Amazon WorkDocs

Administration Guide

Amazon WorkDocs: Administration Guide

Copyright © 2020 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?

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 site settings (p. 31) and Inviting and managing Amazon WorkDocs users (p. 36).

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. 19)
- Getting started with Simple AD: Standard Setup (p. 21)
- Getting started with an existing directory (p. 23)
- Getting started with AD Connector (p. 24)
- Getting started with AWS Managed Microsoft AD (p. 27)

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. 23).

For more information about using Amazon WorkSpaces to get started with Amazon WorkDocs, see Get started with Amazon WorkSpaces Quick Setup in the *Amazon WorkSpaces Administration Guide*. For information about using an Amazon WorkDocs client in Amazon WorkSpaces or an Amazon EC2 instance, see Endpoints for Amazon S3 in the *Amazon VPC User Guide*.

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, complete the following steps to create one.

To sign up for an AWS account

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

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

Your AWS root account credentials identify you to services in AWS and grant you unlimited use of your AWS resources, such as your Amazon WorkDocs sites.

Create IAM users and groups (recommended)

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.

For more information, see Identity and access management for Amazon WorkDocs (p. 4).

Security in Amazon WorkDocs

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS compliance programs. To learn about the compliance programs that apply to Amazon WorkDocs, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon WorkDocs. The following topics show you how to configure Amazon WorkDocs to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Amazon WorkDocs resources.

Topics

Identity and access management for Amazon WorkDocs

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Amazon WorkDocs resources. IAM is an AWS service that you can use with no additional charge.

Topics

- Troubleshooting Amazon WorkDocs identity and access (p. 12)

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work you do in Amazon WorkDocs.

Service user – If you use the Amazon WorkDocs service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon WorkDocs features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Amazon WorkDocs, see Troubleshooting Amazon WorkDocs identity and access (p. 12).

Service administrator – If you're in charge of Amazon WorkDocs resources at your company, you probably have full access to Amazon WorkDocs. It's your job to determine which Amazon WorkDocs features and resources your employees should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Amazon WorkDocs, see How Amazon WorkDocs works with IAM (p. 8).

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Amazon WorkDocs. To view example Amazon WorkDocs identity-based policies that you can use in IAM, see Amazon WorkDocs identity-based policy examples (p. 10).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. For more information about signing in using the AWS Management Console, see The IAM Console and Sign-in Page in the *IAM User Guide*.

You must be *authenticated* (signed in to AWS) as the AWS account root user, an IAM user, or by assuming an IAM role. You can also use your company's single sign-on authentication, or even sign in using Google or Facebook. In these cases, your administrator previously set up identity federation using IAM roles. When you access AWS using credentials from another company, you are assuming a role indirectly.

To sign in directly to the AWS Management Console, use your password with your root user email or your IAM user name. You can access AWS programmatically using your root user or IAM user access keys. AWS provides SDK and command line tools to cryptographically sign your request using your credentials. If you don't use AWS tools, you must sign the request yourself. Do this using *Signature Version 4*, a protocol for authenticating inbound API requests. For more information about authenticating requests, see Signature Version 4 Signing Process in the *AWS General Reference*.

Regardless of the authentication method that you use, you might also be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Using Multi-Factor Authentication (MFA) in AWS in the *IAM User Guide*.

AWS account root user

When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. An IAM user can have long-term credentials such as a user name and password or a set of access keys. To learn how to generate access keys, see Managing Access Keys for IAM Users in the *IAM User Guide*. When you generate access keys for an IAM user, make sure you view and securely save the key pair. You cannot recover the secret access key in the future. Instead, you must generate a new access key pair.

An *IAM group* is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see When to Create an IAM User (Instead of a Role) in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by switching roles. You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Using IAM Roles in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.
- **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as *federated users*. AWS assigns a role to a federated user when access is requested through an identity provider. For more information about federated users, see Federated Users and Roles in the *IAM User Guide*.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see How IAM Roles Differ from Resource-based Policies in the *IAM User Guide*.
- **AWS service access** – A service role is an IAM role that a service assumes to perform actions in your account on your behalf. When you set up some AWS service environments, you must define a role for the service to assume. This service role must include all the permissions that are required for the service to access the AWS resources that it needs. Service roles vary from service to service, but many allow you to choose your permissions as long as you meet the documented requirements for that service. Service roles provide access only within your account and cannot be used to grant access to services in other accounts. You can create, modify, and delete a service role from within IAM. For example, you can create a role that allows Amazon Redshift to access an Amazon S3 bucket on your behalf and then load data from that bucket into an Amazon Redshift cluster. For more information, see Creating a Role to Delegate Permissions to an AWS Service in the *IAM User Guide*.
- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached

to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see Using an IAM Role to Grant Permissions to Applications Running on Amazon EC2 Instances in the *IAM User Guide*.

To learn whether to use IAM roles, see When to Create an IAM Role (Instead of a User) in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to IAM identities or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when an entity (root user, IAM user, or IAM role) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see Overview of JSON Policies in the *IAM User Guide*.

An IAM administrator can use policies to specify who has access to AWS resources, and what actions they can perform on those resources. Every IAM entity (user or role) starts with no permissions. In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, role, or group. These policies control what actions that identity can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM Policies in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see Choosing Between Managed Policies and Inline Policies in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource such as an Amazon S3 bucket. Service administrators can use these policies to define what actions a specified principal (account member, user, or role) can perform on that resource and under what conditions. Resource-based policies are inline policies. There are no managed resource-based policies.

Access control lists

Access control lists (ACLs) are a type of policy that controls which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format. Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see Access Control List (ACL) Overview in the *Amazon Simple Storage Service Developer Guide*.

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions Boundaries for IAM Entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see How SCPs Work in the *AWS Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see Session Policies in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy Evaluation Logic in the *IAM User Guide*.

How Amazon WorkDocs works with IAM

Before you use IAM to manage access to Amazon WorkDocs, you should understand what IAM features are available to use with Amazon WorkDocs. To get a high-level view of how Amazon WorkDocs and other AWS services work with IAM, see AWS services that work with IAM in the *IAM User Guide*.

Topics

Amazon WorkDocs identity-based policies

With IAM identity-based policies, you can specify allowed or denied actions. Amazon WorkDocs supports specific actions. To learn about the elements that you use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

Actions

The `Action` element of an IAM identity-based policy describes the specific action or actions that will be allowed or denied by the policy. Policy actions usually have the same name as the associated AWS API operation. The action is used in a policy to grant permissions to perform the associated operation.

Policy actions in Amazon WorkDocs use the following prefix before the action: `workdocs:`. For example, to grant someone permission to run the Amazon WorkDocs `DescribeUsers` API operation, you include the `workdocs:DescribeUsers` action in their policy. Policy statements must include either an `Action` or `NotAction` element. Amazon WorkDocs defines its own set of actions that describe tasks that you can perform with this service.

To specify multiple actions in a single statement, separate them with commas as follows:

```
"Action": [
      "workdocs:DescribeUsers",
      "workdocs:CreateUser"
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word `Describe`, include the following action:

```
"Action": "workdocs:Describe*"
```

To see a list of Amazon WorkDocs actions, see Actions defined by Amazon WorkDocs in the *IAM User Guide*.

Resources

Amazon WorkDocs does not support specifying resource ARNs in a policy.

Condition keys

Amazon WorkDocs does not provide any service-specific condition keys, but it does support using some global condition keys. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

Examples

To view examples of Amazon WorkDocs identity-based policies, see Amazon WorkDocs identity-based policy examples (p. 10).

Amazon WorkDocs resource-based policies

Amazon WorkDocs does not support resource-based policies.

Authorization based on Amazon WorkDocs tags

Amazon WorkDocs does not support tagging resources or controlling access based on tags.

Amazon WorkDocs IAM roles

An IAM role is an entity within your AWS account that has specific permissions.

Using temporary credentials with Amazon WorkDocs

You can use temporary credentials to sign in with federation, assume an IAM role, or to assume a cross-account role. You obtain temporary security credentials by calling AWS STS API operations such as AssumeRole or GetFederationToken.

Amazon WorkDocs supports using temporary credentials.

Service-linked roles

Service-linked roles allow AWS services to access resources in other services to complete an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view but not edit the permissions for service-linked roles.

Amazon WorkDocs does not support service-linked roles.

Service roles

This feature allows a service to assume a service role on your behalf. This role allows the service to access resources in other services to complete an action on your behalf. Service roles appear in your IAM account and are owned by the account. This means that an IAM administrator can change the permissions for this role. However, doing so might break the functionality of the service.

Amazon WorkDocs does not support service roles.

Amazon WorkDocs identity-based policy examples

By default, IAM users and roles don't have permission to create or modify Amazon WorkDocs resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API. An IAM administrator must create IAM policies that grant users and roles permission to perform specific API operations on the specified resources they need. The administrator must then attach those policies to the IAM users or groups that require those permissions.

To learn how to create an IAM identity-based policy using these example JSON policy documents, see Creating policies on the JSON tab in the *IAM User Guide*.

Topics

Policy best practices

Identity-based policies are very powerful. They determine whether someone can create, access, or delete Amazon WorkDocs resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get Started Using AWS Managed Policies** – To start using Amazon WorkDocs quickly, use AWS managed policies to give your employees the permissions they need. These policies are already available in your account and are maintained and updated by AWS. For more information, see Get Started Using Permissions With AWS Managed Policies in the *IAM User Guide*.
- **Grant Least Privilege** – When you create custom policies, grant only the permissions required to perform a task. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. For more information, see Grant Least Privilege in the *IAM User Guide*.
- **Enable MFA for Sensitive Operations** – For extra security, require IAM users to use multi-factor authentication (MFA) to access sensitive resources or API operations. For more information, see Using Multi-Factor Authentication (MFA) in AWS in the *IAM User Guide*.
- **Use Policy Conditions for Extra Security** – To the extent that it's practical, define the conditions under which your identity-based policies allow access to a resource. For example, you can write conditions to specify a range of allowable IP addresses that a request must come from. You can also write conditions

to allow requests only within a specified date or time range, or to require the use of SSL or MFA. For more information, see IAM JSON Policy Elements: Condition in the *IAM User Guide*.

Using the Amazon WorkDocs console

To access the Amazon WorkDocs console, you must have a minimum set of permissions. Those permissions must allow you to list and view the details of the Amazon WorkDocs resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for IAM user or role entities.

To ensure that those entities can use the Amazon WorkDocs console, also attach the following AWS managed policies to the entities. For more information attaching policies, see Adding permissions to a user in the *IAM User Guide*.

- **AmazonWorkDocsFullAccess**
- **AWSDirectoryServiceFullAccess**
- **AmazonEC2FullAccess**

These policies grant an IAM user full access to Amazon WorkDocs resources, AWS Directory Service operations, and the Amazon EC2 operations that Amazon WorkDocs needs in order to work properly.

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that you're trying to perform.

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Allow users read-only access to Amazon WorkDocs resources

The following AWS managed **AmazonWorkDocsReadOnlyAccess** policy 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": [
        {
            "Effect": "Allow",
            "Action": [
                "workdocs:Describe*",
                "ds:DescribeDirectories",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

More Amazon WorkDocs identity-based policy examples

IAM administrators can create additional policies to allow an IAM role or user to access the Amazon WorkDocs API. For more information, see Authentication and access control for administrative applications in the *Amazon WorkDocs Developer Guide*.

Troubleshooting Amazon WorkDocs identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Amazon WorkDocs and IAM.

Topics

I am not authorized to perform an action in Amazon WorkDocs

If the AWS Management Console tells you that you're not authorized to perform an action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password. Ask that person to update your policies to allow you to pass a role to Amazon WorkDocs.

Some AWS services allow you to pass an existing role to that service, instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Amazon WorkDocs. However, the action requires the service to have permissions granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

In this case, Mary asks her administrator to update her policies to allow her to perform the `iam:PassRole` action.

I want to view my access keys

After you create your IAM user access keys, you can view your access key ID at any time. However, you can't view your secret access key again. If you lose your secret key, you must create a new access key pair.

Access keys consist of two parts: an access key ID (for example, `AKIAIOSFODNN7EXAMPLE`) and a secret access key (for example, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

> **Important**
> Do not provide your access keys to a third party, even to help find your canonical user ID. By doing this, you might give someone permanent access to your account.

When you create an access key pair, you are prompted to save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must add new access keys to your IAM user. You can have a maximum of two access keys. If you already have two, you must delete one key pair before creating a new one. To view instructions, see Managing Access Keys in the *IAM User Guide*.

I'm an administrator and want to allow others to access Amazon WorkDocs

To allow others to access Amazon WorkDocs, you must create an IAM entity (user or role) for the person or application that needs access. They will use the credentials for that entity to access AWS. You must then attach a policy to the entity that grants them the correct permissions in Amazon WorkDocs.

To get started right away, see Creating Your First IAM Delegated User and Group in the *IAM User Guide*.

I want to allow people outside of my AWS account to access my Amazon WorkDocs resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Amazon WorkDocs supports these features, see How Amazon WorkDocs works with IAM (p. 8).
- To learn how to provide access to your resources across AWS accounts that you own, see Providing Access to an IAM User in Another AWS Account That You Own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing Access to AWS Accounts Owned by Third Parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing Access to Externally Authenticated Users (Identity Federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see How IAM Roles Differ from Resource-based Policies in the *IAM User Guide*.

Logging and monitoring in Amazon WorkDocs

Amazon WorkDocs site administrators can view and export the activity feed for an entire site. They can also use AWS CloudTrail to capture events from the Amazon WorkDocs console.

Topics

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"
    }
  ]
}
```

Compliance validation for Amazon WorkDocs

Third-party auditors assess the security and compliance of Amazon WorkDocs as part of multiple AWS compliance programs. These compliance programs include SOC, PCI DSS, FedRAMP, HIPAA, ISO 9001, ISO 27001, ISO 27017, and ISO 27018.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading reports in AWS Artifact.

Your compliance responsibility when using Amazon WorkDocs is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- Architecting for HIPAA Security and Compliance Whitepaper – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- AWS Config – This AWS service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Resilience in Amazon WorkDocs

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between Availability Zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

Infrastructure security in Amazon WorkDocs

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

You use AWS published API calls to access Amazon WorkDocs through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support

cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

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 AD directory and an 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. 21).

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. 27) 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 Managing site settings (p. 31).
4. Under **Manage Users**, choose **Invite Users**. You can also edit user settings.

For more information, see Inviting and managing Amazon WorkDocs users (p. 36).

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. 27).
- 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 Managing site settings (p. 31).
4. Under **Manage Users**, choose **Invite Users**. You can also edit user settings.

For more information, see Inviting and managing Amazon WorkDocs users (p. 36).

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. 27).
- When you launch a new Amazon WorkDocs site, you must specify profile information for the administrator. This information includes first name, last name, and email address. Do not use **Admin** for your Amazon WorkDocs account user name. **Admin** is a reserved user role in Amazon WorkDocs.

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`.

All the users in the directory are added to your account as active Amazon WorkDocs users, by default. They can sign in and start using Amazon WorkDocs at any time. For more information about user roles, see User roles overview (p. 36).

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. Then 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 Managing site settings (p. 31).
4. (Optional) Under **Manage Users**, choose **Invite Users**. You can also edit user settings.

For more information, see Inviting and managing Amazon WorkDocs users (p. 36).

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

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. This information includes first name, last name, and email address. Do not use **Admin** for your Amazon WorkDocs account user name. **Admin** is a reserved user role in Amazon WorkDocs.

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`.

All the users in the directory are added to your account as active Amazon WorkDocs users by default. They can sign in and start using Amazon WorkDocs at any time. For more information about user roles, see User roles overview (p. 36).

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 Managing site settings (p. 31).
4. (Optional) Under **Manage Users**, choose **Invite Users**. You can also edit user settings.

For more information, see Inviting and managing Amazon WorkDocs users (p. 36).

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 an AWS Managed Microsoft AD. For more information, see How to Create a Microsoft AD directory.
- You must create a Trust Relationship between your AD directory and the AWS Managed Microsoft AD. For more information, see When to Create a Trust Relationship.
- When you launch a new Amazon WorkDocs site, you must specify profile information for the administrator. This information includes first name, last name, and email address. Do not use **Admin** for your Amazon WorkDocs account user name. **Admin** is a reserved user role in Amazon WorkDocs.

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`.

All the users in the directory are added to your account as active Amazon WorkDocs users by default. They can sign in and start using Amazon WorkDocs at any time. For more information about user roles, see User roles overview (p. 36).

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 Managing site settings (p. 31).
4. (Optional) Under **Manage Users**, choose **Invite Users**. You can also edit user settings.

For more information, see Inviting and managing Amazon WorkDocs users (p. 36).

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. Amazon WorkDocs administrators can enable single sign-on using the AWS Directory Service console. For more information, see Single sign-on in the *AWS Directory Service Administration Guide*.

After the Amazon WorkDocs administrator enables single sign-on, the Amazon WorkDocs site users might also need to modify their web browser settings to allow single sign-on. For more information, see Single sign-on for IE and Chrome and Single sign-on for Firefox in the *AWS Directory Service Administration 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. 37).

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. 37).

Managing site settings

Administrators can manage site-wide settings, such as choosing a preferred language for site content and email notifications, setting storage limits, and specifying recovery bin retention policy. Administrators can also change site security settings for public sharing, invites, and new users.

Preferred 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.

Hancom Online Editing and Office Online

Enable or disable **Hancom Online Editing** and **Office Online** settings from the **Admin control panel**. For more information, see Enabling collaborative editing (p. 44).

Storage

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. 37).

IP allow list

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 – public share settings

In the **Admin control panel**, under **Security**, choose **Who should be allowed to create 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.

Security – invite settings

Choose from the following settings for **Who should be allowed to join your WorkDocs site?**.

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.

Security – external invites

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

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.

Recovery bin retention

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 user 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. 36).

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.

Deploying Amazon WorkDocs Drive to multiple computers

If you have a domain-joined machine fleet, you can use Group Policy Objects (GPO) or System Center Configuration Manager (SCCM) to install the Amazon WorkDocs Drive client. You can download the client from https://amazonworkdocs.com/en/clients . As you go, remember that Amazon WorkDocs Drive requires HTTPS access on port 443 for all AWS IP addresses.

> **Note**
> As a best practice when using GPO or SCCM, install the Amazon WorkDocs Drive client after users log in.

The MSI installer for Amazon WorkDocs Drive supports the following optional installation parameters:

- **`SITEID`** – Pre-populates the Amazon WorkDocs site information for users during registration. For example, `SITEID`: *`site-name`*.
- **`DefaultDriveLetter`** – Pre-populates the drive letter to be used for mounting Amazon WorkDocs Drive. For example, `DefaultDriveLetter`: *`W`*.

Users can change the drive name, but not the drive letter, after they start Amazon WorkDocs Drive for the first time.

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. 29).

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. 37).

- **Admin**: 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. 29).
- **Power user**: A paid user of the site who can be given a special set of permissions by the administrator. For more information about how to set permissions for a **Power user**, see Security – public share settings (p. 32) and Security – external invites (p. 32).
- **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

Invite new users to join your directory from the admin control panel. You can also enable existing users to invite new users. For more information, see Security – invite settings (p. 32).

To invite new users

1. Sign in to Amazon WorkDocs using your administrator credentials.
2. Under **My Account**, choose **Open admin control panel**.
3. Under **Manage Users**, choose **Invite Users**.
4. 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 a link and instructions about how to create an Amazon WorkDocs account. The invitation link expires after 30 days.

Editing users

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

To edit users

1. Sign in to Amazon WorkDocs using your administrator credentials.
2. Under **My Account**, choose **Open admin control panel**.
3. Under **Manage Users**, choose the pencil icon (✎) next to the user's name.
4. 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. 38).

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. 36).

Storage

Specifies the storage limit for an existing user.

5. 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. Sign in to Amazon WorkDocs using your administrator credentials.
2. Under **My Account**, choose **Open admin control panel**.
3. Under **Manage Users**, choose the pencil icon (✎) next to the user's name.
4. 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. 38).

Deleting pending users (Simple AD only)

You can only delete Simple AD users that are in **Pending** status. To delete one of these users, choose the trash can icon (🗑) next to the user's name.

Your Amazon WorkDocs site must always have at least one active user that is not a guest user. 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.

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. 38).

To transfer document ownership

1. Sign in to Amazon WorkDocs using your administrator credentials.
2. Under **My Account**, choose **Open admin control panel**.

3. Under **Manage Users**, search for the inactive user.
4. Choose the pencil icon (✎) next to the inactive user's name.
5. Select **Transfer Document Ownership** and type the email address of the active user to whom to transfer the files.
6. Choose **Save Changes**.

   Warning
   This action cannot be undone.

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.

To download a list of users

1. Sign in to Amazon WorkDocs using your administrator credentials.
2. Under **My Account**, choose **Open admin control panel**.
3. Under **Manage Users**, choose **Download user**.
4. 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
5. 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. 36).

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. When users share a link, they can configure it to allow one of the following access options:

- All members of the Amazon WorkDocs site can search for, view, and comment on the file.
- Anyone with the link, even people who are not members of the Amazon WorkDocs site, can view the file. This link option restricts permissions 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 site settings (p. 31).

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.

Users can also create team folders to share by invite with directory groups that you create.

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. 36).

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 site settings (p. 31).

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.
- Download folder – Download a folder.
- 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
Download	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 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	
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			
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 ThinkFree

You can enable Hancom ThinkFree 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 Editing with Hancom ThinkFree.

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

To enable Hancom ThinkFree

Enable Hancom ThinkFree 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 ThinkFree

Disable Hancom ThinkFree 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**.

Migrating files to Amazon WorkDocs

Amazon WorkDocs administrators can use the Amazon WorkDocs Migration Service to perform a large-scale migration of multiple files and folders to their Amazon WorkDocs site. The Amazon WorkDocs Migration Service works with Amazon Simple Storage Service (Amazon S3). This lets you migrate departmental file shares and home drive or user file shares to Amazon WorkDocs.

During this process, Amazon WorkDocs provides an AWS Identity and Access Management (IAM) policy for you. Use this policy to create a new IAM role that grants access to the Amazon WorkDocs Migration Service to do the following:

- Read and list the Amazon S3 bucket that you designate.
- Read and write to the Amazon WorkDocs site that you designate.

Complete the following tasks to migrate your files and folders to Amazon WorkDocs. Before you begin, confirm that you have the following permissions:

- Administrator permissions for your Amazon WorkDocs site
- Permissions to create an IAM role

If your Amazon WorkDocs site is set up on the same directory as your Amazon WorkSpaces fleet, you must follow these requirements:

- Do not use **Admin** for your Amazon WorkDocs account user name. **Admin** is a reserved user role in Amazon WorkDocs.
- Your Amazon WorkDocs administrator user type must be **Upgraded WS User**. For more information, see User roles overview (p. 36) and Editing users (p. 37).

> **Note**
> Directory structure, file names, and file content are preserved when migrating to Amazon WorkDocs. File ownership and permissions are not preserved.

Tasks

Step 1: Preparing for migration

To prepare for migration

1. On your Amazon WorkDocs site, under **My Documents**, create a folder that you want to migrate your files and folders to.
2. Confirm that the files to be migrated are less than 5 TB each. Each file name must be 255 characters or fewer. Amazon WorkDocs Drive displays only files with a full directory path of 260 characters or fewer.

Warning
Attempting to migrate files or folders with names containing the following characters can cause errors and stop the migration process. If this occurs, choose **Download report** to download a log listing the errors, the files that failed to migrate, and any successfully migrated files.

- **Trailing spaces**–For example: an extra space at the end of a file name.
- **Periods at the beginning or end**–For example: `.file`, `.file.ppt`, `.`, `..`, or `file.`
- **Tildes at the beginning or end**–For example: `file.doc~`, `~file.doc`, or `~$file.doc`
- **File names ending in `.tmp`**–For example: `file.tmp`
- **File names exactly matching these case-sensitive terms**–`Microsoft User Data`, `Outlook files`, `Thumbs.db`, or `Thumbnails`
- **File names containing any of these characters**–`*` (asterisk), `/` (forward slash), `\` (back slash), `:` (colon), < (less than), > (greater than), `?` (question mark), `|` (vertical bar/pipe), `"` (double quotes), or `\202E` (character code 202E).

Step 2: Uploading files to Amazon S3

To upload files to Amazon S3

1. Create a new Amazon Simple Storage Service (Amazon S3) bucket in your AWS account that you want to upload your files and folders to. The Amazon S3 bucket must be in the same AWS account and AWS Region as your Amazon WorkDocs site. For more information, see Getting started with Amazon Simple Storage Service in the *Amazon Simple Storage Service Getting Started Guide*.
2. Upload your files to the Amazon S3 bucket that you created in the previous step. We recommend using AWS DataSync to upload your files and folders to the Amazon S3 bucket. DataSync provides additional tracking, reporting, and syncing features. For more information, see How AWS DataSync works and Using identity-based policies (IAM policies) for DataSync in the *AWS DataSync User Guide*.

Step 3: Scheduling a migration

After you complete steps 1 and 2, use the Amazon WorkDocs Migration Service to schedule the migration. When you schedule the migration, your Amazon WorkDocs user account **Storage** setting is automatically changed to **Unlimited**.

Note
Migrating files that exceed your Amazon WorkDocs storage limit can result in additional costs. For more information, see Amazon WorkDocs Pricing.

The Amazon WorkDocs Migration Service provides an AWS Identity and Access Management (IAM) policy for you to use for the migration. With this policy, you create a new IAM role that grants the Amazon WorkDocs Migration Service access to the Amazon S3 bucket and Amazon WorkDocs site that you designate. You also subscribe to Amazon SNS email notifications to receive updates when your migration request is scheduled, and when it begins and ends.

To schedule a migration

1. From the Amazon WorkDocs console, choose **Apps**, **Migrations**.
   - If this is your first time accessing Amazon WorkDocs Migration Service, you are prompted to subscribe to Amazon SNS email notifications. Subscribe, confirm in the email message that you receive, then choose **Continue**.
2. Choose **Create Migration**.
3. For **Source Type**, choose **Amazon S3**.

4. Choose **Next**.
5. For **Data Source & Validation**, under **Sample Policy**, copy the supplied IAM policy.
6. Use the IAM policy that you copied in the previous step to create a new IAM policy and role, as follows:

    a. Open the IAM console at https://console.aws.amazon.com/iam/.
    b. Choose **Policies**, **Create policy**.
    c. Choose **JSON** and paste in the IAM policy that you copied to your clipboard earlier.
    d. Choose **Review policy**. Enter a policy name and description.
    e. Choose **Create policy**.
    f. Choose **Roles**, **Create role**.
    g. Select **Another AWS account**. For **Account ID**, enter one of the following:

        - For the US East (N. Virginia) Region, enter `899282061130`
        - For the US West (Oregon) Region, enter `814301586344`
        - For the Asia Pacific (Singapore) Region, enter `900469912330`
        - For the Asia Pacific (Sydney) Region, enter `031131923584`
        - For the Asia Pacific (Tokyo) Region, enter `178752524102`
        - For the Europe (Ireland) Region, enter `191921258524`

    h. Select the new policy that you created and choose **Next: Review**. If you don't see the new policy, choose the refresh icon.
    i. Enter a role name and description. Choose **Create role**.
    j. On the **Roles** page, under **Role name**, choose the role name that you created.
    k. On the **Summary** page, change the **Maximum CLI/API session duration** to 12 hours.
    l. Copy the **Role ARN** to your clipboard to use in the next step.
7. Return to the **Amazon WorkDocs Migration Service**. For **Data Source & Validation**, under **Role ARN**, paste the role ARN from the IAM role that you copied in the previous step.
8. For **Bucket**, select the Amazon S3 bucket to migrate the files from.
9. Choose **Next**.
10. For **Select a destination WorkDocs Folder**, select the destination folder in Amazon WorkDocs to migrate the files to.
11. Choose **Next**.
12. Under **Review**, for **Title**, enter a name for the migration.
13. Select the date and time for the migration.
14. Choose **Send**.

Step 4: Tracking a migration

You can track your migration from within the Amazon WorkDocs Migration Service landing page. To access the landing page from the Amazon WorkDocs site, choose **Apps**, **Migrations**. Choose your migration to view its details and track its progress. You can also choose **Cancel Migration** if you need to cancel it, or choose **Update** to update the timeline for the migration. After a migration is complete, you can choose **Download report** to download a log of the successfully migrated files, any failures, or errors.

The following migration states provide the status of your migration:

Scheduled

The migration is scheduled but not started. You can cancel migrations or update migration start times up to five minutes before the scheduled start time.

Migrating

The migration is in progress.

Success

The migration is complete.

Partial Success

The migration is partially complete. For more details, view the migration summary and download the provided report.

Failed

The migration failed. For more details, view the migration summary and download the provided report.

Canceled

The migration is canceled.

Step 5: Cleaning up resources

When your migration is complete, delete the migration policy and role that you created from the IAM console.

To delete the IAM policy and role

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. Choose **Policies**.
3. Search for and select the policy that you created.
4. For **Policy actions**, choose **Delete**.
5. Choose **Delete**.
6. Choose **Roles**.
7. Search for and select the role that you created.
8. Choose **Delete role**, **Delete**.

When a scheduled migration starts, your Amazon WorkDocs user account **Storage** setting is automatically changed to **Unlimited**. After the migration, you can change your **Storage** settings by editing your user account from the admin control panel. For more information, see Editing users (p. 37).

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, select the AWS Region during setup. For more information, see the tutorial for your particular use case under Getting started with Amazon WorkDocs (p. 19).

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 transfer document ownership

Transfer document ownership to another user in the admin control panel. For more information, see Transferring document ownership (p. 38).

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 Identity and access management for Amazon WorkDocs (p. 4).

Online editing isn't working

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

Managing Amazon WorkDocs for Amazon Business

If you are an administrator for Amazon WorkDocs for Amazon Business, you can manage users by signing in to https://workdocs.aws/ using your Amazon Business credentials.

To invite a new user to Amazon WorkDocs for Amazon Business

1. Sign in with your Amazon Business credentials at https://workdocs.aws/.
2. On the Amazon WorkDocs for Amazon Business home page, open the navigation pane on the left.
3. Choose **Admin Settings**.
4. Choose **Add people**.
5. For **Recipients**, enter the email addresses or user names of the users to invite.
6. (Optional) Customize the invitation message.
7. Choose **Done**.

To search for a user on Amazon WorkDocs for Amazon Business

1. Sign in with your Amazon Business credentials at https://workdocs.aws/.
2. On the Amazon WorkDocs for Amazon Business home page, open the navigation pane on the left.
3. Choose **Admin Settings**.
4. For **Search users**, enter the first name of the user, and press **`Enter`**.

To select user roles on Amazon WorkDocs for Amazon Business

1. Sign in with your Amazon Business credentials at https://workdocs.aws/.
2. On the Amazon WorkDocs for Amazon Business home page, open the navigation pane on the left.
3. Choose **Admin Settings**.
4. Under **People**, next to the user, select the **Role** to assign to the user.

To delete a user on Amazon WorkDocs for Amazon Business

1. Sign in with your Amazon Business credentials at https://workdocs.aws/.
2. On the Amazon WorkDocs for Amazon Business home page, open the navigation pane on the left.
3. Choose **Admin Settings**.
4. Under **People**, choose the ellipsis (**...**) next to the user.
5. Choose **Delete**.
6. If prompted, enter a new user to transfer the user's files to, and choose **Delete**.

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
Managing Amazon WorkDocs for Amazon Business (p. 53)	Amazon WorkDocs for Amazon Business supports user management by administrators. For more information, see Managing Amazon WorkDocs for Amazon Business in the Amazon WorkDocs Administration Guide.	March 26, 2020
Migrating files to Amazon WorkDocs (p. 53)	Amazon WorkDocs administrators can use the Amazon WorkDocs Migration Service to perform a large-scale migration of multiple files and folders to their Amazon WorkDocs site. For more information, see Migrating files to Amazon WorkDocs in the Amazon WorkDocs Administration Guide.	August 8, 2019
IP allow list settings (p. 53)	**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 ThinkFree (p. 53)	Hancom ThinkFree is available. Users can create and collaboratively edit Microsoft Office files from the Amazon WorkDocs web application. For more information, see Enabling Hancom ThinkFree in the Amazon WorkDocs Administration Guide.	June 21, 2018
Open with Office Online (p. 53)	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. 53)	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. 53)	Recovery bin retention period can be modified. For more information, see Recovery bin retention settings in the Amazon WorkDocs Administration Guide.	February 27, 2018

AWS glossary

For the latest AWS terminology, see the AWS glossary in the *AWS General Reference*.