Amazon WorkDocs

Administration Guide

Amazon WorkDocs: Administration Guide

Table of Contents

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. Files are stored in the cloud, safely and securely. Your user's files are only visible to them, and their designated contributors and viewers. Other members of your organization do not have access to other user's files unless they are specifically granted access.

Users can share their 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 Amazon WorkDocs

Administrators use the Amazon WorkDocs console to create and deactivate Amazon WorkDocs sites. With the admin control panel, they can manage users, storage, and security settings. For more information, see Managing Sites (p. 32), Inviting and Managing Amazon WorkDocs Users (p. 17), and Managing Security Settings (p. 21).

Non-administrative users use the client applications to access their files. They never 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 macOS 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 webpage to your Amazon WorkDocs files.

For more information about how users can download Amazon WorkDocs clients and edit their files, and which file types are supported, see:

- Getting Started with Amazon WorkDocs
- Editing Files
- Supported File Types

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.

How to Get Started

To get started with Amazon WorkDocs, try one of the following tutorials:

- Getting Started with Quick Start (p. 6)
- Getting Started with Simple AD: Standard Setup (p. 8)
- Getting Started with an Existing Directory (p. 10)
- Getting Started with AD Connector (p. 11)
- Getting Started with AWS Managed Microsoft AD (p. 13)

If you have an Amazon WorkSpaces administrator account with a directory that is enabled for Amazon WorkDocs, you can sign in to your Amazon WorkDocs site and finish setup from the **Admin control panel**. For more information, see Step 3: Complete Admin Control Panel Setup (p. 10). For more information about using Amazon WorkSpaces to get started with Amazon WorkDocs, see Get Started with Amazon WorkSpaces Quick Setup.

Prerequisites for Amazon WorkDocs

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

Tasks

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 https://aws.amazon.com/, and then choose **Create an AWS Account**.

   Note
   If you previously signed in to the AWS Management Console using AWS account root user credentials, choose **Sign in to a different account**. If you previously signed in to the console using IAM credentials, choose **Sign-in using root account credentials**. Then choose **Create a new AWS account**.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code using the phone keypad.

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 uses a directory to store and manage organization information for your users and their documents. You can create a Simple AD directory using Quick Start or Standard Setup, or create an AD Connector directory to connect to your on-premises directory. Alternatively, you can enable Amazon WorkDocs to work with an existing AWS directory, or you can have Amazon WorkDocs create a directory for you. You can also create a trust relationship between your AWS Directory Service service and a AWS Managed Microsoft AD Directory.

> **Note**
> If you are part of a compliance program, such as PCI, FedRAMP, or DoD, you must set up a AWS Managed Microsoft AD Directory to meet compliance requirements.

Contents

Getting Started with Quick Start

In this tutorial, you'll learn how to set up a new Amazon WorkDocs site and create a Simple AD directory with **Quick Start**. The **Quick Start** option is available only if you have never launched an Amazon WorkDocs site before.

> **Note**
> If you need more control over the directory configuration, such as specifying your own directory domain name or using an existing virtual private cloud (VPC) with the directory, use the **Standard Setup** option. For more information, see Getting Started with Simple AD: Standard Setup (p. 8).

Tasks

Before You Begin

- You must have an AWS account to create or administer an Amazon WorkDocs site. Users do not need an AWS account to connect to and use Amazon WorkDocs. For more information, see Prerequisites for Amazon WorkDocs (p. 3).

- When you launch a new Amazon WorkDocs site, you must specify profile information for the administrator, including first and last name and an email address.
- If you are part of a compliance program, such as PCI, FedRAMP, or DoD, you must set up a Microsoft AD Directory to meet compliance requirements. Follow the instructions on Getting Started with AWS Managed Microsoft AD (p. 13) instead.

Step 1: Launch the Amazon WorkDocs Site

Using Quick Start, you can launch your first Amazon WorkDocs site in minutes.

To launch the Amazon WorkDocs site

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. Choose **Get Started Now** from the Amazon WorkDocs start page or choose **Create a New WorkDocs Site** from the **Manage Your WorkDocs Sites** page.
3. On the **Get Started with WorkDocs** page, next to **Quick Start**, choose **Launch**.

Step 2: Create Access Point and Set Administrator

Follow the steps below to create an access point and set an administrator.

To create access point and set administrator

1. From the **WorkDocs Quick Start** page, enter the following values for **Access Point**:

   Region

   Verify the region.

   Site URL

   Enter the URL for your Amazon WorkDocs site.
2. Enter the following values for **Set WorkDocs Administrator**:

   Email

   The email address of the directory administrator, also used as the username. The registration email is sent here.

   First Name

   The first name of the directory administrator.

   Last Name

   The last name of the directory administrator.
3. Choose **Complete Setup**.

   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`.

Quick Start completes the following tasks on your behalf:

- Creates a virtual private cloud (VPC).
- Sets up a Simple AD directory in the VPC that is used to store user and Amazon WorkDocs site information.
- Creates a directory administrator account. An email is sent to the administrator with instructions to complete registration. Use this account to manage the directory.
- Creates the specified user accounts, adds them to the directory, and sends invitation emails.

Step 3: Complete Admin Control Panel Setup

After you receive the administrator registration email, connect to the Amazon WorkDocs site using the client of your choice and complete setup from your admin control panel.

To complete admin control panel setup

1. In the administrator registration email, use the link to sign in to Amazon WorkDocs.
2. Under **My account**, choose **Open admin control panel**.
3. Change settings for preferred language, storage, security, and recovery bin. For more information, see Storage Settings (p. 32), Managing Security Settings (p. 21), and Recovery Bin Retention Settings (p. 33).
4. Under **Manage Users**, invite new users. You can also edit user settings.

For more information, see Inviting and Managing Amazon WorkDocs Users (p. 17).

Getting Started with Simple AD: Standard Setup

In this tutorial, you'll learn how to set up an Amazon WorkDocs site using **Standard Setup** to create a Simple AD directory in the cloud.

Tasks

Before You Begin

- You must meet the prerequisites identified in Simple AD Prerequisites in the *AWS Directory Service Administration Guide*.
- If you are part of a compliance program, such as PCI, FedRAMP, or DoD, you must set up a AWS Managed Microsoft AD Directory to meet compliance requirements. For more information, see Getting Started with AWS Managed Microsoft AD (p. 13).
- When you launch a new Amazon WorkDocs site, you must specify profile information for the administrator, including first and last name and an email address.

Step 1: Launch the Amazon WorkDocs Site

Follow the steps below to launch your Amazon WorkDocs site using **Standard Setup**.

To launch the Amazon WorkDocs site

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. Choose **Get Started Now** from the Amazon WorkDocs start page or choose **Create a New WorkDocs Site** from the **Manage Your WorkDocs Sites** page.
3. On the **Get Started with WorkDocs** page, next to **Standard Setup**, choose **Launch**.

Step 2: Create Directory and Set Administrator

Follow the steps below to create a Simple AD directory and set an administrator.

To create a Simple AD directory

1. On the **Set up a Directory** page, choose **Create Simple AD**.
2. For **Access Point**, enter the following values and then choose **Continue**.

   Region

   Verify the region.

   Site URL

   Enter the URL for your Amazon WorkDocs site.
3. Enter the following values for **Directory Details**:

   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`.
4. Enter the following values for **Set WorkDocs Administrator**:

   Email

   The email address of the directory administrator, also used as the username. The registration email is sent here.

   First Name

   The first name of the directory administrator.

   Last Name

   The last name of the directory administrator.
5. For **VPC Details**, select **Set up a new VPC on my behalf** to have Amazon WorkDocs create and configure a VPC for you. To use an existing VPC instead, 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 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`.

Step 3: Complete Admin Control Panel Setup

After you receive the administrator registration email, connect to the Amazon WorkDocs site using the client of your choice and complete setup from your admin control panel.

To complete admin control panel setup

1. In the administrator registration email, use the link to sign in to Amazon WorkDocs.
2. Under **My account**, choose **Open admin control panel**.
3. Change settings for preferred language, storage, security, and recovery bin. For more information, see Storage Settings (p. 32), Managing Security Settings (p. 21), and Recovery Bin Retention Settings (p. 33).
4. Under **Manage Users**, invite new users. You can also edit user settings.

For more information, see Inviting and Managing Amazon WorkDocs Users (p. 17).

Getting Started with an Existing Directory

In this tutorial, you'll learn how to set up an Amazon WorkDocs site by enabling an existing AWS Directory Service directory.

Tasks

Before You Begin

- You must have an existing AWS Directory Service directory in the current region. This can be either a Simple AD directory or an AD Connector directory.
- If you are part of a compliance program, such as PCI, FedRAMP, or DoD, you must set up a AWS Managed Microsoft AD Directory to meet compliance requirements. For more information, see Getting Started with AWS Managed Microsoft AD (p. 13).
- When you launch a new Amazon WorkDocs site, you must specify profile information for the administrator, including first and last name and an email address.

Step 1: Launch the Amazon WorkDocs Site

Follow the steps below to launch your Amazon WorkDocs site using an existing AWS Directory Service directory.

To launch the Amazon WorkDocs site

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**.

Step 2: Enable Directory and Set Administrator

Follow the steps below to enable your existing directory and set an administrator.

To enable an existing directory

1. On the **Select a Directory** page, select your AWS Directory Service directory from the **Available Directories** list and choose **Enable Directory**.
2. 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**.

   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`.

Step 3: Complete Admin Control Panel Setup

After you receive the administrator registration email, connect to the Amazon WorkDocs site using the client of your choice and complete setup from your admin control panel.

To complete admin control panel setup

1. In the administrator registration email, use the link to sign in to Amazon WorkDocs.
2. Under **My account**, choose **Open admin control panel**.
3. Change settings for preferred language, storage, security, and recovery bin. For more information, see Storage Settings (p. 32), Managing Security Settings (p. 21), and Recovery Bin Retention Settings (p. 33).
4. Under **Manage Users**, invite new users. You can also edit user settings.

For more information, see Inviting and Managing Amazon WorkDocs Users (p. 17).

Getting Started with AD Connector

In this tutorial, you'll learn how to set up an Amazon WorkDocs site using an AWS Directory Service AD Connector directory to connect to your on-premises directory.

Tasks

- Step 3: Complete Admin Control Panel Setup (p. 13)

Before You Begin

- You must meet the prerequisites identified in AD Connector Prerequisites in the *AWS Directory Service Administration Guide*.
- When you launch a new Amazon WorkDocs site, you must specify profile information for the administrator, including first and last name and an email address.

Step 1: Launch the Amazon WorkDocs Site

Follow the steps below to launch your Amazon WorkDocs site and connect to your on-premises directory.

To launch the Amazon WorkDocs site

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. Choose **Get Started Now** from the Amazon WorkDocs start page or choose **Create a New WorkDocs Site** from the **Manage Your WorkDocs Sites** page.
3. On the **Get Started with WorkDocs** page, next to **Standard Setup**, choose **Launch**.

Step 2: Connect Directory

Follow the steps below to connect to your on-premises directory using an AWS Directory Service AD Connector directory.

To connect your directory

1. On the **Set up a Directory** page, under **AD Connector** choose **Create AD Connector**.
2. For **Directory Details**, enter the following values and choose **Continue**.

   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.

3. For **Access Point**, enter the following values:

   Region

   Verify the region.

   Site URL

   Enter the URL for your Amazon WorkDocs site.

4. For **VPC Configuration**, enter the following values:

   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.

5. Confirm that the directory information is correct, then choose **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`.

Step 3: Complete Admin Control Panel Setup

After you receive the administrator registration email, connect to the Amazon WorkDocs site using the client of your choice and complete setup from your admin control panel.

To complete admin control panel setup

1. In the administrator registration email, use the link to sign in to Amazon WorkDocs.
2. Under **My account**, choose **Open admin control panel**.
3. Change settings for preferred language, storage, security, and recovery bin. For more information, see Storage Settings (p. 32), Managing Security Settings (p. 21), and Recovery Bin Retention Settings (p. 33).
4. Under **Manage Users**, invite new users. You can also edit user settings.

For more information, see Inviting and Managing Amazon WorkDocs Users (p. 17).

Getting Started with AWS Managed Microsoft AD

In this tutorial, you'll learn how to set up an Amazon WorkDocs site by connecting to your on-premises AWS Managed Microsoft AD directory.

Note
If you are part of a compliance program, such as PCI, FedRAMP, or DoD, you must set up a AWS Managed Microsoft AD Directory to meet compliance requirements.

Tasks

Before You Begin

- You must create a Trust Relationship between your AWS Directory service and AWS Managed Microsoft AD. For more information, see When to Create a Trust Relationship.
- You must create a AWS Managed Microsoft AD. For more information, see How to Create a Microsoft AD directory.
- When you launch a new Amazon WorkDocs site, you must specify profile information for the administrator, including first and last name and an email address.

Step 1: Launch the Amazon WorkDocs Site

Follow the steps below to launch your Amazon WorkDocs site.

To launch the Amazon WorkDocs site

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. Choose **Get Started Now** from the Amazon WorkDocs start page or choose **Create a New WorkDocs Site** from the **Manage Your WorkDocs Sites** page.
3. On the **Get Started with WorkDocs** page, next to **Standard Setup**, choose **Launch**.

Step 2: Enable AWS Managed Microsoft AD and Set Administrator

Follow the steps below to enable your AWS Managed Microsoft AD and set an administrator.

To enable your AWS Managed Microsoft AD

1. From the list of available directories, select the AWS Managed Microsoft AD to use for your Amazon WorkDocs site.

   Note
   Make sure that site is being created in the same region as the AWS Managed Microsoft AD.
2. Choose **Enable directory**.
3. On the **Set WorkDocs Administrator** page, enter a username from the AWS Managed Microsoft AD directory to be your Amazon WorkDocs administrator and choose **Select Administrator**.

   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`.

Step 3: Complete Admin Control Panel Setup

After you receive the administrator registration email, connect to the Amazon WorkDocs site using the client of your choice and complete setup from your admin control panel.

To complete admin control panel setup

1. In the administrator registration email, use the link to sign in to Amazon WorkDocs.
2. Under **My account**, choose **Open admin control panel**.
3. Change settings for preferred language, storage, security, and recovery bin. For more information, see Storage Settings (p. 32), Managing Security Settings (p. 21), and Recovery Bin Retention Settings (p. 33).
4. Under **Manage Users**, invite new users. You can also edit user settings.

For more information, see Inviting and Managing Amazon WorkDocs Users (p. 17).

Enabling Single Sign-On

AWS Directory Service allows users to access Amazon WorkDocs from a computer joined to the same directory with which Amazon WorkDocs is registered, without entering credentials separately. For more information, 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*.

Enabling 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 (for example, **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**. While multi-factor authentication is being set up, your users are not able to log in to their Amazon WorkDocs site.

Promoting 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 Editing Users (p. 18).

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 Editing Users (p. 18).

Inviting and Managing Amazon WorkDocs Users

You can change user roles, invite, enable, or disable users, and change user settings under **Manage Users** in the admin control panel in the Amazon WorkDocs web client. You can also promote a user to an administrator. For more information, see Promoting a User to Administrator (p. 16).

To open the admin control panel, in Amazon WorkDocs, under **My Account**, choose **Open admin control panel**.

> **Note**
> Some admin control panel options differ between cloud directories and connected directories.

Contents

User Roles Overview

Amazon WorkDocs defines the following user roles. You can change a user's role by editing the **User profile**. For more information, see Editing Users (p. 18).

- **Administrator**: A paid user who has administrative permissions for the entire site, including user management and site setting configuration. For more information about how to promote a user to an administrator, see Promoting a User to Administrator (p. 16).
- **Power user**: A paid user of the site who can be given a special set of permissions by the administrator.
- **User**: A paid user who can save files and collaborate with others in an Amazon WorkDocs site.
- **Guest user**: An unpaid user who can only view files. Guest users can be upgraded to a User, Power user, or Administrator.

  > **Note**
  > Changing the role of a **Guest user** to any of the other three roles is a one-time operation that can't be reversed.

Amazon WorkDocs also defines the following user types.

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

An 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

Inviting New Users

For more information about enabling users in a connected directory scenario, see Editing Users (p. 18).

For cloud directories, invite new users to join your directory. Existing users can also invite new users when enabled. For more information, see Invite and New User Settings (p. 21).

To invite new users to a cloud directory

1. In the **Admin Control Panel**, under **Manage Users**, choose **Invite Users**.
2. In the **Invite Users** dialog box, for **Who would you like to invite?**, type the invitee's email address, and choose **Send**. Repeat this step for each invitation.

An invitation email is sent to each recipient with instructions about how to create an Amazon WorkDocs account.

Editing Users

You can change existing user information and settings by editing users.

To edit users

1. From the **Admin Control Panel**, under **Manage Users**, choose the pencil icon (✎) next to the user's name.
2. In the **Edit User** dialog box, you can edit the following options:

   First Name (Cloud Directory only)

   The user's first name.

   Last Name (Cloud Directory only)

   The user's last name.

Status

Specifies if the user is **Active** or **Inactive**. For more information, see Disabling Users (p. 19).

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 User Roles Overview (p. 17).

Storage

Specifies the storage limit for an existing user.

3. Choose **Save Changes**.

Disabling Users

You can disable a user's access by changing their status to **Inactive**.

To change user status to Inactive

1. From the **Admin Control Panel**, under **Manage Users**, choose the pencil icon (✎) next to the user's name.
2. Choose **Inactive**, and choose **Save Changes**

The inactivated user no longer has access to your Amazon WorkDocs site.

Note
Changing a user to **Inactive** status does not delete their files, folders, or feedback from your Amazon WorkDocs site. However, you can transfer files and folders to an active user. For more information, see Transferring Document Ownership (p. 19).

Transferring Document Ownership

You can transfer an inactive user's files and folders to an active user. For more information on how to inactivate a user, see Disabling Users (p. 19).

To transfer document ownership

1. From the **Admin Control Panel**, under **Manage Users**, choose the pencil icon (✎) next to the inactive user's name.
2. Select **Transfer Document Ownership** and type the email address of the active user to whom to transfer the files.
3. Choose **Save Changes**.

Warning
This action cannot be undone.

Deleting Users (Cloud Directory Only)

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.

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.

We do not recommend that you delete registered users. Instead, you should switch a user from **Active** to **Inactive** status, so that they do not have access to your Amazon WorkDocs site. For more information about deactivating a user, see Disabling Users (p. 19).

Downloading User List

To download a list of users from the **Admin control panel**, you must install Amazon WorkDocs Companion. To install Amazon WorkDocs Companion, see Apps & Integrations for Amazon WorkDocs.

> **Note**
> The **Download user** option is not available for Amazon WorkDocs sites using an AWS Directory Service AD Connector directory.

To download a list of users

1. From the **Admin control panel**, under **Manage Users**, choose **Download user**.
2. For **Download user**, choose one of the following options to export a list of users as a `.json` file to your desktop:
   - All users
   - Guest user
   - WS User
   - User
   - Power user
   - Admin
3. The file is saved in one of the following locations:
   - **Windows** – **WorkDocsDownloads** folder in your PC's **Downloads** folder
   - **macOS** – `/users/username/WorkDocsDownloads/folder`

For more information about these user roles, see User Roles Overview (p. 17).

Managing Security Settings

Set up external sharing and publicly shareable link options, and configure default settings for user invites, new users, and enabled users.

Contents

Public Share Settings

In the **Admin control panel**, under **Security**, choose **Who should be allowed to send publicly shareable links?** to specify which users are allowed to send file view links to people outside of the organization. Choose from the following settings:

No public sharing

Users cannot send view links to anyone outside the organization.

All managed users can share publicly

All users can send view links to anyone outside the organization.

Only Power users can share publicly

Only Power users can send view links to people outside the organization.

Invite and New User Settings

In the **Admin control panel**, under **Security**, configure default settings for inviting new users to cloud directories, or for enabling users from connected directories.

Cloud Directory Invite Settings

For a cloud directory, choose from the following settings for **Who should be allowed to join your WorkDocs site?**.

Only administrators can invite new users

Users cannot invite new users.

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

Users can invite new people from anywhere 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.

Connected Directory Invite Settings

For a connected directory, choose from the following settings for **Who should be allowed to join your WorkDocs site?**.

Only administrators can enable new users

Only administrators can enable users to use Amazon WorkDocs.

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.

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.

Connected Directory External Invites

Choose from the following settings for **Who should be allowed to invite external users to your WorkDocs site?**

Share with external users

Choose this option to enable sharing with external users.

Only administrators can invite new external users

Only administrators can invite external users to use Amazon WorkDocs.

All managed users can invite new external users

All users can invite new external users to use Amazon WorkDocs.

Only Power users can invite new external users

Only Power users can invite new external users to use Amazon WorkDocs.

Connected Directory New User Settings

Choose from the following settings for **Configure role for new users**.

New users from your directory will be Managed users (they are Guest users by default)

New users from your directory will be assigned the role of Guest user.

New external users will be Managed users (they are Guest users by default)

New external users will be assigned the role of Guest user.

Site-wide Activity Feed

Admins can view and export the activity feed for an entire site. To use this feature, you must first install Amazon WorkDocs Companion. To install Amazon WorkDocs Companion, see Apps & Integrations for Amazon WorkDocs.

To view and export a site-wide activity feed

1. In the web application, choose **Activity feed**.
2. Choose **Filter**, then choose the option to show **Site-wide activity**.
3. Select **Activity Type** filters and choose **Date Modified** settings as needed, then choose **Apply**.
4. When the filtered activity feed results appear, search by file, folder, or user name to narrow your results. You can also add or remove filters as needed.
5. Choose **Export** to export the activity feed to `.csv` and `.json` files on your desktop. The files are saved in one of the following locations:

   - **Windows** – **WorkDocsDownloads** folder in your PC's **Downloads** folder
   - **macOS** – `/users/username/WorkDocsDownloads/folder`

   Any filters you applied are reflected in the exported file.

   Note
   Users who are not administrators can view and export the activity feed for their own content only. For more information, see Viewing the Activity Feed in the *Amazon WorkDocs User Guide*.

Logging Amazon WorkDocs API Calls Using AWS CloudTrail

Amazon WorkDocs is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon WorkDocs. CloudTrail captures all API calls for Amazon WorkDocs as events, including calls from the Amazon WorkDocs console and from code calls to the Amazon WorkDocs APIs. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon WorkDocs. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to Amazon WorkDocs, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

Amazon WorkDocs Information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Amazon WorkDocs, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for Amazon WorkDocs, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all regions. The trail logs events from all regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail

- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

All Amazon WorkDocs actions are logged by CloudTrail and are documented in the Amazon WorkDocs API Reference. For example, calls to the `CreateFolder`, `DeactivateUser` and `UpdateDocument` sections generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or IAM user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity Element.

Understanding Amazon WorkDocs Log File Entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files are not an ordered stack trace of the public API calls, so they do not appear in any specific order.

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. 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",
        "userSid" : "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"
    }
  ]
}
```

Sharing and Collaboration

Users can share content by sending a link or an invite. They can also collaborate with external users if external sharing is enabled.

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

Contents

Sharing

There are multiple ways for users to share content in Amazon WorkDocs.

Share a Link

Users can choose **Share a Link** to quickly copy and share hyperlinks for Amazon WorkDocs content with coworkers and external users both inside and outside their organization. Shareable links can be configured to allow access to site members only or anyone on the internet. Links with access to site members can be configured for viewing and commenting, while links with access to anyone is restricted to viewing only. Recipients with viewing permissions can only view a file. Commenting permissions enable users to comment and perform update or delete operations, such as uploading a new file or deleting an existing file.

By default, all managed users can create public links. To change this setting, update your **Security** settings from your **Admin Control Panel**. For more information, see Managing Security Settings (p. 21).

Share by Invite

Users can choose **Share by invite** to share files or folders with other users by inviting them using their email address. Users can also set the appropriate permission level for each invited user. Invited users automatically receive an invite email notifying them that content has been shared with them. Clicking on the link in the email opens the shared file. Users can share files and folders with other site members or with external users.

External Sharing

External sharing allows managed users of an Amazon WorkDocs site to share files and folders and collaborate with external users in a convenient way without incurring extra costs. Users of a site can share files and folders with external users without requiring recipients to be paid users of the Amazon WorkDocs site. If external sharing is enabled, users can type the email address of the external user they want to share with and set appropriate viewer sharing permissions. When external users are added, permissions are limited to viewer only and other permissions are not available. External users receive an email notification with a link to the shared file or folder. Choosing the link takes external users to the site, where they type their credentials to log in to Amazon WorkDocs. They can see the shared file or folder in the **Shared with me** view.

File owners can modify sharing permissions or remove access for the external user from a file or folder at any time. External sharing for the site must be enabled by the site administrator in order for managed

users to share content with external users. For **Guest users** to become contributors or co-owners, they must be upgraded to the **User** level by a site administrator. For more information, see User Roles Overview (p. 17).

By default, external sharing is turned on and all users can invite external users. To change this setting, update your **Security** settings from your **Admin Control Panel**. For more information, see Managing Security Settings (p. 21).

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

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

Permission	Owner/Co-Owner	Contributor	Viewer	Anonymous Viewer
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 they are not replies 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	

Permission	Folder Owner/ Co-Owner	File Owner*	Folder Contributor	Folder Viewer	Anonymous Viewer
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 who uploaded the original version of a file to a shared folder. 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 only see private comments that are replies to their comments.

Enabling Collaborative Editing

You can enable collaborative editing options under the **Online Editing Settings** section in your **Admin control panel**.

Contents

Enabling Hancom Online Editing

You can enable Hancom Online Editing for your Amazon WorkDocs site, so that users can create and collaboratively edit Microsoft Office files from the Amazon WorkDocs web application. For more information, see Hancom Online Editing.

Hancom Online Editing is available at no additional cost for Amazon WorkDocs users. No additional licensing or software installation is needed.

To enable Hancom Online Editing

Enable Hancom Online Editing from the **Admin control panel**.

1. Under **My account**, choose **Open admin control panel**.
2. For **Hancom Online Editing**, choose **Change**.
3. Select **Enable Hancom Online Editing Feature**, review the terms of usage, and then choose **Save**.

To disable Hancom Online Editing

Disable Hancom Online Editing from the **Admin control panel**.

1. Under **My account**, choose **Open admin control panel**.
2. For **Hancom Online Editing**, choose **Change**.
3. Clear the **Enable Hancom Online Editing Feature** check box, then choose **Save**.

Enabling Open with Office Online

Enable Open with Office Online for your Amazon WorkDocs site, so that users can collaboratively edit Microsoft Office files from the Amazon WorkDocs web application.

Open with Office Online is available at no additional cost for Amazon WorkDocs users who also have a Microsoft Office 365 **Work** or **School** account with a license to edit in Office Online. For more information, see Open with Office Online.

To enable Open with Office Online

Enable Open with Office Online from the **Admin control panel**.

1. Under **My account**, choose **Open admin control panel**.
2. For **Office Online**, choose **Change**.
3. Select **Enable Office Online**, then choose **Save**.

To disable Open with Office Online

Disable Open with Office Online from the **Admin control panel**.

1. Under **My account**, choose **Open admin control panel**.
2. For **Office Online**, choose **Change**.
3. Clear the **Enable Office Online** check box, then choose **Save**.

Managing Sites

Administrators can manage site-wide operations, such as choosing a preferred language for site content and email notifications, setting storage limits, and specifying recovery bin retention policy. They can also change settings for Managing Security Settings (p. 21) and Inviting and Managing Amazon WorkDocs Users (p. 17).

Contents

Language Settings

Specify the language to use for site content and email notifications.

To change language settings

1. Under **My Account**, choose **Open admin control panel**.
2. For **Preferred Language Settings**, choose your preferred language.

Online Editing Settings

Enable or disable online editing settings from the **Admin control panel**. For more information, see Enabling Collaborative Editing (p. 30).

Storage Settings

Specify the amount of storage that new users receive.

To change storage settings

1. Under **My Account**, choose **Open admin control panel**.
2. For **Storage**, choose **Change**.
3. In the **Storage Limit** dialog box, choose whether to give new users unlimited or limited storage.
4. Choose **Save Changes**.

Changing the storage setting affects only 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 Editing Users (p. 18).

IP Allow List Settings

Amazon WorkDocs site administrators can add **IP Allow List** settings to restrict site access to an allowed range of IP addresses. You can add up to 32 **IP Allow List** settings per site.

Note
The **IP Allow List** currently works for IPv4 addresses only. IP address denylisting is not currently supported.

To add an IP range to the IP Allow List

1. Under **My Account**, choose **Open admin control panel**.
2. For **IP Allow List**, choose **Change**.
3. For **Enter CIDR value**, enter the Classless Inter-Domain Routing (CIDR) block for the IP address ranges to allowlist, and choose **Add**.
   - To allow access from a single IP address, specify `/32` as the CIDR prefix.
4. Choose **Save Changes**.
5. Users who connect to your site from the IP addresses on the **IP Allow List** are allowed access. Users who attempt to connect to your site from unauthorized IP addresses receive an unauthorized response.

Warning
If you enter a CIDR value that blocks you from using your current IP address to access the site, a warning message appears. If you choose to continue with the current CIDR value, you will be blocked from accessing the site with your current IP address. This action can only be reversed by contacting AWS Support.

Security Settings

You can manage security settings for users. This includes setting up external sharing and publicly shareable link options, and configuring default settings for user invites, new users, and enabled users. For more information, see Managing Security Settings (p. 21).

Recovery Bin Retention Settings

Files deleted by a user are stored in the user's recycle bin for 30 days. Afterwards, the files are temporarily moved to a recovery bin for 60 days before they are permanently deleted. The recovery bin is visible only to administrators. By changing the site-wide data retention policy, site administrators can change the recovery bin retention period, up to a maximum of 365 days. Files are permanently deleted at the end of the retention period.

To change the recovery bin retention period

1. Under **My Account**, choose **Open admin control panel**.
2. Next to **Recovery bin retention**, choose **Change**.
3. Type the number of days to retain files in the recovery bin, and choose **Save**.

   Note
   The default retention period is 60 days. This can be changed to 0–365 days.

You can restore user files from the recovery bin before they are permanently deleted.

To restore a user's file

1. Under **My Account**, choose **Open admin control panel**.
2. Under **Manage Users**, choose the user's folder icon.
3. Under **Recovery bin**, select the file(s) to restore, then choose the **Recover** icon.
4. For **Restore file**, choose the location to which to restore the file, then choose **Restore**.

Manage Users Settings

You can manage settings for users, including changing user roles and inviting, enabling, or disabling users. For more information, see Inviting and Managing Amazon WorkDocs Users (p. 17).

Deleting a Site

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

Warning
You lose all user information and files when you delete a site. Delete a site only if you are sure that this information is no longer needed.

To delete a site

1. Open the Amazon WorkDocs console at https://console.aws.amazon.com/zocalo/.
2. If necessary, from the navigation bar, choose the AWS Region that you need. For more information, see Regions and Endpoints in the *Amazon Web Services General Reference*.
3. On the **Manage Your WorkDocs Sites** page, choose the site to delete. Choose **Actions**, then choose **Delete WorkDocs Site**.
4. In the **Delete Selected WorkDocs Site** dialog box, choose whether to delete the user directory at the same time.

   - Choose **I also want to delete the user directory** to delete the AWS Directory Service Simple AD or AD Connector for an on-premises Microsoft Active Directory. 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*.
5. Verify that you are deleting the proper site, type **DELETE** in the confirmation field, and choose **Delete WorkDocs Site**.

   The site is immediately deleted and is no longer available.

   Note
   If you didn't provide your own directory for Amazon WorkDocs, then we created one for you. When you delete the Amazon WorkDocs site, you are charged for the directory we created for you unless you delete the directory or use it for another AWS application. For pricing information, see Other Directory Types Pricing.

Troubleshooting Amazon WorkDocs Issues

The following information can help you troubleshoot issues with Amazon WorkDocs.

Issues

Can't set up my Amazon WorkDocs site in a specific AWS Region

If you're setting up a new Amazon WorkDocs site, you can select the AWS Region during setup. For more information, see the tutorial for your particular use case under Getting Started with Amazon WorkDocs (p. 6).

Want to set up my Amazon WorkDocs site in an existing Amazon VPC

When setting up your new Amazon WorkDocs site, create a directory using the existing virtual private cloud (VPC). Amazon WorkDocs uses this directory to authenticate users.

User needs to reset their password

Users can reset their passwords by choosing **Forgot password?** on their sign-in screens.

User accidentally shared a sensitive document

To revoke access to the document, choose **Share by invite** next to the document, then remove the users who should no longer have access. If the document was shared using a link, choose **Share a link** and disable the link.

User left the organization and didn't assign another user as co-owner

Transfer document ownership to another user in the **Admin Control Panel**. For more information, see Transferring Document Ownership (p. 19).

Need to deploy Amazon WorkDocs Drive or Amazon WorkDocs Companion to multiple users

Deploy to multiple users in an enterprise by using group policy. For more information, see Create IAM Users and Groups (Recommended) (p. 3).

Can't access Amazon WorkDocs data without a network connection

Verify that you have the Amazon WorkDocs Sync Client installed so that you can access your Amazon WorkDocs files and folders on your desktop. For more information, see Amazon WorkDocs Sync Client.

Online editing isn't working

Verify that you have Amazon WorkDocs Companion installed. To install Amazon WorkDocs Companion, see Apps & Integrations for Amazon WorkDocs.

Document History

The following table describes important changes to the *Amazon WorkDocs Administration Guide*, beginning in February 2018. For notifications about updates to this documentation, you can subscribe to an RSS feed.

update-history-change	update-history-description	update-history-date
IP Allow List Settings (p. 37)	**IP Allow List** settings are available to filter access to your Amazon WorkDocs site by IP address range. For more information, see **IP Allow List** Settings in the Amazon WorkDocs Administration Guide.	October 22, 2018
Hancom Online Editing (p. 37)	Hancom Online Editing is available. Users can create and collaboratively edit Microsoft Office files from the Amazon WorkDocs web application. For more information, see Enabling Hancom Online Editing in the Amazon WorkDocs Administration Guide.	June 21, 2018
Open with Office Online (p. 37)	Open with Office Online is available. Users can collaboratively edit Microsoft Office files from the Amazon WorkDocs web application. For more information, see Enabling Open with Office Online in the Amazon WorkDocs Administration Guide.	June 6, 2018
Troubleshooting (p. 37)	Troubleshooting topic added. For more information, see Troubleshooting Amazon WorkDocs Issues in the Amazon WorkDocs Administration Guide.	May 23, 2018
Change Recovery Bin Retention Period (p. 37)	Recovery bin retention period can be modified. For more information, see Recovery Bin Retention Settings in the Amazon WorkDocs Administration Guide.	February 27, 2018