owns the connection alias to be associated or disassociated.

For more information about working with IAM, see Identity and access management for WorkSpaces (p. 234).

Security considerations if you stop using cross-Region redirection

If you will no longer be using an FQDN as the registration code for your WorkSpaces users, you must take the following precautions to prevent potential security issues:

- Be sure to issue your WorkSpaces users the Region-specific registration code (for example, \texttt{WSpdx} +ABC12D) for their WorkSpaces directory and instruct them to stop using the FQDN as their registration code.

- If you still own this domain, be sure to update your DNS TXT record to remove this domain so that it cannot be exploited in a phishing attack. If you remove this domain from your DNS TXT record and your WorkSpaces users attempt to use the FQDN as their registration code, their connection attempts will fail harmlessly.

- If you no longer own this domain, your WorkSpaces users must use their Region-specific registration code. If they continue trying to use the FQDN as their registration code, their connection attempts could be redirected to a malicious site.
Security in Amazon WorkSpaces

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to WorkSpaces, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company’s requirements, and applicable laws and regulations

This documentation helps you understand how to apply the shared responsibility model when using WorkSpaces. It shows you how to configure WorkSpaces to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your WorkSpaces resources.

Contents

- Data protection in Amazon WorkSpaces (p. 233)
- Identity and access management for WorkSpaces (p. 234)
- Compliance validation for Amazon WorkSpaces (p. 245)
- Resilience in Amazon WorkSpaces (p. 245)
- Infrastructure security in Amazon WorkSpaces (p. 246)
- Update management in WorkSpaces (p. 248)

Data protection in Amazon WorkSpaces

The AWS shared responsibility model applies to data protection in Amazon WorkSpaces. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the AWS Security Blog.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM). That way each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.
- 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.
• If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers’ email addresses, into tags or free-form fields such as a Name field. This includes when you work with WorkSpaces or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

For more information about WorkSpaces and FIPS endpoint encryption, see Set up Amazon WorkSpaces for FedRAMP authorization or DoD SRG compliance (p. 81).

Encryption at rest

You can encrypt the storage volumes for your WorkSpaces using AWS KMS Key from AWS Key Management Service. For more information, see Encrypted WorkSpaces (p. 160).

When you create WorkSpaces with encrypted volumes, WorkSpaces uses Amazon Elastic Block Store (Amazon EBS) to create and manage those volumes. EBS encrypts your volumes with a data key using the industry-standard AES-256 algorithm. For more information, see Amazon EBS Encryption in the Amazon EC2 User Guide for Windows Instances.

Encryption in transit

For PCoIP, data in-transit is encrypted using TLS 1.2 encryption and SigV4 request signing. The PCoIP protocol uses encrypted UDP traffic, with AES encryption, for streaming pixels. The streaming connection, using port 4172 (TCP and UDP), is encrypted by using AES-128 and AES-256 ciphers, but the encryption defaults to 128-bit. You can change this default to 256-bit, either by using the Configure PCoIP Security Settings Group Policy setting for Windows WorkSpaces, or by modifying the PCoIP Security Settings in the pcoip-agent.conf file for Amazon Linux WorkSpaces.

To learn more about Group Policy administration for Amazon WorkSpaces, see Configure PCoIP security settings (p. 133) in Manage your Windows WorkSpaces (p. 125). To learn more about modifying the pcoip-agent.conf file, see Control PCoIP Agent behavior on Amazon Linux WorkSpaces (p. 143) and PCoIP Security Settings in the Teradici documentation.

For WorkSpaces Streaming Protocol (WSP), streaming and control data in-transit is encrypted using DTLS 1.2 encryption for UDP traffic and TLS 1.2 encryption for TCP traffic, with AES-256 ciphers.

Identity and access management for WorkSpaces

By default, IAM users don’t have permissions for WorkSpaces resources and operations. To allow IAM users to manage WorkSpaces resources, you must create an IAM policy that explicitly grants them permissions, and attach the policy to the IAM users or groups that require those permissions. For more information about IAM policies, see Policies and Permissions in the IAM User Guide guide.

WorkSpaces also creates an IAM role, workspacesDefaultRole, which allows the WorkSpaces service access to required resources.

For more information about IAM, see Identity and Access Management (IAM) and the IAM User Guide. You can find the WorkSpaces-specific resources, actions, and condition context keys for use in IAM permission policies at Actions, Resources, and Condition Keys for Amazon WorkSpaces in the IAM User Guide.
For a tool that helps you create IAM policies, see the AWS Policy Generator. You can also use the IAM Policy Simulator to test whether a policy would allow or deny a specific request to AWS.

**Note**

Amazon WorkSpaces doesn’t support the provisioning of IAM credentials into a WorkSpace (such as with an instance profile).

## Example policies

The following examples show policy statements that you could use to control the permissions that IAM users have to Amazon WorkSpaces.

### Example 1: Perform all WorkSpaces tasks

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

Although Amazon WorkSpaces fully supports the Action and Resource elements when using the API and command line tools, to use Amazon WorkSpaces from the AWS Management Console, an IAM user must have permissions for the following actions and resources:

- **Actions**: "workspaces:*" and "ds:*"
- **Resources**: "Resource": "*"

The following example policy shows how to allow an IAM user to use Amazon WorkSpaces from the AWS Management Console.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
      ],
      "Resource": "*"
    }
  ]
}
```
Example policies

```
"ec2:DescribeSubnets",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeAvailabilityZones",
"ec2:AttachInternetGateway",
"ec2:AssociateRouteTable",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:DeleteSecurityGroup",
"ec2:DeleteNetworkInterface",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"workdocs:RegisterDirectory",
"workdocs:DeregisterDirectory",
"workdocs:AddUserToGroup"
],
"Resource": "**",
}
{
   "Sid": "iamPassRole",
   "Effect": "Allow",
   "Action": "iam:PassRole",
   "Resource": "**",
   "Condition": {
      "StringEquals": {
         "iam:PassedToService": "workspaces.amazonaws.com"
      }
   }
}
```

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.

```
{
   "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 WorkSpaces, add the `workdocs` operation shown in the following example.

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

**Example 3: Perform all WorkSpaces tasks for BYOL WorkSpaces**

The following policy statement grants an IAM user permission to perform all WorkSpaces tasks, including those Amazon EC2 tasks necessary for creating Bring Your Own License (BYOL) WorkSpaces.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeImages",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway"
      ],
      "Resource": "*"
    }
  ]
}
```
Specify WorkSpaces resources in an IAM policy

To specify an WorkSpaces resource in the Resource element of the policy statement, use the Amazon Resource Name (ARN) of the resource. You control access to your WorkSpaces resources by either allowing or denying permissions to use the API actions that are specified in the Action element of your IAM policy statement. WorkSpaces defines ARNs for WorkSpaces, bundles, IP groups, and directories.

**WorkSpace ARN**

A WorkSpace ARN has the syntax shown in the following example.

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

- **region**
  The Region that the WorkSpace is in (for example, us-east-1).

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

- **workspace_identifier**
  The ID of the WorkSpace (for example, ws-a1bcd2efg).

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

```
```

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

A WorkSpace image ARN has the syntax shown in the following example.

```
arn:aws:workspaces:region:account_id:workspaceimage/image_identifier
```

- **region**
  
  The Region that the WorkSpace image is in (for example, us-east-1).

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

- **bundle_identifier**
  
  The ID of the WorkSpace image (for example, wsi-a1bcd2efg).

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

```
```

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

**Bundle ARN**

A bundle ARN has the syntax shown in the following example.

```
```

- **region**
  
  The Region that the WorkSpace is in (for example, us-east-1).

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

- **bundle_identifier**
  
  The ID of the WorkSpace bundle (for example, wsb-a1bcd2efg).

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

```
```

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
```
Specify WorkSpaces resources in an IAM policy

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 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.

**Connection alias ARN**

A connection alias ARN has the syntax shown in the following example.

```
arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier
```

The Region that the connection alias is in (for example, `us-east-1`).

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

The ID of the connection alias (for example, wsca-12345a67b8).

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

```
```

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

**API actions with no support for resource-level permissions**

You can't specify a resource ARN with the following API actions:

- AssociateIpGroups
- CreateIpGroup
- CreateTags
- DeleteTags
- DeleteWorkspaceImage
- DescribeAccount
- DescribeAccountModifications
- DescribeIpGroups
- DescribeTags
- DescribeWorkspaceDirectories
- DescribeWorkspaceImages
- DescribeWorkspaces
- DescribeWorkspacesConnectionStatus
- DisassociateIpGroups
- ImportWorkspaceImage
- ListAvailableManagementCidrRanges
- ModifyAccount

For API actions that don't support resource-level permissions, you must specify the resource statement shown in the following example.

```
"Resource": "*
```

**API actions that don't support account-level restrictions on shared resources**

For the following API actions, you can't specify an account ID in the resource ARN when the resource isn't owned by the account:

- AssociateConnectionAlias
- CopyWorkspaceImage
Create the workspaces_DefaultRole Role

Before you can register a directory using the API, you must verify that a role named workspaces_DefaultRole exists. This role is created by the Quick Setup or if you launch a WorkSpace using the AWS Management Console, and it grants Amazon WorkSpaces permission to access specific AWS resources on your behalf. If this role does not exist, you can create it using the following procedure.

To create the workspaces_DefaultRole role

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane on the left, choose Roles.
3. Choose Create role.
4. Under Select type of trusted entity, choose Another AWS account.
5. For Account ID, enter your account ID with no hyphens or spaces.
6. For Options, do not specify multi-factor authentication (MFA).
7. Choose Next: Permissions.
8. On the Attach permissions policies page, select the AWS managed policies AmazonWorkSpacesServiceAccess and AmazonWorkSpacesSelfServiceAccess.
9. Under Set permissions boundary, we recommend that you not use a permissions boundary because of the potential for conflicts with the policies that are attached to this role. Such conflicts could block certain necessary permissions for the role.
10. Choose Next: Tags.
11. On the Add tags (optional) page, add tags if needed.
12. Choose Next: Review.
13. On the Review page, for Role name, enter workspaces_DefaultRole.
14. (Optional) For Role description, enter a description.
15. Choose Create Role.
16. On the Summary page for the workspaces_DefaultRole role, choose the Trust relationships tab.
17. On the Trust relationships tab, choose Edit trust relationship.
18. On the Edit Trust Relationship page, replace the existing policy statement with the following statement.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
```
AWS managed policies for WorkSpaces

Using AWS managed policies makes adding permissions to users, groups, and roles easier than writing policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. Use AWS managed policies to get started quickly. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the IAM User Guide.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services may occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services don't remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the ReadOnlyAccess AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the IAM User Guide.

AWS managed policy: AmazonWorkSpacesAdmin

This policy provides access to Amazon WorkSpaces administrative actions. It provides the following permissions:

- `workspaces` - Allows access to perform administrative actions on WorkSpaces resources.
- `kms` - Allows access to list and describe KMS keys, as well as list aliases.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "workspaces:CreateTags",
        "workspaces:CreateWorkspaces",
        "workspaces:CreateWorkspaceImage",
        "workspaces:DeleteTags",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesConnectionStatus",
        "workspaces:ModifyWorkspaceProperties",
        "workspaces:ModifySamlProperties",
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:StartWorkspaces",
        "workspaces:StopWorkspaces",
        "workspaces:TerminateWorkspaces"
      ]
    }
  ]
}
```
AWS managed policy: AmazonWorkSpacesServiceAccess

This policy provides customer account access to the Amazon WorkSpaces service for launching a WorkSpace. It is included in the workspaces_DefaultRole role, and it provides the following permissions:

- **ec2** - Allows access to manage Amazon EC2 resources associated with a WorkSpace, such as network interfaces.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS managed policy: AmazonWorkSpacesSelfServiceAccess

This policy provides access to the Amazon WorkSpaces service to perform WorkSpaces self-service actions initiated by a user. It is included in the workspaces_DefaultRole role, and it provides the following permissions:

- **workspaces** - Allows access to self-service WorkSpaces management capabilities for users.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:ModifyWorkspaceProperties"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

WorkSpaces updates to AWS managed policies

View details about updates to AWS managed policies for WorkSpaces since this service began tracking these changes.
Compliance validation for Amazon WorkSpaces

Third-party auditors assess the security and compliance of Amazon WorkSpaces as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

For more information about WorkSpaces and FedRAMP, see Set up Amazon WorkSpaces for FedRAMP authorization or DoD SRG compliance (p. 81).

Your compliance responsibility when using WorkSpaces is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- **Security and Compliance Quick Start Guides** – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- **Architecting for HIPAA Security and Compliance 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.

Amazon WorkSpaces also provides cross-Region redirection, a feature that works with your Domain Name System (DNS) failover routing policies to redirect your WorkSpaces users to alternative WorkSpaces in another AWS Region when their primary WorkSpaces aren't available. For more information, see Cross-region redirection for Amazon WorkSpaces (p. 222).
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 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 WorkSpaces (p. 10).

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. 76).

You can restrict WorkSpace access to trusted devices with valid certificates. For more information, see Restrict WorkSpaces access to trusted devices (p. 55).

Isolation on physical hosts

Different WorkSpaces on the same physical host are isolated from each other through the hypervisor. It is as though they are on separate physical hosts. When a WorkSpace is deleted, the memory allocated to it is scrubbed (set to zero) by the hypervisor before it is allocated to a new WorkSpace.

Authorization of corporate users

With WorkSpaces, directories are managed through the AWS Directory Service. You can create a standalone, managed directory for users. Or you can integrate with your existing Active Directory environment so that your users can use their current credentials to obtain seamless access to corporate resources. For more information, see Manage directories for WorkSpaces (p. 89).

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

Make Amazon WorkSpaces API requests through a VPC interface endpoint

You can connect directly to Amazon WorkSpaces API endpoints through an interface endpoint in your virtual private cloud (VPC) instead of connecting over the internet. When you use a VPC interface endpoint, communication between your VPC and the Amazon WorkSpaces API endpoint is conducted entirely and securely within the AWS network.

Note
This feature can be used only for connecting to WorkSpaces API endpoints. To connect to WorkSpaces using the WorkSpaces clients, internet connectivity is required, as described in IP address and port requirements for WorkSpaces (p. 14).
The Amazon WorkSpaces API endpoints support Amazon Virtual Private Cloud (Amazon VPC) interface endpoints that are powered by AWS PrivateLink. Each VPC endpoint is represented by one or more network interfaces (also known as elastic network interfaces, or ENIs) with private IP addresses in your VPC subnets.

The VPC interface endpoint connects your VPC directly to the Amazon WorkSpaces API endpoint without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. The instances in your VPC don't need public IP addresses to communicate with the Amazon WorkSpaces API endpoint.

You can create an interface endpoint to connect to Amazon WorkSpaces with either the AWS Management Console or AWS Command Line Interface (AWS CLI) commands. For instructions, see Creating an Interface Endpoint.

After you have created a VPC endpoint, you can use the following example CLI commands that use the endpoint-url parameter to specify interface endpoints to the Amazon WorkSpaces API endpoint:

```
aws workspaces copy-workspace-image --endpoint-url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com
aws workspaces delete-workspace-image --endpoint-url VPC_Endpoint_ID.api.workspaces.Region.vpce.amazonaws.com
aws workspaces describe-workspace-bundles --endpoint-url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com --endpoint-name Endpoint_Name --body "Endpoint_Body" --content-type "Content_Type" Output_File
```

If you enable private DNS hostnames for your VPC endpoint, you don't need to specify the endpoint URL. The Amazon WorkSpaces API DNS hostname that the CLI and Amazon WorkSpaces SDK use by default (https://api.workspaces.Region.amazonaws.com) resolves to your VPC endpoint.

The Amazon WorkSpaces API endpoint supports VPC endpoints in all AWS Regions where both Amazon VPC and Amazon WorkSpaces are available. Amazon WorkSpaces supports making calls to all of its public APIs inside your VPC.

To learn more about AWS PrivateLink, see the AWS PrivateLink documentation. For the price of VPC endpoints, see VPC Pricing. To learn more about VPC and endpoints, see Amazon VPC.

To see a list of Amazon WorkSpaces API endpoints by Region, see WorkSpaces API Endpoints (p. 21).

**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.
VPC endpoint policies aren’t supported for Federal Information Processing Standard (FIPS) Amazon WorkSpaces endpoints.

The following example VPC endpoint policy specifies that all users who have access to the VPC interface endpoint are allowed to invoke the Amazon WorkSpaces hosted endpoint named ws-f9abcdefg.

```
{
    "Statement": [
        {
            "Action": "workspaces:*",
            "Effect": "Allow",
            "Principal": "*
        }
    ]
}
```

In this example, the following actions are denied:

- Invoking Amazon WorkSpaces hosted endpoints other than ws-f9abcdefg.
- Performing an action on any resource besides the one specified (WorkSpace ID: ws-f9abcdefg).

Note

In this example, users can still take other Amazon WorkSpaces API actions from outside the VPC. To restrict API calls to those from within the VPC, see Identity and access management for WorkSpaces (p. 234) for information about using identity-based policies to control access to Amazon WorkSpaces API endpoints.

Connect your private network to your VPC

To call the Amazon WorkSpaces API through your VPC, you have to connect from an instance that is inside the VPC, or connect your private network to your VPC by using AWS Virtual Private Network (AWS VPN) or AWS Direct Connect. For information, see VPN Connections in the Amazon Virtual Private Cloud User Guide. For information about AWS Direct Connect, see Creating a Connection in the AWS Direct Connect User Guide.

Update management in WorkSpaces

We recommend that you regularly patch, update, and secure the operating system and applications on your WorkSpaces. You can configure your WorkSpaces to be updated by WorkSpaces during a regular maintenance window or you can update them yourself. For more information, see WorkSpace maintenance (p. 159).

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.
Troubleshoot WorkSpaces issues

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

Enabling advanced logging

To help troubleshoot issues that your users might experience, you can enable advanced logging on any Amazon WorkSpaces client.

Advanced logging generates log files that contain diagnostic information and debugging-level details, including verbose performance data. For the 1.0+ and 2.0+ clients, these advanced logging files are automatically uploaded to a database in AWS.

Note
To 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 4.0+ clients

The Windows client logs are stored in the following location:

%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs

To enable advanced logging for Windows clients

1. Close the Amazon WorkSpaces client.
2. Open the Command Prompt app.
3. Launch the WorkSpaces client with the -l3 flag.

   c:

   cd "C:\Program Files\Amazon Web Services, Inc\Amazon WorkSpaces"

   workspaces.exe -l3

   Note
   If WorkSpaces is installed for one user and not all users, use the following commands:

   c:
   cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
   workspaces.exe -l3

The macOS client logs are stored in the following location:

-/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs

To enable advanced logging for macOS clients

1. Close the Amazon WorkSpaces client.
2. Open Terminal.
3. Run the following command.
   
   open -a workspaces --args -l3

To enable advanced logging for Android clients
1. Close the Amazon WorkSpaces client.
2. Open the Android client menu.
4. Select Logging settings.
5. Select Enable advanced logging.

To retrieve logs for Android clients after enabling advanced logging:
• Select Extract log to save zipped logs locally.

The Linux client logs are stored in the following location:

~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs

To enable advanced logging for Linux clients
1. Close the Amazon WorkSpaces client.
2. Open Terminal.
3. Run the following command.
   
   /opt/workspacesclient/workspacesclient -l3

To enable advanced logging for 3.0 clients

The Windows client logs are stored in the following location:

%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs

To enable advanced logging for Windows clients
1. Close the Amazon WorkSpaces client.
2. Open the Command Prompt app.
3. Launch the WorkSpaces client with the -l3 flag.
   
   c:
   
   cd "C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"
   
   workspaces.exe -l3

   **Note**
   If WorkSpaces is installed for one user and not all users, use the following commands:
   
   c:
   
   cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
   
   workspaces.exe -l3

250
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.

   ```sh
   open -a workspaces --args -l3
   ```

**To enable advanced logging for Android clients**

1. Close the Amazon WorkSpaces client.
2. Open the Android client menu.
3. Select **Support**.
4. Select **Logging settings**.
5. Select **Enable advanced logging**.

**To retrieve logs for Android clients after enabling advanced logging:**

- Select **Extract log** to save zipped logs locally.

The Linux client logs are stored in the following location:

`~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs`

**To enable advanced logging for Linux clients**

1. Close the Amazon WorkSpaces client.
2. Open Terminal.
3. Run the following command.

   ```sh
   /opt/workspacesclient/workspacesclient -l3
   ```

**To enable advanced logging for 1.0+ and 2.0+ clients**

1. Open the WorkSpaces client.
2. Choose the gear icon in the upper-right corner of the client application.
3. Choose **Advanced Settings**.
4. Select the **Enable Advanced Logging** check box.
5. Choose **Save**.

The Windows client logs are stored in the following location:

%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\1.0\Logs

The macOS client logs are stored in the following location:

`~/Library/Logs/Amazon Web Services/Amazon WorkSpaces/1.0`
Troubleshoot specific issues

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

Issues

- I can't create an Amazon Linux WorkSpace because there are non-valid characters in the user name (p. 253)
- I changed the shell for my Amazon Linux WorkSpace and now I can't provision a PCoIP session (p. 253)
- My Amazon Linux WorkSpaces won't start (p. 253)
- Launching WorkSpaces in my connected directory often fails (p. 254)
- Launching WorkSpaces fails with an internal error (p. 254)
- When I try to register a directory, the registration fails and leaves the directory in an ERROR state (p. 255)
- My users can't connect to a Windows WorkSpace with an interactive logon banner (p. 255)
- My users can't connect to a Windows WorkSpace (p. 255)
- My users are having issues when they try to log on to WorkSpaces from WorkSpaces Web Access (p. 256)
- The Amazon WorkSpaces client displays a gray "Loading..." screen for a while before returning to the login screen. No other error message appears. (p. 256)
- My users receive the message "WorkSpace Status: Unhealthy. We were unable to connect you to your WorkSpace. Please try again in a few minutes." (p. 257)
- My users receive the message "This device is not authorized to access the WorkSpace. Please contact your administrator for assistance." (p. 257)
- My users receive the message "No network. Network connection lost. Check your network connection or contact your administrator for help." when trying to connect to a WSP WorkSpace (p. 257)
- The WorkSpaces client gives my users a network error, but they are able to use other network-enabled apps on their devices (p. 258)
- My WorkSpace users see the following error message: "Device can't connect to the registration service. Check your network settings." (p. 259)
- My PCoIP zero client users are receiving the error "The supplied certificate is invalid due to timestamp" (p. 259)
- USB printers and other USB peripherals aren't working for PCoIP zero clients (p. 260)
- My users skipped updating their Windows or macOS client applications and aren't getting prompted to install the latest version (p. 260)
- My users are unable to install the Android client application on their Chromebooks (p. 261)
- My users aren't receiving invitation emails or password reset emails (p. 261)
- My users don't see the Forgot password? option on the client login screen (p. 261)
- 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. 261)
- No WorkSpaces in my directory can connect to the internet (p. 262)
- My WorkSpace has lost its internet access (p. 262)
- I receive a "DNS unavailable" error when I try to connect to my on-premises directory (p. 262)
- I receive a "Connectivity issues detected" error when I try to connect to my on-premises directory (p. 263)
- I receive an "SRV record" error when I try to connect to my on-premises directory (p. 263)
- My Windows WorkSpace goes to sleep when it's left idle (p. 263)
- One of my WorkSpaces has a state of UNHEALTHY (p. 264)
- My WorkSpace is unexpectedly crashing or rebooting (p. 265)
I can't create an Amazon Linux WorkSpace because there are non-valid characters in the user name

For Amazon Linux WorkSpaces, user names:

- Can contain a maximum of 20 characters
- Can contain letters, spaces, and numbers that are representable in UTF-8
- Can include the following special characters: _.-#
- Cannot begin with a dash symbol (-) as the first character of the user name

**Note**

These limitations do not apply to Windows WorkSpaces. Windows WorkSpaces support the @ and - symbols for all characters in the user name.

I changed the shell for my Amazon Linux WorkSpace and now I can't provision a PCoIP session

To override the default shell for Linux WorkSpaces, see Override the default shell for Amazon Linux WorkSpaces (p. 146).

My Amazon Linux WorkSpaces won't start

Starting July 20, 2020, Amazon Linux WorkSpaces will be using new license certificates. These new certificates are compatible only with versions 2.14.1.1, 2.14.7, 2.14.9, and 20.10.6 or later of the PCoIP agent.

If you're using an unsupported version of the PCoIP agent, you must upgrade it to the latest version (20.10.6), which has the latest fixes and performance improvements that are compatible with the new certificates. If you don't make these upgrades by July 20, session provisioning for your Linux WorkSpaces will fail and your end users won't be able to connect to their WorkSpaces.
To upgrade your PCoIP agent to the latest version

2. In the navigation pane, choose WorkSpaces.
3. Select your Linux WorkSpace, and reboot it by choosing Actions, Reboot WorkSpaces. If the WorkSpace status is STOPPED, you must choose Actions, Start WorkSpaces first and wait until its status is AVAILABLE before you can reboot it.
4. After your WorkSpace has rebooted and its status is AVAILABLE, we recommend that you change the status of the WorkSpace to ADMIN_MAINTENANCE while you are performing this upgrade. When you are finished, change the status of the WorkSpace to AVAILABLE. For more information about ADMIN_MAINTENANCE mode, see Manual Maintenance.

To change the status of a WorkSpace to ADMIN_MAINTENANCE, do the following:

a. Select the WorkSpace and choose Actions, Modify WorkSpace.
b. Choose Modify State.
c. For Intended State, select ADMIN_MAINTENANCE.
d. Choose Modify.
5. Connect to your Linux WorkSpace through SSH. For more information, see Enable SSH connections for your Linux WorkSpaces (p. 82).
6. To update the PCoIP agent, run the following command:

   ```
   sudo yum --enablerepo=pcoip-stable install pcioip-agent-standard-20.10.6
   ```

7. To verify the agent version and to confirm that the update succeeded, run the following command:

   ```
   rpm -q pcioip-agent-standard
   ```

   The verification command should produce following result:

   ```
   pcioip-agent-standard-20.10.6-1.el7.x86_64
   ```

8. Disconnect from the WorkSpace and reboot it again.
9. If you set the status of the WorkSpace to ADMIN_MAINTENANCE in Step 4 (p. 254), repeat Step 4 (p. 254) and set Intended State to AVAILABLE.

If your Linux WorkSpace still fails to start after you upgrade the PCoIP agent, contact AWS Support.

Launching WorkSpaces in my connected directory often fails

Verify that the two DNS servers or domain controllers in your on-premises directory are accessible from each of the subnets that you specified when you connected to your directory. You can verify this connectivity by launching an Amazon EC2 instance in each subnet and joining the instance to your directory using the IP addresses of the two DNS servers.

Launching WorkSpaces fails with an internal error

Check whether your subnets are configured to automatically assign IPv6 addresses to instances launched in the subnet. To check this setting, open the Amazon VPC console, select your subnet, and choose Subnet Actions, Modify auto-assign IP settings. If this setting is enabled, you cannot launch
When I try to register a directory, the registration fails and leaves the directory in an ERROR state

This problem can occur if you're trying to register an AWS Managed Microsoft AD directory that has been configured for multi-Region replication. Although the directory in the primary Region can be successfully registered for use with Amazon WorkSpaces, attempting to register the directory in a replicated Region fails. Multi-Region replication with AWS Managed Microsoft AD isn't supported for use with Amazon WorkSpaces within replicated Regions.

My users can't connect to a Windows WorkSpace with an interactive logon banner

If an interactive logon message has been implemented to display a logon banner, this prevents users from being able to access their Windows WorkSpaces. The interactive logon message Group Policy setting is not currently supported by WorkSpaces. Move the WorkSpaces to an organizational unit (OU) where the Interactive logon: Message text for users attempting to log on Group Policy isn't applied.

My users can't connect to a Windows WorkSpace

My users receive the following error when they try to connect to their Windows WorkSpaces:

"An error occurred while launching your WorkSpace. Please try again."

This error often occurs when the WorkSpace can't load the Windows desktop using PCoIP. Check the following:

• This message appears if the PCoIP Standard Agent for Windows service is not running. Connect using RDP to verify that the service is running, that it's set to start automatically, and that it can communicate over the management interface (eth0).

• If the PCoIP agent was uninstalled, reboot the WorkSpace through the Amazon WorkSpaces console to reinstall it automatically.

• You might also receive this error on the Amazon WorkSpaces client after a long delay if the WorkSpaces security group (p. 75) was modified to restrict outbound traffic. Restricting outbound traffic prevents Windows from communicating with your directory controllers for login. Verify that your security groups allow your WorkSpaces to communicate with your directory controllers on all required ports (p. 14) over the primary network interface.

Another cause of this error is related to the User Rights Assignment Group Policy. If the following group policy is incorrectly configured, it prevents users from being able to access their Windows WorkSpaces:

Computer Configuration"Windows SettingsSecurity SettingsLocal PoliciesUser Rights Assignment

• Incorrect policy:

Policy: Access this computer from the network

Setting: Domain nameDomain Computers
Winning GPO: Allow File Access

- Correct policy:

Policy: **Access this computer from the network**

Setting: `Domain name\Domain Users`

Winning GPO: Allow File Access

**Note**
This policy setting should be applied to **Domain Users** instead of **Domain Computers**.

For more information, see [Access this computer from the network - security policy setting](#) and [Configure security policy settings](#) in the Microsoft Windows documentation.

---

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

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

To enable Web Access users to log on to their WorkSpaces, you must configure a Group Policy setting and three Security Policy settings. If these settings are not correctly configured, users might experience long logon times or black screens when they try to log on to their WorkSpaces. To configure these settings, see [Enable and configure Amazon WorkSpaces Web Access](#) (p. 78).

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

**The Amazon WorkSpaces client displays a gray "Loading..." screen for a while before returning to the login screen. No other error message appears.**

This behavior usually indicates that the WorkSpaces client can authenticate over port 443, but can't establish a streaming connection over port 4172 (PCoIP) or port 4195 (WSP). This situation can occur when [network prerequisites](#) aren't met. Issues on the client side often cause the network check in the client to fail. To see which health checks are failing, choose the network check icon (typically a red triangle with an exclamation point in the bottom-right corner of the login screen for 2.0+ clients or the network icon ![network icon](#) in the upper-right corner of the 3.0+ clients).

**Note**
The most common cause of this problem is a client-side firewall or proxy preventing access over port 4172 or 4195 (TCP and UDP). If this health check fails, check your local firewall settings.

If the network check passes, there might be a problem with the network configuration of the WorkSpace. For example, a Windows Firewall rule might block port UDP 4172 or 4195 on the management interface. Connect to the WorkSpace using a Remote Desktop Protocol (RDP) client to verify that the WorkSpace meets the necessary [port requirements](#).
My users receive the message "WorkSpace Status: Unhealthy. We were unable to connect you to your WorkSpace. Please try again in a few minutes."

This error usually indicates the SkyLightWorkSpacesConfigService service isn't responding to health checks.

If you just rebooted or started your WorkSpace, wait a few minutes, and then try again.

If the WorkSpace has been running for some time and you still see this error, connect using RDP to verify that the SkyLightWorkSpacesConfigService service:

• Is running.

• Is set to start automatically.

• Can communicate over the management interface (eth0).

• Isn't blocked by any third-party antivirus software.

My users receive the message "This device is not authorized to access the WorkSpace. Please contact your administrator for assistance."

This error indicates that IP access control groups (p. 76) are configured on the WorkSpace directory, but the client IP address isn't whitelisted.

Check the settings on your directory. Confirm that the public IP address the user is connecting from allows access to the WorkSpace.

My users receive the message "No network. Network connection lost. Check your network connection or contact your administrator for help." when trying to connect to a WSP WorkSpace

If this error occurs and your users don't have connectivity issues, make sure that port 4195 is open on your network's firewalls. For WorkSpaces using the WorkSpaces Streaming Protocol (WSP), the port used to stream the client session was changed from 4172 to 4195.
The WorkSpaces client gives my users a network error, but they are able to use other network-enabled apps on their devices

The WorkSpaces client applications rely on access to resources in the AWS Cloud, and require a connection that provides at least 1 Mbps download bandwidth. If a device has an intermittent connection to the network, the WorkSpaces client application might report an issue with the network.

WorkSpaces enforces the use of digital certificates issued by Amazon Trust Services, as of May 2018. Amazon Trust Services is already a trusted Root CA on the operating systems that are supported by WorkSpaces. If the Root CA list for the operating system is not up to date, the device cannot connect to WorkSpaces and the client gives a network error.

To recognize connection issues due to certificate failures

- **PCoIP zero clients** — The following error message is displayed.
  
  Failed to connect. The server provided a certificate that is invalid. See below for details:  
  - The supplied certificate is invalid due to timestamp  
  - The supplied certificate is not rooted in the devices local certificate store

- **Other clients** — The health checks fail with a red warning triangle for Internet.

To resolve certificate failures

- **Windows client application** (p. 258)
- **PCoIP zero clients** (p. 259)
- **Other client applications** (p. 259)

**Windows client application**

Use one of the following solutions for certificate failures.

**Solution 1: Update the client application**

Download and install the latest Windows client application from [https://clients.amazonworkspaces.com/](https://clients.amazonworkspaces.com/). During installation, the client application ensures that your operating system trusts certificates issued by Amazon Trust Services.

**Solution 2: Add Amazon Trust Services to the local Root CA list**

1. Open [https://www.amazontrust.com/repository/](https://www.amazontrust.com/repository/).
2. Download the Starfield certificate in DER format (2b071c59a0a0ae76b0eab2bad23bad4580b69c3601b630c2eaf0613afa83f92).
3. Open the Microsoft Management Console. (From the Command Prompt, 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.
My Workspace users see the following error message: "Device can't connect to the registration service. Check your network settings."

7. Follow the wizard to import the certificate that you downloaded.
8. Exit and restart the WorkSpaces client application.

Solution 3: Deploy Amazon Trust Services as a trusted CA using Group Policy

Add the Starfield certificate to the trusted Root CAs for the domain using Group Policy. For more information, see Use Policy to Distribute Certificates.

PCoIP zero clients

To connect directly to a WorkSpace using firmware version 6.0 or later, download and install the certificate issued by Amazon Trust Services.

To add Amazon Trust Services as a trusted Root CA

1. Open https://certs.secureserver.net/repository/.
2. Download the certificate under Starfield Certificate Chain with the thumbprint 14 65 FA 20 53 97 B8 76 FA A6 F0 A9 95 8E 55 90 E4 0F CC 7F AA 4F B7 C2 C8 67 75 21 FB 5F B6 58.
3. Upload the certificate to the zero client. For more information, see Uploading Certificates in the Teradici documentation.

Other client applications

Add the Starfield certificate (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92) from Amazon Trust Services. For more information about how to add a Root CA, see the following documentation:

- Android: Add & remove certificates
- Chrome OS: Manage client certificates on Chrome devices
- macOS and iOS: Installing a CA’s Root Certificate on Your Test Device

My Workspace users see the following error message: "Device can't connect to the registration service. Check your network settings."

When a registration service failure occurs, your Workspace users might see the following error message on the Connection Health Check page: "Your device is not able to connect to the WorkSpaces Registration service. You will not be able to register your device with WorkSpaces. Please check your network settings."

This error occurs when the WorkSpaces client application can't reach the registration service. Typically, this happens when the WorkSpaces directory has been deleted. To resolve this error, make sure that the registration code is valid and corresponds to a running directory in the AWS Cloud.

My PCoIP zero client users are receiving the error "The supplied certificate is invalid due to timestamp"

If Network Time Protocol (NTP) isn’t enabled in Teradici, your PCoIP zero client users might receive certificate failure errors. To set up NTP, see Set up PCoIP zero clients for WorkSpaces (p. 77).
USB printers and other USB peripherals aren't working for PCoIP zero clients

Starting with version 20.10.4 of the PCoIP agent, Amazon WorkSpaces disables USB redirection by default through the Windows registry. This registry setting affects the behavior of USB peripherals when your users are using PCoIP zero client devices to connect to their WorkSpaces.

If your WorkSpaces are using version 20.10.4 or later of the PCoIP agent, USB peripheral devices won't work with PCoIP zero client devices until you've enabled USB redirection.

Note
If you're using 32-bit virtual printer drivers, you must also update those drivers to their 64-bit versions.

To enable USB redirection for PCoIP zero client devices

We recommend that you push out these registry changes to your WorkSpaces through Group Policy. For more information, see Configuring the agent and Configurable settings in the Teradici documentation.

1. Set the following registry key value to 1 (enabled):

   KeyPath = HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP\pcoip_admin
   KeyName = pcoip.enable_usb
   KeyType = DWORD
   KeyValue = 1

2. Set the following registry key value to 1 (enabled):

   KeyPath = HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP\pcoip_admin_defaults
   KeyName = pcoip.enable_usb
   KeyType = DWORD
   KeyValue = 1

3. If you haven't already done so, log out of the WorkSpace, and then log back in. Your USB devices should now work.

My users skipped updating their Windows or macOS client applications and aren't getting prompted to install the latest version

When users skip updates to the Amazon WorkSpaces Windows client application, the SkipThisVersion registry key gets set, and they are no longer prompted to update their clients when a new version of the client is released. To update to the latest version, you can edit the registry as described in Update the WorkSpaces Windows Client Application to a Newer Version in the Amazon WorkSpaces User Guide. You can also run the following PowerShell command:

```powershell
Remove-ItemProperty -Path "HKCU:\Software\Amazon Web Services. LLC\Amazon WorkSpaces \WinSparkle" -Name "SkipThisVersion"
```
When users skip updates to the Amazon WorkSpaces macOS client application, the SUSkippedVersion preference gets set, and they are no longer prompted to update their clients when a new version of the client is released. To update to the latest version, you can reset this preference as described in Update the WorkSpaces macOS Client Application to a Newer Version in the Amazon WorkSpaces User Guide.

**My users are unable to install the Android client application on their Chromebooks**

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

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

In some cases, you might need to enable your users' Chromebooks to install Android applications. For more information, see Set up Android for Chromebooks (p. 78).

**My users aren't receiving invitation emails or password reset emails**

Users do not automatically receive welcome or password reset emails for WorkSpaces that were created using AD Connector or a trusted domain. Invitation emails also aren't sent automatically if the user already exists in Active Directory.

To manually send welcome emails to these users, see Send an invitation email (p. 118).

To reset user passwords, see Set up Active Directory Administration Tools for WorkSpaces (p. 101).

**My users don't see the Forgot password? option on the client login screen**

If you're using AD Connector or a trusted domain, your users won't be able to reset their own passwords. (The Forgot password? option on the WorkSpaces client application login screen won't be available.) For information about how to reset user passwords, see Set up Active Directory Administration Tools for WorkSpaces (p. 101).

**I receive the message "The system administrator has set policies to prevent this installation" when I try to install applications on a Windows WorkSpace**

You can address this issue by modifying the Windows Installer Group Policy setting. To deploy this policy to multiple WorkSpaces in your directory, apply this setting to a Group Policy object that is linked to the WorkSpaces organizational unit (OU) from a domain-joined EC2 instance. If you are using AD Connector, you can make these changes from a domain controller. For more information about using the Active Directory administration tools to work with Group Policy objects, see Installing the Active Directory Administration Tools in the AWS Directory Service Administration Guide.

The following procedure shows how to configure the Windows Installer setting for the WorkSpaces Group Policy object.
1. Make sure that the most recent WorkSpaces Group Policy administrative template (p. 127) is installed in your domain.

2. Open the Group Policy Management tool on your Windows WorkSpace client and navigate to and select the WorkSpaces Group Policy object for your WorkSpaces machine accounts. From the main menu, choose Action, Edit.


4. Open the Turn Off Windows Installer setting.

5. In the Turn Off Windows Installer dialog box, change Not Configured to Enabled, and then set Disable Windows Installer to Never.

6. Choose OK.

7. To apply the group policy changes, do one of the following:
   - Reboot the WorkSpace (in the WorkSpaces console, select the WorkSpace, then choose Actions, Reboot WorkSpaces).
   - From an administrative command prompt, enter `gpupdate /force`.

---

**No WorkSpaces in my directory can connect to the internet**

WorkSpaces cannot communicate with the internet by default. You must explicitly provide internet access. For more information, see Provide internet access from your WorkSpace (p. 74).

**My WorkSpace has lost its internet access**

If your WorkSpace has lost access to the internet and you can't connect to the WorkSpace by using RDP, this issue is probably caused by the loss of the public IP address for the WorkSpace. If you have enabled automatic assignment of Elastic IP addresses (p. 92) at the directory level, an Elastic IP address (from the Amazon-provided pool) is assigned to your WorkSpace when it is launched. However, if you associate an Elastic IP address that you own to a WorkSpace, and then you later disassociate that Elastic IP address from the WorkSpace, the WorkSpace loses its public IP address, and it doesn't automatically get a new one from the Amazon-provided pool.

To associate a new public IP address from the Amazon-provided pool with the WorkSpace, you must rebuild the WorkSpace (p. 167). If you don't want to rebuild the WorkSpace, you must associate another Elastic IP address that you own to the WorkSpace.

We recommend that you not modify the elastic network interface of a WorkSpace after the WorkSpace is launched. After an Elastic IP address has been assigned to a WorkSpace, the WorkSpace retains the same public IP address (unless the WorkSpace is rebuilt, in which case it gets a new public IP address).

**I receive a "DNS unavailable" error when I try to connect to my on-premises directory**

You receive an error message similar to the following when connecting to your on-premises directory.

```plaintext
DNS unavailable (TCP port 53) for IP: dns-ip-address
```

AD Connector must be able to communicate with your on-premises DNS servers via TCP and UDP over port 53. Verify that your security groups and on-premises firewalls allow TCP and UDP communication over this port.
I receive a "Connectivity issues detected" error when I try to connect to my on-premises directory

You receive an error message similar to the following when connecting to your on-premises directory.

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: ip-address
Kerberos/authentication unavailable (TCP port 88) for IP: ip-address
Please ensure that the listed ports are available and retry the operation.
```

AD Connector must be able to communicate with your on-premises domain controllers via TCP and UDP over the following ports. Verify that your security groups and on-premises firewalls allow TCP and UDP communication over these ports:

- 88 (Kerberos)
- 389 (LDAP)

I receive an "SRV record" error when I try to connect to my on-premises directory

You receive an error message similar to one or more of the following when connecting to your on-premises directory.

```
SRV record for LDAP does not exist for IP: dns-ip-address
SRV record for Kerberos does not exist for IP: dns-ip-address
```

AD Connector needs to obtain the `_ldap._tcp.dns-domain-name` and `_kerberos._tcp.dns-domain-name` SRV records when connecting to your directory. You get this error if the service cannot obtain these records from the DNS servers that you specified when connecting to your directory. Make sure that your DNS servers contain these SRV records. For more information, see SRV Resource Records on Microsoft TechNet.

My Windows WorkSpace goes to sleep when it's left idle

To resolve this issue, connect to the WorkSpace and change the power plan to High performance by using the following procedure:

1. From the WorkSpace, open Control Panel, then choose Hardware or choose Hardware and Sound (the name might differ, depending on your version of Windows).
2. Under Power Options, choose Choose a power plan.
3. In the Choose or customize a power plan pane, choose the High performance power plan, and then choose Change plan settings.
   - If the option to choose the High performance power plan is disabled, choose Change settings that are currently unavailable, and then choose the High performance power plan.
   - If the High performance plan isn't visible, choose the arrow to the right of Show additional plans to display it, or choose Create a power plan in the left navigation, choose High performance, give the power plan a name, and then choose Next.
4. On the Change settings for the plan: High performance page, make sure Turn off the display and (if available) Put the computer to sleep are set to Never.
One of my WorkSpaces has a state of UNHEALTHY

The WorkSpaces service periodically sends status requests to a WorkSpace. A WorkSpace is marked UNHEALTHY when it fails to respond to these requests. Common causes for this problem are:

- An application on the WorkSpace is blocking network ports, which prevents the WorkSpace from responding to the status request.
- High CPU utilization is preventing the WorkSpace from responding to the status request in a timely manner.
- The computer name of the WorkSpace has been changed. This prevents a secure channel from being established between WorkSpaces and the WorkSpace.

You can attempt to correct the situation using the following methods:

- Reboot the WorkSpace from the WorkSpaces console.
- Connect to the unhealthy WorkSpace using the following procedure, which should be used only for troubleshooting purposes:
  1. Connect to an operational WorkSpace in the same directory as the unhealthy WorkSpace.
  2. From the operational WorkSpace, use Remote Desktop Protocol (RDP) to connect to the unhealthy WorkSpace using the IP address of the unhealthy WorkSpace. Depending on the extent of the problem, you might not be able to connect to the unhealthy WorkSpace.
  3. On the unhealthy WorkSpace, confirm that the minimum port requirements (p. 14) are met.
- Make sure the SkyLightWorkSpacesConfigService service can respond to health checks. To troubleshoot this issue, see My users receive the message "WorkSpace Status: Unhealthy. We were unable to connect you to your WorkSpace. Please try again in a few minutes." (p. 257).
- Rebuild the WorkSpace from the WorkSpaces console. Because rebuilding a WorkSpace can potentially cause a loss of data, this option should be used only if all other attempts to correct the problem have been unsuccessful.
My WorkSpace is unexpectedly crashing or rebooting

If your WorkSpace configured for PCoIP is repeatedly crashing or rebooting and your error logs or crash dumps are pointing to problems with spacedeskHookKmode.sys or spacedeskHookUmode.dll, or if you're receiving the following error messages, you might need to disable Web Access to the WorkSpace:

- The kernel power manager has initiated a shutdown transition.  
  Shutdown reason: Kernel API
- The computer has rebooted from a bugcheck.

**Note**

- These troubleshooting steps are not applicable to WorkSpaces that are configured for WorkSpaces Streaming Protocol (WSP). They are applicable only to WorkSpaces that are configured for PCoIP.
- You should disable Web Access only if you aren't allowing your users to use Web Access.

To disable Web Access to the WorkSpace, you must set a group policy and modify two registry settings. For 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.

**Step 1: Set a Group Policy to disable Web Access at the directory level**

You must make these changes from a PCoIP WorkSpace instead of a domain controller because the STXHD Hosted Application Service must be present.

1. Edit the Security Group used by WorkSpaces to allow RDP connections. For more information, see How do I connect to my WorkSpace using RDP?
2. Use RDP to connect to a WorkSpace. Make sure that you are using a user account that has permissions on the domain to create and modify GPOs. If you are using Simple AD for your WorkSpace directory, the username is Administrator. If you are using Microsoft AD, the administrator username is Admin.
3. Install the Active Directory Administration Tools (RSAT) to get the Group Policy Management Editor tool. To install these tools, see Installing the Active Directory Administration Tools in the AWS Directory Service Administration Guide.

   You can also install these tools by running the following Windows PowerShell command as an administrator:

   ```powershell
   Install-WindowsFeature -Name GPMC,RSAT-AD-PowerShell,RSAT-AD-AdminCenter,RSAT-ADDS-Tools,RSAT-DNS-Server
   ```

4. Open the Group Policy Management Editor (gpmc.msc) and locate the Group Policy Object (GPO) policy at the domain controller level of your directory.

   **Note**
   If the domain backing the WorkSpaces is an AWS Managed Microsoft AD directory, you cannot use the Default Domain Policy to create your GPO. Instead, you must create and link the GPO under the domain container that has delegated privileges.
   When you create a directory with AWS Managed Microsoft AD, AWS Directory Service creates a `yourdomainname` organizational unit (OU) under the domain root. The name of this OU is based on the NetBIOS name that you entered when you created your directory.
If you didn't specify a NetBIOS name, it will default to the first part of your Directory DNS name (for example, in the case of corp.example.com, the NetBIOS name is corp).

To create your GPO, instead of selecting Default Domain Policy, select the yourdomainname OU (or any OU under that one), open the context (right-click) menu, and choose Create a GPO in this domain, and Link it here.

For more information about the yourdomainname OU, see What Gets Created in the AWS Directory Service Administration Guide.

5. Choose Action, Edit.
6. Navigate to the following setting:

   Computer Configuration\Policies\Windows Settings\Security Settings\System Services\STXHD Hosted Application Service

7. In the STXHD Hosted Application Service Properties dialog box, on the Security Policy Setting tab, select the Define this policy setting check box.
8. Under Select Service Startup Mode, select Disabled.
9. Choose OK.
10. Prevent the machine from rebooting until you have finished editing the registry (Step 2).

**Step 2: Edit the Registry to disable Web Access**

We recommend that you push out these registry changes through GPO.

1. Set the following registry key value to 1 (enabled):

   KeyPath = HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\update-webaccess.ps1

   KeyName = RebootCount

   KeyType = DWORD

   KeyValue = 1

2. Set the following registry key value to 4 (disabled):

   KeyPath = HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\spacedeskHookKmode

   KeyName = Start

   KeyType = DWORD

   KeyValue = 4

3. Reboot the machine.

The same username has more than one WorkSpace, but the user can log in to only one of the WorkSpaces

If you delete a user in Active Directory (AD) without first deleting their WorkSpace and then you add the user back to Active Directory and create a new WorkSpace for that user, the same username will now have two WorkSpaces in the same directory. However, if the user tries to connect to their original WorkSpace, they will receive the following error:

"Unrecognized user. No WorkSpace found under your username. Contact your administrator to request one."
Additionally, searches for the username in the Amazon WorkSpaces console return only the new
WorkSpace, even though both WorkSpaces still exist. (You can find the original WorkSpace by searching
for the WorkSpace ID instead of the username.)

This behavior can also occur if you rename a user in Active Directory without first deleting their
WorkSpace. If you then change their username back to the original username and create a new
WorkSpace for the user, the same username will have two WorkSpaces in the directory.

This problem occurs because Active Directory uses the user's security identifier (SID), rather than the
username, to uniquely identify the user. When a user is deleted and recreated in Active Directory, the
user is assigned a new SID, even if their username remains the same. During searches for a username,
the Amazon WorkSpaces console uses the SID to search Active Directory for matches. The Amazon
WorkSpaces clients also use the SID to identify users when they are connecting to WorkSpaces.

To resolve this problem, do one of the following:

- If this problem occurred because the user was deleted and recreated in Active Directory, you might be
  able to restore the original deleted user object if you have enabled the Recycle Bin feature in Active
  Directory. If you're able to restore the original user object, make sure the user can connect to their
  original WorkSpace. If they can, you can delete the new WorkSpace (p. 179) after manually backing up
  and transferring any user data from the new WorkSpace to the original WorkSpace (if needed).

- If you can't restore the original user object, delete the user's original WorkSpace (p. 179). The user
  should be able to connect to and use their new WorkSpace instead. Be sure to manually back up and
  transfer any user data from the original WorkSpace to the new WorkSpace.

  Warning
  Deleting a WorkSpace is a permanent action and cannot be undone. The WorkSpace user's
data does not persist and is destroyed. For help with backing up user data, contact AWS
  Support.

I'm having trouble using Docker with Amazon
WorkSpaces

Windows WorkSpaces

Nested virtualization (including the use of Docker) is not supported on Windows WorkSpaces. For more
information, see the Docker documentation.

Linux WorkSpaces

To use Docker on Linux WorkSpaces, make sure that the CIDR blocks used by Docker don't overlap with
the CIDR blocks used in the two elastic network interfaces (ENIs) associated with the WorkSpace. If you
encounter problems with using Docker on Linux WorkSpaces, contact Docker for assistance.

I receive ThrottlingException errors to some of my
API calls

The default allowed rate for WorkSpaces API calls is a constant rate of two API calls per second, with a
maximum allowed "burst" rate of five API calls per second. The following table shows how the burst rate
limit works for API requests.
My WorkSpace keeps disconnecting when I let it run in the background

For Mac users, check to see if the Power Nap feature is on. If it is on, turn it off. To turn Power Nap off, open your terminal and run the following command:

```
defaults write com.amazon.workspaces NSAppSleepDisabled -bool YES
```

SAML 2.0 federation isn't working. My users are not authorized to stream their WorkSpaces desktop.

This might happen because the inline policy that is embedded for the SAML 2.0 federation IAM role does not include permissions to stream from the directory Amazon Resource Name (ARN). The IAM role is assumed by the federated user who is accessing a WorkSpaces directory. Edit the role permissions to include the directory ARN and ensure that the user has a WorkSpace in the directory. For more information, see SAML 2.0 Authentication and Troubleshooting SAML 2.0 Federation with AWS.
My users are getting disconnected from their WorkSpaces session every 60 minutes.

If you have configured SAML 2.0 authentication to WorkSpaces, depending on your identity provider (IdP), you might need to configure the information that the IdP passes as SAML attributes to AWS as part of the authentication response. This includes configuring the Attribute element with the SessionDuration attribute set to https://aws.amazon.com/SAML/Attributes/SessionDuration.

SessionDuration specifies the maximum amount of time that a federated streaming session can remain active for a user before reauthentication is required. Although SessionDuration is an optional attribute, we recommend that you include it in the SAML authentication response. If you don't specify this attribute, the session duration defaults to 60 minutes.

To resolve this issue, configure your IdP to include the SessionDuration value in the SAML authentication response and set the value as required. For more information, see Step 5: Create assertions for the SAML authentication response.

My users get a redirect URI error when they federate using the SAML 2.0 identity provider (IdP)-initiated flow, or an additional instance of the WorkSpaces client application starts every time my users attempt to sign in from the client after federating to the IdP.

This error occurs due to a relay state URL that's not valid. Make sure that the relay state in your IdP federation setup is correct, and that the user access URL and relay state parameter name are configured correctly for your IdP federation in the WorkSpaces directory properties. If they are valid and the problem still persists, contact AWS Support. For more information, see Setting Up SAML.

My users receive the message, "Something went wrong: An error occurred while launching your WorkSpace" when they attempt to sign in to the WorkSpaces client application after federating to the IdP.

Review the SAML 2.0 assertions for your federation. The SAML Subject NameID value must match the WorkSpaces user name, and is typically the same as the sAMAccountName attribute for the Active Directory user. In addition, the Attribute element that has the PrincipalTag:Email attribute set to https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email must match the WorkSpaces user's email address as defined in the WorkSpaces directory. For more information, see Setting Up SAML.
My users receive the message, "Unable to validate tags" when they attempt to sign in to the WorkSpaces client application after federating to the IdP.

Review the PrincipalTag attribute values in the SAML 2.0 assertions for your federation, such as https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email. Tag values may include combinations of the characters _ . : / = + - @, letters, numbers, and spaces. For more information, see Rules for tagging in IAM and AWS STS.

My users receive the message, "The client and the server cannot communicate, because they do not possess a common algorithm"

This problem can occur if you do not enable TLS 1.2.
### Amazon WorkSpaces quotas

Amazon WorkSpaces provides different resources that you can use in your account in a given Region, including WorkSpaces, images, bundles, directories, connection aliases, and IP control groups. When you create your Amazon Web Services account, we set default quotas (also referred to as limits) on the number of resources that you can create.

The following are the default quotas for WorkSpaces for your AWS account. You can use the Service Quotas console to view the default quota and applied quota, or to request quota increases for adjustable quotas.

In some Regions, where Service Quotas is not available, you must submit a support case to request limit increase. For more information, see Viewing service quotas and Requesting a quota increase in the Service Quotas User Guide.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default</th>
<th>Description</th>
<th>Adjustable</th>
</tr>
</thead>
<tbody>
<tr>
<td>WorkSpaces</td>
<td>1</td>
<td>The maximum number of WorkSpaces in this account in the current Region.</td>
<td>Yes</td>
</tr>
<tr>
<td>Graphics WorkSpaces</td>
<td>0</td>
<td>The maximum number of Graphics WorkSpaces in this account in the current Region.</td>
<td>Yes</td>
</tr>
<tr>
<td>Graphics.g4dn WorkSpaces</td>
<td>0</td>
<td>The maximum number of Graphics.g4dn WorkSpaces in this account in the current Region.</td>
<td>Yes</td>
</tr>
<tr>
<td>GraphicsPro WorkSpaces</td>
<td>0</td>
<td>The maximum number of GraphicsPro WorkSpaces in this account in the current Region.</td>
<td>Yes</td>
</tr>
<tr>
<td>GraphicsPro.g4dn WorkSpaces</td>
<td>0</td>
<td>The maximum number of GraphicsPro.g4dn WorkSpaces in this account in the current Region.</td>
<td>Yes</td>
</tr>
<tr>
<td>Bundles</td>
<td>50</td>
<td>The maximum number of bundles in this account in the current Region. This quota applies only to custom bundles, not to public bundles.</td>
<td>No</td>
</tr>
<tr>
<td>Resource</td>
<td>Default</td>
<td>Description</td>
<td>Adjustable</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Connection aliases</td>
<td>20</td>
<td>The maximum number of connection aliases in this account in the current Region.</td>
<td>No</td>
</tr>
<tr>
<td>Directories</td>
<td>50</td>
<td>The maximum number of directories that can be registered for use with Amazon WorkSpaces in this account in the current Region.</td>
<td>No</td>
</tr>
<tr>
<td>Images</td>
<td>40</td>
<td>The maximum number of images in this account in the current Region.</td>
<td>Yes</td>
</tr>
<tr>
<td>IP access control groups</td>
<td>100</td>
<td>The maximum number of IP access control groups in this account in the current Region.</td>
<td>No</td>
</tr>
<tr>
<td>IP access control groups per directory</td>
<td>25</td>
<td>The maximum number of IP access control groups per directory in this account in the current Region.</td>
<td>No</td>
</tr>
<tr>
<td>Rules per IP access control group</td>
<td>10</td>
<td>The maximum number of rules per IP access control group in this account in the current Region.</td>
<td>No</td>
</tr>
</tbody>
</table>

**API throttling**

The allowed rate is two calls per second. For more information, see Throttling exceptions (p. 267).
# Document history for WorkSpaces

The following table describes the important changes to the WorkSpaces service and to the *Amazon WorkSpaces Administration Guide* from January 1, 2018, onward. We also update the documentation frequently to address the feedback that you send us.

For notification about these updates, you can subscribe to the WorkSpaces RSS feed.

<table>
<thead>
<tr>
<th>update-history-change</th>
<th>update-history-description</th>
<th>update-history-date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amazon WorkSpaces webcam support</strong></td>
<td>Amazon WorkSpaces now supports real-time audio-video (AV) by seamlessly redirecting local webcam video input to Windows WorkSpaces desktops using the WorkSpaces Streaming Protocol (WSP).</td>
<td>April 5, 2021</td>
</tr>
<tr>
<td><strong>Amazon WorkSpaces smart card support with the WorkSpaces macOS client application</strong></td>
<td>You can now use the Amazon WorkSpaces macOS client application with Common Access Card (CAC) and Personal Identity Verification (PIV) smart cards. Smart card support is available on WorkSpaces using the WorkSpaces Streaming Protocol (WSP).</td>
<td>April 5, 2021</td>
</tr>
<tr>
<td><strong>Amazon WorkSpaces bundle management APIs</strong></td>
<td>Amazon WorkSpaces bundle management APIs are now available. These API actions support creation, deletion, and image association operations for WorkSpaces bundles.</td>
<td>March 15, 2021</td>
</tr>
<tr>
<td><strong>Amazon WorkSpaces launched in Asia Pacific (Mumbai)</strong></td>
<td>Amazon WorkSpaces is available in the Asia Pacific (Mumbai) Region.</td>
<td>March 8, 2021</td>
</tr>
<tr>
<td><strong>WorkSpaces Streaming Protocol (WSP)</strong></td>
<td>The WorkSpaces Streaming Protocol (WSP) is now available for both license-included (Windows Server 2016) and BYOL Windows 10-based WorkSpaces on all bundle types except for Graphics and GraphicsPro. WSP is also available for Linux WorkSpaces in the AWS GovCloud (US-West) Region.</td>
<td>December 1, 2020</td>
</tr>
<tr>
<td><strong>Smart Cards</strong></td>
<td>Amazon WorkSpaces now supports pre-session (login) and in-session smart card authentication on Windows and</td>
<td>December 1, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Share Custom Images</td>
<td>You can now share custom WorkSpaces images across AWS accounts. After an image has been shared, the recipient account can copy the image and use it to create bundles for launching new WorkSpaces.</td>
<td>October 1, 2020</td>
</tr>
<tr>
<td>Cross-Region Redirection</td>
<td>You can now use cross-Region redirection, a feature that works with your Domain Name System (DNS) routing policies to redirect your users to alternative WorkSpaces when their primary WorkSpaces aren't available.</td>
<td>September 10, 2020</td>
</tr>
<tr>
<td>Subscribe to Microsoft Office 2016 or 2019 for BYOL WorkSpaces</td>
<td>You can now subscribe to Microsoft Office Professional 2016 or 2019 provided by AWS on Bring Your Own Windows License (BYOL) WorkSpaces.</td>
<td>September 3, 2020</td>
</tr>
<tr>
<td>BYOL Automation in China (Ningxia)</td>
<td>You can use Bring Your Own License (BYOL) automation to simplify the process of using your Windows 10 desktop licenses for your WorkSpaces in China (Ningxia).</td>
<td>April 2, 2020</td>
</tr>
<tr>
<td>Image Checker</td>
<td>The Image Checker tool helps you determine whether your Windows WorkSpace meets the requirements for image creation. The Image Checker performs a series of tests on the WorkSpace that you want to use to create your image, and provides guidance on how to resolve any issues it finds.</td>
<td>March 30, 2020</td>
</tr>
<tr>
<td>Migrate WorkSpaces</td>
<td>The Amazon WorkSpaces migrate feature enables you to migrate a WorkSpace from one bundle to another, while retaining the data on the user volume. You can use this feature to migrate WorkSpaces from the Windows 7 desktop experience to the Windows 10 desktop experience. You can also use this feature to migrate WorkSpaces from one public or custom bundle to another.</td>
<td>January 9, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<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>Linux client for Amazon WorkSpaces</td>
<td>Users can now use the Linux client to access their WorkSpaces.</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 your Windows 7 and Windows 10 desktop licenses for your WorkSpaces.</td>
<td>November 16, 2018</td>
</tr>
<tr>
<td>PowerPro and GraphicsPro bundles</td>
<td>The PowerPro and GraphicsPro bundles are now available for WorkSpaces.</td>
<td>October 18, 2018</td>
</tr>
</tbody>
</table>
Monitor successful WorkSpace logins

You can use events from Amazon CloudWatch Events to monitor and respond to successful WorkSpace logins.

September 17, 2018

Web Access for Windows 10 WorkSpaces

Users can now use the web access client to access a WorkSpace running the Windows 10 desktop experience.

August 24, 2018

URI login

You can use uniform resource identifiers (URIs) to provide users with access to their WorkSpaces.

July 31, 2018

Amazon Linux WorkSpaces

You can provision Amazon Linux WorkSpaces for your users.

June 26, 2018

IP access control groups

You can control the IP addresses from which users can access their WorkSpaces.

April 30, 2018

In-place upgrades

You can upgrade your Windows 10 BYOL WorkSpaces to a newer version of Windows 10.

March 9, 2018

## Earlier Updates

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

<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>Web Access</td>
<td>You can access your Windows WorkSpaces from a web browser using WorkSpaces Web Access.</td>
<td>November 18, 2016</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</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>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 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>WorkSpaces launched in Asia Pacific (Singapore)</td>
<td>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 WorkSpaces PCoIP zero client devices.</td>
<td>October 15, 2014</td>
</tr>
<tr>
<td>WorkSpaces launched in Asia Pacific (Tokyo)</td>
<td>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>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>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>WorkSpaces launched in Asia Pacific (Sydney)</td>
<td>WorkSpaces is available in the Asia Pacific (Sydney) Region.</td>
<td>May 15, 2014</td>
</tr>
<tr>
<td>WorkSpaces launched in Europe (Ireland)</td>
<td>WorkSpaces is available in the Europe (Ireland) Region.</td>
<td>May 5, 2014</td>
</tr>
<tr>
<td>Public beta</td>
<td>WorkSpaces is available as a public beta.</td>
<td>March 25, 2014</td>
</tr>
</tbody>
</table>