Amazon WorkSpaces

Administration Guide

Version 1.0

Amazon Web Services

Amazon WorkSpaces: Administration Guide

Amazon Web Services

What is Amazon WorkSpaces?

Amazon WorkSpaces offers you an easy way to provide a cloud-based desktop experience to your end-users. You simply select from a choice of WorkSpace bundles that offer a range of different amounts of CPU, memory, storage, and a choice of applications. Then, enter user information and launch the number of WorkSpaces that you require. As soon as the WorkSpaces are ready, users can download the Amazon WorkSpaces client and connect to their WorkSpace. Users can connect from a PC or Mac desktop computer, or an iPad, Kindle, or Android tablet.

Amazon WorkSpaces provides you with the choice of creating a standalone, managed directory for users who will use WorkSpaces, or you can use WorkSpaces Connect to connect to your on-premises directory so that your users can use their existing credentials to obtain seamless access to corporate resources. This integration works via a secure hardware VPN connection to your on-premises network using Amazon Virtual Private Cloud (Amazon VPC) or with AWS Direct Connect.

You don't have to worry about procuring or deploying hardware or installing complex software to deliver a desktop experience to your users. Amazon WorkSpaces takes care of all the heavy lifting of managing hardware and software, and tasks such as patching and maintenance, enabling you to easily deliver a high quality desktop experience to your users. When you connect Amazon WorkSpaces to your on-premises directory, you can manage your WorkSpaces with the existing tools you are using for your on-premises desktops and you maintain full administrative control.

For more information, see Amazon WorkSpaces.

This guide is divided into the following major sections:

- Amazon WorkSpaces Getting Started Guide (p. 2) is intended for system administrators and provides information about how to quickly get up and running with Amazon WorkSpaces.
- Amazon WorkSpaces Administration (p. 12) is intended for system administrators and contains information about setting up and managing Amazon WorkSpaces.
- Amazon WorkSpaces Client Help (p. 55) is intended for users of the Amazon WorkSpaces client applications and contains information about using each of the client applications.

Amazon WorkSpaces Getting Started Guide

The Amazon WorkSpaces Getting Started Guide allows you to get up and running with Amazon WorkSpaces quickly and easily. Click on the link below to get started.

Next: Prerequisites (p. 2)

Prerequisites

To use Amazon WorkSpaces, the following prerequisites must be met.

AWS Account Prerequisites

In order to use Amazon WorkSpaces, you must have an AWS account. For more information, see Sign up for AWS (p. 3).

Amazon WorkSpaces Client Prerequisites

The Amazon WorkSpaces client applications have the following requirements.

- An Amazon WorkSpaces user requires a client device, such as a PC, Mac, iPad, Kindle, or Android tablet on which to run the Amazon WorkSpaces client application.
- The Amazon WorkSpaces client applications require a broadband Internet connection.
- The network that the client is connected to, and any firewall on the client itself, must have the following ports open to the IP address ranges for certain Amazon EC2 instances:
  - Port 4172 for UDP and TCP traffic
  - Port 443 for TCP

  Some networks may have some or all of these ports closed. In this case, you will need to work with your network administrators to have these ports enabled. For more information, and to test that these ports are correctly configured, see Port Access (p. 13) in the Advanced Administration guide.
- A round trip time (RTT) to the region that your WorkSpaces are in of less than 100ms is suggested. For more information, and to test the network latency, see Latency Threshhold (p. 14) in the Advanced Administration guide.

- If your users are accessing a WorkSpace through a virtual private network (VPN), the connection must support a maximum transmission unit (MTU) of at least 1200 bytes.
- The Amazon WorkSpaces client applications require HTTPS access to Amazon WorkSpaces resources hosted by the service and Amazon Simple Storage Service (S3). The Amazon WorkSpaces client applications do not support proxy redirection at the application level. This is required to successfully register and use the Amazon WorkSpaces client application.

Sign up for AWS

Your AWS account gives you access to all services, but you are charged only for the resources that you use.

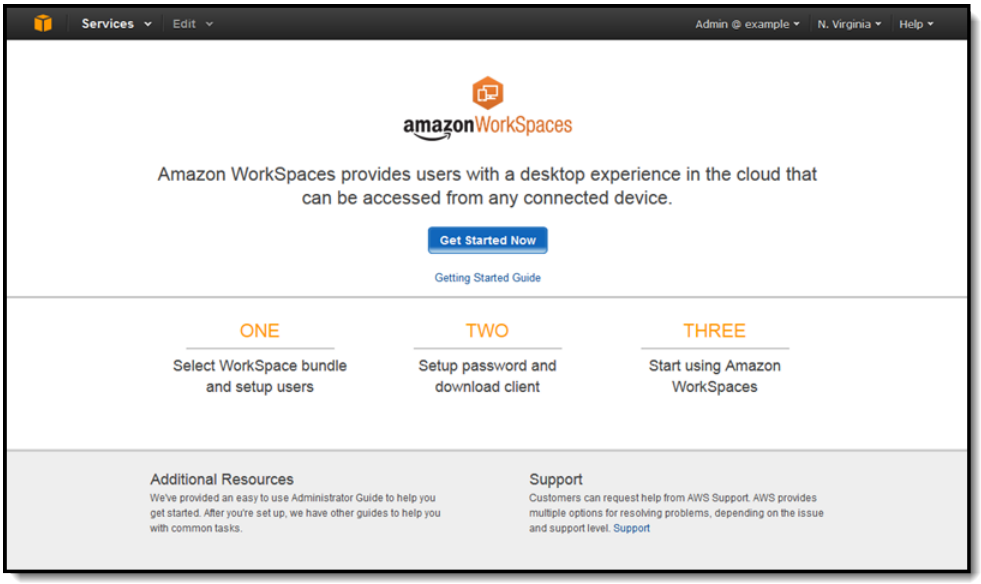
If you do not have an AWS account, use the following procedure to create one.

To sign up for AWS

1. Go to http://aws.amazon.com and click **Sign Up**.
2. Follow the on-screen instructions.

Get Started

Open the Amazon WorkSpaces console for your desired region, sign in with your AWS credentials, and click **Get Started Now**.



Amazon WorkSpaces provides users with a desktop experience in the cloud that can be accessed from any connected device.

ONE: Select WorkSpace bundle and setup users

TWO: Setup password and download client

THREE: Start using Amazon WorkSpaces

Additional Resources

We've provided an easy to use Administrator Guide to help you get started. After you're set up, we have other guides to help you with common tasks.

Support

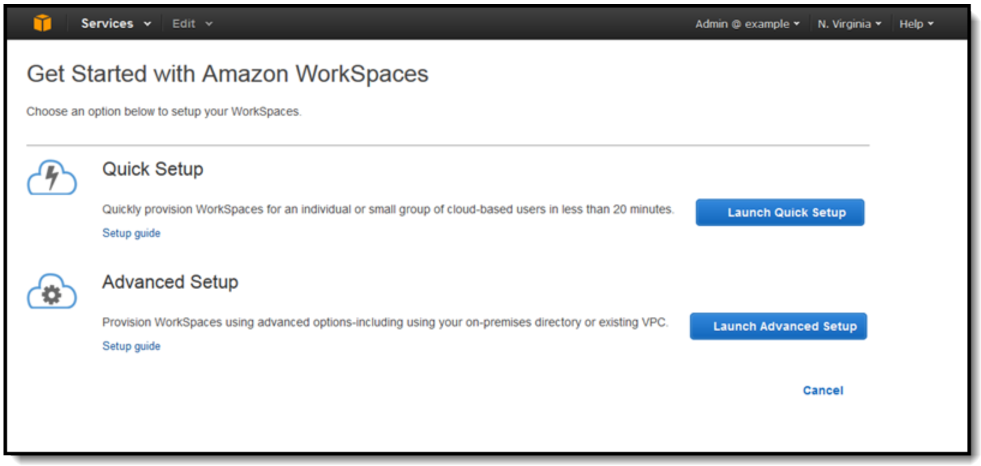
Customers can request help from AWS Support. AWS provides multiple options for resolving problems, depending on the issue and support level. Support

Choose Setup Type

Amazon WorkSpaces uses a network directory to store its user and WorkSpace information. Choose the type of Amazon WorkSpaces directory setup you want to use.

The **Quick Setup** procedure allows you to get you up and running with Amazon WorkSpaces quickly and easily. Amazon WorkSpaces creates and sets up a directory in the cloud that requires minimal management. To use the quick setup, click **Launch Quick Setup** and proceed to Quick Setup (p. 4).

The **Advanced Setup** procedure allows you to have more control over the setup of your Amazon WorkSpaces directory. The directory can either be in the cloud, or connected to your on-premises directory. To use advanced setup, click **Launch Advanced Setup** and proceed to Advanced Setup (p. 11).



Get Started with Amazon WorkSpaces

Choose an option below to setup your WorkSpaces.

Quick Setup

Quickly provision WorkSpaces for an individual or small group of cloud-based users in less than 20 minutes.

Setup guide

Advanced Setup

Provision WorkSpaces using advanced options-including using your on-premises directory or existing VPC.

Setup guide

Quick Setup

The quick setup procedure allows you to get you up and running with Amazon WorkSpaces quickly and easily. Amazon WorkSpaces creates and sets up a directory in the cloud that requires minimal management.

Quick Setup Prerequisites

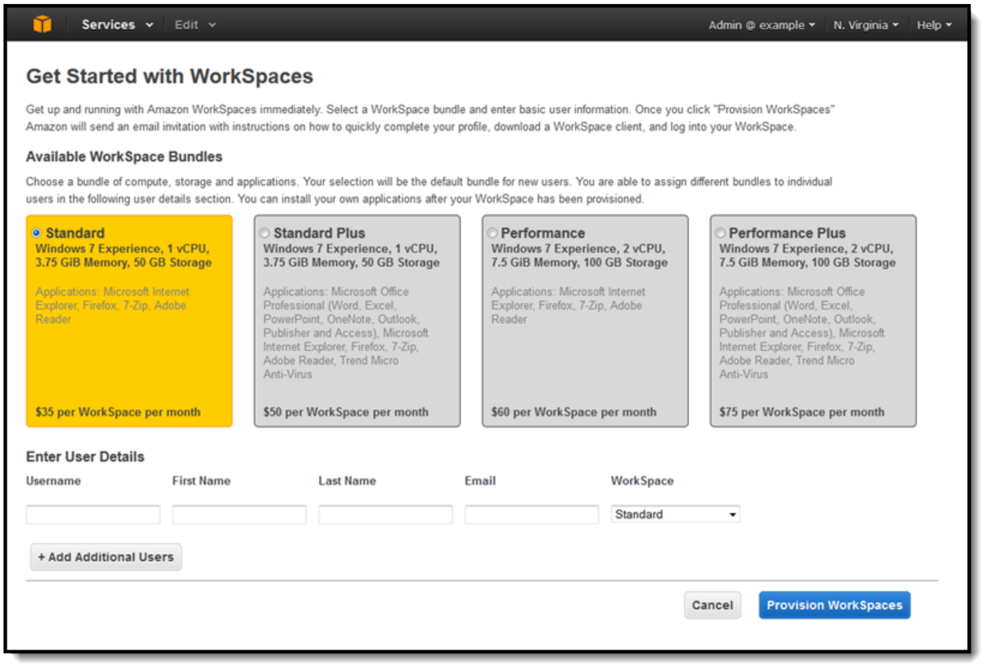
This procedure creates a virtual private cloud (VPC) on your behalf. Because of this, your AWS account must have at least one VPC available to be created in the region within which you are creating WorkSpaces. Within this VPC, Amazon WorkSpaces must also create an Internet gateway, so your AWS account must have at least one Internet gateway available to be created in the region within which you are creating WorkSpaces.

For more information about VPCs, see What is Amazon VPC? in the *Amazon Virtual Private Cloud User Guide*.

For more information about Internet gateways, see Adding an Internet Gateway to Your VPC in the *Amazon Virtual Private Cloud User Guide*.

Select WorkSpace Bundle and Create Users

1. In the **Available WorkSpace Bundles** section, select the desired WorkSpace bundle.
2. In the **Enter User Details** section, enter the requested information for the WorkSpace user. The first user entered is made the Amazon WorkSpaces administrator, and will have administrator privileges.
3. To add more than one user, click **Add Another User**, and enter the fields for the next user. Repeat this for all users. When all of the user information has been entered, click **Provision WorkSpaces**.



Get Started with WorkSpaces

Get up and running with Amazon WorkSpaces immediately. Select a WorkSpace bundle and enter basic user information. Once you click "Provision WorkSpaces" Amazon will send an email invitation with instructions on how to quickly complete your profile, download a WorkSpace client, and log into your WorkSpace.

Available WorkSpace Bundles

Choose a bundle of compute, storage and applications. Your selection will be the default bundle for new users. You are able to assign different bundles to individual users in the following user details section. You can install your own applications after your WorkSpace has been provisioned.

● **Standard**
Windows 7 Experience, 1 vCPU, 3.75 GiB Memory, 50 GB Storage
Applications: Microsoft Internet Explorer, Firefox, 7-Zip, Adobe Reader
$35 per WorkSpace per month

○ **Standard Plus**
Windows 7 Experience, 1 vCPU, 3.75 GiB Memory, 50 GB Storage
Applications: Microsoft Office Professional (Word, Excel, PowerPoint, OneNote, Outlook, Publisher and Access), Microsoft Internet Explorer, Firefox, 7-Zip, Adobe Reader, Trend Micro Anti-Virus
$50 per WorkSpace per month

○ **Performance**
Windows 7 Experience, 2 vCPU, 7.5 GiB Memory, 100 GB Storage
Applications: Microsoft Internet Explorer, Firefox, 7-Zip, Adobe Reader
$60 per WorkSpace per month

○ **Performance Plus**
Windows 7 Experience, 2 vCPU, 7.5 GiB Memory, 100 GB Storage
Applications: Microsoft Office Professional (Word, Excel, PowerPoint, OneNote, Outlook, Publisher and Access), Microsoft Internet Explorer, Firefox, 7-Zip, Adobe Reader, Trend Micro Anti-Virus
$75 per WorkSpace per month

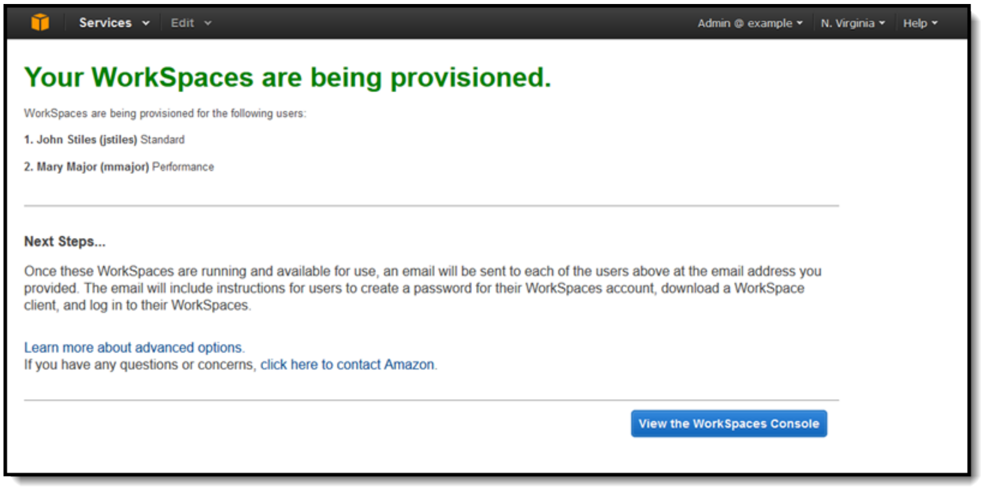
Enter User Details

Username	First Name	Last Name	Email	WorkSpace
				Standard

For more information about what Amazon WorkSpaces does during the quick start procedure, see Quick Setup Details (p. 10).

Provisioning WorkSpaces

It takes several minutes for the Amazon WorkSpaces infrastructure to be created and the WorkSpaces to be provisioned and initialized. You can monitor the status of the WorkSpaces by clicking**View the WorkSpaces Console**.



Your WorkSpaces are being provisioned.

WorkSpaces are being provisioned for the following users:

1. **John Stiles (jstiles)** Standard
2. **Mary Major (mmajor)** Performance

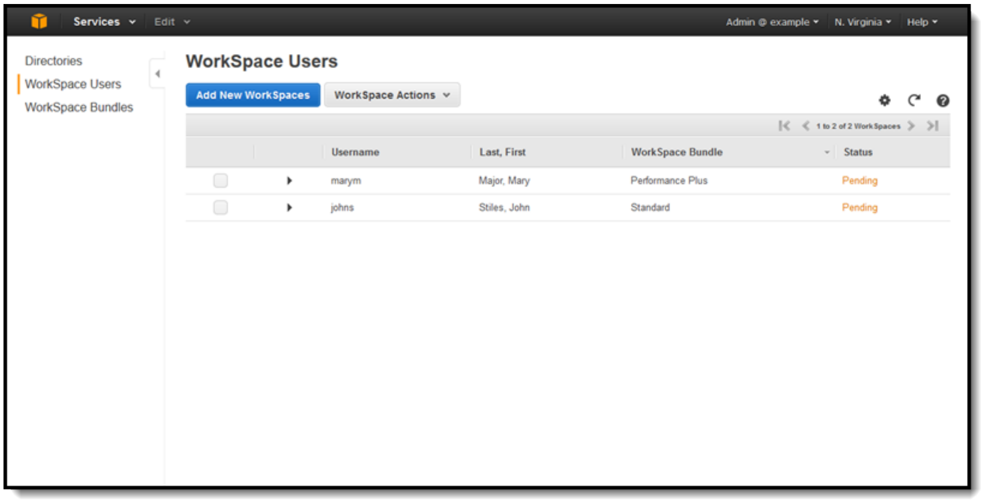
Next Steps...

Once these WorkSpaces are running and available for use, an email will be sent to each of the users above at the email address you provided. The email will include instructions for users to create a password for their WorkSpaces account, download a WorkSpace client, and log in to their WorkSpaces.

Learn more about advanced options.
If you have any questions or concerns, click here to contact Amazon.

Monitor WorkSpace Status

While the WorkSpaces are being provisioned and initialized, you can monitor the status in the **WorkSpaces** sections of the Amazon WorkSpaces console. The WorkSpaces start in the "Pending" state and change to the "Running" state when the provisioning and initialization are complete.



WorkSpace Users

		Username	Last, First	WorkSpace Bundle	Status
□	▸	marym	Major, Mary	Performance Plus	Pending
□	▸	johns	Stiles, John	Standard	Pending

WorkSpaces are Ready

When the WorkSpaces are ready for use, a welcome email is sent to each of the users. The welcome email contains instructions for the user to create their account, download and install a Amazon WorkSpaces client, and log in to their WorkSpace. The text of the email will be similar to the following:

Greetings,

A new Amazon WorkSpace has been provided for you. Follow the steps below to quickly get up and running with your WorkSpace:

1. Complete your user profile and download a WorkSpace client using the following link: *link_to_registration*.

2. Launch the Client and enter the following registration code: *registration_code*.

3. Login with your newly created password. Your username is *username*.

If you have any issues connecting to your WorkSpace, please contact your administrator.

You may download clients for additional devices at http://clients.amazonworkspaces.com/

Sincerely,

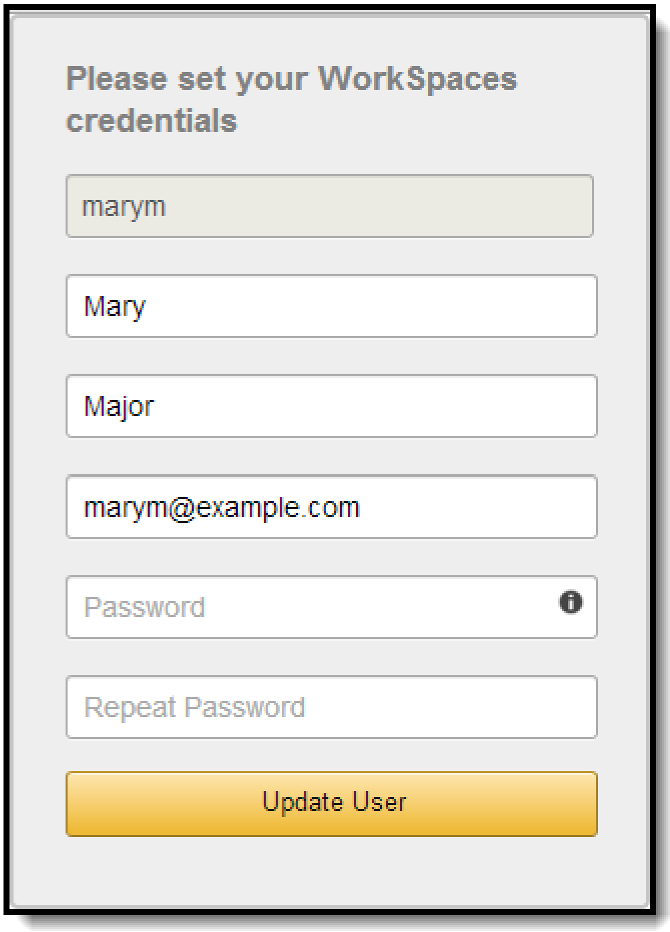
Amazon WorkSpaces

User Registration

The user must first complete their profile by going to the registration link provided in the email. The user must complete their registration within seven days of the email being sent; otherwise, the invitation expires and you must send another invitation.

The username and email address cannot be changed, but the user can change their first name and last name. The user must also set their password for the account. The password is case-sensitive and must be between 8 and 64 characters in length, inclusive. It must also contain at least one character from three of the following categories:

- Lowercase characters (a-z)
- Uppercase characters (A-Z)
- Numbers (0-9)
- Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)



Please set your WorkSpaces credentials

marym

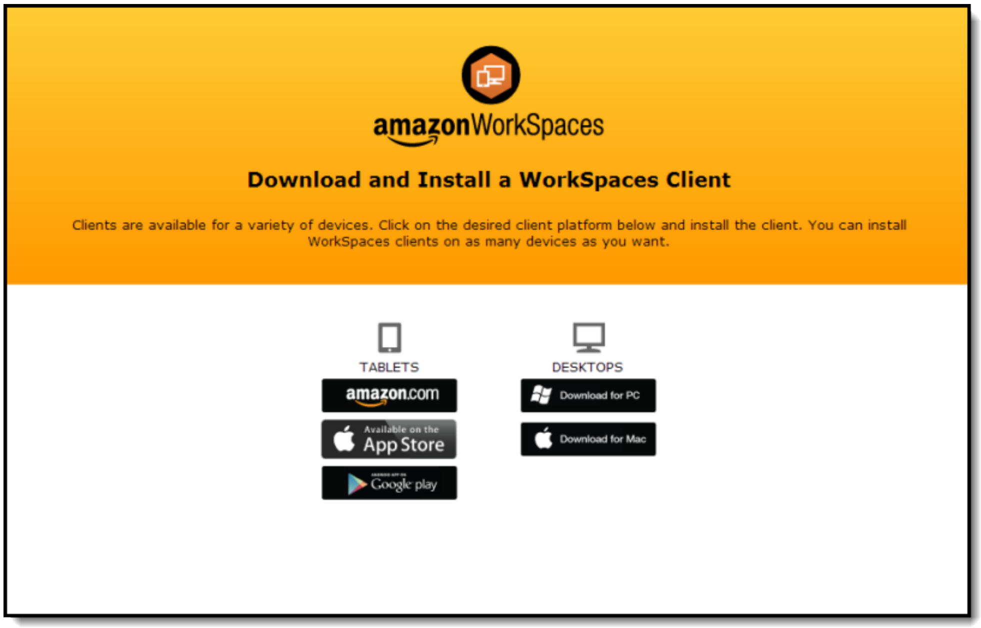
Mary

Major

marym@example.com

Download the Client

Your users can download their client applications at any time from the Amazon WorkSpaces Client Downloads page. For more information about available client applications, see Supported Platforms and Devices (p. 55).



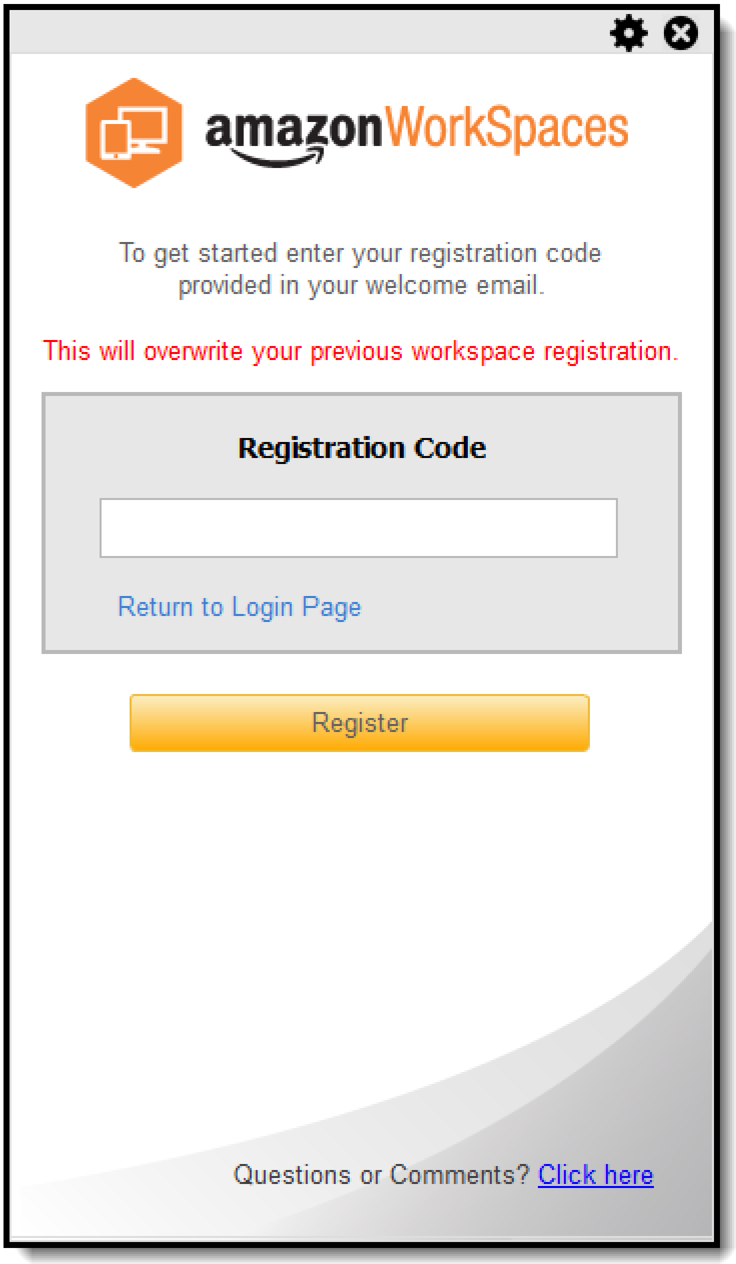
amazonWorkSpaces

Download and Install a WorkSpaces Client

Clients are available for a variety of devices. Click on the desired client platform below and install the client. You can install WorkSpaces clients on as many devices as you want.

Client Application Registration

The first time the user opens the client application, they need to enter the registration code included in their invitation email. This is how the client application knows which Amazon WorkSpaces directory to connect to. After the client application is registered, this step is skipped for subsequent logins. If the user needs to register the application again for any reason, they can click the gear icon at the top of the client sign in page, and select **Register**.

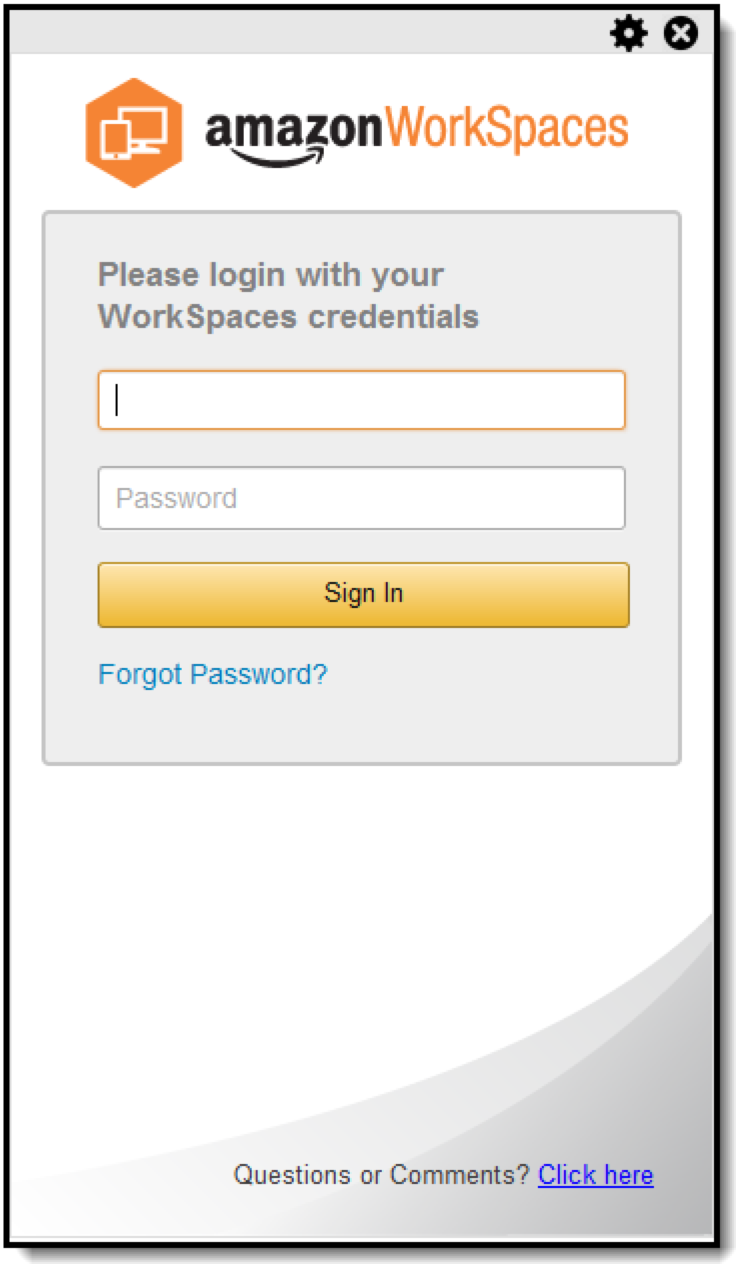


To get started enter your registration code provided in your welcome email.

This will overwrite your previous workspace registration.

Client Sign In

After the client application is registered, the user is taken to the sign in page. Here, the user enters their Amazon WorkSpaces username and the password they entered when they completed their user profile (p. 6). After the user signs in, the client application connects to their WorkSpace and displays the WorkSpace desktop.



Please login with your WorkSpaces credentials

Quick Setup Details

When you run the Amazon WorkSpaces quick setup procedure, Amazon WorkSpaces performs the following tasks on your behalf:

- Creates an IAM role to allow the Amazon WorkSpaces service to create elastic network interfaces and list your Amazon WorkSpaces directories. This role has the name `workspaces_DefaultRole`.
- Creates a virtual private cloud (VPC) under your account.

  Caution
  You must not modify any of the security groups, gateways, or other settings for this VPC. If you do, you run the risk of making your Amazon WorkSpaces environment inoperable.
- Sets up a directory within the VPC that is used to store user and WorkSpace information.

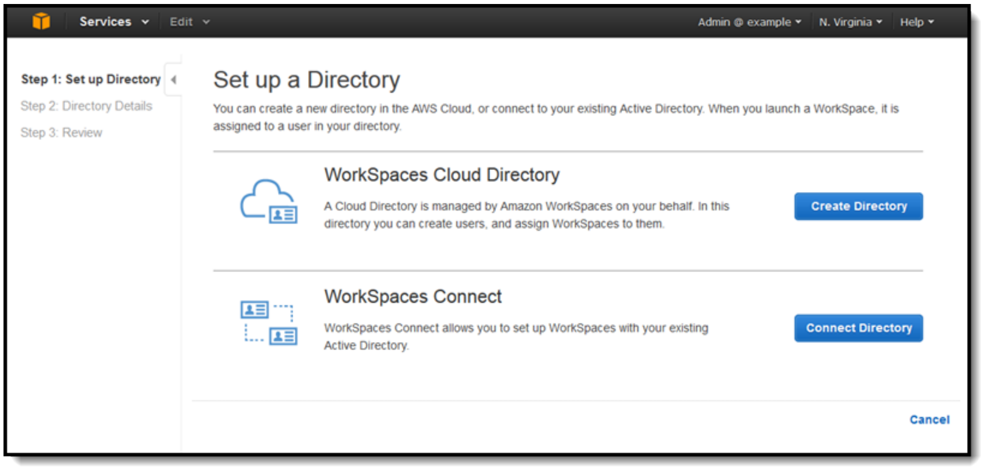
- Creates a directory administrator account.
- Creates the specified user accounts and adds them to the directory.
- Creates the WorkSpace instances.
- Sends invitation emails to the specified users.

Advanced Setup

The advance setup procedure allows you more control over the setup of your Amazon WorkSpaces directory. You can either create a stand-alone directory in the cloud, or connect Amazon WorkSpaces to your on-premises directory. You can also choose the name for your directory, as well as the VPC and subnets that are used for the directory.

To create a directory in the cloud, click **Create Directory** and proceed to Amazon WorkSpaces Directory in the Cloud (p. 17) to learn how to create a directory in the cloud and provision WorkSpaces in the directory.

To use WorkSpaces Connect to connect to your on-premises directory, click **Connect Directory** and proceed to Connect Amazon WorkSpaces to Your Directory (p. 24) to learn how to connect to, and provision WorkSpaces in, your directory.



Set up a Directory

You can create a new directory in the AWS Cloud, or connect to your existing Active Directory. When you launch a WorkSpace, it is assigned to a user in your directory.

WorkSpaces Cloud Directory

A Cloud Directory is managed by Amazon WorkSpaces on your behalf. In this directory you can create users, and assign WorkSpaces to them.

WorkSpaces Connect

WorkSpaces Connect allows you to set up WorkSpaces with your existing Active Directory.

Amazon WorkSpaces Administration

Amazon WorkSpaces is a fully managed desktop computing service in the cloud. Amazon WorkSpaces allows customers to easily provision cloud-based desktops that allow end-users to access the documents, applications, and resources they need with the device of their choice, including laptops, iPads, Kindle Fire, or Android tablets. For more information, see Amazon WorkSpaces.

Topics

Prerequisites

To use Amazon WorkSpaces, you must satisfy the following prerequisites.

Topics

AWS Account

Your AWS account gives you access to all services, but you are charged only for the resources that you use.

If you do not have an AWS account, use the following procedure to create one.

To sign up for AWS

1. Go to http://aws.amazon.com and click **Sign Up**.

2. Follow the on-screen instructions.

Your root account credentials identify you to services in AWS and grant you unlimited use of your AWS resources, such as your WorkSpaces. To allow other users to manage Amazon WorkSpaces resources without sharing your security credentials, use AWS Identity and Access Management (IAM). We recommend that everyone work as an IAM user, even the account owner. You should create an IAM user for yourself, give that IAM user administrative privileges, and use it for all your work.

Amazon WorkSpaces Client Prerequisites

The Amazon WorkSpaces client applications have minimum requirements that must be met in order to operate correctly and give your users a satisfactory client experience.

Topics

Port Access

To be able to connect to your WorkSpaces, your network must have port 4172 open to UDP and TCP traffic to the IP address ranges for certain Amazon EC2 instances. These are the EC2 instances that Amazon WorkSpaces uses to stream information to and from the Amazon WorkSpaces clients. This is necessary to allow the Amazon WorkSpaces clients to connect to their WorkSpaces from your network. These address ranges vary by AWS region. For a list of IP address ranges for different regions, see Announcement: Amazon EC2 Public IP Ranges. These same ports must also be open on any firewall that is running on the client as well.

To verify that these ports are configured properly on your network, perform the following steps.

To configure port access

1. In Amazon EC2, Launch an Amazon Linux instance in the same region that you will be creating your WorkSpaces in. This instance will be the host.
2. Add the following inbound rules to the security group you launched the host with. For all rules, specify your network CIDR for the source.

    - SSH on port 22 (needed to use SSH to connect to the instance)
    - TCP on port 4172
    - UDP on port 4172

3. Connect to the host using an SSH client and enter the following command. This sets up a listener on port 4172 for UDP traffic.

```
nc –l -u 4172
```

4. On a client computer on your network, download and install the netcat utility, if needed, and enter the following command.

```
netcat -u <host_public_IP_address> 4172
```

Type some characters on the client computer. If you see the characters echoed on the host, your network allows UDP traffic on port 4172.

5. On the host, enter the following command. This sets up a listener on port 4172 for TCP traffic.

   ```
   nc –l 4172
   ```

6. On a client computer on your network, enter the following command.

   ```
   netcat <host_public_IP_address> 4172
   ```

   Type some characters on the client computer. If you see the characters echoed on the Amazon EC2 instance, your network allows TCP traffic on port 4172.

Latency Threshhold

As with any networking service, network latency has an affect on the performance of the Amazon WorkSpaces client applications. For optimal performance, the round trip time (RTT) from the client's network to the region that your WorkSpaces are in should be less than 100ms. The Amazon WorkSpaces client applications remains functional with an RTT between 100ms and 250ms, although performance is degraded. You can test the RTT by performing the following procedure.

To test the round trip time on the client network

1. Launch an Amazon EC2 instance in the same region that you will be creating your WorkSpaces in.
2. Add an inbound rule to the security group you launched the instance with to allow ICMP from your network CIDR.
3. On a client computer on your network, ping the public IP address of the instance.

   ```
   ping <ec2_instance_public_IP_address>
   ```

   In the response from the ping request, the RTT is the `time` value.

MTU Threshhold

If you are accessing a WorkSpace through a virtual private network (VPN), your connection must support a maximum transmission unit (MTU) of at least 1200 bytes.

HTTPS Access

The Amazon WorkSpaces client applications require HTTPS access to Amazon WorkSpaces resources hosted by the service and Amazon Simple Storage Service (Amazon S3). This is required to successfully register and use the Amazon WorkSpaces client application.

Controlling Access to Amazon WorkSpaces Resources

AWS Identity and Access Management (IAM) enables you to do the following:

- Create users and groups under your AWS account

- Assign unique security credentials to each user under your AWS account
- Control each user's permissions to perform tasks using AWS resources
- Allow the users in another AWS account to share your AWS resources
- Create roles for your AWS account and define the users or services that can assume them
- Use existing identities for your enterprise to grant permissions to perform tasks using AWS resources

For more information about IAM, see the following:

- Identity and Access Management (IAM)
- Using IAM

IAM Policies for Amazon WorkSpaces

By default, IAM users don't have permission to Amazon WorkSpaces resources. To allow IAM users to manage Amazon WorkSpaces resources, you must create an IAM policy that explicitly grants IAM users permission to create and manage Amazon WorkSpaces and Amazon EC2 resources, and attach the policy to the IAM users or groups that require those permissions. For more information about IAM policies, see Permissions and Policies in the *Using IAM* guide.

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

The following policy statement grants an IAM user permission to manage Amazon WorkSpaces and Amazon EC2 resources, and grants an IAM user permission to create an IAM role. The `Action` and `Resource` elements use a wildcard to indicate that users have access to all actions and resources for this service.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "workspaces:*",
        "iam:PassRole",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:DeleteSecurityGroup",
    "ec2:DeleteNetworkInterface",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress"
    ],
   "Effect": "Allow",
   "Resource": "*"
  }
 ]
}
```

Directory Management

Topics

Amazon WorkSpaces Details

Topics

Directories

Amazon WorkSpaces uses a network directory to store its user and WorkSpace information. This directory can either be a directory in the cloud, or connected to your on-premises directory.

In a cloud directory, the user and WorkSpace information is stored in a standalone directory that resides in one of your VPCs. WorkSpace users exist solely within this directory and are not linked to any external entities. Amazon WorkSpaces sets up this directory for you when you create a cloud directory. You should use a cloud directory if you do not already have an on-premises directory, or if your users do not need access to any on-premises resources. For more information, see Amazon WorkSpaces Directory in the Cloud (p. 17).

In a connected directory, user and WorkSpace information is stored in your on-premises directory. WorkSpace users are selected from the users that already exist within your on-premises directory. The WorkSpaces that you create are represented as machine accounts within your directory. You should use a connected directory if your users need access to any on-premises resources. For more information, see Connect Amazon WorkSpaces to Your Directory (p. 24).

No matter which type of directory you use, you are responsible for providing Internet access to the WorkSpaces. More detailed information about how to provide this is given in specific topics.

Because Amazon WorkSpaces uses Active Directory to store its user and WorkSpace information, you can use whichever Active Directory tools you are familiar with to administrate these objects. You can easily set up a directory management WorkSpace within Amazon WorkSpaces to perform these operations from. For more information, see Set Up a Directory Administration WorkSpace (p. 37). As an alternative, you can join a Windows EC2 instance to this directory and install the Active Directory Administration Tools on the instance. For more information about joining a Windows instance to a directory, see Joining an Amazon EC2 Instance to a Directory (p. 37). For more information about installing the Active Directory Administration Tools on either a WorkSpace or instance, see Installing the Active Directory Administration Tools (p. 41).

Network Interfaces

Each WorkSpace has two network interfaces. One interface provides connectivity to the resources within your VPC as well as the Internet, and is used to join to the WorkSpaces directory. The other interface, known as the management network interface, is connected to a secure Amazon WorkSpaces management network. The management network interface is used for interactive streaming of the WorkSpace desktop with the Amazon WorkSpaces client application, and also allows the Amazon WorkSpaces service to manage the WorkSpace.

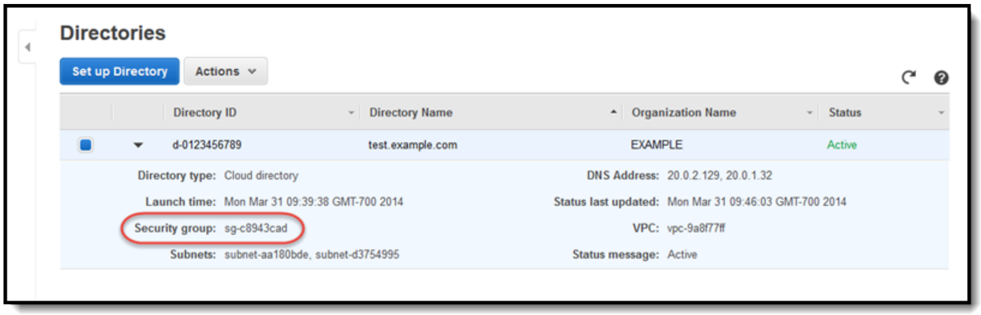
To prevent IP address conflicts with your VPC, the Amazon WorkSpaces service selects the IP address for the management network interface from two different address ranges. The two address ranges are 172.31.0.0/16 and 192.168.0.0/16. It is not possible to specify which address range is used.

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

- Inbound TCP on port 4172. This is used for establishment of the streaming connection.
- Inbound UDP on port 4172. This is used for streaming user input.
- Inbound TCP on port 8200. This is used for management and configuration of the WorkSpace.
- Outbound UDP on port 55000. This is used for PCoIP streaming.

WorkSpaces Security Group

When a cloud directory is created, Amazon WorkSpaces creates a security group that is used for the WorkSpaces in that directory. For a connected directory, the default security group for the VPC is used. You can find the identifier of the security group used for your WorkSpaces in the **Security group** field of the directory details, as shown in the following image.



Directories

	Directory ID	Directory Name	Organization Name	Status
■	d-0123456789	test.example.com	EXAMPLE	Active

Directory type: Cloud directory
Launch time: Mon Mar 31 09:39:38 GMT-700 2014
Security group: sg-c8943cad
Subnets: subnet-aa180bde, subnet-d3754995
DNS Address: 20.0.2.129, 20.0.1.32
Status last updated: Mon Mar 31 09:46:03 GMT-700 2014
VPC: vpc-9a8f77ff
Status message: Active

Amazon WorkSpaces Directory in the Cloud

Amazon WorkSpaces uses a network directory to store and manage WorkSpace and user information, and you can have Amazon WorkSpaces create this directory in the cloud for you.

Topics

Prerequisites

To create a directory in the cloud, you need the following:

- A VPC, with an Internet gateway and at least two subnets. Each of the subnets must be in a different Availability Zone. For more information, see the following topics in the *Amazon Virtual Private Cloud User Guide*:
  - What is Amazon VPC?
  - Subnets in Your VPC

Cloud Directory Internet Access

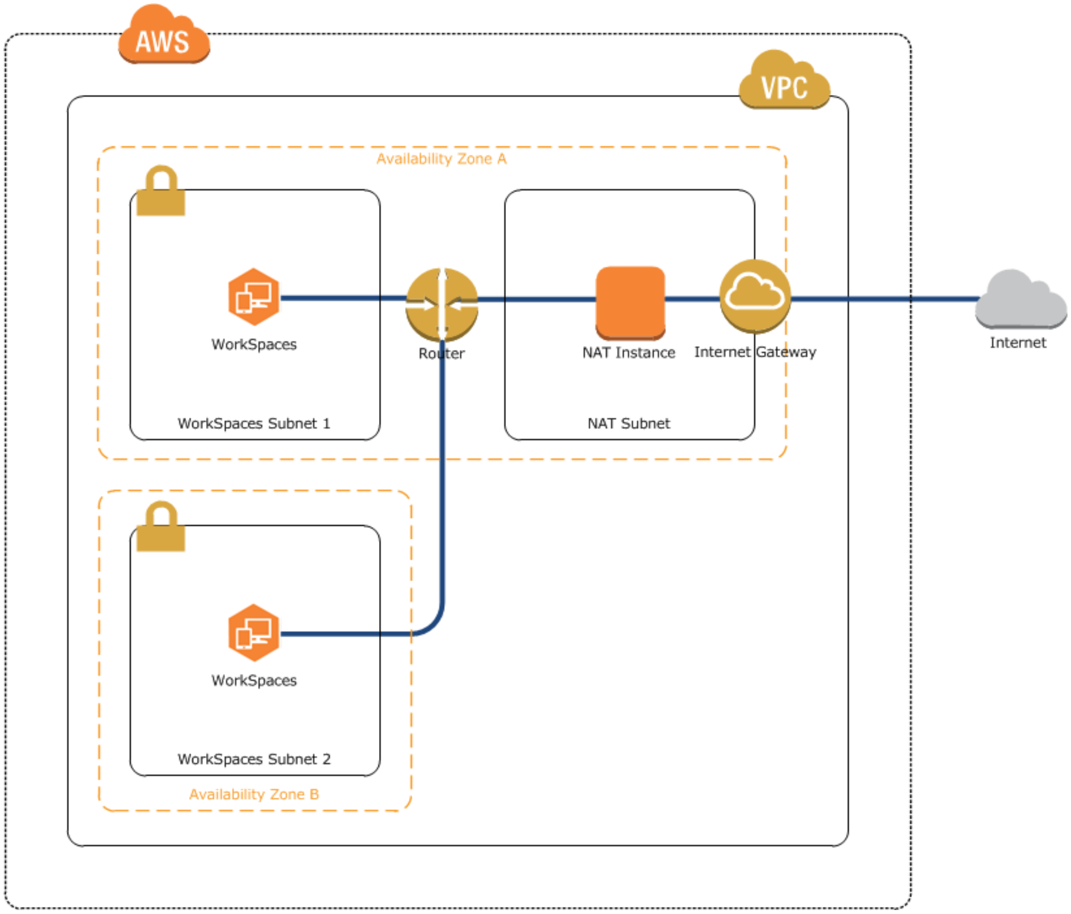
The WorkSpaces that you provision in a cloud directory cannot communicate with the Internet by default. You must use one of the following methods to provide Internet access to your WorkSpaces.

Topics

Cloud Directory NAT Instance

Implement a network address translation (NAT) instance in a public subnet (a subnet that has an Internet gateway attached to it) in the VPC used by the WorkSpaces directory. The NAT instance must be in a separate subnet from your WorkSpaces. This allows all of your WorkSpaces to access the Internet. For more information about this procedure, see NAT Instances in the *Amazon Virtual Private Cloud User Guide*.

To set up a NAT instance and give your WorkSpaces Internet access, perform the following steps. This example procedure assumes you have an existing VPC with two private subnets for your WorkSpaces. When completed, your VPC will look something like this:



To set up a NAT instance

1. Create a separate subnet for the NAT instance and launch the NAT instance in this subnet. After the NAT instance is running, disable the `SrcDestCheck` attribute for the NAT instance. For more information, see Disabling Source/Destination Checks in the *Amazon Virtual Private Cloud User Guide*.
2. Create an Internet gateway and attach it to the VPC.
3. Modify the route table that is assigned to the subnet containing the NAT instance to route all non-VPC traffic to the Internet gateway.

NAT Subnet Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	Internet gateway

4. Create a route table that routes all non-VPC traffic to the NAT instance and assign this route table to both WorkSpaces subnets. The route table will look like the following.

WorkSpaces Subnets Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	NAT Instance

5. Make sure the security group for your WorkSpaces allows outbound traffic on ports 80 (HTTP) and 443 (HTTPS) to all destinations (0.0.0.0/0). For information about how to find the WorkSpaces security group, see WorkSpaces Security Group (p. 17).
6. Your WorkSpaces now have access to the Internet. Connect to a WorkSpace and verify that you can connect to the Internet with a web browser.

For high availability, you can create a second NAT instance in a different Availability Zone.

Cloud Elastic IP Addresses

You can attach an Internet gateway to the VPC used by the WorkSpaces directory and assign an Elastic IP address to the network interface for each WorkSpace after it is created. This method should only be used for testing purposes and is not recommended as a long-term solution.

To assign an Elastic IP address to the network interface

1. Create an Internet gateway and attach it to the VPC used by the WorkSpaces directory. For more information, see Adding an Internet Gateway to Your VPC in the Amazon Virtual Private Cloud User Guide.
2. Open the Amazon WorkSpaces console for your desired region.
3. In the navigation pane, select **WorkSpaces**, select the WorkSpace you want to apply the Elastic IP address to, and click the right arrow button to display the details for the WorkSpace. Make a note of the **WorkSpace IP** value.
4. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/ and select your desired region.
5. In the navigation pane, select **Elastic IPs** and either select an unused VPC address or allocate a new address for VPC.
6. Select the address, click **Associate Address**, and enter the WorkSpace IP value found in step 3 in the **Network Interface** field. The identifier of the elastic network interface (ENI) that is assigned that IP address will be displayed in the search list. This is the ENI of the WorkSpace. Select the ENI identifier. The WorkSpace IP will be displayed in the **Private IP Address** field.
7. Select **Reassociation** so that the EIP can be reassigned later if needed, and click **Associate**.
8. Make sure the security group for your WorkSpaces allows outbound traffic on ports 80 (HTTP) and 443 (HTTPS) to all destinations (0.0.0.0/0). For information about how to find the WorkSpaces security group, see WorkSpaces Security Group (p. 17).
9. Modify the route table for both WorkSpaces subnets to route all non-VPC traffic to the Internet gateway.

WorkSpaces Subnet Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	Internet gateway

10. Your WorkSpaces will now have access to the Internet. Connect to a WorkSpace and verify that you can connect to the Internet with a web browser.

Using Amazon WorkSpaces With A Cloud Directory

When you create an Amazon WorkSpaces cloud directory, you are creating the directory that Amazon WorkSpaces will use as the source of identities for users that will be using the WorkSpaces.

Topics

Creating a Cloud Directory

Topics

Create the Directory

To create an Amazon WorkSpaces cloud directory, perform the following steps.

To create a cloud directory

1. Open the Amazon WorkSpaces console for your desired region.
2. In the navigation pane, select **Directories**, select **Set up Directory**, then select **Create Directory**.
3. Enter the following values and then click **Continue**.

Directory Details

Field	Description
Organization Name	A globally unique name for the organization. This must be at least four characters in length and can contain only alphanumeric characters and hyphens. The name cannot begin or end with a hyphen.
Directory DNS	The fully-qualified name of the directory, such as `corp.example.com`.
NetBIOS name	The NetBIOS name of the directory, such as `CORP`.
Administrator password	The password for the directory administrator. The directory creation process creates an administrator account with the username `Administrator` and this password. For password requirements, see the note following the table.
Confirm password	Re-enter the administrator password.

Note

The directory administrator password is case-sensitive and must be between 8 and 64 characters in length, inclusive. It must also contain at least one character from three of the following four categories:

- Lowercase letters (a-z)
- Uppercase letters (A-Z)
- Numbers (0-9)
- Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

VPC Details

Field	Description
VPC	The VPC that the directory is created in.
Subnets	The subnets in the VPC that the directory is created in. The two subnets must be in different Availability Zones.

4. Review the directory information and make any necessary changes. When the information is correct, click **Create Directory**.

It takes several minutes for the directory to be created. When it has been successfully created, the **Status** value changes to `Active`.

Cloud Directory Setup Details

When you create a cloud directory, Amazon WorkSpaces performs the following tasks on your behalf:

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

Cloud Directory Administration

When you created the directory, Amazon WorkSpaces created a directory administrator account for you. The username is `Administrator` and the password is the password you specified when you created the directory. You use this account to administrate your cloud directory.

To administrate your directory, connect to a WorkSpace and install the Active Directory Administration Tools on the WorkSpace as shown in Install the Active Directory Domain Administration Tools on a WorkSpace or Windows Server 2008 (p. 41). When you run any of the Active Directory Administration Tools, you must run them as the directory administrator by following these steps:

1. Open the **Administrative Tools**.
2. Hold down the shift key, right-click on the tool shortcut, and select **Run as different user**.
3. Enter `Administrator` for the user name and the administrator password.

You can now perform any directory administration tasks that are needed. You can also promote any of your Amazon WorkSpaces user accounts to a directory administrator. To do this, perform the following steps:

Promote a user to a directory administrator

1. Run the Active Directory Users and Computers tool as the directory administrator.
2. Navigate to the **Users** folder under your domain and select the user to promote.
3. In the menu, select **Action** -> **Properties**.
4. In the user properties dialog box, select the **Member of** tab.
5. Add the user to the following groups and click **OK**.

   - Administrators
   - Domain Admins
   - Enterprise Admins
   - Group Policy Creator Owners
   - Schema Admins

   The user is now a directory administrator.

Provisioning WorkSpaces

With an Amazon WorkSpaces cloud directory, you use Amazon WorkSpaces to create users that can access your WorkSpaces.

To provision a WorkSpace for a user

1. Open the Amazon WorkSpaces console for your desired region.
2. In the navigation pane, select **WorkSpaces** then select **Launch WorkSpaces**.
3. In **Select Directory**, select your cloud directory. This is the directory that users will be selected from.

   If this is the first time you have provisioned a WorkSpace in this directory, you can select to have WorkSpaces Sync enabled or disabled for all users in the directory. For more information about WorkSpaces Sync, see Amazon WorkSpaces Sync Application Help (p. 71). Make your choice and click **Next**.

   > **Note**
   > The Amazon WorkSpaces Sync service is currently not available in the following region:
   >
   > - Asia Pacific (Sydney) Region

4. In **Identify Users**, select the users for which to provision a WorkSpace. You can search for all or part of the user's name, or use the wildcard character (*) to extend the search. If a user does not have an email address, you will not be able to provision a WorkSpace for that user.

   When you have selected the desired users, click **Add Selected**. The selected users are added to the **WorkSpace Users** list.

   If you want to create a new user, enter the information for the new user. If you want to create another user, click **Create Additional Users** and enter the information for the additional user. Repeat this process for all new users and click **Create Users**. The new users are added to the **WorkSpaces** list.

   Repeat this step until you have selected or created all of the desired users, then click **Next**.

5. In **Assign Bundles**, select the default WorkSpace bundle to be used when provisioning the WorkSpaces. The WorkSpace bundle for individual users can also be selected here, if desired.
6. Make any changes needed to the list of users or the bundle to use for the WorkSpaces, then click **Launch WorkSpaces**.

When provisioning WorkSpaces in a cloud directory, Amazon WorkSpaces assigns the security group it created for directory members to the WorkSpace. For more information about the security group, see WorkSpaces Security Group (p. 17).

It takes several minutes for the WorkSpaces to be provisioned. When the WorkSpaces are ready for use, an invitation email is sent to unregistered users with registration instructions. If a user has already registered, you must send a welcome email instead. The welcome email contains instructions to download and install a Amazon WorkSpaces client and log in to their WorkSpace. For more information, see Resend an Invitation (p. 51).

Deleting a Directory

Before you can delete a directory, you must first remove all WorkSpaces from the directory. For more information about removing WorkSpaces, see Remove a WorkSpace (p. 53). To delete a directory, perform the following steps.

To delete a directory

1. Open the Amazon WorkSpaces console for your desired region.
2. In the navigation pane, select **Directories**.
3. Select the directory to delete, click **Actions**, and select **Delete**.
4. Verify the information in the **Delete Directory** dialog box, and click **Delete**.

Connect Amazon WorkSpaces to Your Directory

Amazon WorkSpaces uses a network directory to store and manage WorkSpace and user information. You can use WorkSpaces Connect to connect Amazon WorkSpaces to your on-premises directory, which allows your users to sign into their WorkSpace using their on-premises credentials. It also gives them access, from their WorkSpace, to the same on-premises resources that they have access to locally.

Topics

Prerequisites

To use WorkSpaces Connect to connect to your on-premises directory, you need the following:

- A VPC, with an Internet gateway and at least two subnets. Each of the subnets must be in a different Availability Zone. The VPC must also be connected to your on-premises network through a virtual private network (VPN) connection or AWS Direct Connect. For more information, see the following topics in the *Amazon Virtual Private Cloud User Guide*:
  - What is Amazon VPC?
  - Subnets in your VPC

  - Adding a Hardware Virtual Private Gateway to Your VPC
  - AWS Direct Connect User Guide
- An on-premises network with an Active Directory domain.
- Credentials for an account in the on-premises directory with the following privileges. For more information, see Delegating Connect Privileges (p. 26).
  - Read users and groups.
  - Create computer objects.
  - Join computers to the domain.
- The IP addresses of two DNS servers or domain controllers in your on-premises directory.
- For Amazon WorkSpaces to communicate with your on-premises directory, the firewall for your on-premises network must have the following ports open to the CIDRs for both subnets in the VPC.

Port	Type of Traffic
TCP 53	DNS
TCP 88	Kerberos
TCP 135	EPM
TCP 139	NetBIOS Session Service
TCP 389	LDAP
TCP 445	DFS, LsaRpc, NbtSS, NetLogonR, SamR, SMB, SrvSvc
TCP 464	Kerberos Change/Set Password
TCP 636	LDAPS
TCP 3268	GC, LDAP
TCP 3269	GC, LDAPS
TCP 5722	DFS-R
TCP 9389	Active Directory Web Services
UDP 53	DNS
UDP 88	Kerberos
UDP 123	NTP
UDP 137	NetBIOS Name Service
UDP 138	NetBIOS Datagram Service
UDP 389	C-LDAP
UDP 445	SMB
UDP 464	Kerberos Change/Set Password
UDP 2535	MADCAP

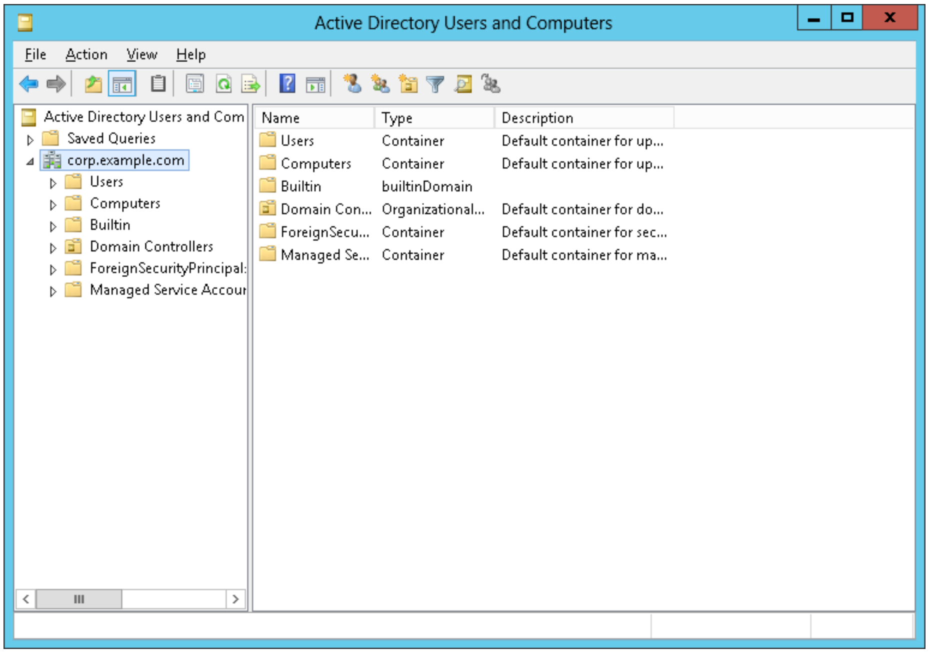
To test if these criteria are met, before connecting to your on-premises directory, see Connect Verification (p. 28).

Delegating Connect Privileges

For WorkSpaces Connect to connect to your on-premises directory, you must have the credentials for an account in the on-premises directory that has certain privileges. While members of the **Domain Admins** group have sufficient privileges to connect to the directory, as a best practice, you should use an account that only has the minimum privileges necessary to connect to the directory. The following procedure demonstrates how to create a new group called `WorkSpaces_Connectors`, and delegate the privileges to this group that are needed to connect Amazon WorkSpaces to the directory.

This procedure must be performed on a machine that is joined to your directory and has the **Active Directory User and Computers** MMC snap-in installed. You must also be logged in as a domain administrator.

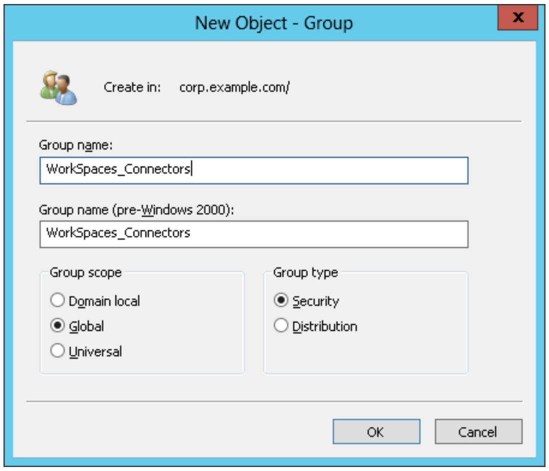
1. Open **Active Directory User and Computers** and select your domain root in the navigation tree.



Name	Type	Description
Users	Container	Default container for up...
Computers	Container	Default container for up...
Builtin	builtinDomain	
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...

2. In the list in the left-hand pane, right-click **Users**, select **New**, and then select **Group**.
3. In the **New Object - Group** dialog box, enter the following and click **OK**.

Field	Value/Selection
Group name	`WorkSpaces_Connectors`
Group scope	**Global**
Group type	**Security**



New Object - Group

Create in: corp.example.com/

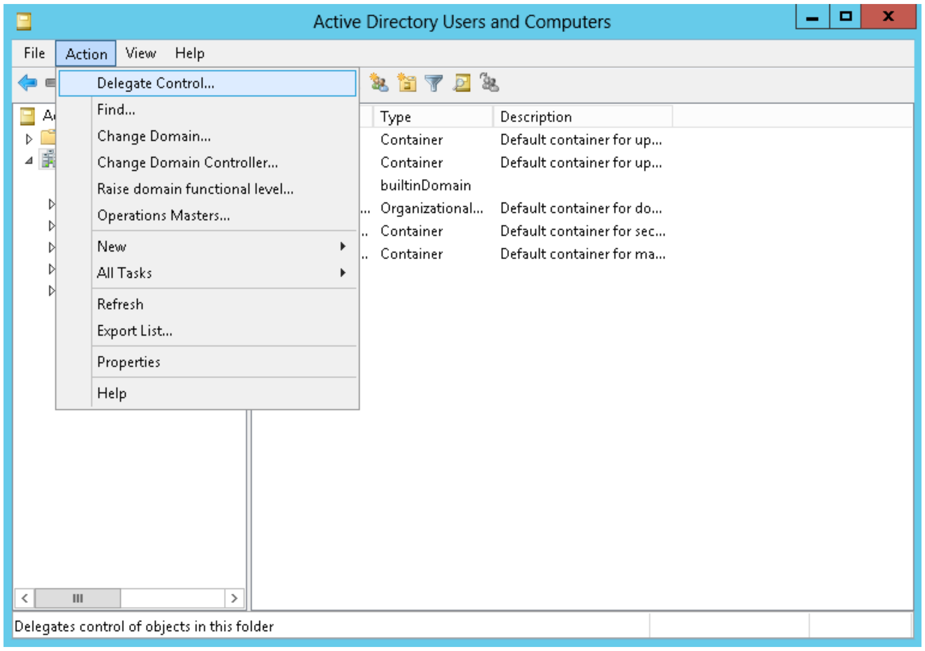
Group name:
WorkSpaces_Connectors

Group name (pre-Windows 2000):
WorkSpaces_Connectors

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

4. In the **Active Directory User and Computers** navigation tree, select your domain root. In the menu, select **Action**, and then **Delegate Control**.

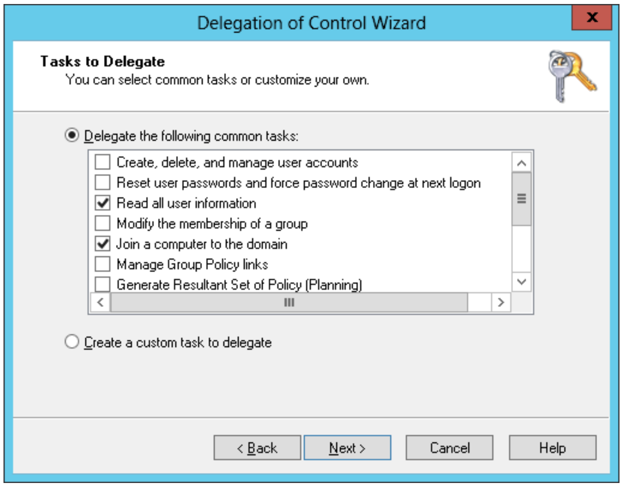


Active Directory Users and Computers

Type	Description
Container	Default container for up...
Container	Default container for up...
builtinDomain	
Organizational...	Default container for do...
Container	Default container for sec...
Container	Default container for ma...

Delegates control of objects in this folder

5. On the **Delegation of Control Wizard** page, click **Next**, then click **Add**.
6. In the **Select Users, Computers, or Groups** dialog box, enter `WorkSpaces_Connectors` and click **OK**. If more than one object is found, select the `WorkSpaces_Connectors` group created above. Click **Next**.
7. On the **Tasks to Delegate** page, select only **Read all user information** and **Join a computer to the domain**, then click **Next**.



Tasks to Delegate
You can select common tasks or customize your own.

● Delegate the following common tasks:

- □ Create, delete, and manage user accounts
- □ Reset user passwords and force password change at next logon
- ☑ Read all user information
- □ Modify the membership of a group
- ☑ Join a computer to the domain
- □ Manage Group Policy links
- □ Generate Resultant Set of Policy (Planning)

○ Create a custom task to delegate

8. Verify the information on the **Completing the Delegation of Control Wizard** page, and click **Finish**.
9. Create a user with a strong password and add that user to the `WorkSpaces_Connectors` group. The user will have sufficient privileges to connect Amazon WorkSpaces to the directory.

Connect Verification

For Amazon WorkSpaces to connect to your on-premises directory, the firewall for your on-premises network must have certain ports open to the CIDRs for both subnets in the VPC, and you must have the credentials for an account in the directory that has sufficient privileges. To test if these conditions are met, perform the following steps:

To verify the connection

1. Launch a Windows instance in the VPC and connect to it over RDP. The remaining steps are performed on the VPC instance.
2. Download and install the PortQry port scanning utility from PortQry Command Line Port Scanner Version 2.0.
3. Open a PowerShell command window and set the execution policy to **Unrestricted** with the following command. Answer "Y" to the verification.

```
PS C:\> Set-ExecutionPolicy Unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust.
 Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help
topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the
execution policy?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

PS C:\>
```

4. Add the PortQry install directory to the path environment.

```
PS C:/> $env:Path = "[PortQry install path]"
```

5. Copy the following script and save it as a PowerShell script file (`.ps1`).

```
<# Verify the ports and credentials. #>
$groups = @("domain admins","enterprise admins")
$members = @()
$memberNames = @()
$hasPrivilege = $False
$domainName = Read-Host "Please enter the domain name"
$cred = Get-Credential
$username = $cred.Username
$password = $cred.GetNetWorkCredential().password

$assem = ("System.DirectoryServices.AccountManagement", "System")
$source = @"
using System;
using System.Collections.Generic;
using System.DirectoryServices.AccountManagement;

public class groupsOfUser {
   public List<GroupPrincipal> getGroups(string domainName, string username,
 string password) {
        List<GroupPrincipal> result = new List<GroupPrincipal>();
        PrincipalContext domain = new PrincipalContext(ContextType.Domain,
 domainName, username, password);
       UserPrincipal user = UserPrincipal.FindByIdentity(domain, username);

        if(user != null) {
           PrincipalSearchResult<Principal> groups = user.GetAuthorization
Groups();
            foreach(Principal p in groups) {
                if(p is GroupPrincipal) {
                    result.Add((GroupPrincipal)p);
                }
            }
        }
        return result;
   }
}
"@

Add-Type -ReferencedAssemblies $assem  -TypeDefinition $source
$getGroupsObject = New-Object groupsOfUser;

<# Check account credentials. #>
Write-Host "=======================================";
Write-Host "Checking domain name, user name, and password `n";
try {
   $groups = $getGroupsObject.getGroups($domainName, $username, $password);
} catch [Exception] {
    Write-Host  $_.Exception.ToString() "`n" -ForegroundColor red;
}
$groupNames = @();
$count = 0;
while($groups[$count] -ne $null) {
    $groupNames += $groups[$count].name;
    $count++;
}
```

```
<# Check forest functional level. #>
Write-Host "=======================================";
Write-Host "Checking forest functional level `n";
try {
    $ForestContext = New-Object System.DirectoryServices.ActiveDirectory.Dir
ectoryContext("Forest", $domainName, $username, $password);
    $Forest = [System.DirectoryServices.ActiveDirectory.Forest]::Get
Forest($ForestContext);
} catch [Exception] {
    Write-Host $_.Exception.ToString() "`n" -ForegroundColor red;
}
Write-Host "`n The forest functional level is" $Forest.ForestMode;
if($Forest.ForestMode -ge "Windows2008R2Forest") {
    Write-Host "`n The forest functional level is correct. `n" -Foreground
Color green;
} else {
    Write-Host "`n The forest functional level must be Windows2008R2Forest
 or greater. You cannot connect to the directory! `n" -ForegroundColor red;
}

<# Check domain functional level. #>
Write-Host "=======================================";
Write-Host "Checking domain functional level. `n";
try {
    $DomainContext = New-Object System.DirectoryServices.ActiveDirectory.Dir
ectoryContext("Domain", $domainName, $username, $password);
    $Domain = [System.DirectoryServices.ActiveDirectory.Domain]::GetDomain($Do
mainContext);
} catch [Exception] {
    Write-Host $_.Exception.ToString() "`n" -ForegroundColor red;
}
Write-Host "`n The domain functional level is:" $Domain.DomainMode;
if($Domain.DomainMode -ge "Windows2008R2Domain") {
    Write-Host "`n The domain functional level is correct. `n" -Foreground
Color green;
} else {
    Write-Host "`n The domain functional level must be Windows2008R2Domain
 or greater. You cannot connect to the directory! `n" -ForegroundColor red;
}

<# Verify identity of customer. #>
Write-Host "=======================================";
Write-Host "Verifying account privileges.";
if(($groupNames -contains "domain admins") -or ($groupNames -contains "en
terprise admins")) {
    Write-Host "`n The account has the privileges necessary to connect to
the directory. `n" -Foregroundcolor green;
} else {
    Write-Host "`n The account does not have the privileges necessary to
connect to the directory. `n" -Foregroundcolor yellow;
}

<#check ports#>
$serviceName = "PortTest"
$allTcpPorts = @(389,636,3268,3269,88,53,445,135,5722,464,9389,139)
$allUdpPorts = @(389,88,53,445,123,464,138,2535,137)
Write-Host "=======================================";
```

```
Write-Host "Start to check ports `n";
Write-Host "In order to create an additional domain controller, please make
 sure all of the following ports are open. This test may take a while. `n";



foreach ($tcpPort in $allTcpPorts) {
    try {
        $cmd = "PortQry.exe";
        $argList = "-n $domainName -e $tcpPort -p TCP";
        $fileName = $serviceName + "output-TCP-$tcpPort.txt";
       Start-Process "$cmd" "$argList" -NoNewWindow -RedirectStandardOutput
 "$fileName" -Wait;
        $content = Get-Content "$fileName";
        $portListen = $content | Select-String "LISTENING";
        $portNotListen = $content | Select-String "NOT LISTENING";
        $portFiltered = $content | Select-String "FILTERED";

        if(($portListen -ne $NULL) -and ($portNotListen -eq $NULL) -and
($portFiltered -eq $NULL)) {
            $result = $domainName + " has TCP " + $tcpPort + " Open";
            Write-Host $result;
        }else {
            $result = $domainName + " has TCP " + $tcpPort + " Closed";
            Write-Host $result -ForegroundColor yellow;
        }
    } catch [Exception] {
        Write-Host "`n" $_.Exception.ToString() -ForegroundColor red;
        break;
    }
}

foreach ($udpPort in $allUdpPorts) {
   try {
        $cmd = "PortQry.exe";
        $argList = "-n $domainName -e $udpPort -p UDP";
        $fileName = $serviceName + "output-UDP-$udpPort.txt";
       Start-Process "$cmd" "$argList" -NoNewWindow -RedirectStandardOutput
 "$fileName" -Wait;
        $content = Get-Content "$fileName";
        $portListen = $content | Select-String "LISTENING";
        $portNotListen = $content | Select-String "NOT LISTENING";
        $portFiltered = $content | Select-String "FILTERED";

        if(($portListen -ne $NULL) -and ($portNotListen -eq $NULL) -and
($portFiltered -eq $NULL)) {
            $result = $domainName + " has UDP " + $udpPort + " Open";
            Write-Host $result;
        }else {
            $result = $domainName + " has UDP " + $udpPort + " Closed";
            Write-Host $result -ForegroundColor yellow;
        }
    } catch [Exception] {
        Write-Host "`n" $_.Exception.ToString() -ForegroundColor red;
        break;
    }
}
```

6. Run the PowerShell script. When prompted, enter the domain name and the credentials for a domain account that has the privileges defined in Prerequisites (p. 24). The script tells you if the proper ports are or are not open, and if the supplied account has sufficient privileges to connect to the directory.

Connected Directory Internet Access

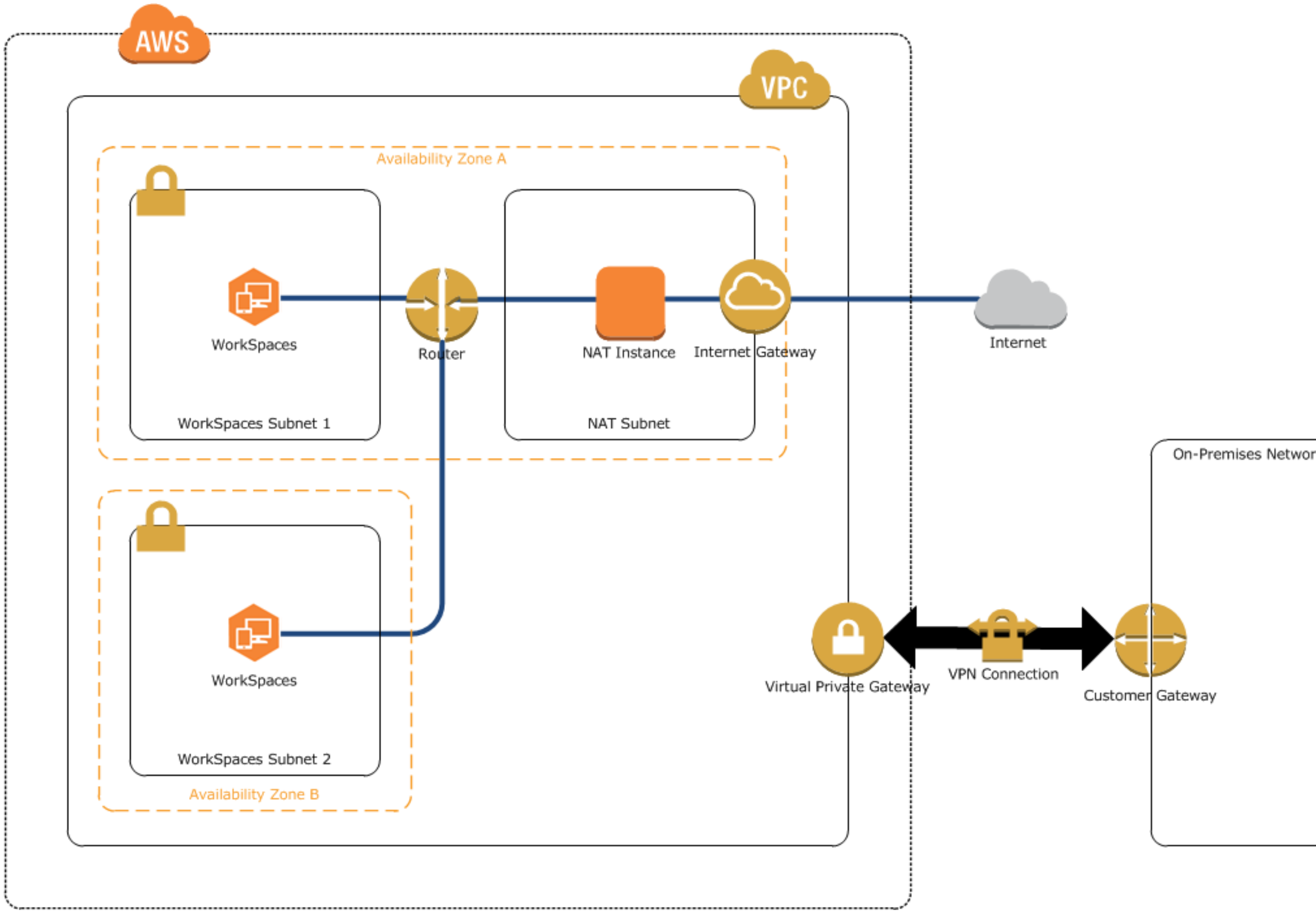
The WorkSpaces that you provision in a connected directory cannot communicate with the Internet by default. You must use one of the following methods to provide Internet access to your WorkSpaces.

Topics

Connected Directory NAT Instance

Implement a network address translation (NAT) instance in a public subnet (a subnet that has an Internet gateway attached to it) in the VPC used by the WorkSpaces directory. This allows all of your WorkSpaces access to the Internet. For more information about this procedure, see NAT Instances in the Amazon Virtual Private Cloud User Guide.

For more information about how to set up a NAT instance to give your WorkSpaces Internet access, see Cloud Directory NAT Instance (p. 18). When completed, your VPC will look something like this:



To set up a NAT instance

1. Create a separate subnet for the NAT instance and launch the NAT instance in this subnet. After the NAT instance is running, disable the *SrcDestCheck* attribute for the NAT instance. For more information, see Disabling Source/Destination Checks in the *Amazon Virtual Private Cloud User Guide*.
2. Create an Internet gateway and attach it to the VPC.
3. Modify the route table that is assigned to the subnet containing the NAT instance to route all non-VPC traffic to the Internet gateway.

   NAT Subnet Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	Internet gateway

4. Create a route table that routes all non-VPC traffic to the NAT instance and assign this route table to both WorkSpaces subnets. The route table will look like the following.

   WorkSpaces Subnets Route Table

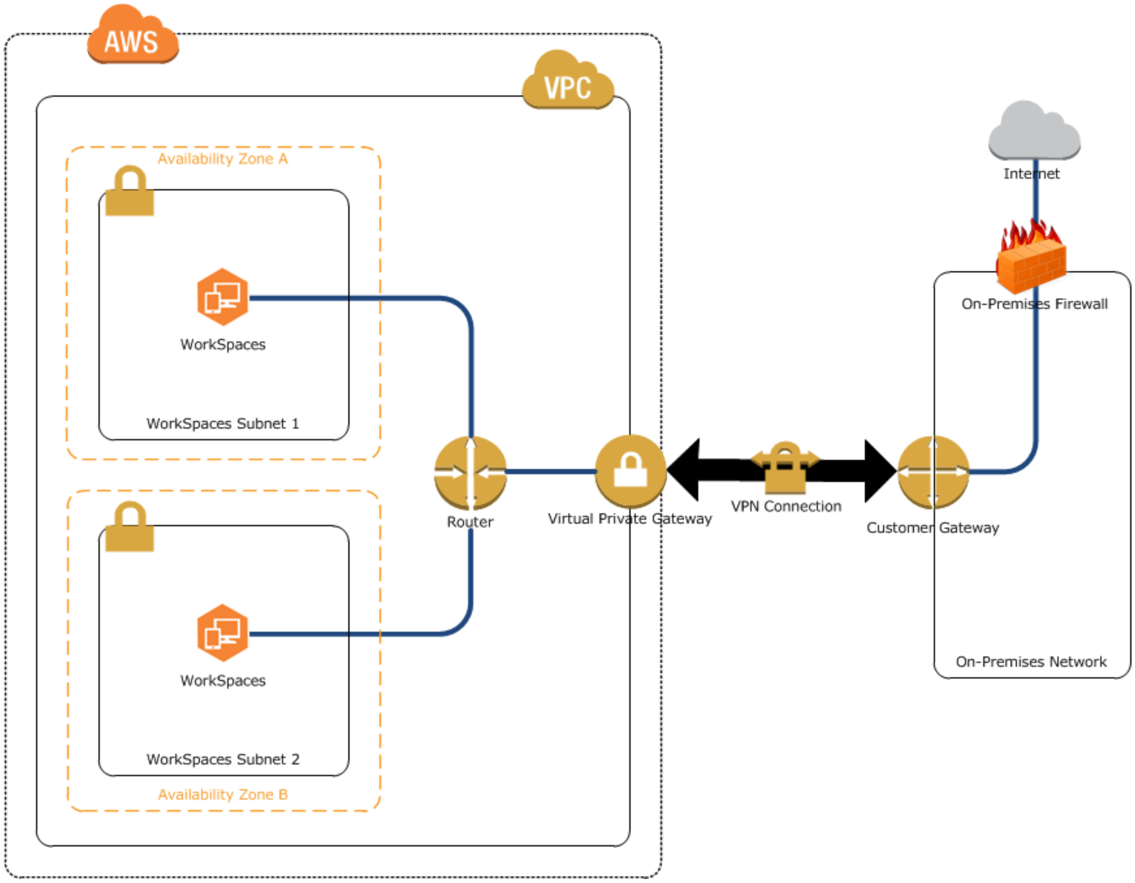
Destination	Target
VPC CIDR	local
0.0.0.0/0	NAT Instance

5. Make sure the security group for your WorkSpaces allows outbound traffic on ports 80 (HTTP) and 443 (HTTPS) to all destinations (0.0.0.0/0). For information about how to find the WorkSpaces security group, see WorkSpaces Security Group (p. 17).
6. Your WorkSpaces now have access to the Internet. Connect to a WorkSpace and verify that you can connect to the Internet with a web browser.

For high availability, you can create a second NAT instance in a different Availability Zone.

On-Premises Firewall

Give the WorkSpaces access to your on-premises network's Internet firewall. You need to adjust the route tables to give the subnets access to your firewall.



Connect Elastic IP Addresses

Attach an Internet gateway to the VPC used by the WorkSpaces directory and modify the routing tables for all subnets to use the Internet gateway. Then, assign an Elastic IP address to the network interface for each WorkSpace after it is created. For more information about this process, see Adding an Internet Gateway to Your VPC in the Amazon Virtual Private Cloud User Guide. This method should only be used for testing purposes and is not recommended as a long-term solution.

For more information about how to set up Elastic IP addresses to give your WorkSpaces Internet access, see Cloud Elastic IP Addresses (p. 20).

Using Amazon WorkSpaces With Your Directory

When connecting Amazon WorkSpaces to your on-premises directory, you direct Amazon WorkSpaces to use your on-premises directory as a source of identities for users who will be using the WorkSpaces.

Topics

Connecting to Your Directory

To use WorkSpaces Connect to connect to your on-premises directory, perform the following steps.

To connect to a directory

1. Open the Amazon WorkSpaces console for your desired region.
2. In the navigation pane, select **Directories**, select **Set up Directory**, then select **Connect Directory**.
3. Enter the following values and then click **Continue**.

   #### Directory Details

Field	Description
Organization Name	A globally unique name for the organization. This must be at least four characters in length and can contain only alphanumeric characters and hyphens. The name cannot begin or end with a hyphen.
Directory DNS	The fully-qualified name of the on-premises directory, such as `corp.example.com`. Amazon WorkSpaces can only access user accounts in this directory. User accounts cannot be contained in a parent directory, such as `example.com`.
NetBIOS name	The NetBIOS name of the on-premises directory, such as `CORP`.
Account username	The username of a user in the on-premises directory. For more information about this account, see the Prerequisites (p. 24) section.
Account password	The password for the on-premises user account.
Confirm password	Re-enter the password for the on-premises user account. This is required to prevent typing errors before the directory is connected.
DNS Addresses	The IP addresses of two different DNS servers or domain controllers in your on-premises directory. These servers must be accessible from each subnet specified below.

   #### VPC Details

Field	Description
VPC	The VPC that the directory is connected to.
Subnets	The subnets in the VPC to use to connect to your on-premises directory. The two subnets must be in different Availability Zones.

4. Review the directory information and make any necessary changes. When the information is correct, click **Connect Directory**.

It takes several minutes for the directory to be connected. When it has been successfully connected, the **Status** value changes to `Active`.

Provisioning WorkSpaces

When Amazon WorkSpaces is connected to your on-premises directory, you do not add or remove users with the Amazon WorkSpaces console. Instead, you select existing users in your directory when you are provisioning WorkSpaces.

To provision a WorkSpace for an existing user

1. Open the Amazon WorkSpaces console for your desired region.
2. In the navigation pane, select **WorkSpaces** then select **Launch WorkSpaces**.
3. In **Select a Directory**, select your connected directory. This is the directory that users are selected from.

   If this is the first time you have provisioned a WorkSpace in this directory, you can select to have WorkSpaces Sync enabled or disabled for all users in the directory. For more information about WorkSpaces Sync, see Amazon WorkSpaces Sync Application Help (p. 71). Make your choice and click **Next**.

   > **Note**
   > The Amazon WorkSpaces Sync service is currently not available in the following region:
   >
   > - Asia Pacific (Sydney) Region

4. In **Identify Users**, select the users for which to provision a WorkSpace. You can search for all or part of the user's name, or use the wildcard character (*) to extend the search. If a user does not have an email address, you will not be able to provision a WorkSpace for that user.

   When you have selected the desired users, click **Add Selected**. The selected users are moved to the **WorkSpaces** list.

   Repeat this step until you have selected all of the desired users, then click **Next**.
5. In **Assign Bundles**, select the default WorkSpace bundle to be used when provisioning the WorkSpaces. The WorkSpace bundle for individual users can also be selected here, if desired.
6. Make any changes needed to the list of users or the bundle to use for the WorkSpaces, then click **Launch WorkSpaces**.

When provisioning WorkSpaces in a connected directory, Amazon WorkSpaces assigns the default VPC security group to the WorkSpace.

It takes several minutes for the WorkSpaces to be provisioned. When the WorkSpaces are ready for use, you must send a welcome email to each of the users. The welcome email contains instructions for the users to download and install a Amazon WorkSpaces client and log in to their WorkSpace. For more information, see Resend an Invitation (p. 51).

Update Connected Directory Information

You can use the Amazon WorkSpaces console to update the on-premises directory account information for a connected directory. This is the account that is used to read users and groups, and join Amazon WorkSpaces machines to your directory. For more information about this account, see the Prerequisites (p. 24) section.

To update directory information

1. Open the Amazon WorkSpaces console for your desired region.
2. In the navigation pane, select **Directories**.
3. Select your directory, click **Actions**, and select **Update Details**.

4. Enter the new service account username and password in the **Update Details** dialog box and click **Update**.

Disconnecting a Directory

Before you can disconnect from your directory, you must first remove all WorkSpaces from the directory. For more information about removing WorkSpaces, see Remove a WorkSpace (p. 53). To disconnect a directory, perform the following steps.

To disconnect from your directory

1. Open the Amazon WorkSpaces console for your desired region.
2. In the navigation pane, select **Directories**.
3. Select the directory to disconnect, click **Directory Actions**, and select **Deregister**.
4. Verify the information in the **Deregister Directory** dialog box, and click **Deregister**.

Set Up a Directory Administration WorkSpace

To set up an administration WorkSpace

1. Create a WorkSpace for you or another directory administrator.
2. After the WorkSpace is set up and running, connect to the WorkSpace with one of the Amazon WorkSpaces client applications.
3. Install the Active Directory Administration Tools on the instance as explained in Installing the Active Directory Administration Tools (p. 41).

The following are just some of the administration tools that you can use from this WorkSpace.

Tool	Description
redircmp.exe	Changes the default container that new WorkSpaces are created in to the specified organizational unit (OU).
Event Viewer	Allows you to view the event logs of a WorkSpace. Connect the Event Viewer to the IP address of the WorkSpace, which is available from the WorkSpace details page.
Active Directory Users and Computers	Used to administer and publish information in the directory, such as users, groups, and organizational units.

Joining an Amazon EC2 Instance to a Directory

To join an Amazon EC2 instance to a directory, you must launch the instance in the proper region and subnet, using the correct security group, then join the instance to the directory.

Topics

Launching an Instance

To launch an instance to be joined to a directory in a VPC

1. Sign in to the AWS Management Console and open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. From the region selector in the navigation bar, select the same region as your WorkSpaces.
3. From the Amazon EC2 console dashboard, click **Launch Instance**.
4. Select the appropriate AMI.
5. In the **Configure Instance Details** page of the launch wizard, make the following selections.

Setting	Description
Network	Select the VPC that Amazon WorkSpaces is using.
Subnet	Select one of the subnets belonging to the selected VPC.
Public IP	Check this selection. You need a public IP address for the instance to be able to connect to it.

6. In the **Configure Security Group** page of the launch wizard, you must select a security group that has the proper ports open, to allow the instance to communicate with the domain controllers. If Amazon WorkSpaces created the directory for you, you can use the security group that the service created. To find the WorkSpaces security group, see WorkSpaces Security Group (p. 17). You need to open inbound port RDP-3389 from your network CIDR on this security group to be able to use RDP to connect to this instance.

Joining an Instance

The following topics explain how to join a Windows Amazon EC2 instance to a directory.

Topics

Get the DNS Server Addresses

In all cases, you need the IP addresses of the DNS servers in the directory. To obtain this information for a directory that Amazon WorkSpaces created for you, perform the following steps.

To obtain the directory DNS server addresses and directory name

1. Open the Amazon WorkSpaces console for your desired region.
2. In the navigation pane, select **Directories**.
3. Select the desired directory and click the arrow button to expand the display for the directory. The DNS addresses are in the **DNS Address** field.

Joining a Windows Instance to a Directory

To join an existing Amazon EC2 Windows instance to a directory, the instance must be launched as specified in Launching an Instance (p. 38).

To join a Windows instance to a directory

1. Connect to the instance using any Remote Desktop Protocol client.
2. Open the TCP/IPv4 properties dialog box on the instance.

   a. Open **Network Connections**.

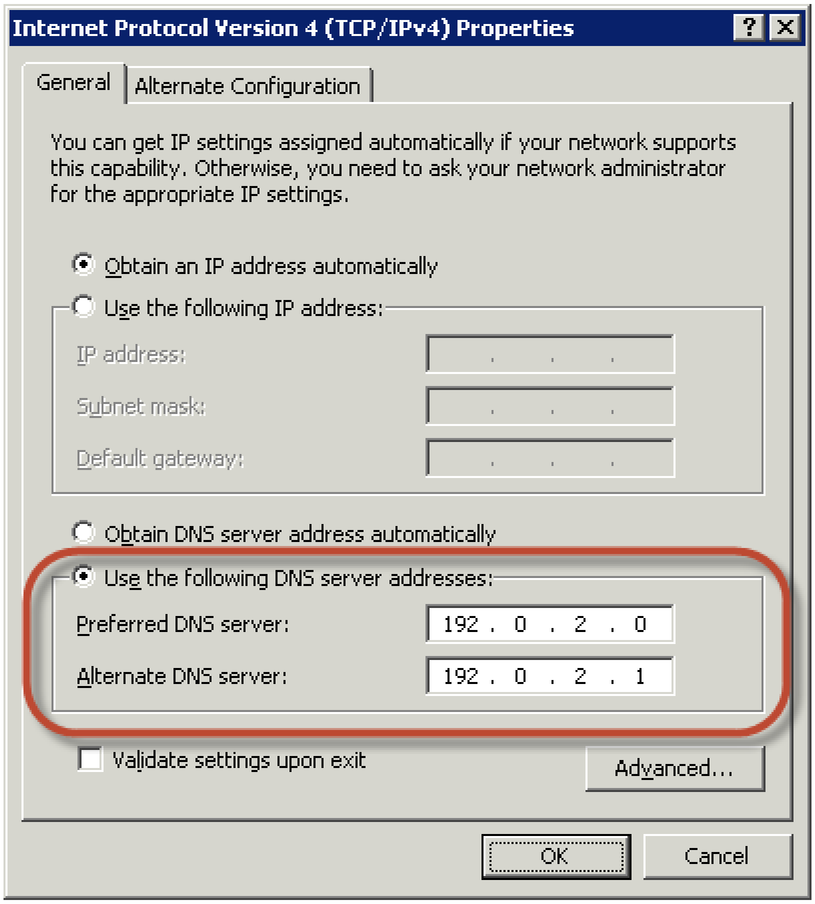
      Tip
      You can open **Network Connections** directly by running the following from a command prompt on the instance.

      ```
      %SystemRoot%\system32\control.exe ncpa.cpl
      ```

   b. Right-click any enabled network connection and select **Properties**.

   c. In the connection properties dialog box, double-click **Internet Protocol Version 4**.

3. Select **Use the following DNS server addresses**, change the **Preferred DNS server** and **Alternate DNS server** addresses to the IP addresses of the directory DNS servers, and click **OK**. For more information about how to obtain the DNS server IP address, see Get the DNS Server Addresses (p. 38).



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 0 . 2 . 0

Alternate DNS server: 192 . 0 . 2 . 1

□ Validate settings upon exit

4. Open the **System Properties** dialog box for the instance, select the **Computer Name** tab, and click **Change**.

   Tip
   You can open the **System Properties** dialog box directly by running the following from a command prompt on the instance.

   ```
   %SystemRoot%\system32\control.exe sysdm.cpl
   ```

5. In the **Member of** field, select **Domain**, enter the fully-qualified name of the directory, and click **OK**.
6. When prompted for the name and password for the domain administrator, enter the name and password for a user that has privileges to join machines to the directory.
7. After you receive the message welcoming you to the domain, restart the instance to have the changes take effect.

Now that your instance has been joined to the domain, you can log into that instance remotely and install utilities to manage the directory, such as adding users and groups. For more information, see Installing the Active Directory Administration Tools (p. 41).

Managing Your Directory

After your directory is created, you can use directory management tools, such as the Active Directory Administration Tools, to manage your directory.

Topics

Installing the Active Directory Administration Tools

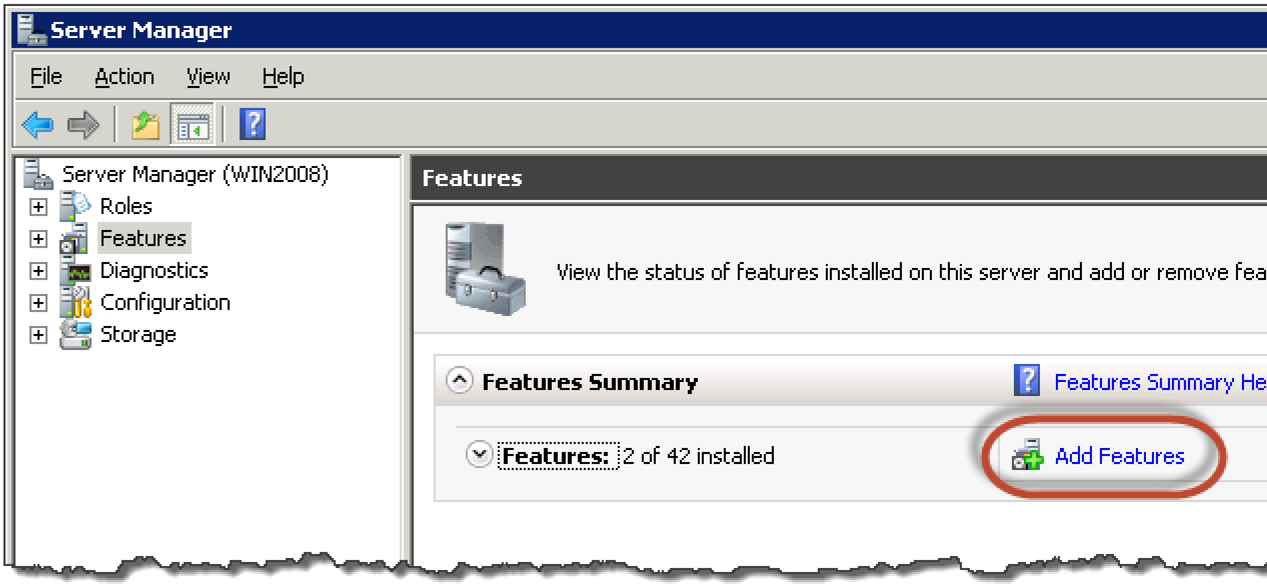
To manage your directory from an EC2 Windows instance, you need to install the Active Directory Domain Services and Active Directory Lightweight Directory Services Tools on the instance.

Topics

Install the Active Directory Domain Administration Tools on a WorkSpace or Windows Server 2008

To install the Active Directory Domain administration tools on a WorkSpace or Windows Server 2008

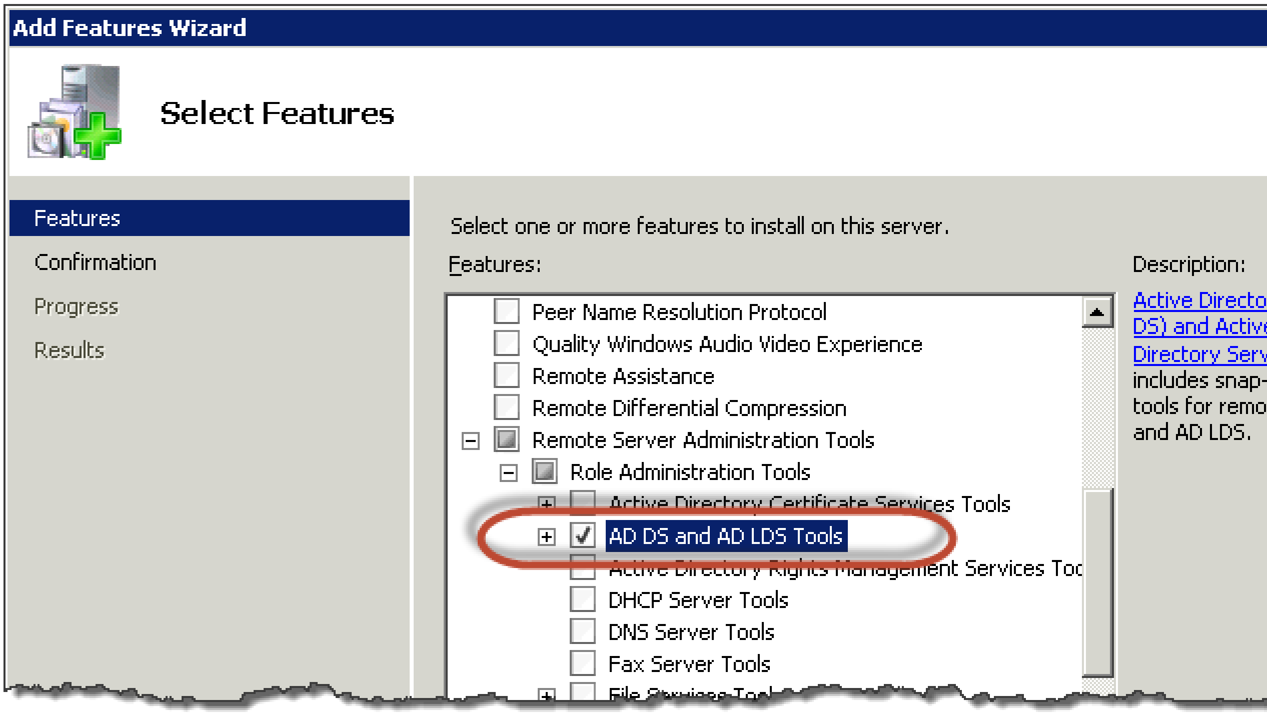
1. Open Server Manager by clicking **Start**, **Control Panel**, **Administrative Tools**, **Server Manager**.
2. In the **Server Manager** tree pane, select **Features**, and click **Add Features**,



View the status of features installed on this server and add or remove fea

Features: 2 of 42 installed

3. In the **Add Features Wizard**, open **Remote Server Administration Tools**, **Role Administration Tools**, and select **AD DS and AD LDS Tools**. If you plan to use Group Policy settings to manage your directory, also select the **Group Policy Management** feature. When your selections are complete, click **Next**.



- ☐ Peer Name Resolution Protocol
- ☐ Quality Windows Audio Video Experience
- ☐ Remote Assistance
- ☐ Remote Differential Compression
- ▣ Remote Server Administration Tools
  - ▣ Role Administration Tools
    - ☐ Active Directory Certificate Services Tools
    - ☑ AD DS and AD LDS Tools
    - ☐ Active Directory Rights Management Services Toc
    - ☐ DHCP Server Tools
    - ☐ DNS Server Tools
    - ☐ Fax Server Tools
    - ☐ File Services Tools

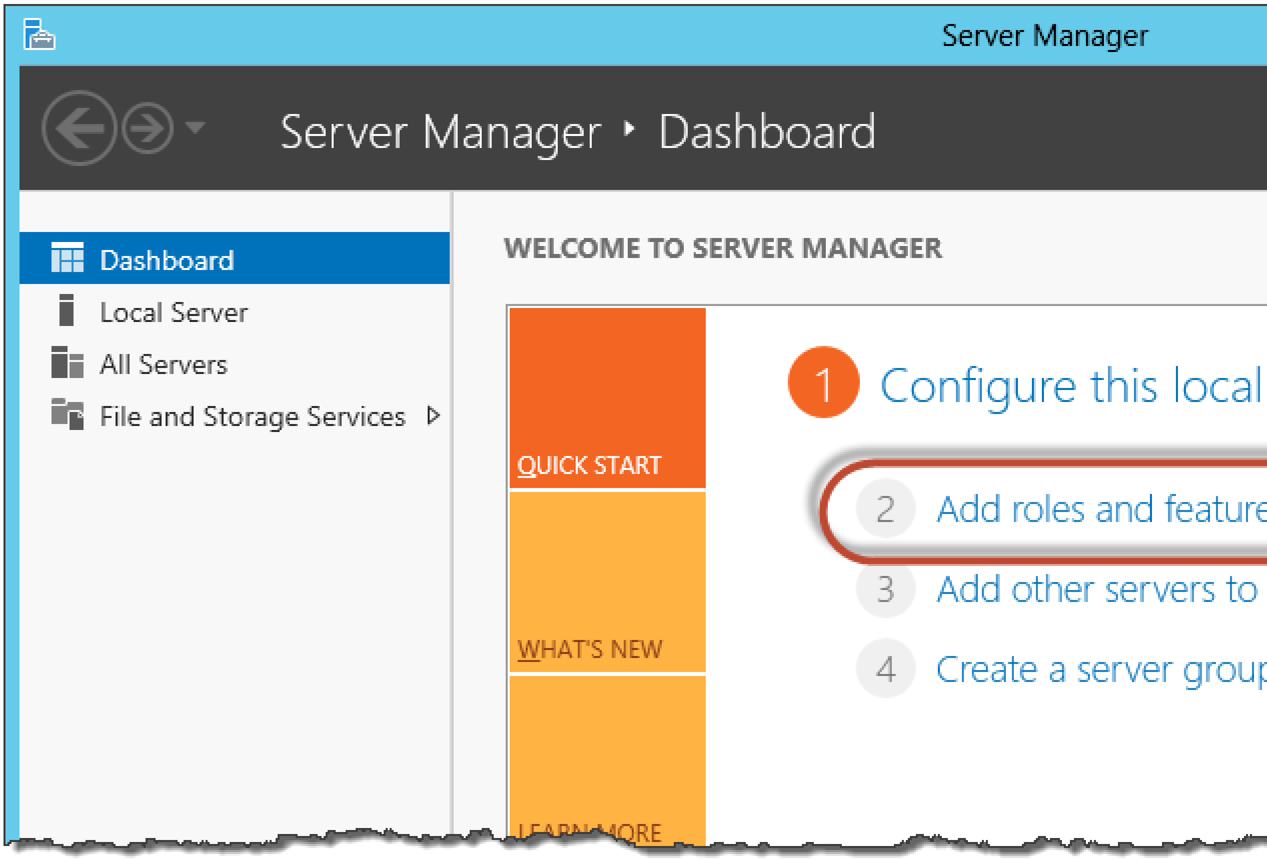
Active Directo DS) and Active Directory Serv includes snap- tools for remo and AD LDS.

4. Review the information and click **Install**. The feature installation requires that the instance be restarted. When the instance has restarted, the Active Directory Domain Services and Active Directory Lightweight Directory Services Tools are available on the **Start** menu, under **All Programs** > **Administrative Tools**.

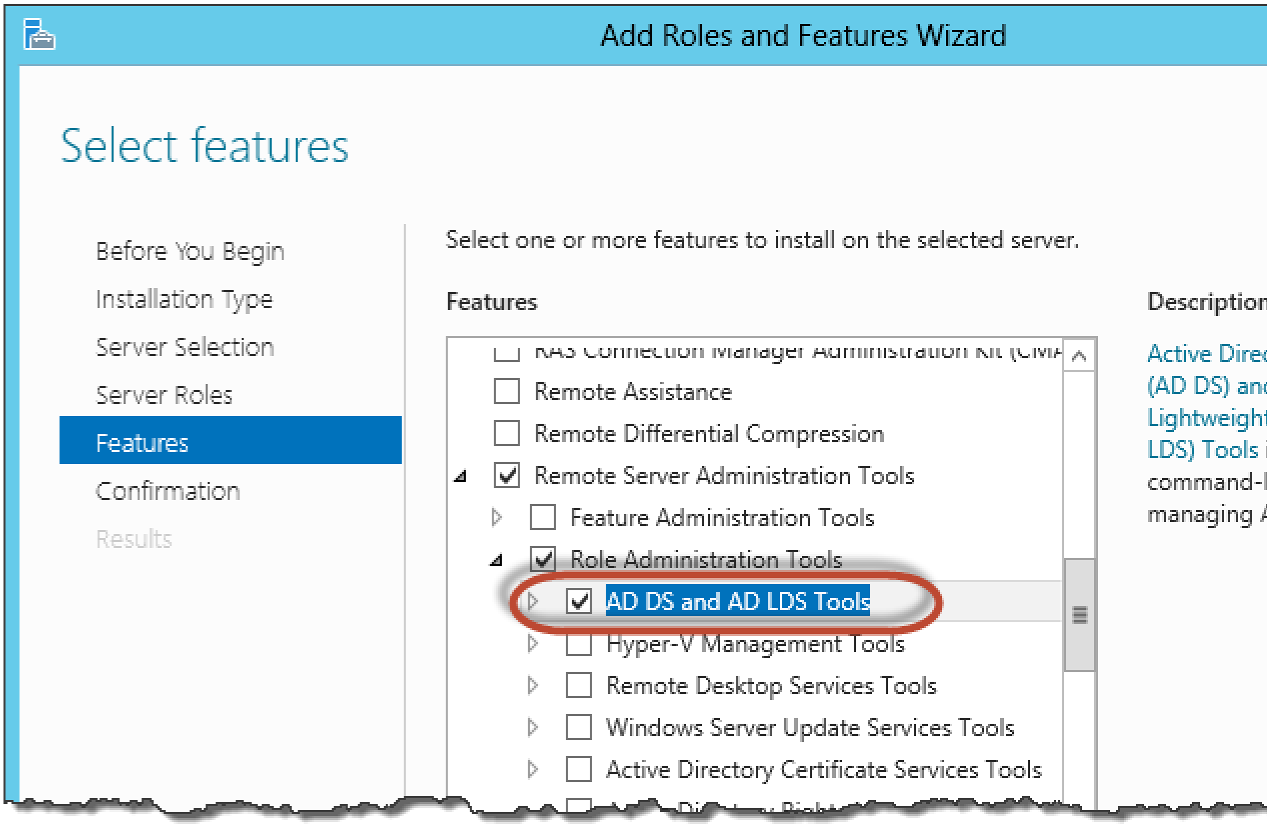
Install the Active Directory Domain Administration Tools on Windows Server 2012

To install the Active Directory Domain administration tools on Windows Server 2012

1. Open Server Manager by from the Start screen by clicking **Server Manager**.
2. In the **Server Manager Dashboard**, click **Add roles and features**,



3. In the **Add Roles and Features Wizard** click **Installation Type**, select **Role-based or feature-based installation**, and click **Next**.
4. Under **Server Selection**, make sure the local server is selected, and click **Features**.
5. In the **Features** tree, open **Remote Server Administration Tools**, **Role Administration Tools**, and select **AD DS and AD LDS Tools**. If you plan to use Group Policy settings to manage your directory, also select the **Group Policy Management** feature. When your selections are complete, click **Next**.



Select one or more features to install on the selected server.

- □ RAS Connection Manager Administration Kit (CMA
- □ Remote Assistance
- □ Remote Differential Compression
- ☑ Remote Server Administration Tools
  - □ Feature Administration Tools
  - ☑ Role Administration Tools
    - ☑ AD DS and AD LDS Tools
    - □ Hyper-V Management Tools
    - □ Remote Desktop Services Tools
    - □ Windows Server Update Services Tools
    - □ Active Directory Certificate Services Tools

Active Direc
(AD DS) and
Lightweight
LDS) Tools i
command-l
managing A

6. Review the information and click **Install**. When the feature installation is finished, the Active Directory Domain Services and Active Directory Lightweight Directory Services Tools are available on the Start screen in the **Administrative Tools** folder.

Creating Users and Groups

You can create users and groups with the Active Directory Users and Computers tool, which is part of the Active Directory Domain Services and Active Directory Lightweight Directory Services Tools. Users represent individual people or entities that have access to your directory. Groups are very useful for giving or denying privileges to groups of users, rather than having to apply those privileges to each individual user. If a user moves to a different organization, you move that user to a different group and they automatically receive the privileges needed for the new organization.

The following examples demonstrate how to create a user, create a group, and add the user to the group. To create users and groups in a directory, you must be connected to a Windows instance that is a member of the directory, and be logged in as a user that has privileges to create users and groups.

To create a user

1. Open the Active Directory Users and Computers tool. There is a shortcut to this tool in the **Administrative Tools** folder.

   Tip
   You can run the following from a command prompt on the instance to open the Active Directory Users and Computers tool box directly.

```
%SystemRoot%\system32\dsa.msc
```

2. In the directory tree, open your directory and select the **Users** folder.
3. On the **Action** menu, click **New**, and then click **User** to open the new user wizard.
4. In the first page of the new user wizard, enter `Mary` for **First name**, `Major` for **Last name**, and `marym` for **User logon name**. Click **Next**.
5. In the second page of the new user wizard, enter a temporary password for **Password** and **Confirm Password**. Make sure the **User must change password at next logon** option is selected. None of the other options should be selected. Click **Next**.
6. In the third page of the new user wizard, verify the new user information is correct and click **Finish**. The new user, **Mary Major**, appears in the **Users** folder.

To create a group

1. Open the Active Directory Users and Computers tool. There is a shortcut to this tool in the **Administrative Tools** folder.

   Tip
   You can run the following from a command prompt on the instance to open the Active Directory Users and Computers tool box directly.

   ```
   %SystemRoot%\system32\dsa.msc
   ```

2. In the directory tree, open your directory and select the **Users** folder.
3. On the **Action** menu, click **New**, and then click **Group** to open the new group wizard.
4. Enter `Division Managers` for the **Group name**, select **Global** for the **Group scope**, and select **Security** for the **Group type**. Click **OK**. The new group, **Division Managers**, appears in the **Users** folder.

To add a user to a group

1. Open the Active Directory Users and Computers tool. There is a shortcut to this tool in the **Administrative Tools** folder.

   Tip
   You can run the following from a command prompt on the instance to open the Active Directory Users and Computers tool box directly.

   ```
   %SystemRoot%\system32\dsa.msc
   ```

2. In the directory tree, open your directory, select the **Users** folder, and select the **Division Managers** group.
3. On the **Action** menu, click **Properties** to open the properties dialog box for the **Division Managers** group.
4. Select the **Members** tab and click **Add...**.
5. For **Enter the object names to select**, enter `marym` and click **OK**. **Mary Major** is displayed in the **Members** list. Click **OK** again to update the group membership.
6. Verify that Mary Major is now a member of the **Division Managers** group by selecting **Mary Major** in the **Users** folder, click **Properties** in the **Action** menu to open the properties dialog box for Mary Major. Select the **Member Of** tab. **Division Managers** is in the list of groups that Mary Major belongs to.

File Sharing

You can allow file sharing between your WorkSpaces, as well as Amazon EC2 instances that are joined to your directory, by modifying the security group that the WorkSpace or instance is attached to. Modify the security group to allow inbound and outbound TCP and UDP traffic on ports 135-139 and 445 from the VPC that the WorkSpaces/instances are running in, such as `10.0.0.0/16`. You can find both the security group and VPC identifiers in the directory details in the Amazon WorkSpaces console.

When you share a folder, you should, at a minimum, only share the folder with authenticated users from the directory that the WorkSpace or instance belongs to. To do this, select the `Authenticated Users` group when selecting the users to share the folder with. You can select individual users or groups if you want to restrict access to the share even further.

After you share a folder, the shared folder can be accessed from another WorkSpace or instance using the UNC path of the folder, such as `\\<machine_name>\<share_name>`.

Group Policy Settings

Just as with the other computers joined to your directory, you can apply Group Policy settings to the WorkSpaces that are joined to your directory. It is recommended that you create and manage an organizational unit for your WorkSpaces, and add all of your WorkSpaces to this organizational unit. You can then apply Group Policy settings that are specific to your WorkSpaces to this organizational unit, and those settings will be applied to all of your WorkSpaces.

Group Policy settings can affect your WorkSpace users' experience in several ways:

- Depending on the number of custom Group Policy settings applied to a WorkSpace, a user's first login to their WorkSpace after it is launched or rebooted may take several minutes.
- Changes to Group Policy settings may cause an active session to be closed when a user is not connected to the WorkSpace.
- Some Group Policy settings force a user logoff when they are disconnected from a session. Any applications that a user has open on the WorkSpace will be closed.
- Implementing an interactive logon message to display a logon banner prevents users from being able to access their WorkSpace. The interactive logon message Group Policy setting is not currently supported by Amazon WorkSpaces.

Group Policy Tutorial: Distributing an Application

A common use of Group Policy settings is to install a particular application on the WorkSpaces of particular users. The following example walks you through all of the steps necessary to install the AWS CLI on the WorkSpaces of all users that belong to a specific Active Directory organizational unit (OU). To complete this scenario, you need the following:

- An Amazon WorkSpaces cloud directory.
- One of the following:
  - An administration WorkSpace that has the Active Directory Administration Tools and Group Policy Management tools installed. For more information, see Set Up a Directory Administration WorkSpace (p. 37) and Installing the Active Directory Administration Tools (p. 41).
  - An EC2 instance joined to the directory that has the Active Directory Administration Tools and Group Policy Management tools installed. For more information, see Joining an Amazon EC2 Instance to a Directory (p. 37) and Installing the Active Directory Administration Tools (p. 41).
- One or more WorkSpaces to install the application on.

Note
With Group Policy, you can only install `.msi` and `.zap` files. You cannot install `.exe` files.

Topics

Launch a File Server

Launch an EC2 instance in your VPC to serve as a file server. The file server will be the source of the application installation package.

To launch a file server

1. From within the instance, change the name of the instance to something meaningful, such as `FS1`. It is much easier to change the machine name before it is joined to the Amazon WorkSpaces directory.
2. Join this instance to your directory, as explained in Joining an Amazon EC2 Instance to a Directory (p. 37).
3. Modify the security group for the file server and directory members to allow inbound and outbound TCP and UDP traffic on ports 135-139 and 445 from all addresses within the VPC. Depending on your implementation, these may or may not be the same security group. For more information, see File Sharing (p. 46).
4. Create a directory on the file server and give the directory a meaningful name, such as `Installers`.
5. Share the directory with the **Authenticated Users** group from the directory, giving them read-only access to the share. This share can be accessed using a UNC path such as `\\FS1\Installers`.
6. Download the 64-bit AWS CLI installer from https://s3.amazonaws.com/aws-cli/AWSCLI64.msi and copy it to the `\\FS1\Installers` share.

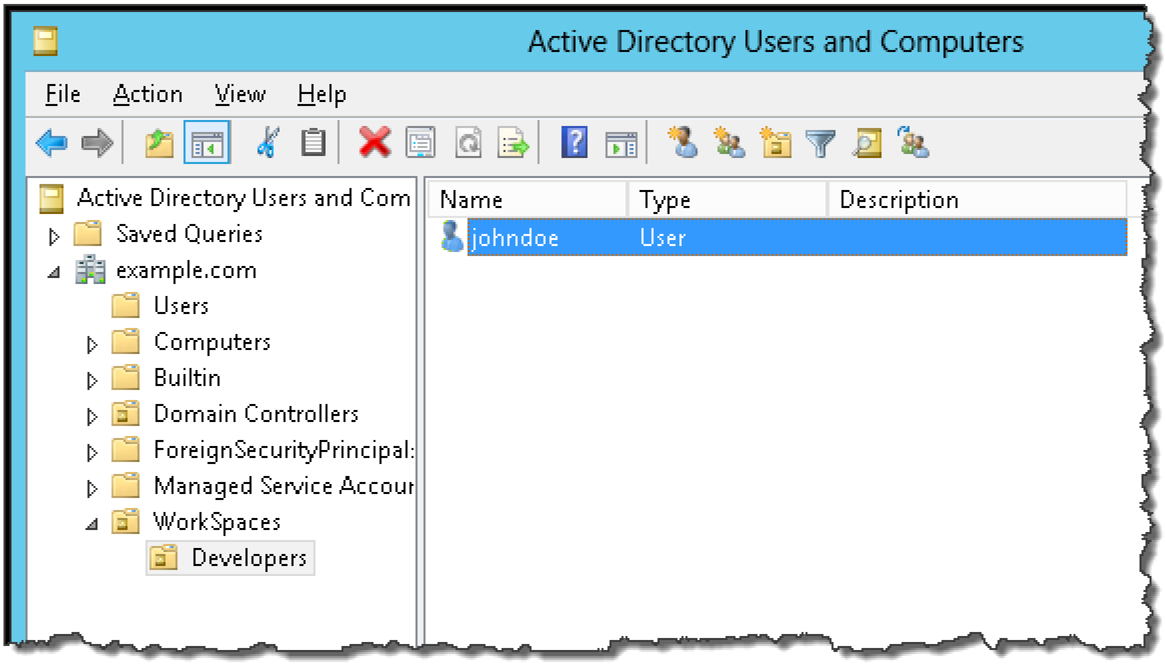
Create an Organizational Unit

Create an Active Directory organizational unit to assign the group policy to. All users that are members of this OU will have the Group Policy applied.

In **Active Directory Users and Computers**, perform the following steps.

To create an organizational unit

1. Create a **WorkSpaces** organizational unit (OU). Under the **WorkSpaces** OU, create a **Developers** OU.
2. Move the Amazon WorkSpaces user that the application should be installed for to the **Developers** OU. By default, Amazon WorkSpaces creates its users in the **Users** folder under the domain.



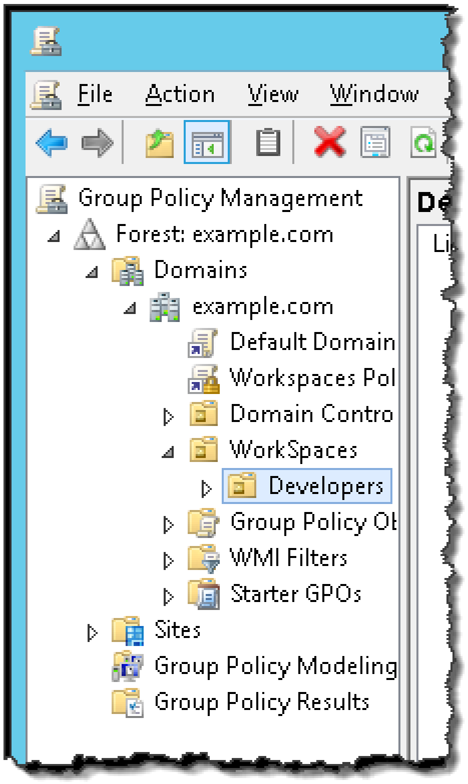
Name	Type	Description
johndoe	User	

Create a Group Policy to Install the Application

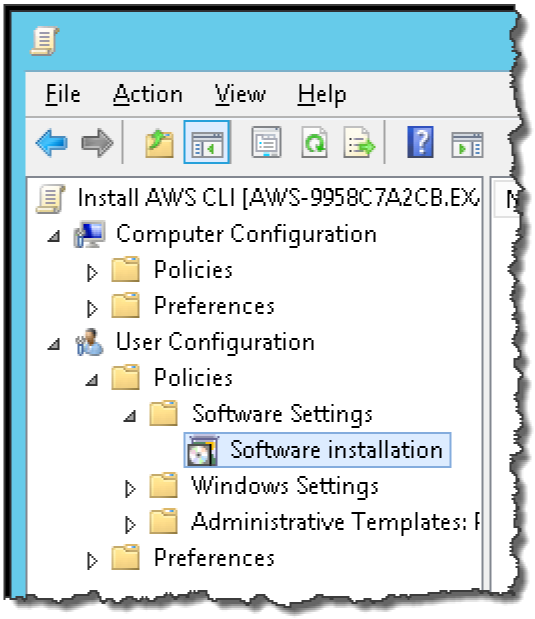
Add a Group Policy setting to the OU that installs the AWS CLI.

To install an application using Group Policy

1. Open the Group Policy Management tool and navigate to the **Developers** OU in your domain. This is the OU you created in Create an Organizational Unit (p. 47).



2. Right-click on the **Developers** OU and select **Create a GPO in this domain, and link it here**.
3. In the **New GPO** dialog box, enter **Install AWS CLI** for the **Name** and leave **Source Starter GPO** set to **(none)**. Click **OK**.
4. Right-click on the **Install AWS CLI** GPO and select **Edit**.
5. In the **Group Policy Management Editor**, navigate to **User Configuration** - **Policies** - **Software Settings** - **Software installation**. Right-click on **Software installation** and select **New** - **Package**. In the **Open** dialog box, enter the UNC path of the shared folder that contains the AWS CLI installer (e.g. `\\FS1\Installers`) and select the AWS CLI installer. In the **Deploy Software** dialog box, select **Assigned** and click **OK**.



6. Right-click on the AWS Command Line Interface package just created and select **Properties**. In the properties dialog box, select the **Deployment** tab. Under **Deployment options**, select **Install this application at logon**. Under **Installation user interface options**, select **Basic**. Click **OK**.
7. Close the **Group Policy Management Editor**.

The next time the user that belongs to the **Developers** OU logs in to their WorkSpace, the AWS CLI is installed. You can verify the installation by opening a command prompt on the WorkSpace and issuing the **aws --version** command.

```
D:\Users\johndoe>aws --version
aws-cli/x.x.x Python/x.x.x Windows/2008ServerR2
```

The AWS CLI version information is displayed. If the AWS CLI is not installed, an error is returned.

Restrictions

Amazon WorkSpaces has the following restrictions:

Topics

User Access Control

User Access Control (UAC) is not supported on your WorkSpaces. If you or your users change the UAC settings on a WorkSpace, you may not be able to connect to the WorkSpace and a WorkSpace rebuild will be necessary.

Firewalls

You should not install any type of security or firewall software. Amazon WorkSpaces requires that certain inbound and outbound ports are open on the WorkSpaces. If any of these ports are not open, the WorkSpace may not function correctly or will be unreachable.

Network Interfaces

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

WorkSpace Management

In Amazon WorkSpaces, each user is paired with a single WorkSpace. Therefore, whenever you provision a new WorkSpace, you must create a new user to assign to that WorkSpace. WorkSpaces are only available to a single user and cannot be shared between separate users.

As an Amazon WorkSpaces administrator, you perform the following tasks to manage users and WorkSpaces.

Topics

Provision a WorkSpace

How you provision a WorkSpace varies depending on the type of directory your WorkSpaces are using.

- To provision a WorkSpace in a cloud directory, see Using Amazon WorkSpaces With A Cloud Directory (p. 21).
- To provision a WorkSpace in a connected directory, see Using Amazon WorkSpaces With Your Directory (p. 34).

Resend an Invitation

On some occasions, you may need to send an invitation email to a user manually.

To resend an invitation email

1. Open the Amazon WorkSpaces console for your desired region.
2. In the navigation pane, select **WorkSpaces**.
3. Select the user to send the invitation to, click **Actions**, and select **Invite User**.

4. Copy the email body text and paste it into an email to the user using your own email application. You can modify the body text if desired. When the invitation email is ready, send it to the user.

Apply Policies, Patches, and Updates to WorkSpaces

The WorkSpaces created by Amazon WorkSpaces are stored in an Active Directory-compatible directory as directory-joined computers. Because of this, you can apply policies, patches, and updates as you would with any other computers in Active Directory.

Edit User Information

You can use the Amazon WorkSpaces console to edit the following information for a user:

- First Name
- Last Name
- Email Address

To edit user information

1. Open the Amazon WorkSpaces console for your desired region.
2. In the navigation pane, select **WorkSpaces**.
3. Select a user, click **Actions**, and select **Edit User**.
4. Modify the user information in the **Edit User** dialog box and click **Update**.

Reboot a WorkSpace

Occasionally, you may find it necessary to reboot a WorkSpace manually.

To reboot a WorkSpace

1. Open the Amazon WorkSpaces console for your desired region.
2. In the navigation pane, select **WorkSpaces**.
3. Select the user assigned to the WorkSpace to be rebooted, click **Actions**, and select **Reboot WorkSpace**.
4. Verify the information in the **Reboot WorkSpace** dialog box and click **Reboot WorkSpace**.

Rebuild a WorkSpace

If needed, you can rebuild the operating system of a WorkSpace to its original state by performing the following steps.

> **Important**
> Any changes a user has made to the WorkSpace are lost when the WorkSpace is rebuilt. The user's data, however, is retained.

To rebuild a WorkSpace

1. Open the Amazon WorkSpaces console for your desired region.
2. In the navigation pane, select **WorkSpaces**.

3. Select the user assigned to the WorkSpace to be rebuilt, click **Actions**, and select **Rebuild WorkSpace**.
4. Verify the information in the **Rebuild WorkSpace** dialog box, and click **Rebuild WorkSpace**.

The WorkSpace is rebuilt and ready for use after the **Status** value changes to **Running**.

Remove a WorkSpace

When you remove a WorkSpace, the user is no longer be able to access the WorkSpace.

> **Important**
> This is a permanent action and cannot be undone. The user's data is not maintained and will be destroyed. If you need to archive any user data, contact Amazon Web Services before revoking access to the WorkSpace.

To remove a WorkSpace

1. Open the Amazon WorkSpaces console for your desired region.
2. In the navigation pane, select **WorkSpaces**.
3. Select the user assigned to the WorkSpace to be removed, click **Actions**, and select **Remove WorkSpace**.
4. Verify the information in the **Remove WorkSpace** dialog box and click **Remove WorkSpace**.

Remove a User

Because Amazon WorkSpaces uses Active Directory to store its user information, you can use whichever Active Directory tools you are familiar with to delete a user object. For more information about accessing these objects, see Directories (p. 16).

> **Note**
> Before you can remove a user, you must remove the WorkSpace assigned to that user. For more information about removing WorkSpaces, see Remove a WorkSpace (p. 53).

Printing From a WorkSpace

Amazon WorkSpaces does not support local printer redirection. You can use one of the following methods to print from a WorkSpace.

- In a connected directory, you can attach your WorkSpace to network printers that are exposed thorough Active Directory.
- Use a cloud printing service, such as Google Cloud Print or HP Mobile Printing.
- Print to a file, transfer the file to your local desktop, and print the file locally to an attached printer.

Amazon WorkSpaces Limits

To prevent denial of service attacks, accounts new to the Amazon WorkSpaces service are limited to two WorkSpaces per region. If you need to increase your limit in a region, you can request a limit increase by performing the following steps.

To request a limit increase

1. Go to the AWS Support Center page, sign in, if necessary, and click **Open a new case**.

2. Under **Regarding**, select **Service Limit Increase**.
3. Under **Limit Type**, select **WorkSpaces**.
4. Fill in all of the necessary fields in the form and click the button at the bottom of the page for your desired method of contact.

The Amazon WorkSpaces Sync application allows a maximum of 10 GB of file storage per Amazon WorkSpaces user.

Troubleshooting Amazon WorkSpaces Administration Issues

Topics

Provisioning WorkSpaces in my connected directory often fails

Verify that the two DNS servers or domain controllers in your on-premises directory are accessible from each of the subnets that you specified when you connected to your directory. You can verify this connectivity by launching an EC2 instance in each subnet and joining the instance to your directory, using the IP addresses of the two DNS servers. For more information about joining an instance to your directory, see Joining an Amazon EC2 Instance to a Directory (p. 37).

Can't connect to a WorkSpace with an interactive logon banner

Implementing an interactive logon message to display a logon banner will prevent users from being able to access their WorkSpace. The interactive logon message Group Policy setting is not currently supported by Amazon WorkSpaces.

None of the WorkSpaces in my directory can connect to the Internet

WorkSpaces cannot communicate with the Internet by default. You must explicitly provide Internet access. For a cloud directory, see Cloud Directory Internet Access (p. 18). For a connected directory, see Connected Directory Internet Access (p. 32).

Amazon WorkSpaces Client Help

Topics

Supported Platforms and Devices

Client applications are available for the following platforms and devices:

- Microsoft Windows 7 and later
- Apple Mac OS X 10.7 and later
- Apple iPad 2 with iOS 6.1.2 and later
- Apple iPad Retina with iOS 6.1.2 and later
- Amazon Kindle Fire HDX, Kindle Fire Gen2, Fire 8.9, and HD 7
- Samsung, Motorola, and Nexus tablets with Android OS 2.3.5 and later

Most keyboards and pointing devices are supported by the Amazon WorkSpaces client applications. This includes many different types of USB and Bluetooth input devices. If you encounter an issue with a particular device, report the problem at https://aws.amazon.com/support/. Other locally attached peripherals, such as printers and storage devices, are not supported.

System Requirements

- No matter which Amazon WorkSpaces client you use, you need a broadband Internet connection. The network you use to connect must have the following network ports open:

- UDP 4172
- TCP 4172

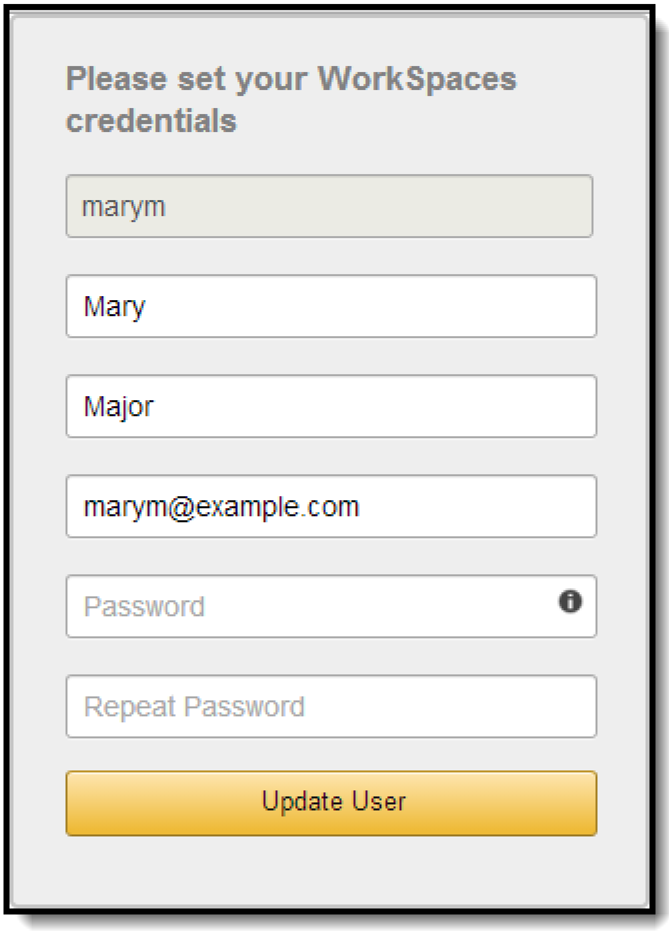
Some managed network environments might have disabled the higher-level (UDP and TCP 4172) ports to network traffic. In this case, you need to work with your network administrators to have these ports enabled. For more information about the networking requirements for an Amazon WorkSpaces client, see Amazon WorkSpaces Client Prerequisites (p. 13).

Completing Your User Profile

When your user account is first created, you need to use the registration link specified in the welcome email to complete your user profile. You must complete your registration within seven days of the email being sent; otherwise, the invitation expires and your administrator will have to send another invitation. Your username and email address cannot be changed, but you can change your first name and last name. You must also set your password for the account. The password is case-sensitive and must be between 8 and 64 characters in length, inclusive. It must also contain at least one character from three of the following categories:

- Lowercase characters (a-z)
- Uppercase characters (A-Z)
- Numbers (0-9)
- Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Enter your information in the page and click **Update User**.



Please set your WorkSpaces credentials

marym

Mary

Major

marym@example.com

After you have completed your user registration, you can download the Amazon WorkSpaces client applications from Amazon WorkSpaces Client Downloads.

Amazon WorkSpaces Windows Client Help

Topics

Setup and Installation

The Amazon WorkSpaces Windows client application requires one of the following:

- Microsoft Windows 7 or later.
- Windows Server 2008 or later.

Download and install the Windows client application from Amazon WorkSpaces Client Downloads.

Connecting to Your WorkSpace

To connect to your WorkSpace

1. The first time you run the client application, you are prompted for your registration code, which is contained in your welcome email. The Amazon WorkSpaces client application uses the registration code and username to identify which WorkSpace to connect to. When you launch the client application later, the same registration code is used. You can enter a different registration code by launching the client application and clicking **Options** - **Register** on the login screen menu.
2. Enter your username and password in the login screen and click **Sign In**. After the client application connects to your WorkSpace, your WorkSpace desktop is displayed.

Client Views

You can switch to full screen mode by clicking **View** - **Show Fullscreen** in the client application menu.

While in full screen mode, you can switch back to window mode by moving the mouse cursor to the top of the screen. The client application menu is displayed, and you can click **View** - **Exit Fullscreen** in the client application menu.

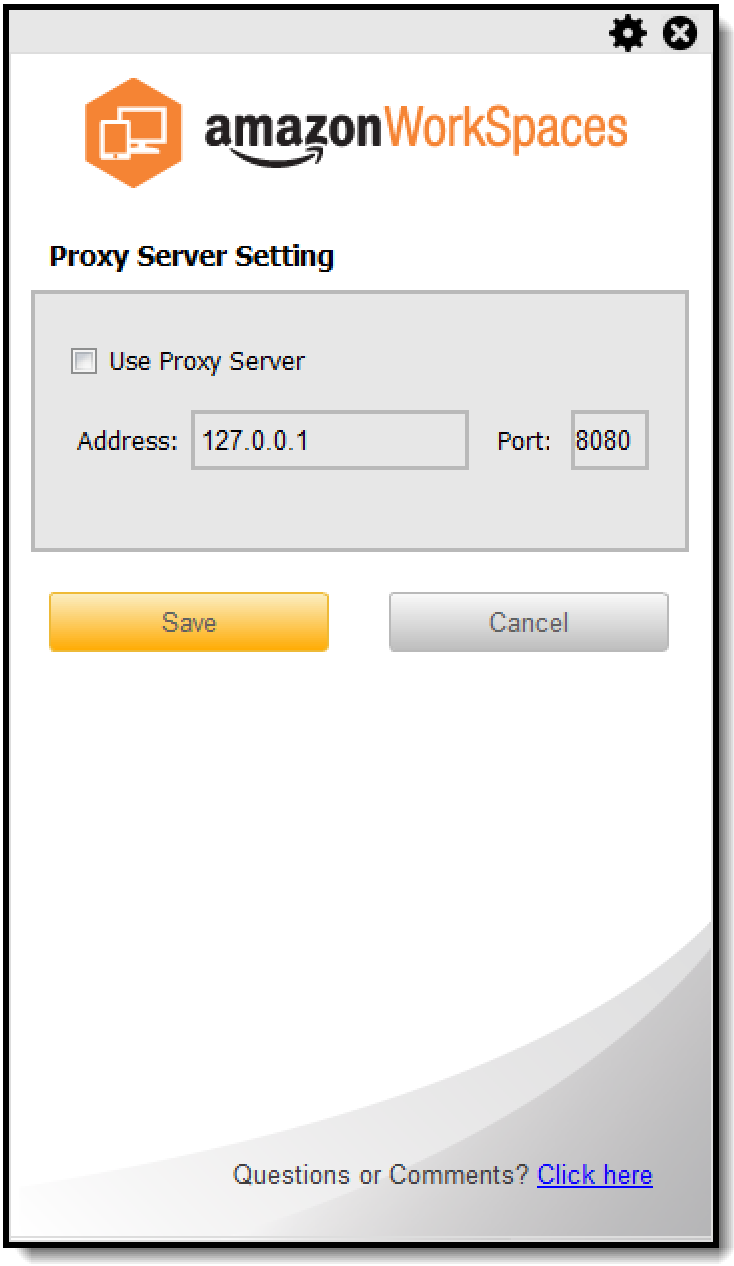
The Amazon WorkSpaces Windows client application supports up to two monitors. The client application automatically uses the first two monitors when it goes into full-screen mode.

Proxy Server

If your network requires you to use a proxy server to access the Internet, you can enable the Amazon WorkSpaces client application to use a proxy.

To use a proxy server

1. In the Amazon WorkSpaces client application, open the **Settings** dialog box.



Proxy Server Setting

□ Use Proxy Server

Address: 127.0.0.1 Port: 8080

2. In the **Proxy Server Setting** area, check **Use Proxy Server**, enter the proxy server address and port, and click **Save**.

Command Shortcuts

The Amazon WorkSpaces Windows client supports the following command shortcuts:

- Ctrl+Alt+Enter - Toggle fullscreen display
- Ctrl+Alt+F12 - Disconnect session

Troubleshooting

Topics

After logging in, the client application only displays a white page and I cannot connect to my WorkSpace.

This problem can be caused by expired VeriSign/Symantec certificates on your client computer (not your WorkSpace). To find and remove these certificates, perform the following steps.

To find and remove expired VeriSign/Symantec certificates

1. In the Windows **Control Panel**, click **Internet Options**.
2. In the **Internet Properties** dialog box, select the **Content** tab and click **Certificates**.
3. In the **Certificates** dialog box, select the **Intermediate Certificate Authorities** tab. In the list of certificates, select all certificates that were issued by VeriSign or Symantec that are also expired, and click **Remove**. Do not remove any certificates that are not expired.
4. On the **Trusted Root Certificate Authorities** tab, select all certificates that were issued by VeriSign or Symantec that are also expired, and click **Remove**. Do not remove any certificates that are not expired.
5. Close the **Certificates** dialog box as well as the **Internet Properties** dialog box.

When you launch the client application again, you should be able to connect.

Amazon WorkSpaces OS X Client Help

Topics

Setup and Installation

The Amazon WorkSpaces OS X client application requires the following:

- Mac OS X 10.7 or later.

Download and install the Amazon WorkSpaces OS X client from Amazon WorkSpaces Client Downloads.

Connecting to Your WorkSpace

To connect to your WorkSpace

1. The first time you run the client application, you are prompted for your registration code, which is contained in your welcome email. The Amazon WorkSpaces client application uses the registration code and username to identify which WorkSpace to connect to. When you launch the client application later, the same registration code is used. You can enter a different registration code by launching the client application and clicking **Options** - **Register** on the login screen menu.
2. Enter your username and password in the login screen and click **Sign In**. After the client application connects to your WorkSpace, your WorkSpace desktop is displayed.

Client Views

You can switch to full screen mode by clicking **View** - **Show Fullscreen** in the client application menu.

While in full screen mode, you can switch back to window mode by moving the mouse cursor to the top of the screen. The client application menu is displayed, and you can click **View** - **Exit Fullscreen** in the client application menu.

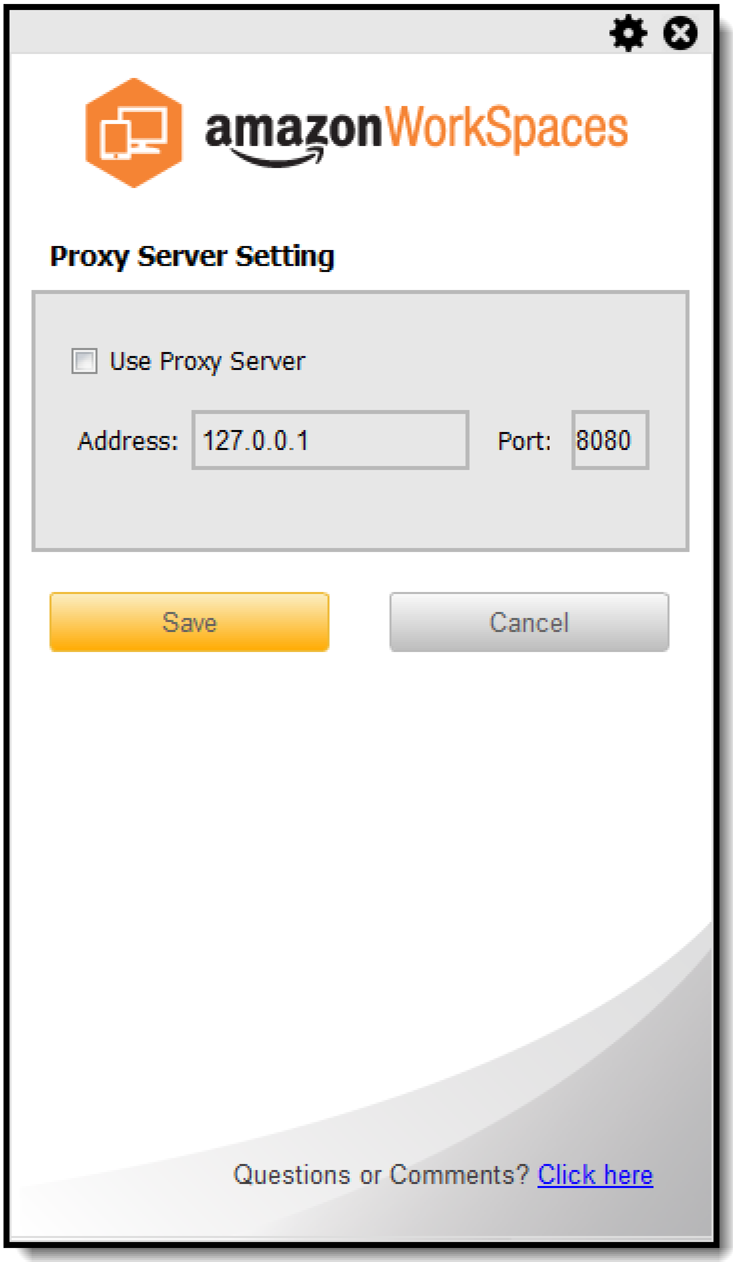
The Amazon WorkSpaces OS X client application supports up to two monitors. The client application automatically uses the first two monitors when it goes into full-screen mode.

Proxy Server

If your network requires you to use a proxy server to access the Internet, you can enable the Amazon WorkSpaces client application to use a proxy.

To use a proxy server

1. In the Amazon WorkSpaces client application, open the **Settings** dialog box.



Proxy Server Setting

□ Use Proxy Server

Address: 127.0.0.1 Port: 8080

2. In the **Proxy Server Setting** area, check **Use Proxy Server**, enter the proxy server address and port, and click **Save**.

Command Shortcuts

The Amazon WorkSpaces OS X client supports the following command shortcuts:

- Control+Option+Return - Toggle fullscreen display
- Control+Option+F12 - Disconnect session

Amazon WorkSpaces iPad Client Help

Topics

Setup and Installation

The Amazon WorkSpaces iPad client application requires the following:

- An iPad 2 or iPad Retina with iOS 6.1.2 or later.

Installation

To download and install the client application, perform the following steps:

To download and install the client application

1. On your iPad, search the App Store for the Amazon WorkSpaces client application.
2. Download and install the application.
3. Verify that the Amazon WorkSpaces client application icon appears on one of the iPad desktops.

Connecting to Your WorkSpace

To connect to your WorkSpace

1. On your iPad, open the Amazon WorkSpaces client application.
2. The first time you run the client application, you are prompted for your registration code, which is contained in your welcome email. The Amazon WorkSpaces client application uses the registration code and username to identify which WorkSpace to connect to. When you launch the client application later, the same registration code is used. You can enter a different registration code by launching the client application and tapping **Enter new registration code** on the login screen.
3. Enter your username and password and tap **Sign In**.

Gestures

The following are the gestures that are supported for the Amazon WorkSpaces iPad client application.

Single tap

Equivalent to a single click in Windows.

Double tap

Equivalent to a double click in Windows.

Two finger single tap

Equivalent to a right-click in Windows.

Two finger double tap

Toggles the on-screen keyboard display.

Swipe from left

Displays the radial menu. For more information, see Radial Menu (p. 64)

Two finger scroll

Scrolls vertically.

Two finger pinch

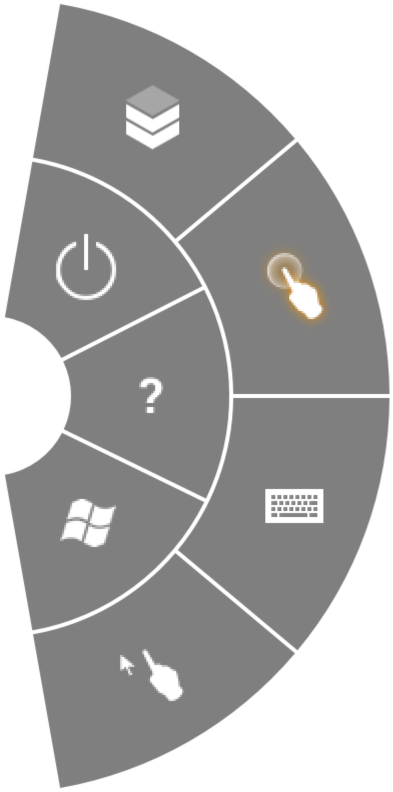
Zooms display in or out.

Two finger pan

Pans the desktop when zoomed in.

Radial Menu

The radial menu is displayed by swiping from the left side of the screen.



The radial menu provides quick access to the following features:

Connection Status

Displays the connection status.

Disconnect

Allows you to disconnect the client application without logging off.

Direct Mouse Mode

Sets the input to direct mouse mode. For more information, see Mouse Modes (p. 66).

Help

Displays the command and gesture tutorial.

Keyboard

Toggles the display of the on-screen keyboard.

Windows Start Menu

Displays the Windows Start Menu.

Offset Mouse Mode

Sets the input to offset mouse mode. For more information, see Mouse Modes (p. 66).

Keyboard

To toggle the display of the on-screen keyboard, double-tap with two fingers anywhere on the screen. Special key combinations are displayed in the top row of the keyboard.

Mouse Modes

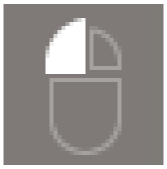
The mouse mode is set using the radial menu (p. 64).

Direct Mode

In direct mouse mode, the mouse cursor is placed wherever you tap your finger. In this mode, a single tap is equivalent to a left mouse button click and a two finger single tap is equivalent to a right mouse button click.

Offset Mode

In offset mouse mode, the mouse cursor tracks the movement of your finger on the screen. In this mode, simulate a left mouse button click by tapping the left mouse button icon.



Simulate a right mouse button click by tapping the right mouse button icon.

Disconnect

To disconnect the iPad client, display the radial menu, tap the disconnect icon, and tap **Disconnect**. You can also log off the WorkSpace, which disconnects the client.

Amazon WorkSpaces Android Client Help

Topics

Setup and Installation

The Amazon WorkSpaces Android client application requires the following:

- An Android tablet with Android 2.3.3 or later.

Installation

To download and install the client application, perform the following steps:

To download and install the client application

1. On your tablet, go to http://clients.amazonworkspaces.com/ and click on the link for your tablet.
2. Download and install the application.
3. Verify that the Amazon WorkSpaces client application icon appears on one of the tablet desktops.

Connecting to Your WorkSpace

To connect to your WorkSpace

1. On your tablet, open the Amazon WorkSpaces client application.
2. The first time you run the client application, you are prompted for your registration code, which is contained in your welcome email. The Amazon WorkSpaces client application uses the registration code and username to identify which WorkSpace to connect to. When you launch the client application later, the same registration code is used. You can enter a different registration code by launching the client application and tapping **Enter new registration code** on the login screen.
3. Enter your username and password and tap **Sign In**.

Gestures

The following are the gestures that are supported for the Amazon WorkSpaces Android client application.

Single tap

Equivalent to a single click in Windows.

Double tap

Equivalent to a double click in Windows.

Two finger single tap

Equivalent to a right-click in Windows.

Two finger double tap

Toggles the on-screen keyboard display.

Swipe from left

Displays the radial menu. For more information, see Radial Menu (p. 68)

Two finger scroll

Scrolls vertically.

Two finger pinch

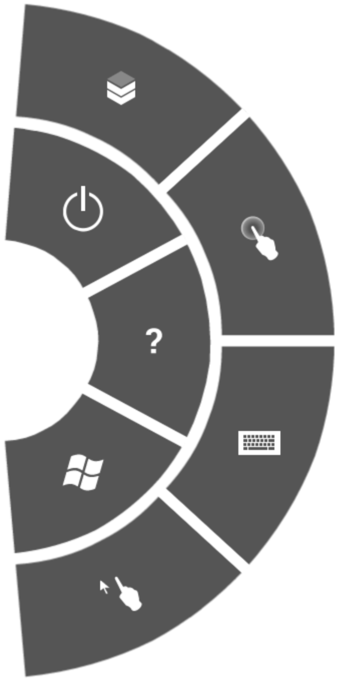
Zooms display in or out.

Two finger pan

Pans the desktop when zoomed in.

Radial Menu

The radial menu is displayed by swiping from the left side of the screen.



The radial menu provides quick access to the following features:

Connection Status

Displays the connection status.

Disconnect

Allows you to disconnect the client application without logging off.

Direct Mouse Mode

Sets the input to direct mouse mode. For more information, see Mouse Modes (p. 70).

Help

Displays the command and gesture tutorial.

Keyboard

Toggles the display of the on-screen keyboard.

Windows Start Menu

Displays the Windows Start Menu.

Offset Mouse Mode

Sets the input to offset mouse mode. For more information, see Mouse Modes (p. 70).

Keyboard

To toggle the display of the on-screen keyboard, double-tap with two fingers anywhere on the screen. Special key combinations are displayed in the top row of the keyboard.

Mouse Modes

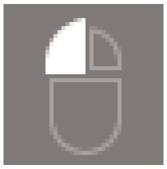
The mouse mode is set using the radial menu (p. 68).

Direct Mode

In direct mouse mode, the mouse cursor is placed wherever you tap your finger. In this mode, a single tap is equivalent to a left mouse button click and a two finger single tap is equivalent to a right mouse button click.

Offset Mode

In offset mouse mode, the mouse cursor tracks the movement of your finger on the screen. In this mode, simulate a left mouse button click by tapping the left mouse button icon.



Simulate a right mouse button click by tapping the right mouse button icon.

Disconnect

To disconnect the Android client, display the radial menu, tap the disconnect icon, and tap **Disconnect**. You can also log off the WorkSpace, which disconnects the client.

Amazon WorkSpaces Sync Application Help

The Amazon WorkSpaces Sync application is a file backup and synchronization application that allows you to continuously, automatically, and securely back up documents from your WorkSpaces to Amazon Simple Storage Service. You can also synchronize your documents with your local desktop computer. All of the files and folders under the sync folder, up to 10 GB total size per user, are replicated. The files are stored in a secure location in the cloud, so your files remain safe if you lose and regain connectivity.

> **Note**
> The Amazon WorkSpaces Sync service is currently not available in the following region:
>
> - Asia Pacific (Sydney) Region

To set up the Amazon WorkSpaces Sync application, you need to register the application, sign in, and select a sync folder. You need to perform these steps on both your local desktop and your WorkSpace.

Topics

System Requirements

The Amazon WorkSpaces Sync application requires one of the following.

- A WorkSpace.
- A personal computer with one of the following operating systems:
  - Windows 7
  - Windows 8 and later
  - Windows Server 2008
- An Apple Mac with OS X 10.7 or later.

> **Note**
> On all Windows clients, including all WorkSpaces, you must enable JavaScript in Internet Explorer. For more information about how to enable JavaScript in Internet Explorer, go to How to enable JavaScript in a web browser?.

WorkSpace Setup for the Amazon WorkSpaces Sync application

To complete the initial setup of the Amazon WorkSpaces Sync application, register the application on your WorkSpace.

To complete the initial setup of the Amazon WorkSpaces Sync application on your WorkSpace

1. Open the Amazon WorkSpaces application and log in to your WorkSpace.
2. Download and run the Amazon WorkSpaces Sync application for Windows from Amazon WorkSpaces Sync Application Downloads.
3. In the **Amazon WorkSpaces Sync Setup** dialog box, click **Get Started**.
4. Enter the registration code that you used to access the WorkSpace and click **Next**.
5. Enter your Amazon WorkSpaces username and password and click **Sign In**.
6. The sync folder defaults to your WorkSpace's My Documents folder. If you would like to synchronize a different folder, click **Change** and select the desired folder. When the desired sync folder has been selected, click **Next**.
7. Verify the information in the **Success** dialog box and click **Ok**.

Local Desktop Setup

Download and Install the Amazon WorkSpaces Sync Application

You can download the Amazon WorkSpaces Sync application for your local desktop from Amazon WorkSpaces Sync Application Downloads.

Windows Installation

Open the `AmazonWorkSpacesSync.application` file. The Amazon WorkSpaces Sync application is downloaded, installed, and launched.

Mac Installation

1. Open the `AmazonWorkSpacesSync.dmg` file to download and install the Amazon WorkSpaces Sync application.
2. Drag the Amazon WorkSpaces Sync icon into the Applications folder.
3. Go to your Applications folder and open **Amazon WorkSpaces Sync**.

Local Setup for the Amazon WorkSpaces Sync Application

The next step is registering the Amazon WorkSpaces Sync application.

To complete the initial setup of the Amazon WorkSpaces Sync application on your local desktop

1. In the **Amazon WorkSpaces Sync Setup** dialog box, click **Get Started**.
2. Enter the registration code that was provided in your Amazon WorkSpaces welcome email and click **Next**.

3. Enter your Amazon WorkSpaces username and password and click **Sign In**.
4. The sync folder defaults to your local My Documents folder. If you would like to synchronize a different folder, click **Change** and select the desired folder. When the desired sync folder has been selected, click **Next**.
5. Verify the information in the **Success** dialog box and click **Ok**.

You can run the Amazon WorkSpaces Sync application on more than one local desktop. No matter how many desktops you synchronize, all of the files and folders in the sync folder will be replicated on all of the desktops, as well as the WorkSpace.

Excluded Files

Any files that meet the following criteria are not synchronized:

- Any file name that starts with a period (.), such as the following:
  - `".lock"`
  - `".~doctor.ppt"`
- Any file name that starts and/or ends with a tilde (~), such as the following:
  - `"hello.txt~"`
  - `"~WRD0000.tmp"`
  - `".~doctor.ppt"`
- Any file name ending with "`.tmp`", such as the following:
  - `"pptC407.tmp"`
  - `"~WRD0000.tmp"`
- Any file in a folder with one of the following names. The name and case must be an exact match.
  - `Microsoft User Data`
  - `Outlook Files`

Changing the Registration Code

You can change the registration code for the Amazon WorkSpaces Sync application after it is set up and running, by right-clicking on the **Amazon WorkSpaces Sync** icon in the taskbar and selecting **Deregister** from the menu. This deregisters the Amazon WorkSpaces Sync application. After the app is deregistered, click **Get Started**. You can now perform the Local Setup for the Amazon WorkSpaces Sync Application (p. 72) process to register the application.

Troubleshooting Amazon WorkSpaces Client Issues

Topics

My WorkSpaces client gives me a network error, but I am able to use other network enabled apps on my device

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 your device has an intermittent connection to the network, the WorkSpaces client application may report an issue with the network.

It sometimes takes several minutes to log in to my WorkSpace

Group Policy settings set by your system administrator can cause a delay on login after your WorkSpace has been provisioned or rebooted. This delay occurs while the Group Policy settings are being applied to the WorkSpace and is normal.

Sometimes I am logged off of my WorkSpace, even though I closed the session, but did not log off

Your system administrator applied a new or updated Group Policy setting to your WorkSpace that requires a logoff of a disconnected session.

I can't connect to the Internet from my WorkSpace

WorkSpaces cannot communicate with the Internet by default. Contact your system administrator for assistance.

I installed a third-party security software package and now I can't connect to my WorkSpace

You should not install any type of security or firewall software on your WorkSpace. Amazon WorkSpaces requires that certain inbound and outbound ports are open on the WorkSpace. If any of these ports are not open, the WorkSpace may not function correctly or will be unreachable. To correct this, ask your administrator to rebuild your WorkSpace.

Document History

The following table describes important additions to the Amazon WorkSpaces documentation set. We also update the documentation frequently to address the feedback that you send us.

- **Latest documentation update:** March 25, 2014

Change	Description	Date Changed
Public beta	Public beta.	March 25th, 2014