

---

# Amazon WorkDocs

## **Administration Guide**





## **Amazon WorkDocs: Administration Guide**

Copyright © 2016 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

---

## Table of Contents

What Is Amazon WorkDocs? .....	1
Accessing .....	1
Related Services .....	1
Pricing .....	2
Setting Up .....	3
Sign Up for AWS .....	3
Create IAM Users and Groups (Recommended) .....	3
Grant IAM Users Permissions for Amazon WorkDocs .....	4
Getting Started .....	6
Enable an Existing Directory .....	6
Create a Directory .....	7
Quick Start .....	7
Standard Setup .....	8
Connect to a Directory .....	9
Amazon WorkDocs Administration .....	11
Amazon WorkDocs Console .....	11
Create or Connect to a Directory .....	11
Promote a User to Administrator .....	11
Delete a Site .....	12
Multi-factor Authentication .....	12
Single Sign-On .....	13
Amazon WorkDocs Administration Dashboard .....	13
User Roles .....	13
Permissions .....	14
Anonymous Viewers .....	17
Cloud Directories .....	18
Connected Directories .....	20
CloudTrail Logging .....	22
Amazon WorkDocs Information in CloudTrail .....	22
Understanding Amazon WorkDocs Log File Entries .....	23
Document History .....	25

# What Is Amazon WorkDocs?

---

Amazon WorkDocs is a fully managed, secure, enterprise storage and sharing service with strong administrative controls and feedback capabilities that improve user productivity. Your files are stored in [the cloud](#), safely and securely. Amazon WorkDocs even includes a synchronization application that always keeps selected folders on your local computer in sync with your cloud folders. Your files are only visible to you, and your designated contributors and viewers. Other members of your organization do not have access to any of your files unless you specifically grant them access.

You can share your files with other members of your organization for collaboration or review. The Amazon WorkDocs client applications can be used to view many different types of files, depending on the Internet media type of the file. Amazon WorkDocs supports all common document and image formats, and support for additional media types is constantly being added.

For more information, see [Amazon WorkDocs](#).

## Accessing

Administrators use the [Amazon WorkDocs console](#) to create and deactivate Amazon WorkDocs sites and the [Amazon WorkDocs Administration Dashboard \(p. 13\)](#) to manage permissions and users.

End users use the client applications to access their files. Non-administrative users never need to use the Amazon WorkDocs console or the administration dashboard. Amazon WorkDocs offers several different client applications and utilities:

- A web application used for document management and reviewing.
- Native apps for mobile devices used for document review.
- A document synchronization app used to synchronize a folder on your Mac or Windows desktop with your Amazon WorkDocs files.
- Web clipper browser extensions for several popular web browsers that allow you to save an image of a web page to your Amazon WorkDocs files.

## Related Services

Amazon WorkDocs is closely related to [Amazon WorkSpaces](#). In fact, you can connect Amazon WorkDocs to your Amazon WorkSpaces user directory. For more information, see [Enabling an Existing AWS Directory Service Directory \(p. 6\)](#).

## Pricing

With Amazon WorkDocs, there are no upfront fees or commitments. You pay only for active user accounts, and the storage you use. For more information, see [Pricing](#).

# Setting Up Amazon WorkDocs

---

To set up new Amazon WorkDocs sites, or manage existing sites, you must complete the following tasks.

## Tasks

- [Sign Up for AWS \(p. 3\)](#)
- [Create IAM Users and Groups \(Recommended\) \(p. 3\)](#)
- [Grant IAM Users Permissions for Amazon WorkDocs \(p. 4\)](#)

## 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. Open <http://aws.amazon.com/> and choose **Create an AWS Account**.
2. Follow the online instructions.

Your root account credentials identify you to services in AWS and grant you unlimited use of your AWS resources, such as your Amazon WorkDocs sites. To allow other users to set up new Amazon WorkDocs sites, or manage existing sites, 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.

## Create IAM Users and Groups (Recommended)

The AWS Management Console requires your username and password so that the service can determine whether you have permission to access its resources. We recommend that you avoid using root account credentials to access AWS because root account credentials cannot be revoked or limited in any way. Instead, use AWS Identity and Access Management (IAM) to create an IAM user and add

the IAM user to an IAM group with administrative permissions. This grants the IAM user administrative permissions. You can then access the AWS Management Console using the credentials for the IAM user.

If you signed up for AWS but have not created an IAM user for yourself, you can create one using the IAM console. For more information about creating an IAM user, see [Create individual IAM users](#) in the *IAM User Guide* guide.

## Grant IAM Users Permissions for Amazon WorkDocs

By default, IAM users don't have permissions to manage Amazon WorkDocs resources; you must create an IAM policy that explicitly grants IAM users those permissions, and attach the policy to the specific IAM users or groups that require those permissions. For more information about IAM policies, see [Permissions and Policies](#) in the *IAM User Guide* guide.

The following policy statement grants an IAM user full access to Amazon WorkDocs resources. The policy gives the user access to all Amazon WorkDocs and AWS Directory Service operations, as well as several Amazon EC2 operations that Amazon WorkDocs needs to be able to perform on your behalf.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "workdocs:*",
        "ds:*",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

The following policy statement grants an IAM user read-only access to Amazon WorkDocs resources. The policy gives the user access to all of the Amazon WorkDocs `Describe` operations. Access to the two Amazon EC2 operations are necessary so Amazon WorkDocs can obtain a list of your VPCs and subnets. Access to the AWS Directory Service `DescribeDirectories` operation is needed to obtain information about your AWS Directory Service directories.



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

# Getting Started with Amazon WorkDocs

---

Amazon WorkDocs is based on organizations that include the users who belong to the organization, as well as information about each user's folders and documents. The organization information is stored in an AWS Directory Service directory, either a Simple AD directory or an AD Connector directory. You can enable Amazon WorkDocs to work with an existing directory, or you can have Amazon WorkDocs create a directory for you.

## Contents

- [Enabling an Existing AWS Directory Service Directory \(p. 6\)](#)
- [Creating a Simple AD Directory \(p. 7\)](#)
- [Connecting to Your On-Premises Directory \(p. 9\)](#)

## Enabling an Existing AWS Directory Service Directory

If you have an existing AWS Directory Service directory in the current region, you can connect Amazon WorkDocs to your existing directory. This can be either a Simple AD directory or an AD Connector directory. To connect to an existing AWS Directory Service directory, perform the following steps.

### To connect to an existing directory

1. Open the Amazon WorkDocs console at <https://console.aws.amazon.com/zocalo/>.
2. On the **Manage Your WorkDocs Sites** page, choose **Create a New WorkDocs Site**.
3. On the **Select a Directory** page, select your AWS Directory Service directory from the **Available Directories** list and choose **Enable Directory**.
4. On the **Set WorkDocs Administrator** page, enter a username from the AWS Directory Service directory to be your Amazon WorkDocs administrator and choose **Select Administrator**.

When the directory has been successfully enabled, the **Status** value of the site changes to `Active`.

## Creating a Simple AD Directory

Amazon WorkDocs uses an AWS Directory Service Simple AD directory to store user information in the cloud. You can create a Simple AD directory in one of two ways. The [Quick Start procedure \(p. 7\)](#) is used to get set up quickly and is designed for small organizations. The Quick Start procedure creates and configures a VPC for use with the directory, and also creates the administrator account. After you create a directory in a particular region, the Quick Start option is no longer available.

When you create a Simple AD directory, Amazon WorkDocs performs the following tasks on your behalf:

- Sets up a Simple AD directory within the VPC that is used to store user information.
- Creates a directory administrator account with the administrator email as the username. An email is sent to the administrator with instructions to complete registration. You use this account to manage your directory.

If you need more control over the directory configuration, you can choose the [standard setup \(p. 8\)](#), which allows you to specify your own directory domain name, as well as one of your existing VPCs to use with the directory. There is also an option to have Amazon WorkDocs create and configure a VPC for you.

### Contents

- [Creating a Simple AD Directory Using the Quick Start \(p. 7\)](#)
- [Creating a Simple AD Directory Using the Standard Setup \(p. 8\)](#)

## Creating a Simple AD Directory Using the Quick Start

To create a Simple AD directory using the Quick Start procedure, perform the following steps.

### To create a Simple AD directory using the Quick Start

1. Open the Amazon WorkDocs console at <https://console.aws.amazon.com/zocalo/>.

If you have never created or connected a directory in the selected region, you see the Amazon WorkDocs start page. After you create a directory in a particular region, the start page is no longer available and you see the **Manage Your WorkDocs Sites** page instead.

2. If you are on the Amazon WorkDocs start page, perform the following steps:
  1. Choose **Get Started Now**.
  2. On the **Get Started with WorkDocs** page, choose **Launch** under **Quick Start**.

If you are on the **Manage Your WorkDocs Sites** page, perform the following steps:

1. Choose **Create a New WorkDocs Site**.
2. On the **Get Started with WorkDocs** page, choose **Launch** under **Quick Start**.
3. Enter the following values and then choose **Complete Setup**.
4. Enter the following values in the **Access Point** section:

#### Region

Verify the region.

**Site URL**

Enter the URL for your Amazon WorkDocs site.

Enter the following values in the **Set WorkDocs Administrator** section:

**Email**

The email address of the directory administrator. The registration email is sent to this email address.

**First Name**

The first name of the directory administrator.

**Last Name**

The last name of the directory administrator.

It takes several minutes for the directory to be created, and the Amazon WorkDocs site to be created. When the directory has been successfully created, the **Status** value of the site changes to *Active*.

## Creating a Simple AD Directory Using the Standard Setup

To create a Simple AD directory, you must meet the prerequisites identified in [Simple AD Prerequisites](#) in the *AWS Directory Service Administration Guide*.

To create an Amazon WorkDocs cloud directory using the standard setup, perform the following steps.

### To create a cloud directory using the standard setup

1. Open the Amazon WorkDocs console at <https://console.aws.amazon.com/zocalo/>.

If you have never created or connected a directory in the selected region, you see the Amazon WorkDocs start page. After you create a directory in a particular region, the start page is no longer available and you see the **Manage Your WorkDocs Sites** page instead.

2. If you are on the Amazon WorkDocs start page, perform the following steps:
  1. Choose **Get Started Now**.
  2. On the **Get Started with WorkDocs** page, choose **Launch** under **Standard Setup**.

If you are on the **Manage Your WorkDocs Sites** page, perform the following steps:

1. Choose **Create a New WorkDocs Site**.
2. On the **Get Started with WorkDocs** page, choose **Launch** under **Standard Setup**.
3. In the **Set up a Directory** page, choose **Create Simple AD**.
4. Enter the following values and then choose **Continue**.
5. Enter the following values in the **Access Point** section:

**Region**

Verify the region.

**Site URL**

Enter the URL for your Amazon WorkDocs site.

Enter the following values in the **Directory Details** section:

**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`.

Enter the following values in the **Set WorkDocs Administrator** section:

**Email**

The email address of the directory administrator. The registration email is sent to this email address.

**First Name**

The first name of the directory administrator.

**Last Name**

The last name of the directory administrator.

For **VPC Details**, you can either use an existing VPC, or have Amazon WorkDocs create and configure a VPC for you. To have Amazon WorkDocs create the VPC for you, select **Set up a new VPC on my behalf**. To use an existing VPC, select **Select an existing VPC to use with WorkDocs** and enter the following values.

**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. If you choose **No Preference**, two different subnets are randomly selected.

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

It takes several minutes for the directory to be created, and the Amazon WorkDocs site to be created. When the directory has been successfully created, the **Status** value of the site changes to *Active*.

## Connecting to Your On-Premises Directory

Amazon WorkDocs uses an AWS Directory Service AD Connector directory to connect to your on-premises directory. To use AD Connector to connect to your on-premises directory, you must meet the prerequisites identified in [AD Connector Prerequisites](#) in the *AWS Directory Service Administration Guide*.

**Note**

If you use AD Connector with Amazon WorkDocs, you won't be able to share file view links outside the company or invite external users to become contributors.

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

**To connect to your on-premises directory**

1. Open the Amazon WorkDocs console at <https://console.aws.amazon.com/zocalo/>.

If you have never created or connected a directory in the selected region, you see the Amazon WorkDocs start page. After you create a directory in a particular region, the start page is no longer available and you see the **Manage Your WorkDocs Sites** page instead.

2. If you are on the Amazon WorkDocs start page, perform the following steps:

1. Choose **Get Started Now**.
2. On the **Get Started with WorkDocs** page, choose **Launch** under **Standard Setup**.

If you are on the **Manage Your WorkDocs Sites** page, perform the following steps:

1. Choose **Create a New WorkDocs Site**.
2. On the **Get Started with WorkDocs** page, choose **Launch** under **Standard Setup**.
3. In the **Set up a Directory** page, choose **Create AD Connector**.
4. Enter the following values and then choose **Continue**.
5. Enter the following values in the **Directory Details** section:

**Directory DNS**

The fully-qualified name of the on-premises directory, such as `corp.example.com`. Amazon WorkDocs 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.

**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 Address**

The IP address of a DNS server or domain controller in your on-premises directory. This server must be accessible from each subnet specified below.

Enter the following values in the **Access Point** section:

**Region**

Verify the region.

**Site URL**

Enter the URL for your Amazon WorkDocs site.

Enter the following values in the **VPC Configuration** section:

**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.

6. 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 and the Amazon WorkDocs site to be created. When the directory has been successfully connected, the **Status** value of the site changes to *Active*.

# Amazon WorkDocs Administration

---

The majority of Amazon WorkDocs administration is performed in the administration dashboard of the Amazon WorkDocs web application, while the Amazon WorkDocs console is used to manage your Amazon WorkDocs directories and sites.

## Contents

- [Amazon WorkDocs Console \(p. 11\)](#)
- [Amazon WorkDocs Administration Dashboard \(p. 13\)](#)

## Amazon WorkDocs Console

The Amazon WorkDocs console is used to manage your Amazon WorkDocs directories and sites. The following operations can be performed with the Amazon WorkDocs console:

### Tasks

- [Create or Connect to a Directory \(p. 11\)](#)
- [Promote a User to Administrator \(p. 11\)](#)
- [Delete a Site \(p. 12\)](#)
- [Multi-factor Authentication \(p. 12\)](#)
- [Single Sign-On \(p. 13\)](#)

## Create or Connect to a Directory

You use the Amazon WorkDocs console to create a cloud directory, or connect to your on-premises directory. For more information about creating a directory in the cloud, see [Creating a Simple AD Directory \(p. 7\)](#). For more information about connecting to your on-premises directory, see [Connecting to Your On-Premises Directory \(p. 9\)](#).

## Promote a User to Administrator

Use the Amazon WorkDocs console to promote a user to administrator. The user must be active to be promoted. For more information about activating a user, see [Edit Users \(p. 19\)](#).

### To promote a user to administrator

1. Open the Amazon WorkDocs console at <https://console.aws.amazon.com/zocalo/>.
2. In the **Manage Your WorkDocs Sites** page, select the desired directory and choose **Actions** and **Set an Administrator**.
3. In the **Set WorkDocs Administrator** page, enter the user name to promote and choose **Set Administrator**.

You can also use the Amazon WorkDocs administration dashboard to demote an administrator. For more information, see [Edit Users \(p. 19\)](#).

## Delete a Site

Use the Amazon WorkDocs console to delete an Amazon WorkDocs site.

### Warning

Deleting a site causes the loss of all user information and all files. You should only delete a site if you are absolutely sure this information is no longer needed.

### To delete a site

1. Open the Amazon WorkDocs console at <https://console.aws.amazon.com/zocalo/>.
2. In the **Manage Your WorkDocs Sites** page, select the desired site and choose **Actions** and **Delete WorkDocs Site**.
3. In the **Delete Selected WorkDocs Site** dialog box, choose if you also want to delete the user directory. This deletes the AWS Directory Service Simple AD or AD Connector directory that is used to store the Amazon WorkDocs user information. If you want to delete the directory, it cannot have any other AWS applications enabled. For more information, see [Deleting a Simple AD Directory](#) or [Deleting an AD Connector Directory](#) in the *AWS Directory Service Administration Guide*.
4. Verify that you are deleting the proper site, enter `DELETE` in the confirmation field, and choose **Delete WorkDocs Site**.

The site is immediately deleted and is no longer available.

## Multi-factor Authentication

You can enable multi-factor authentication for your AD Connector directory by performing the following procedure.

### Note

Multi-factor authentication is not available for Simple AD directories.

### To enable multi-factor authentication

1. Open the Amazon WorkDocs console at <https://console.aws.amazon.com/zocalo/>.
2. In the **Manage Your WorkDocs Sites** page, select the desired site and choose **Actions** and **Manage MFA**.
3. Enter the following values and choose **Update MFA**.

#### Enable Multi-Factor Authentication

Check to enable multi-factor authentication.

#### RADIUS server IP address(es)

The IP addresses of your RADIUS server endpoints, or the IP address of your RADIUS server load balancer. You can enter multiple IP addresses by separating them with a comma (e.g., `192.0.0.0,192.0.0.12`).



**Port**

The port that your RADIUS server is using for communications. Your on-premises network must allow inbound traffic over the default RADIUS server port (1812) from the AD Connector servers.

**Shared secret code**

The shared secret code that was specified when your RADIUS endpoints were created.

**Confirm shared secret code**

Confirm the shared secret code for your RADIUS endpoints.

**Protocol**

Select the protocol that was specified when your RADIUS endpoints were created.

**Server timeout**

The amount of time, in seconds, to wait for the RADIUS server to respond. This must be a value between 1 and 60.

**Max retries**

The number of times that communication with the RADIUS server is attempted. This must be a value between 0 and 10.

Multi-factor authentication is available when the **RADIUS Status** changes to **Enabled**. During the time that the multi-factor authentication is being set up, your users are not able to log in to their Amazon WorkDocs site.

## Single Sign-On

AWS Directory Service provides the ability for your users to access Amazon WorkDocs from a computer that is joined to the same directory that Amazon WorkDocs is registered with, without having to enter their credentials separately. For information about enabling single sign-on for your directory, see [Single Sign-On](#) in the *AWS Directory Service Administration Guide*.

Your Amazon WorkDocs users may need to modify their web browser settings to enable single sign-on. For more information, see [Enabling Single Sign-On](#) in the *Amazon WorkDocs User Guide*.

## Amazon WorkDocs Administration Dashboard

The administration dashboard allows you to manage your Amazon WorkDocs site. The administration dashboard is available to Amazon WorkDocs administrators in the Amazon WorkDocs web application. To get to the administration dashboard, open the Amazon WorkDocs web application for your site, and choose **Administration** in the user control pane.

The administration dashboard is different depending on if you are using a cloud directory or a connected directory.

**Contents**

- [User Roles](#) (p. 13)
- [Permissions](#) (p. 14)
- [Anonymous Viewers](#) (p. 17)
- [Cloud Directories](#) (p. 18)
- [Connected Directories](#) (p. 20)

## Amazon WorkDocs User Roles

Amazon WorkDocs defines the following user roles.

### **WS User**

A user that has an assigned Amazon WorkSpaces workspace.

- Access to all Amazon WorkDocs features
- Default storage of 50 GB (can pay to upgrade to 1 TB)
- No monthly charges

### **Upgraded WS User**

A user that has an assigned Amazon WorkSpaces workspace and has been upgraded.

- Access to all Amazon WorkDocs features
- Default storage of 1 TB (additional storage available on a pay-as-you go basis)
- Monthly charges apply

### **Amazon WorkDocs User**

A active Amazon WorkDocs user that does not have an assigned Amazon WorkSpaces workspace.

- Access to all Amazon WorkDocs features
- Default storage of 1 TB (additional storage available on a pay-as-you go basis)
- Monthly charges apply

For more information about upgrading or downgrading an Amazon WorkSpaces user, see [Cloud Directory Users \(p. 19\)](#) and [Connected Directory Users \(p. 20\)](#). For more information about pricing, see [Amazon WorkDocs Pricing](#).

## **Amazon WorkDocs Sharing Permissions**

Amazon WorkDocs controls access to folders and files through the use of permissions. Permissions are applied based on the role of the user.

### **Contents**

- [Roles \(p. 14\)](#)
- [Shared Folder Permissions \(p. 15\)](#)
- [File Permissions \(p. 15\)](#)
- [Shared File Permissions \(p. 16\)](#)

## **Roles**

Both folder and file permissions are granted based on user roles. The following are the roles defined by Amazon WorkDocs that apply to folders:

- Folder owner – The owner of the folder or file.
- Folder co-owner – A user or group that the owner designates as the co-owner of the folder or file.
- Folder contributor – Someone who the folder has been shared with, without limited access to the folder.
- Folder viewer – Someone who a folder has been shared with, but has been given limited access (view only) to the folder.

The following roles apply to files:

- Owner – The owner of the file.
- Co-Owner – A user or group that the owner designates as the co-owner of the file.
- Contributor – Someone who has been asked for feedback on file.
- Viewer – Someone who a file has been shared with, but has been given limited access (view only) to the file.
- Anonymous viewer – A non-registered user outside of the organization who can view a file that has been shared via an external viewing link. Unless otherwise indicated, an anonymous viewer has the same permissions as a viewer.

## Shared Folder Permissions

The following are the permissions defined by Amazon WorkDocs for shared folders:

- View – View the contents of a shared folder.
- View sub-folder – View a sub-folder.
- View shares – View the other users a folder is shared with.
- Add sub-folder – Add a sub-folder.
- Share – Share the top-level folder with other users.
- Revoke share – Revoke the sharing of the top-level folder.
- Delete sub-folder – Delete a sub-folder.
- Delete top-level folder – Delete the top-level shared folder.

### Permissions for shared folders

Permission	Folder owner	Folder co-owner	Folder contributor	Folder viewer
View	X	X	X	X
View Sub-folders	X	X	X	X
View Shares	X	X	X	X
Add Sub-folder	X	X	X	
Share	X	X		
Revoke Sharing	X	X		
Delete Sub-folder	X	X		
Delete Top-level folder	X			

## File Permissions

The following are the permissions defined by Amazon WorkDocs for files that are not in a shared folder:

- View – View a file.
- Delete – Delete a file.

- Annotate – Can add feedback to a file.
- View Shares – View the other users that a file is shared with.
- View Annotations – View feedback from other users.
- View Activity – View the activity history of a file.
- View Versions – View previous versions of a file.
- Download – Download a file. This is the default permission. The ability to download shared files can be allowed or denied in the file properties.
- Prevent Download – Prevent a file from being downloaded.
- Upload – Upload new versions of a file.
- Share – Share a file with other users.
- Revoke Sharing – Revoke the sharing of a file.

### Permissions for a file not in a shared folder

Permission	Owner/Co-Owner	Contributor	Viewer	Anonymous Viewer
View	X	X	X	X
View Shares	X	X	X	X
Download	X	X	X	
Annotate	X	X		
View Annotations	X	X		
View Activity	X	X		
View Versions	X	X		
Upload	X	X		
Delete	X			
Prevent Download	X			
Share	X			
Revoke Sharing	X			

## Shared File Permissions

The following are the permissions defined by Amazon WorkDocs for files in a shared folder:

- View – View a file in a shared folder.
- View Shares – View the other users that a file is shared with.
- Download – Download a file.
- Annotate – Can add feedback to a file.
- View Annotations – View feedback from other users.
- View Activity – View the activity history of a file.
- View Versions – View previous versions of a file.
- Upload – Upload new versions of a file.

- Delete – Delete a file in a shared folder.
- Prevent Download – Prevent a file from being downloaded. This is the default permission for files in the folder.
- Share – Share a file with other users.
- Revoke Sharing – Revoke the sharing of a file.
- Private Comments – Owner/Co-owner can see all private comments for a document, even if it is not a reply to their comment.

#### Permissions for a file in a shared folder

Permission	Folder Owner/ Co-Owner	File Owner*	Folder Contributor	Folder Viewer	Anonymous Viewer
View	X	X	X	X	X
View Shares	X	X	X	X	X
Download	X	X	X	X	
Annotate	X	X	X		
View Annotations	X	X	X		
View Activity	X	X	X		
View Versions	X	X	X		
Upload	X	X	X		
Delete	X	X	X		
Rename	X	X	X		
Prevent Download	X	X			
Share	X	X			
Revoke Sharing	X	X			
See All Private Comments**	X	X			

\* - The file owner, in this case, is the person that uploaded the original version of a file to a folder that was shared with them. The permissions for this role apply only to the owned file, not all files in the shared folder.

\*\* File Owner/Co-Owner can see all private comments. Contributors can see private comments only if they are replies to their comments.

## Amazon WorkDocs Anonymous Viewers

You can configure your organization so that anonymous users can be invited to view files using Amazon WorkDocs. Anonymous viewers can also download files that are shared with them, as long as the **Disallow others to download** option is not enabled.

To support anonymous viewers, the following must be true:

- The **External Share Settings** for your organization must be set to **Users can send external view links to anyone**. For a Simple AD directory, see [Security \(p. 18\)](#). For an AD Connector directory, see [Security \(p. 20\)](#).
- The **Invite Settings** for your organization must be set to **Only administrators can invite new users**.

If all of these criteria are met, an Amazon WorkDocs user can invite an anonymous viewer to view a document by entering the email address of the anonymous viewer when the user sends the invitation.

## Amazon WorkDocs Cloud Directories

In the Amazon WorkDocs administration dashboard for a cloud directory, you can manage the following.

### Contents

- [Storage \(p. 18\)](#)
- [Security \(p. 18\)](#)
- [Cloud Directory Users \(p. 19\)](#)

## Storage

In the **Storage** section, you can specify the amount of storage that new users receive. To change this setting, choose **Change** in the **Storage** section. In the **Storage Limit** dialog box, give new users unlimited storage or limit users to a specific amount of storage. This setting only affects users that are added after the setting is changed. It does not change the amount of storage allocated to existing users. To change the storage limit for an existing user, see [Edit Users \(p. 19\)](#).

## Security

In the **Security** section, you can specify the following.

### External Share Settings

Specifies if users can send file view links to people outside of the organization. Choose from the following settings:

**Users can send external view links to anyone**

Users can send links to anyone outside the organization.

**Users can send external view links to a few specific domains**

Users can send links to people who are members of the specified domains.

**Users cannot send external view links**

Users cannot send view links to anyone outside the organization.

### Invite Settings

Specifies how users can invite new users to the cloud organization, if applicable. For a cloud directory, choose from the following settings:

**Users can invite new people from anywhere by sharing files or folders with them**

Users can invite new people from outside the organization by sharing files or folders with them.

**Users can invite new people from a few specific domains by sharing files or folders with them**

Users can invite new people from the specified domains by sharing files or folders with them.

### Only administrators can invite new users

Users cannot invite new users.

## Cloud Directory Users

In the **Manage Users** section for a cloud directory, you can perform the following tasks.

### Tasks

- [Invite New Users \(p. 19\)](#)
- [Edit Users \(p. 19\)](#)
- [Delete Users \(p. 19\)](#)


## Invite New Users

For cloud directories, you invite new users to join your directory.

### To invite new users to a cloud directory

1. In the **Manage Users** section, choose **Invite Users**.
2. In the **Invite Users** dialog box, enter the email address of the person you would like to invite in the **Who would you like to invite** field, and press **Enter**. Repeat for each person you would like to invite.
3. Enter a customized subject and message body, if desired, and choose **Send**. An invitation email is sent to each recipient with instructions about how to create an Amazon WorkDocs account.

## Edit Users

You can modify an existing user by clicking on the pencil icon () next to the user's name.

In the **Edit User** dialog box, you can change the following settings:

### First Name

The user's first name.

### Last Name

The user's last name.

### Status

Specifies if the user is active or inactive.


### Role

Specifies whether the user is a user or administrator. You can also upgrade or downgrade a user that has an Amazon WorkSpaces workspace assigned to them. For more information, see [Amazon WorkDocs User Roles \(p. 13\)](#).

### Storage

Specifies the storage limit for an existing user.

## Delete Users

Using the Amazon WorkDocs administration dashboard, you can only delete a cloud user that has not created their Amazon WorkDocs account yet. To delete one of these users, choose the trash can icon () next to the user's name.

We do not recommend that you delete registered users. Instead, you should deactivate users, so they do not have access to your Amazon WorkDocs site. For more information about deactivating a user, see [Edit Users \(p. 19\)](#).

You must always have at least one active user for your Amazon WorkDocs site. If you want to delete all users, you must delete your entire Amazon WorkDocs site.

## Amazon WorkDocs Connected Directories

In the administration dashboard for a connected directory, you can manage the following.

### Contents

- [Storage \(p. 20\)](#)
- [Security \(p. 20\)](#)
- [Connected Directory Users \(p. 20\)](#)

## Storage

In the **Storage** section, you can specify the amount of storage that new users receive. To change this setting, choose **Change** in the **Storage** section. In the **Storage Limit** dialog box, give new users unlimited storage or limit users to a specific amount of storage. This setting only affects users that are enabled after the setting is changed. It does not change the amount of storage allocated to currently enabled users. To change the storage limit for an enabled user, see [Edit Users \(p. 21\)](#).

## Security

In the **Security** section, you can specify the following.

### External Share Settings

Specifies if users can send file view links to people outside of the organization. Choose from the following settings:

**Users can send external view links to anyone**

Users can send links to anyone outside the organization.

**Users can send external view links to a few specific domains**

Users can send links to people who are members of the specified domains.

**Users cannot send external view links**

Users cannot send view links to anyone outside the organization.

### Invite Settings

For connected directories, you don't invite new users to join your directory, you can only enable users that already exist in your directory to use Amazon WorkDocs. For a connected directory, choose from the following settings:

**Users can enable new people from your directory by sharing files or folders with them**

Users can enable people that already exist in your directory to use Amazon WorkDocs by sharing files or folders with them.

**Only administrators can enable new users**

Only Amazon WorkDocs administrators can enable users to use Amazon WorkDocs.

## Connected Directory Users

In the **Manage Users** section for a connected directory, you can perform the following tasks.

### Tasks




- [Enable Users \(p. 21\)](#)
- [Edit Users \(p. 21\)](#)

## Enable Users

For connected directories, you don't invite new users to join your directory, you enable users that already exist in your directory to use Amazon WorkDocs. For more information about enabling a user, see [Edit Users \(p. 21\)](#).

## Edit Users

You can modify an existing user by choosing the pencil icon () next to the user's name.

In the **Edit User** dialog box, you can change the following settings:

### **Status**

Specifies if the user is active or inactive.

### **Role**

Specifies whether the user is a user or administrator. You can also upgrade or downgrade a user that has an Amazon WorkSpaces workspace assigned to them. For more information, see [Amazon WorkDocs User Roles \(p. 13\)](#).

### **Storage**

Specifies the storage limit for an existing user.

# Logging Amazon WorkDocs API Calls Using AWS CloudTrail

---

Amazon WorkDocs is integrated with CloudTrail, a service that captures API calls made by or on behalf of Amazon WorkDocs in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the Amazon WorkDocs console. Using the information collected by CloudTrail, you can determine what request was made to Amazon WorkDocs, the source IP address from which the request was made, who made the request, when it was made, and so on. For more information about CloudTrail, including how to configure and enable it, see the [AWS CloudTrail User Guide](#).

## Amazon WorkDocs Information in CloudTrail

When CloudTrail logging is enabled in your AWS account, API calls made to Amazon WorkDocs actions are tracked in log files. Amazon WorkDocs records are written together with other AWS service records in a log file. CloudTrail determines when to create and write to a new file based on a time period and file size.

Every log entry contains information about who generated the request. The user identity information in the log helps you determine whether the request was made with root or IAM user credentials, with temporary security credentials for a role or federated user, or by another AWS service. For more information, see the **userIdentity** field in the [CloudTrail Event Reference](#).

You can store your log files in your bucket for as long as you want, but you can also define Amazon S3 lifecycle rules to archive or delete log files automatically. By default, your log files are encrypted by using Amazon S3 server-side encryption (SSE).

You can choose to have CloudTrail publish Amazon SNS notifications when new log files are delivered if you want to take quick action upon log file delivery. For more information, see [Configuring Amazon SNS Notifications](#).

You can also aggregate Amazon WorkDocs log files from multiple AWS regions and multiple AWS accounts into a single Amazon S3 bucket. For more information, see [Aggregating CloudTrail Log Files to a Single Amazon S3 Bucket](#).

## Understanding Amazon WorkDocs Log File Entries

CloudTrail log files can contain one or more log entries where each entry is made up of multiple JSON-formatted events. A log entry represents a single request from any source and includes information about the requested action, any parameters, the date and time of the action, and so on. The log entries are not guaranteed to be in any particular order. That is, they are not an ordered stack trace of the public API calls.

There are two different types of CloudTrail entries that Amazon WorkDocs generates, those from the control plane and those from the data plane. The important difference between the two is that the user identity for control plane entries is an IAM user, while the user identity for data plane entries is the Amazon WorkDocs directory user.

Sensitive information, such as passwords, authentication tokens, file comments, and file contents are redacted in the log entries.

The following example shows two CloudTrail log entries for Amazon WorkDocs: the first record is for a control plane action and the second is for a data plane action.

```
{
  Records : [
    {
      "eventVersion" : "1.01",
      "userIdentity" :
      {
        "type" : "IAMUser",
        "principalId" : "user_id",
        "arn" : "user_arn",
        "accountId" : "account_id",
        "accessKeyId" : "access_key_id",
        "userName" : "user_name"
      },
      "eventTime" : "event_time",
      "eventSource" : "workdocs.amazonaws.com",
      "eventName" : "RemoveUserFromGroup",
      "awsRegion" : "region",
      "sourceIPAddress" : "ip_address",
      "userAgent" : "user_agent",
      "requestParameters" :
      {
        "directoryId" : "directory_id",
        "userId" : "user_sid",
        "group" : "group"
      },
      "responseElements" : null,
      "requestID" : "request_id",
      "eventID" : "event_id"
    },
    {
      "eventVersion" : "1.01",
      "userIdentity" :
      {
        "type" : "Unknown",
        "principalId" : "user_id",
        "accountId" : "account_id",
        "userName" : "user_name"
      }
    }
  ]
}
```

```
    },  
    "eventTime" : "event_time",  
    "eventSource" : "workdocs.amazonaws.com",  
    "eventName" : "LogoutUser",  
    "awsRegion" : "region",  
    "sourceIPAddress" : "ip_address",  
    "userAgent" : "user_agent",  
    "requestParameters" :  
    {  
      "AuthenticationToken" : "***-redacted-***"  
    },  
    "responseElements" : null,  
    "requestID" : "request_id",  
    "eventID" : "event_id"  
  }  
]  
}
```

---

# Document History

---

The following table describes important additions to the *Amazon WorkDocs Administration Guide*.

- **Latest documentation update:** November 22, 2016

Change	Description	Date Changed
Storage limit increased to 1 TB	Added documentation for the new storage limits for users. For more information, see <a href="#">Amazon WorkDocs User Roles (p. 13)</a> .	November 22, 2016
Single sign-on support added	Added documentation to support single sign-on. For more information, see <a href="#">Single Sign-On (p. 13)</a> .	March 31, 2015
Multi-factor authentication support.	Added multi-factor authentication information.	November 3, 2014
Initial release	Initial release of the <i>Amazon WorkDocs Administration Guide</i> .	July 10, 2014