Amazon WorkDocs

Administration Guide

aws

Amazon WorkDocs: Administration Guide

Table of Contents

What is Amazon WorkDocs?

Amazon WorkDocs is a fully managed, secure enterprise storage and sharing service with strong administrative controls and feedback capabilities that improve user productivity. Files are stored in the cloud, safely and securely. Your user's files are only visible to them, and their designated contributors and viewers. Other members of your organization do not have access to other user's files unless they are specifically granted access.

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

For more information, see Amazon WorkDocs.

Accessing Amazon WorkDocs

Administrators use the Amazon WorkDocs console to create and deactivate Amazon WorkDocs sites. With the admin control panel, they can manage users, storage, and security settings. For more information, see Managing Amazon WorkDocs from the site admin control panel (p. 26) and Inviting and managing Amazon WorkDocs users (p. 30).

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.
- Amazon WorkDocs Drive, an app that synchronizes a folder on your macOS or Windows desktop with 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, see Creating an Amazon WorkDocs site (p. 19).

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 (p. 2)
- Create IAM users and groups (recommended) (p. 2)

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.

   When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to an administrative user, and use only the root user to perform tasks that require root user access.

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. 3).

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** – The AWS service that you use determines your responsibility. You are also responsible for other factors, including the sensitivity of your data, your company's requirements, and applicable laws and regulations. The topics in this section help you understand how to apply the shared responsibility model when using Amazon WorkDocs.

> **Note**
> The users in a given WorkDocs organization can collaborate with users outside that organization by sending a link or invitation to a file. Review the the shared link settings (p. 32) for your site and select the option that best meets your company's requirements.

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

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that 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 service users 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. You must be *authenticated* (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (successor to AWS Single Sign-On) (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see How to sign in to your AWS account in the *AWS Sign-In User Guide*.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see Signature Version 4 signing process in the *AWS General Reference*.

Regardless of the authentication method that you use, you might 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 Multi-factor authentication in the *AWS IAM Identity Center (successor to AWS Single Sign-On) User Guide* and Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one 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 don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the *AWS Account Management Reference Guide*.

IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see Rotate access keys regularly for use cases that require long-term credentials in the *IAM User Guide*.

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:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see Creating a role for a third-party Identity Provider in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see Permission sets in the *AWS IAM Identity Center (successor to AWS Single Sign-On) User Guide*.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **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*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
    - **Principal permissions** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you

might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see in the *Service Authorization Reference*.

- **Service role** – A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Creating a role to delegate permissions to an AWS service in the *IAM User Guide*.

- **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform 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.

- **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 or IAM users, 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 AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) 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*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

Every IAM entity (user or role) starts with no permissions. 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, group of users, or role. These policies control what actions users and roles 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. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Access control lists

Access control lists (ACLs) control 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 an 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*.

  Note
  Amazon WorkDocs doesn't support Service Control Policies for Slack Organizations.

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 need to understand which 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 (p. 8)
- Amazon WorkDocs resource-based policies (p. 9)
- Authorization based on Amazon WorkDocs tags (p. 9)
- Amazon WorkDocs IAM roles (p. 9)

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

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions 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*"
```

> **Note**
> To ensure backward compatibility, include the `zocalo` action. For example:
>
> ```
> "Action": [
> "zocalo:*",
> "workdocs:*"
> ```

```
    ],
```

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.

> **Note**
> To ensure backward compatibility, include the `zocalo` action in your policies. For example:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
            "zocalo:*",
            "workdocs:*"
            ],
            "Resource": "*"
        }
    ]
}
```

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 (p. 10)
- Using the Amazon WorkDocs console (p. 11)
- Allow users to view their own permissions (p. 11)
- Allow users read-only access to Amazon WorkDocs resources (p. 12)
- More Amazon WorkDocs identity-based policy examples (p. 12)

Policy best practices

Identity-based policies 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 with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see AWS managed policies or AWS managed policies for job functions in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they

are used through a specific AWS service, such as AWS CloudFormation. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.

- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see IAM Access Analyzer policy validation in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or root users in your account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Configuring MFA-protected API access in the *IAM User Guide*.

For more information about best practices in IAM, see Security best practices in IAM 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 (p. 13)
- I am not authorized to perform iam:PassRole (p. 13)

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, your policies must be updated 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 that are 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's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

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
- Exporting the site-wide activity feed (p. 14)
- Using AWS CloudTrail to log Amazon WorkDocs API calls (p. 15)

Exporting the 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**.
2. Choose **Filter**, then move the **Site-wide activity** slider to turn the filter on.
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 system exports the files to one of the following locations:

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

The exported file reflects any filters that you apply.

> **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*.

Using AWS CloudTrail to log Amazon WorkDocs API calls

You can use AWS CloudTrail; to log Amazon WorkDocs API calls. CloudTrail 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 create a trail, you can still view the most recent events in the CloudTrail console in **Event history**.

The information collected by CloudTrail includes requests, the IP addresses from which the requests were made, the users who made the requests, and the request dates.

For more information 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",
        "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. In turn, you attach a directory to a site when you provision that site. When you do, an Amazon WorkDocs feature called Auto activation adds the users in the directory to the site as managed users, meaning they don't need separate credentials to log in to your site, and they can share and collaborate on files. Each user has 1 TB of storage unless they purchase more.

You no longer need to add and activate users manually, though you still can. You can also change user roles and permissions whenever you need to. For more information about doing that, see Inviting and managing Amazon WorkDocs users (p. 30), later in this guide.

If you need to create directories, you can:

- Create a Simple AD directory.
- Create an AD Connector directory to connect to your on-premises directory.
- Enable Amazon WorkDocs to work with an existing AWS directory.
- 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 belong to a compliance program such as PCI, FedRAMP, or DoD, you must set up an AWS Managed Microsoft AD Directory to meet compliance requirements. The steps in this section explain how to use an existing Microsoft AD Directory. For information about creating a Microsoft AD Directory, see AWS Managed Microsoft AD in the *AWS Directory Service Administration Guide*.

Contents

Creating an Amazon WorkDocs site

The steps in the following sections explain how to set up a new Amazon WorkDocs site.

Tasks

Before you begin

You must have the following items before you create an Amazon WorkDocs site.

- An AWS account for creating and administering Amazon WorkDocs sites. However, users do not need an AWS account to connect to and use Amazon WorkDocs. For more information, see Prerequisites for Amazon WorkDocs (p. 2).
- If you plan to use Simple AD, you must meet the prerequisites identified in Simple AD Prerequisites in the *AWS Directory Service Administration Guide*.
- An AWS Managed Microsoft AD Directory if you belong to a compliance program such as PCI, FedRAMP, or DoD. The steps in this section explain how to use an existing Microsoft AD Directory. For information about creating a Microsoft AD Directory, see AWS Managed Microsoft AD in the *AWS Directory Service Administration Guide*.
- Profile information for the administrator, including first and last name, and an email address.

Creating an Amazon WorkDocs site

Follow these steps to create an Amazon WorkDocs site in minutes.

To create the Amazon WorkDocs site

1. Open the Amazon WorkDocs console at https://console.aws.amazon.com/zocalo/.
2. On the console's Home page, under **Create a WorkDocs site**, choose **Get Started now**.

   —OR—

   In the navigation pane, choose **My sites**, and on the **Manage your WorkDocs sites** page, choose **Create a WorkDocs site**.

   What happens next depends on whether you have a directory.

   - If you have a directory, The **Select a directory** page appears and allows you to choose an existing directory or create a directory.
   - If you don't have a directory, the **Set up a directory type** page appears and allows you to create a Simple AD or AD Connector directory

   The following steps explain how to do both tasks.

   To use an existing directory

   1. Open the **Available directories** list and choose the directory that you want to use.
   2. Choose **Enable directory**.

   To create a directory

   1. Repeat steps 1 and 2 above.

      At this point, what you do depends on whether you want to use Simple AD or create an AD Connector.

      To use Simple AD

      a. Choose **Simple AD**, then choose **Next**.

         The **Create Simple AD site page appears.**

      b. Under **Access point**, in the **Site URL** box, enter the URL for the site.

c. Under **Set WorkDocs administrator**, enter the administrator's email address, first name, and last name.

d. As needed, complete the options under **Directory details** and **VPC configuration**.

e. Choose **Create Simple AD site**.

To create an AD Connector directory

a. Choose **AD Connector**, then choose **Next**.

The **Create AD Connector site** page appears.

b. Complete all the fields under **Directory details**.

c. Under **Access point**, in the **Site URL** box, enter your site's URL.

d. As desired, complete the optional fields under **VPC configuration**.

e. Choose **Create AD Connector site**.

Amazon WorkDocs does the following:

- If you chose **Set up a VPC on my behalf** in step 4 above, Amazon WorkDocs creates a VPC for you. A directory in the VPC stores user and Amazon WorkDocs site information.

- If you used Simple AD, Amazon WorkDocs creates a Directory User and sets that user as an Amazon WorkDocs administrator. If you created an AD Connector directory, Amazon WorkDocs sets the exisitng directory user that you provided as a WorkDocs administrator.

- If you used an existing directory, Amazon WorkDocs prompts you to enter the user name of the Amazon WorkDocs administrator. The user must be a member of the directory.

Note
Amazon WorkDocs doesn't notify users about the new site. You need to communicate the URL to them, and let them know that they don't need a separate login to use the site.

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 use the AWS Directory Services Console at https://console.aws.amazon.com/directoryservicev2/ to enable multi-factor authentication for your AD Connector directory. To enable MFA, you must have an MFA solution that is a Remote authentication dial-in user service (RADIUS) server, or you must have an MFA plugin to a RADIUS server already implemented in your on-premises infrastructure. Your MFA solution should implement One Time Passcodes (OTP) that users obtain from a hardware device or from software running on a device such as a cell phone.

RADIUS is an industry-standard client/server protocol that provides authentication, authorization, and accounting management to enable users to connect to network services. AWS Managed Microsoft AD includes a RADIUS client that connects to the RADIUS server upon which you have implemented your MFA solution. Your RADIUS server validates the username and OTP code. If your RADIUS server successfully validates the user, AWS Managed Microsoft AD then authenticates the user against AD. Upon successful AD authentication, users can then access the AWS application. Communication between the AWS Managed Microsoft AD RADIUS client and your RADIUS server require you to configure AWS security groups that enable communication over port 1812.

For more information, see Enable multi-factor authentication for AWS Managed Microsoft AD in the *AWS Directory Service Administration Guide*.

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

Promoting a user to administrator

Use the Amazon WorkDocs console to promote a user to administrator. Remember, you can only promote activated users. For more information about activating users, see Editing users (p. 34).

To promote a user to administrator

1. Open the Amazon WorkDocs console at https://console.aws.amazon.com/zocalo/.
2. In the navigation pane, choose **My sites**.

    The **Manage your WorkDocs Sites** page appears.
3. Select the button next to the desired site, choose **Actions**, then choose **Set an administrator**.

    The **Set WorkDocs administrator** dialog box appears.
4. In the **Username** box, enter the user name of the person that you want to promote, then choose **Set administrator**.

You can also use the Amazon WorkDocs site admin control panel to demote an administrator. For more information, see Editing users (p. 34).

Managing Amazon WorkDocs from the AWS console

You use these tools to manage your Amazon WorkDocs sites:

* The AWS console at https://console.aws.amazon.com/zocalo/.
* The site admin control panel, available to administrators on all Amazon WorkDocs sites.

Each of those tools provides a different set of actions, and the topics in this section explain the actions provided by the AWS console. For information about the site admin control panel, see Managing Amazon WorkDocs from the site admin control panel (p. 26).

Setting site administrators

If you're an administrator, you can give users access to the site control panel and the actions that it provides.

To set an administrator

1. Open the Amazon WorkDocs console at https://console.aws.amazon.com/zocalo/.
2. In the navigation pane, choose **My sites**.

   The **Manage your WorkDocs sites** page appears and displays a list of your sites.
3. Choose the button next to the site for which you want to set an administrator.
4. Open the **Actions** list and choose **Set an administrator**.

   The **Set WorkDocs administrator** dialog box appears.
5. In the **Username** box, enter the new administrator's name, then choose **Set administrator**.

Resending invitation emails

You can resend an invitation email at any time.

To resend the invitation email

1. Open the Amazon WorkDocs console at https://console.aws.amazon.com/zocalo/.
2. In the navigation pane, choose **My sites**.

   The **Manage your WorkDocs sites** page appears and displays a list of your sites.
3. Choose the button next to the site for which you want to resend the email.
4. Open the **Actions** list and choose **Resend invitation email**.

   A success message in a green banner appears at the top of the page.

Managing multifactor authentication

You can enable multi-factor authentication after you create an Amazon WorkDocs site. For more information about authentication, see Enabling multi-factor authentication (p. 21).

Setting site URLs

Note
If you followed the site creation process in Getting started with Amazon WorkDocs (p. 19), you entered a site URL. As a result, Amazon WorkDocs makes the **Set site URL** command unavailable, because you can only set a URL once. You only follow these steps if you deploy Amazon WorkSpaces and integrate it with Amazon WorkDocs. The Amazon WorkSpaces integration process has you enter a serial number instead of a site URL, so you have to enter a URL after you finish the integration. For more information about integrating Amazon WorkSpaces and Amazon WorkDocs see Integrate with WorkDocs in the *Amazon WorkSpaces User Guide*.

To set a site URL

1. Open the Amazon WorkDocs console at https://console.aws.amazon.com/zocalo/.
2. In the navigation pane, choose **My sites**.

   The **Manage your WorkDocs sites** page appears and displays a list of your sites.
3. Select the site that you integrated with Amazon WorkSpaces. The URL contains the directory ID of your Amazon WorkSpaces instance, such as **https://{directory_id}.awsapps.com**.
4. Choose the button next to that URL, open the **Actions** list, and choose **Set site URL**.

   The **Set site URL** dialog box appears.
5. In the **Site URL** box, enter the URL for the site, then choose **Set site URL**.
6. On the **Manage your WorkDocs sites** page, choose **Refresh** to see the new URL.

Managing notifications

Notifications allow IAM users or roles to call the CreateNotificationSubscription API, which you can use to set your own endpoint for processing the SNS messages that WorkDocs sends. For more information about notifications, see Setting up notifications for an IAM user or role in the *Amazon WorkDocs Developer Guide*.

You can create and delete notifications, and the following steps explain how to do both tasks.

To create a notification

1. Open the Amazon WorkDocs console at https://console.aws.amazon.com/zocalo/.
2. In the navigation pane, choose **My sites**.

   The **Manage your WorkDocs sites** page appears and displays a list of your sites.
3. Choose the button next to the desired site.
4. Open the **Actions** list and choose **Manage notifications**.

   The **Set WorkDocs administrator** dialog box appears.
5. In the **Username** box, enter the new administrator's name, then choose **Set administrator**.

To delete a notification

1. Open the Amazon WorkDocs console at https://console.aws.amazon.com/zocalo/.
2. In the navigation pane, choose **My sites**.

   The **Manage your WorkDocs sites** page appears and displays a list of your sites.
3. Choose the button next to the site for which you want to set an administrator.
4. Open the **Actions** list and choose **Set an administrator**.

   The **Set WorkDocs administrator** dialog box appears.
5. In the **Username** box, enter the new administrator's name, then choose **Set administrator**.

Deleting a site

Use the Amazon WorkDocs console to delete a site.

> **Warning**
> You lose all 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. In the navigation bar, choose **My sites**.

   The **Manage your WorkDocs sites** page appears.
3. Choose the button next to the site that you want to delete, then choose **Delete**.

   The **Delete** *site URL* dialog box appears.
4. Optionally, choose **Also delete the user directory**.

   > **Important**
   > If you don't provide your own directory for Amazon WorkDocs, we create one for you. When you delete the Amazon WorkDocs site, you are charged for the directory that we create unless you delete that directory or use it for another AWS application. For pricing information, see AWS Directory Service Pricing.
5. In the **Site URL** box, enter the site URL, then choose **Delete**.

   The site is immediately deleted and is no longer available.

Managing Amazon WorkDocs from the site admin control panel

You use these tools to manage your Amazon WorkDocs sites:

- The site admin control panel, available to administrators on all Amazon WorkDocs sites, and described in the following topics.
- The AWS console at https://console.aws.amazon.com/zocalo/.

Each of those tools provides a different set of actions. The topics in this section explain the actions provided by the site admin control panel. For information about the tasks available in the console, see Managing Amazon WorkDocs from the AWS console (p. 23).

Preferred language settings

You can specify the language for 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. 41).

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. 34).

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, 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 **Change**. Under **Who should be allowed to create publicly shareable links**, choose from the following settings:

Under **Choose your setting for shareable links**, select an option:

- **Users cannot send internal view links.** – Disables link sharing for all users.
- **Users cannot send external view links.** – Limits link sharing to just site members. Managed users can create this type of link.
- **Users can send external view links to anyone.** – Managed users can create site-wide links, but only power users can create public links. Public links allow access to anyone on the internet.
- **Users cannot send external view links to a few specific domains.** – Managed users can create public links.

Security – invitation settings

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

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

Users can invite 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 invitations

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

When a user deletes a file, Amazon WorkDocs stores the file in the user's recycle bin for 30 days. Afterwards, Amazon WorkDocs moves the files to a temporary recovery bin for 60 days, then deletes them permanently. Only administrators can see the temporary recovery bin. By changing the site-wide data retention policy, site administrators can change the recovery bin retention period to a minimum of zero days and maximum of 365.

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. Enter the number of days to retain files in the recovery bin, and choose **Save**.

   Note
   The default retention period is 60 days. You can use a period of 0–365 days.

Administrators can restore user files from the recovery bin before Amazon WorkDocs deletes them permanently.

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. 30).

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. You'll also want to confirm that your target systems meet the installation requirements for Amazon WorkDocs Drive. For more information, see Installing Amazon WorkDocs Drive in the *Amazon WorkDocs User Guide*.

> **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*. Remember, each user must have a different drive letter. Also, users can change the drive name, but not the drive letter, after they start Amazon WorkDocs Drive for the first time.

The following example deploys Amazon WorkDocs Drive with no user interfaces and no restarts. Note that it uses the MSI file's default name:

```
msiexec /i "AWSWorkDocsDriveClient.msi" SITEID=your_workdocs_site_ID
DefaultDriveLetter=your_drive_letter REBOOT=REALLYSUPPRESS /norestart /qn
```

Inviting and managing Amazon WorkDocs users

By default, when you attach a directory during site creation, the Auto activation feature in Amazon WorkDocs adds all the users in that directory to the new site as *managed users*.

In WorkDocs, managed users don't need to log in with separate credentials. They can share and collaborate on files, and they automatically have 1 TB of storage. However, you can turn Auto activation off when you only want to add some of the users in a directory, and steps in the next sections explain how to do that.

In addition, you can invite, enable, or disable users, and change user roles and settings. You can also promote a user to an administrator. For more information about promoting users, see Promoting a user to administrator (p. 22).

You do those tasks in the admin control panel in the Amazon WorkDocs web client, and the steps in the following sections explain how. But, if you're new to Amazon WorkDocs, take a few minutes and learn about the various user roles before you dive into administrative tasks.

Contents

User roles overview

Amazon WorkDocs defines the following user roles. You can change users' roles by editing their user profiles. For more information, see Editing users (p. 34).

- **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. 22).
- **Power user**: A paid user who has a special set of permissions from the administrator. For more information about how to set permissions for a Power user, see Security – public share settings (p. 27) and Security – external invitations (p. 28).
- **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. You can upgrade Guest users to the User, Power user, or Administrator roles.

   Note
   When you change a guest user's role, you perform a one-time action that you cannot reverse.

Amazon WorkDocs also defines these additional user types.

WS user

A user with an assigned 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 with an assigned WorkSpaces WorkSpace and upgraded storage.

- 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 without an assigned 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

Starting the admin control panel

You use the administrative control panel in the Amazon WorkDocs web client to turn Auto activation off and on, and change user roles and settings.

To open the admin control panel

1. Choose the profile icon in the upper-right corner of the WorkDocs client.

2. Under **Admin**, choose **Open admin control panel**.

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

Turning off Auto activation

You turn off Auto activation when you don't want to add all the users in a directory to a new site, and when you want to set different permissions and roles for the users that you invite to a new site. When

you turn Auto activation off, you can also decide who has the ability to invite new users to the site —
current users, power users, or administrators. These steps explain how to do both tasks.

To turn off Auto activation

1. Choose the profile icon in the upper-right corner of the WorkDocs client.

2. Under **Admin**, choose **Open admin control panel**.
3. Scroll down to **Security** and choose **Change**.

    The **Policy Settings** dialog box appears.
4. Under **Auto activation**, clear the check box next to **Allow all users in your directory to be
    automatically activated upon their first login to your WorkDocs site.**

    The options change under **Who should be allowed to activate directory users in your WorkDocs
    site**. You can let current users invite new users, or you can give that ability to power users or other
    administrators.
5. Select an option, then choose Save Changes.

    Repeat steps 1-4 to re-enable Auto activation.

Managing link sharing

This topic explains how to manage link sharing. Amazon WorkDocs users can share their files and folders
by sharing links to them. They can share file links inside and outside your organization, but they can only
share folder links internally. As an administrator, you manage who can share links.

To enable link sharing

1. Choose the profile icon in the upper-right corner of the WorkDocs client.

2. Under **Admin**, choose **Open admin control panel**.
3. Scroll down to **Security** and choose **Change**.

    The **Policy Settings** dialog box appears.
4. Under **Choose your setting for shareable links**, select an option:

    *   **Do not allow site-wide links** – Disables link sharing for all users.
    *   **Allow site-wide shareable links, but do not allow public shareable links** – Limits link sharing to
        just site members. Managed users can create this type of link.
    *   **Only power users can create public shareable links** – Managed users can create site-wide links,
        but only power users can create public links. Public links allow access to anyone on the internet.
    *   **All managed users can create public shareable links** – Managed users can create public links.
5. Choose **Save Changes**.

Controlling user invitations with Auto activation enabled

When you enable Auto activation—and remember, it's on by default—you can give users the ability to invite other users. You can grant permission to one of the following:

- All users
- Power users
- Administrators.

You can also disable permissions entirely, and these steps explain how.

To set invitation permissions

1. Choose the profile icon in the upper-right corner of the WorkDocs client.

2. Under **Admin**, choose **Open admin control panel**.
3. Scroll down to **Security** and choose **Change**.

    The **Policy Settings** dialog box appears.
4. Under **Who should be allowed to activate directory users in your WorkDocs site**, select the **Share with external users** check box, select one of the options below the check box, then choose **Save Changes**.

    —OR—

    Clear the check box if you don't want anyone to invite new users, then choose **Save Changes**.

Inviting new users

You can invite new users to join a directory. You can also enable existing users to invite new users. For more information, see Security – invitation settings (p. 27).

To invite new users

1. Choose the profile icon in the upper-right corner of the WorkDocs client.

2. Under **Admin**, 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?**, enter the invitee's email address, and choose **Send**. Repeat this step for each invitation.

Amazon WorkDocs sends an invitation email to each recipient. The mail contains a link and instructions about how to create an Amazon WorkDocs account. The invitation link expires after 30 days.

Editing users

You can change user information and settings.

To edit users

1. Choose the profile icon in the upper-right corner of the WorkDocs client.

2. Under **Admin**, 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 whether the user is **Active** or **Inactive**. For more information, see Disabling users (p. 34).

    Role

    > Specifies whether someone is a user or administrator. You can also upgrade or downgrade users that have an WorkSpaces WorkSpace assigned to them. For more information, see User roles overview (p. 30).

    Storage

    > Specifies the storage limit for an existing user.

5. Choose **Save Changes**.

Disabling users

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

To change user status to Inactive

1. Choose the profile icon in the upper-right corner of the WorkDocs client.

2. Under **Admin**, 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 can't access 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 an inactive user's files and folders to an active user. For more information, see Transferring document ownership (p. 35).

Deleting pending users

You can delete Simple AD, AWS Managed Microsoft, and AD Connector users in **Pending** status. To delete one of those users, choose the trash can icon ( ) next to the user's name.

Your Amazon WorkDocs site must always have at least one active user who is not a guest user. If you need to delete all users, delete the entire site (p. 25).

We do not recommend that you delete registered users. Instead, you should switch a user from **Active** to **Inactive** status to prevent them from accessing 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 deactivate a user, see Disabling users (p. 34).

> **Warning**
> You can't undo this action.

To transfer document ownership

1. Choose the profile icon in the upper-right corner of the WorkDocs client.

2. Under **Admin**, 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 enter the new owner's email address.
6. Choose **Save Changes**.

Downloading user lists

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. Choose the profile icon in the upper-right corner of the WorkDocs client.

2. Under **Admin**, 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. WorkDocs saves the file to one of the following locations:

   - **Windows** – `Downloads/WorkDocsDownloads`
   - **macOS** – *hard drive*`/users/`*username*`/WorkDocsDownloads/folder`

     Note
     Downloads may take some time. Also, downloaded files do not land in your `/~users` folder.

For more information about these user roles, see User roles overview (p. 30).

Sharing and collaboration

Your users can share content by sending a link or an invite. Users can also collaborate with external users if you enable external sharing.

Amazon WorkDocs controls access to folders and files through the use of permissions. The system applies permissions based on a user's role.

Contents

Sharing links

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 Amazon WorkDocs from the site admin control panel (p. 26).

Sharing 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 without incurring extra costs. Site users can share files and folders with external users without requiring recipients to be paid users of the Amazon WorkDocs site. When you

enable external sharing, users can enter 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 enter 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. 30).

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 Amazon WorkDocs from the site admin control panel (p. 26).

Permissions

Amazon WorkDocs uses permissions to control access to folders and files. Permissions are applied based on user roles.

Contents

User roles

User roles control folder and file permissions. You can apply the following user roles at the folder level:

- **Folder owner** – The owner of a folder or file.
- **Folder co-owner** – A user or group that the owner designates as the co-owner of a folder or file.
- **Folder contributor** – Someone with unlimited access to a folder.
- **Folder viewer** – Someone with limited access (read-only permissions) to a folder.

You can apply the following user roles at the individual file level:

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

Permissions for shared folders

The following permissions apply to user roles for shared folders:

> **Note**
> Permissions applied for a folder also apply to the sub-bolders and files in that folder.

- **View** – View the contents of a shared folder.
- **View sub-folders** – 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.

	View	View sub-folders	View shares	Download folder	Add sub-folder	Share	Revoke share	Delete sub-folder	Delete top-level folder
Folder owner	✓	✓	✓	✓	✓	✓	✓	✓	✓
Folder co-owner	✓	✓	✓	✓	✓	✓	✓	✓	✓
Folder contributor	✓	✓	✓	✓	✓				
Folder viewer	✓	✓	✓	✓					

Permissions for files in shared folders

The following permissions apply to user roles for files in a shared folder:

- **Annotate** – Add feedback to a file.
- **Delete** – Delete a file in a shared folder.
- **Rename** – Rename files.
- **Upload** – Upload new versions of a file.
- **Download** – Download a file.
- **Prevent download** – Prevent a file from being downloaded. This is the default permission for files in the folder.

> **Note**
> When the owner or co-owner of an MP4 file disallows downloads for that file, contributors and viewers cannot play it in the Amazon WorkDocs web client.

- **Share** – Share a file with other users.
- **Revoke sharing** – Revoke the sharing of a file.
- **View** – View a file in a shared folder.
- **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.
- **Delete versions** – Delete one or more versions of a file.
- **Recover versions** – Recover one or more deleted versions of a file.
- **View all private comments** – Owner/co-owner can see all private comments for a document, even if they are not replies to their comment.

	Annotate	Delete	Rename	Upload	Download	Prevent download	Share	Revoke share	View shared	View annotations	View activity	View versions	Delete versions	Recover versions	View all private comments**
File owner*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Folder owner	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Folder co-owner	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Folder contributor	✓		✓	✓					✓	✓	✓	✓	✓		
Folder viewer					✓				✓	✓					
Anonymous viewer									✓	✓					

* 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.

Permissions for files not in shared folders

The following permissions apply to user roles for files that do not reside in a shared folder:

- **Annotate** – Add feedback to a file.
- **Delete** – Delete a file.
- **Rename** – Rename files.
- **Upload** – Upload new versions of a file.
- **Download** – Download a file. This is the default permission. You can use file properties to allow or deny the ability to download shared files.
- **Prevent download** – Prevent a file from being downloaded.

    Note
    When the owner or co-owner of an MP4 file disallows downloads for that file, contributors and viewers cannot play it in the Amazon WorkDocs web client.

- **Share** – Share a file with other users.
- **Revoke share** – Revoke the sharing of a file.
- **View** – View 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.
- **Delete versions** – Delete one or more versions of a file.
- **Recover versions** – Recover one or more deleted versions of a file.

	Annotate	Delete	Rename	Upload	Download	Prevent download	Share	Revoke share	View shares	View annotations	View activity	View versions	Delete versions	Recover versions
Owner	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Co-owner	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Contributor	✓			✓	✓				✓	✓	✓	✓	✓	✓
Viewer					✓				✓	✓				
Anonymous viewer									✓	✓				

Enabling collaborative editing

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

Contents
- Enabling Hancom ThinkFree (p. 41)
- Enabling Open with Office Online (p. 42)

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 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 and .

> **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 content for migration

To prepare your content 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 the following:

   - The source folder contains no more than 100,000 files and subfolders. Migrations fail if you exceed that limit.

- No individual files exceed 5 TB.
- Each file name contains 255 characters or less. Amazon WorkDocs Drive only displays files with a full directory path of 260 characters or less.

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 User 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. The Migration Service can take up to a week to process your migration request and send you an email saying that you can begin your migration. If you start the migration before you receive the email, the management console displays a message telling you to wait.

When you schedule the migration, your Amazon WorkDocs user account **Storage** setting automatically changes 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. 34).

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

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 (p. 47)
- Want to set up my Amazon WorkDocs site in an existing Amazon VPC (p. 47)
- User needs to reset their password (p. 47)
- User accidentally shared a sensitive document (p. 47)
- User left the organization and didn't transfer document ownership (p. 48)
- Need to deploy Amazon WorkDocs Drive or Amazon WorkDocs Companion to multiple users (p. 48)
- Online editing isn't working (p. 26)

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.

Amazon WorkDocs Administration Guide
User left the organization and
didn't transfer document ownership

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. 35).

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. 3). For specific information about deploying Amazon WorkDocs Drive to multiple users, see Deploying Amazon WorkDocs Drive to multiple computers (p. 29).

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**.

IP address and domains to add to your allow list

If you implement IP filtering on devices that access Amazon WorkDocs, add the following IP addresses and domains to your allow list. Doing so enables Amazon WorkDocs and Amazon WorkDocs Drive to connect to the WorkDocs service.

- zocalo.ap-northeast-1.amazonaws.com
- zocalo.ap-southeast-2.amazonaws.com
- zocalo.eu-west-1.amazonaws.com
- zocalo.eu-central-1.amazonaws.com
- zocalo.us-east-1.amazonaws.com
- zocalo.us-gov-west-1.amazonaws.com
- zocalo.us-west-2.amazonaws.com
- awsapps.com
- amazonaws.com
- cloudfront.net
- aws.amazon.com
- amazonworkdocs.com
- console.aws.amazon.com
- cognito-identity.us-east-1.amazonaws.com
- firehose.us-east-1.amazonaws.com

If you want to use IP address ranges, see AWS IP address ranges in the *AWS general reference.*

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.

Change	Description	Date
New file owner permissions (p. 51)	Administrators can now provide the Delete Version and Recover Version permissions. The permissions are part of the release of the DeleteDocumentVersion and RecoverDocumentVersion APIs.	July 29, 2022
Amazon WorkDocs Backup (p. 51)	Removed the Amazon WorkDocs Backup documentation from the Amazon WorkDocs Administration Guide because the component is no longer supported.	June 24, 2021
Managing Amazon WorkDocs for Amazon Business (p. 51)	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. 51)	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. 51)	**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. 51)	Hancom ThinkFree is available. Users can create and collaboratively edit Microsoft	June 21, 2018

	Office files from the Amazon WorkDocs web application. For more information, see Enabling Hancom ThinkFree in the Amazon WorkDocs Administration Guide.	
Open with Office Online (p. 51)	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. 51)	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. 51)	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*.