Amazon WorkLink: Administration Guide
Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

- What Is Amazon WorkLink? ................................................................. 1
  Terms to know when using Amazon WorkLink .................................................. 1
- Services that work with Amazon WorkLink .................................................. 2
- Accessing Amazon WorkLink ........................................................................ 2
  Managing access to Amazon WorkLink ............................................................ 2
- Resources ........................................................................................................ 3
- Setting up Amazon WorkLink ........................................................................... 4
  Sign up for AWS ............................................................................................... 4
  Create an IAM user .......................................................................................... 4
  Prepare TLS certificates for company domains in AWS Certificate Manager .... 5
  Verify resources ............................................................................................... 5
- Getting started ............................................................................................... 6
  Create a fleet .................................................................................................... 6
  Configure your identity provider (IdP) .............................................................. 7
  Validate IdP federation ..................................................................................... 8
  Associate your domains ................................................................................... 8
  Upload website certificate authorities (optional) ............................................. 9
  Validate associated domains .......................................................................... 9
  Configure your company network ................................................................... 10
  Associate website authorization providers ..................................................... 11
  Configure your device policies (optional) ....................................................... 11
  Deploy a device certificate on an iOS Device ................................................. 12
  Deploy a device certificate on an Android device ......................................... 13
  Configure your audit log stream (optional) .................................................... 14
  Invite users ...................................................................................................... 14
- Managing fleets ............................................................................................. 16
  View fleet details ............................................................................................ 16
  Edit a fleet ....................................................................................................... 16
  Delete a fleet .................................................................................................... 17
- Managing your domains ................................................................................ 19
  Associate an additional domain ..................................................................... 19
  View domain details ....................................................................................... 19
  Edit a domain .................................................................................................. 20
  Revoke a domain ............................................................................................ 20
  Restore a domain ........................................................................................... 20
  Disassociate a domain .................................................................................... 20
- Managing website certificate authorities ...................................................... 21
  View your website certificate authorities ....................................................... 21
  Download your website certificate authorities .............................................. 21
  Delete website certificate authorities ............................................................ 21
  Upload additional website certificate authorities ........................................ 21
- Managing your company network ................................................................. 23
  View company network details ..................................................................... 23
  Edit your company network .......................................................................... 23
- Managing website authorization providers ................................................... 24
  View website authorization providers ........................................................... 24
  Disassociate website authorization providers ............................................... 24
- Managing your device policies ....................................................................... 25
  View your device policies .............................................................................. 25
  Edit your device policies ............................................................................... 25
  Remove a device certificate .......................................................................... 25
What Is Amazon WorkLink?

Amazon WorkLink is a cloud-based service that provides secure access to internal websites and web apps from iOS and Android phones. In a single step, your users or employees can access internal websites as efficiently as they access any other public website. They enter a URL in their web browser, or choose a link to an internal website in an email. Amazon WorkLink authenticates the user's access and securely renders authorized internal web content in a secure rendering service in the AWS cloud. Amazon WorkLink doesn't download or store any internal web content on mobile devices.

Because website data is never stored or cached locally on mobile browsers, Amazon WorkLink reduces the risk of information loss or theft. In addition, all cached content is deleted from AWS when users end their browsing session. As an administrator, you can enforce your company's security and access policies.

Amazon WorkLink works with SAML-based identity providers, and can be used with device management solutions. Amazon WorkLink is also a fully managed service, which means that it automatically handles the following for you:

- Deployment
- Capacity provisioning
- Automatic scaling
- Updates to browsers and resources in the cloud

To use Amazon WorkLink, your users download the Amazon WorkLink app to their mobile device and log in with their company credentials. They can use Amazon WorkLink with Safari on iOS phones and Google Chrome on Android phones to access internal websites.

For more information, see https://aws.amazon.com/worklink/.

Topics

- Terms to know when using Amazon WorkLink (p. 1)
- Services that work with Amazon WorkLink (p. 2)
- Accessing Amazon WorkLink (p. 2)
- Resources (p. 3)

Terms to know when using Amazon WorkLink

To help you get started with Amazon WorkLink, you should get familiar with the following concepts.

Fleet

A fleet consists of resources and the configuration necessary to make your internal websites available to your authorized users who download and set up the Amazon WorkLink app.

Identity Provider (IdP)

An identity provider verifies your users’ credentials. It then issues authentication assertions to provide access to a service provider. You can configure your existing IdP to work with Amazon WorkLink.

Service Provider (SP)

A service provider accepts authentication assertions and provides a service to the user. Amazon WorkLink acts as a service provider to users who have been authenticated by their IdP.
SAML 2.0

A standard for exchanging authentication and authorization data between an IdP and a service provider.

Domains

A list of company websites that your users can access from their mobile devices with Amazon WorkLink.

Virtual Private Cloud (VPC)

You can use an existing or new VPC, corresponding subnets, and security groups to link your content with Amazon WorkLink. For more information, see Managing your company network (p. 23).

Company code

The identifier users input to sign into the Amazon WorkLink app. Amazon WorkLink uses the company code to fetch the company-specific configuration details.

Device policy

A set of requirements an employee device must meet before that employee can access internal content with Amazon WorkLink.

Services that work with Amazon WorkLink

Amazon WorkLink is a part of End User Computing in AWS, which consists of Amazon WorkSpaces, Amazon AppStream 2.0, and Amazon WorkLink. A typical enterprise has use cases for each service. For example, software developers in an organization can use Amazon WorkSpaces to access all desktop resources from any computer or tablet. Engineers can use AppStream 2.0 to stream GPU intensive apps. And sales leaders can use Amazon WorkLink to access internal web-based content, such as sales data, from their mobile devices.

Amazon WorkLink works with the following AWS offerings:

- AWS Direct Connect – For content hosted on-premises, customers can use DX or a site-to-site virtual private network to obtain secure on-premises connectivity to their VPC. Amazon WorkLink relies on that VPC to fetch content from on-premises origin services and render that content in AWS.
- Transit Gateway Network Manager – Provision a dedicated VPC to route Amazon WorkLink traffic and connect it to your company network with the Transit Gateway Network Manager.
- Amazon Kinesis – Use an Amazon Kinesis Data Stream to send your user activity logs to your preferred data storage and analytics solution.
- AWS CloudTrail – Amazon WorkLink records all console, SDK, CLI, and API operations in AWS CloudTrail. This lets you audit the actions taken to manage your Amazon WorkLink fleets.

Accessing Amazon WorkLink

Administrators access Amazon WorkLink through the AWS Management Console, SDK, CLI, or API. Your users access it through the Amazon WorkLink app, which is downloaded from their app store onto their mobile devices. After initial setup, the Amazon WorkLink app works in the background while employees browse internal websites using Safari on iOS phones and Google Chrome on Android phones.

Managing access to Amazon WorkLink

By default, users in your AWS account can’t access Amazon WorkLink resources. To allow your users to access Amazon WorkLink, attach one of the following AWS managed policies to your AWS Identity and
Access Management, groups of users, or IAM roles. For more information, see Creating Your First IAM Delegated User and Group and Adding IAM Identity Permissions (Console) in the IAM User Guide.

- Read only (ARN: arn:aws:iam::aws:policy/AmazonWorkLinkReadOnly)
  The read-only policy provides access to all of the actions that let customers interact in a read-only manner with the console and the API operation. These actions include Describe, List, and Search. This is the minimal set of permissions needed for full functionality in the console. The permissions are suitable for users who need only audit access and don't need to configure Amazon WorkLink.

- Full access (ARN: arn:aws:iam::aws:policy/AmazonWorkLinkFullAccess)
  The full-access policy grants access to all Amazon WorkLink actions. This is the appropriate permission for Amazon WorkLink administrators.

Resources

The following related resources can help you as you work with this service.

- **Classes & Workshops** – Links to role-based and specialty courses, in addition to self-paced labs to help sharpen your AWS skills and gain practical experience.
- **AWS Developer Tools** – Links to developer tools, SDKs, IDE toolkits, and command line tools for developing and managing AWS applications.
- **AWS Whitepapers** – Links to a comprehensive list of technical AWS whitepapers, covering topics such as architecture, security, and economics and authored by AWS Solutions Architects or other technical experts.
- **AWS Support Center** – The hub for creating and managing your AWS Support cases. Also includes links to other helpful resources, such as forums, technical FAQs, service health status, and AWS Trusted Advisor.
- **AWS Support** – The primary webpage for information about AWS Support, a one-on-one, fast-response support channel to help you build and run applications in the cloud.
- **Contact Us** – A central contact point for inquiries concerning AWS billing, account, events, abuse, and other issues.
- **AWS Site Terms** – Detailed information about our copyright and trademark; your account, license, and site access; and other topics.
Setting up Amazon WorkLink

To access Amazon WorkLink, first create an AWS account and an IAM user. To associate company domains, you will also need TLS certificates secured by AWS Certificate Manager.

Topics
- Sign up for AWS (p. 4)
- Create an IAM user (p. 4)
- Prepare TLS certificates for company domains in AWS Certificate Manager (p. 5)
- Verify resources (p. 5)

Sign up for AWS

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account
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.

Create an IAM user

In this procedure, create an administrator user, then create users and add them to an administrator's group.

To create an administrator user for yourself and add the user to an administrators group (console)
1. Sign in to the IAM console as the account owner by choosing Root user and entering your AWS account email address. On the next page, enter your password.
   Note
   We strongly recommend that you adhere to the best practice of using the Administrator IAM user that follows and securely lock away the root user credentials. Sign in as the root user only to perform a few account and service management tasks.
2. In the navigation pane, choose Users and then choose Add user.
3. For User name, enter Administrator.
4. Select the check box next to AWS Management Console access. Then select Custom password, and then enter your new password in the text box.
5. (Optional) By default, AWS requires the new user to create a new password when first signing in. You can clear the check box next to User must create a new password at next sign-in to allow the new user to reset their password after they sign in.
6. Choose Next: Permissions.
7. Under Set permissions, choose Add user to group.
8. Choose Create group.
9. In the Create group dialog box, for Group name enter Administrators.

10. Choose Filter policies, and then select AWS managed - job function to filter the table contents.

11. In the policy list, select the check box for AdministratorAccess. Then choose Create group.

   Note
   You must activate IAM user and role access to Billing before you can use the AdministratorAccess permissions to access the AWS Billing and Cost Management console. To do this, follow the instructions in step 1 of the tutorial about delegating access to the billing console.

12. Back in the list of groups, select the check box for your new group. Choose Refresh if necessary to see the group in the list.

13. Choose Next: Tags.

14. (Optional) Add metadata to the user by attaching tags as key-value pairs. For more information about using tags in IAM, see Tagging IAM entities in the IAM User Guide.

15. Choose Next: Review to see the list of group memberships to be added to the new user. When you are ready to proceed, choose Create user.

You can use this same process to create more groups and users and to give your users access to your AWS account resources. To learn about using policies that restrict user permissions to specific AWS resources, see Access management and Example policies.

Prepare TLS certificates for company domains in AWS Certificate Manager

You can manage TLS certificates used to associate your company domains with Amazon WorkLink by using AWS Certificate Manager. With ACM, you can upload your existing certificate or create a new one. You need an ACM certificate in the Issued state before you use the Amazon WorkLink console, SDK, or CLI to associate a company domain. For more information about ACM, see AWS Certificate Manager.

   Note
   ACM certificates used to associate domains with Amazon WorkLink must be created in the US East (N. Virginia) Region.

Verify resources

Make sure that you have all the necessary resources before you begin working with Amazon WorkLink. For more information, see the Quick Start checklist.
Getting started with Amazon WorkLink

There are three required steps to set up Amazon WorkLink:

1. the section called “Configure your identity provider (IdP)” (p. 7).
2. the section called “Configure your company network” (p. 10).
3. the section called “Associate your domains” (p. 8) that will be accessed with Amazon WorkLink.

If your company domain servers use TLS certificates issued by private certificate authorities (CA), you also need to upload the root certificate for those CAs. Use the verification guide provided with each step to ensure that your configuration is correct. We recommend that you download the Amazon WorkLink app on your mobile device to complete the verification steps. If you have any issues, see Troubleshooting (p. 46).

Topics

- Create a fleet (p. 6)
- Configure your identity provider (IdP) (p. 7)
- Validate IdP federation (p. 8)
- Associate your domains (p. 8)
- Upload website certificate authorities (optional) (p. 9)
- Validate associated domains (p. 9)
- Configure your company network (p. 10)
- Associate website authorization providers (p. 11)
- Configure your device policies (optional) (p. 11)
- Configure your audit log stream (optional) (p. 14)
- Invite users (p. 14)

Create a fleet

To create a fleet, you must select a home AWS Region. All audit logs for your fleet are stored in the home AWS Region. If your domains are hosted on-premises, you must create a VPC that provides connectivity with on-premises origin hosts in this Region.

After you determine your home Region, switch to that Region in the AWS Management Console.

To create a fleet

1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, choose Create fleet.
3. On the Create fleet page, under Fleet name, type the name identifier for the fleet. This is used to create an Amazon Resource Name (ARN).
Configure your identity provider (IdP)

You must link your existing identity provider (IdP) to your fleet. Use your existing SAML 2.0 provider to add users who you want to access your internal websites.

**Note**
You must create an end user account for each end user authorized to access Amazon WorkLink. Each end user may be permitted to use a limited number of devices or sessions in any calendar month. For more information about end user accounts and device or session limits, please see the documentation for your IdP.

**To configure your identity provider (IdP)**

1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the fleet, and choose View details.
3. Choose Identity provider (IdP), Link IdP.
4. Under Provider type, select SAML.
5. Under IdP metadata document, choose Choose file to select an XML document generated by your IdP that supports SAML 2.0.
6. Choose Service provider metadata document to download and upload it to your IdP. Some identity providers don’t support uploading the service provider SAML metadata file downloaded from the Amazon WorkLink console, SDK, or CLI directly into their system. Instead, you must copy the entityID (or Audience URI) and AssertionConsumerService (or ACS) URL from the service provider SAML metadata file into the identity provider portal manually.

**Note**

- Okta doesn’t support uploading the service provider metadata document directly, so you must manually copy the entity ID and the ACS URL.
- You can upload the service provider metadata document directly in AWS Single Sign-On.
- You can upload the service provider metadata document directly in Ping Identity.
- G Suite doesn’t support uploading the service provider metadata document directly, so you must manually copy the entity ID and the ACS URL.
7. Choose **Link IdP**.

**Validate IdP federation**

After you the section called "Configure your identity provider (IdP)" (p. 7) to federate your SAML 2.0 identity provider, you can use the Amazon WorkLink app on your iPhone or Android phone to validate that it has been federated.

**To validate that your SAML 2.0 identity provider has been federated**

1. Download and open the Amazon WorkLink app on your phone.
   
   **Note**
   
   If you can't download the app, make sure that your device is connected to the internet. If you're using a test device, make sure that your device has been registered. The App Store and Play Store don't allow unregistered devices to download applications.

2. Enter the company code for your Amazon WorkLink fleet.
   
   **Note**
   
   Company codes are alphanumeric and listed in the Amazon WorkLink console on the Fleets and User invites pages,

3. Sign in with your SAML 2.0 credentials.
   
   **Note**
   
   If you see an error message that says **WorkLink is unable to connect to your company's Identity Provider**, then Amazon WorkLink can't log in with your company SAML 2.0 provider. Check your identity provider availability, and confirm that you correctly completed the steps in the section called "Configure your identity provider (IdP)" (p. 7).

4. Grant the Amazon WorkLink app VPN permissions.

5. Confirm that the VPN on your phone is running.
   
   **Note**
   
   Most devices display this as a lock icon on the top of the screen, but for some iOS devices (iPhone X+), you might need to confirm that the VPN is connected. To do this, choose Settings, General, and VPN. This ensures that your SAML 2.0 IdP has properly federated with Amazon WorkLink.

**Associate your domains**

Associate your company's domains to allow users to securely access them from their devices.

**Note**

If you have an endpoint for the same Fully Qualified Domain Name (FQDN) deployed with Amazon CloudFront, then you can't associate that domain with Amazon WorkLink.

**To associate a domain**

1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the fleet, and choose View details.
3. Choose Domains, Associate domain, and then Associate domain again.
4. Under Domain name, type the web address of the site that you want to secure with a TLS certificate.
5. Under Display name, enter a user-friendly name that is unique to your AWS account and can be easily searched, and choose Next.
6. **Under Certificate**, choose the certificate that you created in **the section called “Prepare TLS certificates for company domains in AWS Certificate Manager” (p. 5).**

   **Note**
   If you need to add a certificate with multiple Subject Alternate Names (SAN), use the Amazon Resource Name (ARN) to identify the correct certificate for your domain.

7. Choose **Submit**.

### Upload website certificate authorities (optional)

If your domains are protected with TLS certificates issued by specific certificate authorities (CAs), then upload the root certificates for those CAs.

**To upload CAs**

1. Open the Amazon WorkLink console at [https://console.aws.amazon.com/worklink/](https://console.aws.amazon.com/worklink/).
2. On the **Fleets** page, select the fleet, and choose **View details**.
3. Choose **Website certificate authorities - optional, Upload CAs**.
4. To upload the root certificates for the CAs, choose **Choose file**.
5. Choose **Upload CAs**.

### Validate associated domains

After you the section called “Configure your identity provider (IdP)” (p. 7), the section called “Validate IdP federation” (p. 8), and the section called “Associate your domains” (p. 8), you can use the Amazon WorkLink app on your iPhone 12+ or Android 6+ to validate that your domains have been successfully associated.

**To validate your associated domains**

1. Log into the Amazon WorkLink app on your phone:
   1. Download the Amazon WorkLink app on your phone.
   2. Enter the company code for your Amazon WorkLink fleet.
      **Note**
      This is listed in the Amazon WorkLink console on the **Fleet** page or **User Invite** template.
   3. Sign in with your SAML 2.0 credentials.
   4. Grant the Amazon WorkLink app VPN permissions.
   5. Confirm that the VPN is connected.
      **Note**
      Most devices display this as a lock icon on the top of the screen, but for some iOS devices (iPhone X+), you might need to confirm that the VPN is connected. Choose **Settings**, **General**, and **VPN**.
2. Open the Safari browser on your iPhone or Chrome browser on your Android phone.
3. Type the fully qualified domain name (FQDN) into the URL bar of the browser (for example, www.example.com).
4. Observe one of the following results:
   - If you see an error page that says `net:ERR_NAME_NOT_RESOLVED`, then your domain has been successfully associated with Amazon WorkLink. You can skip to the next step to the section called “Configure your company network” (p. 10).
Configure your company network

After you create your fleet, provide the fleet with access to a VPC with on-premises connectivity. You can use an existing or new VPC to link a network. This allows your users to access your company’s internal web content.

For more information about common VPC scenarios, see the following:

- Scenario 1: VPC with a Single Public Subnet
- Scenario 2: VPC with Public and Private Subnets (NAT)
- Scenario 3: VPC with Public and Private Subnets and AWS Site-to-Site VPN Access
- Scenario 4: VPC with a Private Subnet Only and AWS Site-to-Site VPN Access

To configure your company network

1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the fleet, and choose View details.
4. Under VPC, select the VPC that you want your fleet to access. The VPC must meet the following criteria:
   - The VPC must have, or be granted, a path to the servers of origin for the websites you want to associate with Amazon WorkLink. Examples of paths include the following:
     - Peer the VPC with another VPC in AWS that contains the servers of origin. For more information, see What is VPC Peering?
     - Use AWS Direct Connect or an IPsec tunnel to reach the servers of origin outside of AWS. For more information, see Getting Started with AWS Direct Connect.
   - The VPC is highly dependent on your network architecture. Common scenarios include the following:
     - If you use one VPC in AWS for all use cases, you can choose the common VPC.
     - If you use one VPC for a single use case, you can create or use an existing unused VPC. This allows you to use VPC Flow Logs to inspect traffic within the VPC. For more information, see VPC Flow Logs.
5. Under Subnets, select the VPC subnets that Amazon WorkLink should use to set up your VPC configuration. Subnets must meet the following criteria:
   - We recommend that you select at least two subnets in different Availability Zones for high availability.
   - Subnets can only be selected from the VPC you chose in the previous step. These subnets could already be in use. To prevent availability risks, verify that they’re allocated to networking for Amazon WorkLink and have enough IP addresses to allow Amazon WorkLink to scale dynamically.
   - Subnets need to have enough available IP addresses in them to support the number of users going through the fleet. Amazon WorkLink uses an ENI to support multiple browsing sessions, and scales up and down dynamically to meet demand.
   - If your servers of origin are within AWS, identify subnets with network connectivity to reach the servers of origin. To test connectivity, you can create an Amazon Elastic Compute Cloud (Amazon
EC2) instance in the given subnet and test connectivity to the servers of origin. Depending on your network topology, you might need to peer the VPC containing these subnets with the VPC with service to enable connectivity.

- If your servers of origin are outside of AWS, identify subnets with AWS Direct Connect integration that will be used for on-premise integration with Amazon WorkLink. To test connectivity, create an Amazon EC2 instance in the given subnet, and test connectivity to the servers of origin outside of AWS.

Amazon WorkLink uses the VPC information that you provide to set up ENIs that allow Amazon WorkLink to access VPC resources. Each ENI is assigned a private IP address from the IP address range within the subnets you specify, but is not assigned any public IP addresses. Therefore, you can configure a NAT instance inside your VPC or you can use the Amazon VPC NAT gateway. For more information, see NAT Gateways in the Amazon VPC User Guide. You can't use an internet gateway attached to your VPC, because that requires the ENI to have public IP addresses.

**Important**

Do not attach it to a public subnet or to a private subnet without internet access. Instead, attach it only to private subnets with internet access through a NAT instance or an Amazon VPC NAT gateway.

6. Under **Security groups**, select at least one VPC security group that Amazon WorkLink should use to set up your VPC configuration.

**Note**

Security groups are a method of governing traffic within the subnets allocated for Amazon WorkLink. Amazon WorkLink uses the security group to apply to the ENI that is created in the customer subnet.

All AWS accounts include a default security group. Most customers create their own security group to reflect their organization's security policies.

To modify traffic from Amazon WorkLink, modify the outbound rules of the security group.

7. Choose **Link company network**.

### Associate website authorization providers

If your domains use any additional authorization providers besides the one configured through your fleet’s identity provider configuration, you can associate those providers to your fleet.

**To configure website authorization providers**

1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the **Fleets** page, select the fleet, and choose **View details**.
3. Choose **Website authorization providers - optional, Associate provider**.
4. Select the **Provider type**.

**Note**

Currently, SAML is the only supported type.

5. Under **Domain**, enter the domain name of the authorization provider, and choose **Associate provider**.

### Configure your device policies (optional)

You can configure device policies that must be met before users can access internal content.
To configure your device policies in the Amazon WorkLink console

1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the fleet, and choose View details.
3. Choose Device policies - optional and Configure device policies.
4. Under Device certificate authority, choose Choose file to select the certificate chain, including intermediate certificates and the root certificate authority certificate used to issue device certificates.
5. Choose Configure device policies.

Deploy a device certificate on an iOS Device

To deploy a device certificate that works with Amazon WorkLink on an iOS device, the certificate must be deployed as part of a configuration profile. A configuration profile (.mobileconfig file) allows you to distribute configuration information to iOS devices. The configuration profile for Amazon WorkLink includes the device certificate and the VPN configuration that is required for Amazon WorkLink. After you have a device certificate, you can create a profile with it and deploy it by using one of the following options.

Option 1: Create and deploy a profile with the Apple Configurator 2 app

1. From the App Store, install Apple Configurator 2 on your macOS device and open it.
2. Choose File, New Profile.
3. Choose General and enter a name for the profile. (Optionally, add any other settings required by your organization.)
4. Choose Certificates, choose Configure, and select the .p12 file that represents the certificate that you want to use with Amazon WorkLink. Enter the password that was used to configure and export the certificate.
5. In the VPN section, choose Configure and enter the following settings:
   • Connection Name – Amazon WorkLink
   • Connection Type – Custom SSL
   • Identifier – com.amazon.worklink
   • Server – 54.190.62.41
   • ProviderBundleIdentifier – com.amazon.worklink.tunnel
   • User Authentication – Certificate
   • Identity Certificate – The device certificate that you configured in the previous steps
6. Choose File, Save.
7. To deploy the profile, you can make it available in an Amazon Simple Storage Service (Amazon S3) bucket, email the profile to your users, and ask them to install it on their devices. Alternatively, you can use the following steps:
   1. Connect the iPhone to a MacOS device that contains the profile.
   2. Open the Apple Configurator 2 app and select the iPhone.
   3. Choose Add, choose Profiles, select the profile that you created in the previous step, and choose Add.
   4. Follow the steps on the iPhone to install the profile.

Option 2: Create and deploy a profile with Apple Over-the-Air (OTA)

- For information about how to do this, see Over-the-Air Profile Delivery and Configuration.
Option 3: Create and deploy a profile with VMware AirWatch

1. Go to your VMware AirWatch mobile device management portal.
2. Choose Devices, Profiles, Resources, Profiles, Add, and Apple iOS.
3. Under General, configure the profile's general settings. These settings determine how the profile is deployed and who receives it. For more information about these settings, see the VMware AirWatch iOS Platform Guide.
4. Choose Credentials and the Credential Source that you want to use. Fill out the rest of the fields according to the credential source that you selected.
5. Choose VPN and enter the following Connection info settings:
   - Connection Name – Amazon WorkLink
   - Connection Type – Custom
   - Identifier – com.amazon.worklink
   - Server – 54.190.62.41
   - Custom Data
     - Key – ProviderBundleIdentifier
     - Value – com.amazon.worklink.tunnel
   - User Authentication – Certificate
   - Identity Certificate – The device certificate that you configured

Option 4: Create and deploy a profile with Microsoft Intune

- For information about how to do this, see Create VPN profiles in Intune and Create a profile with custom settings in Intune.

Deploy a device certificate on an Android device

Use one of the following options to deploy a device certificate on an Android device.

Note
At this time, you can't remove certificates that are manually deployed with a USB cable.

Option 1: Manually deploy the certificate with a USB cable

1. Copy the certificates to the Android device's internal storage.
2. Choose Settings, Security, Install from Storage, then choose the certificate.
3. If prompted, enter your PIN or unlock pattern.
4. Enter the Certificate Name, then choose VPN and apps.
5. To install the certificate, choose OK.
6. To see the certificate, choose Settings, Security, Trusted Credentials, then choose the User tab.

Option 2: Create and deploy a profile with VMware AirWatch

1. Go to your VMware AirWatch mobile device management portal.
2. Choose Devices, Profiles, Resources, Profiles, Add, and Android.
3. Under General, configure the profile's general settings. These settings determine how the profile is deployed and who receives it. For more information about these settings, see the VMware AirWatch iOS Platform Guide.
4. Choose Credentials and the Credential Source that you want to use. Fill out the rest of the fields according to the credential source that you selected.
Configure your audit log stream (optional)

Amazon WorkLink creates activity logs that allow you to track the following information:

- The total number of users accessing content through Amazon WorkLink
- The content accessed
- When users accessed content
- What devices users accessed content from

These logs are delivered to a Kinesis data stream in your account, and you can direct that information to a data store or tool of your choice. For example, you can stream these logs to Amazon S3 and use a tool like Splunk to analyze the information. Or, you can direct this data to Amazon Redshift through an Amazon Kinesis Data Firehose and use Amazon QuickSight to generate reports and dashboards.

For more information, see Amazon Kinesis.

To configure your audit log delivery

1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the fleet, and choose View details.
4. If you haven't created a Kinesis data stream with the "AmazonWorkLink-" name prefix to receive audit logs, choose Create Kinesis Stream to do so. After you create a Kinesis data stream with the necessary prefix, go back and select that stream.
5. Choose Link audit logs.

Invite users

After completing all the previous steps, you can copy an email invitation template to send to your users. This email invites them to use Amazon WorkLink and provides them with the company code required during login in the Amazon WorkLink app.

Before your proceed, make sure that you meet the following prerequisites:

- You granted users permissions to the Amazon WorkLink service provider in the the section called “Configure your identity provider (IdP)” (p. 7) step.
- Your users have one of the following supported web browsers:
  - Safari on iOS
• Google Chrome on Android
• Your users have a phone with one of the following supported operating systems:
  • iOS 11 or later
  • Android 6 or later

To invite users to use Amazon WorkLink

1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the fleet, and choose View details.
3. Choose User invites, and View details.
4. You can either copy and paste the template, or download it.
5. Review the email and make any necessary edits, then send it to your users.
Managing fleets

After you set up your fleets in the section called “Create a fleet” (p. 6), you can view their details, edit them, and delete them at any time.

Topics
• View fleet details (p. 16)
• Edit a fleet (p. 16)
• Delete a fleet (p. 17)

View fleet details

You can view detailed information about your fleets, including identity provider (IdP), network, and domain details.

To view fleet details
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. To view detailed information about the fleet, choose the button on any of the following categories:
   • Identity provider (IdP)
   • Domains
   • Company network
   • Website authorization providers
   • Website certificate authorities
   • Device policies
   • Audit logs
   • Tags
   • User invites

Edit a fleet

After setting up a fleet, you can continue to make configuration updates to that fleet.

To edit a fleet
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. To edit the category, choose the button on any of the following categories:
   • Identity provider (IdP)
   • Domains
   • Company network
   • Website authorization providers
   • Website certificate authorities
Delete a fleet

If you no longer need a fleet, delete it. This permanently prevents users from accessing any of the websites that you associated to the fleet.

To delete a fleet

1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose Delete.
Managing your identity provider (IdP)

After you set up your IdP in the section called “Configure your identity provider (IdP)” (p. 7), you can view and edit its details.

Topics
• View IdP details (p. 18)
• Edit your IdP (p. 18)

View IdP details

You can view detailed information about your IdP, including details about provider type.

To view IdP details
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. Under Identity provider (IdP), choose the button to view the following related information:
   • Provider type
   • IdP metadata document
   • Service provider metadata document

Edit your IdP

You can edit information about the IdP at any time.

To edit your IdP
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. Under Identity provider (IdP), choose the button to edit any of the following information:
   • Provider type
   • IdP metadata document
   • Service provider metadata document
4. Save your changes.
Managing your domains

After you initially set up your domains in the section called “Associate your domains” (p. 8), you can associate more domains. You can also revoke or disassociate them to prevent users from accessing them.

Topics
- Associate an additional domain (p. 19)
- View domain details (p. 19)
- Edit a domain (p. 20)
- Revoke a domain (p. 20)
- Restore a domain (p. 20)
- Disassociate a domain (p. 20)

Associate an additional domain

You can continue to associate additional domains to your fleet at any time.

To associate an additional domain
- For information about associating domains, see the section called “Associate your domains” (p. 8).

View domain details

The Domains page lists all of the approved company domains that users can access on their secure devices. Refresh the page to update the list or see a newly approved domain.

To view domain details
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. Under Domains, choose the button to view the following related information:
   - Display name
   - Domain
   - Date created
   - Status
4. To view the following information about a specific domain, select the check box next to the domain, and choose Actions, View details:
   - Display name
   - Date added
   - Status
   - Validation record type
   - Validation record name
   - Validation record value
Edit a domain

You can edit the details of a domain at any time.

To edit a domain
1. Follow the steps in the section called “View domain details” (p. 19) to see the details that you want to change.
2. Make the necessary changes and save them to update the domain.

Revoke a domain

You can temporarily block access to a specific domain and restore access later. Revoking a domain does not disassociate the domain from Amazon WorkLink. If you choose to restore it after revoking, you don’t need to validate the domain or get a certificate again.

To revoke a domain
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. Under Domains, choose the button to view your domains.
4. Select the check box next to the domain that you want to revoke, and choose Actions, Revoke.

Restore a domain

You can restore access to a domain after revoking it, to reinstate user access to the domain.

To restore a domain
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. Under Domains, choose the button to view your domains.
4. Select the check box next to the domain that you want to restore, and choose Actions, Restore.

Disassociate a domain

You can permanently disassociate a domain from your list of associated domains. If you do, users no longer have access to it. If you want to temporarily revoke access to a domain, see the section called “Revoke a domain” (p. 20).

To disassociate a domain
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. Under Domains, choose the button to view your domains.
4. Select the check box next to the domain that you want to disassociate, and choose Actions, Disassociate.
Managing website certificate authorities

After you upload website certificate authorities in the section called “Upload website certificate authorities (optional)” (p. 9), you can view details, download or delete them, or upload more CAs.

Topics
- View your website certificate authorities (p. 21)
- Download your website certificate authorities (p. 21)
- Delete website certificate authorities (p. 21)
- Upload additional website certificate authorities (p. 22)

View your website certificate authorities

You can view the website certificate authorities that you uploaded.

To view your website certificate authorities
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. Under Website certificate authorities - optional, choose the button to view the CAs that you uploaded.

Download your website certificate authorities

You can download your CAs at any time.

To download your CA
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. Under Website certificate authorities - optional, choose the button to download a CA.
4. Select the CA and choose Download.

Delete website certificate authorities

You can delete a CA if you don't need it anymore.

To delete a CA
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. Under Website certificate authorities - optional, choose the button to delete a CA.
4. Select the CA and choose Delete.

Upload additional website certificate authorities

You can also upload additional CAs.

To upload an additional CA

1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. Under Website certificate authorities - optional, choose the button to upload another CA.
4. Choose Upload CAs.
Managing your company network

After you set up your company network in the section called “Configure your company network” (p. 10), you can view and edit details about the network.

Topics
• View company network details (p. 23)
• Edit your company network (p. 23)

View company network details

You can view detailed information about your network, including details about the VPC, subnets, and security groups.

To view company network details
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. Under Company network, choose the button to view the following related information:
   • VPC
   • Subnets
   • Security groups

Edit your company network

You can edit information about the company network at any time.

To edit your company network
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. Under Company network, choose the button to edit any of the following information:
   • VPC
   • Subnets
   • Security groups
4. Save your changes.
Managing website authorization providers

After you associate a website authorization provider in the section called “Associate website authorization providers” (p. 11), you can view details of the provider. You can also disassociate it when you need to.

Topics
- View website authorization providers (p. 24)
- Disassociate website authorization providers (p. 24)

View website authorization providers

You can view information about your providers, including the domain and provider type.

To view website authorization provider details
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. In the left navigation, choose Website authorization providers to view the following information:
   - Domain
   - Provider type
   - Date created

Disassociate website authorization providers

You can disassociate a website authorization provider from a fleet at any time.

To disassociate a website authorization provider from a fleet
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. In the left navigation, choose Website authorization providers.
4. Select the provider that you want to disassociate, and choose Disassociate.
Managing your device policies

After you set up your device policies in the section called “Configure your device policies (optional)” (p. 11), you can view and edit their details.

Topics

• View your device policies (p. 25)
• Edit your device policies (p. 25)
• Remove a device certificate (p. 25)

View your device policies

You can view the certificate chain that you uploaded for your device policies.

To view your device policies

1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. Under Device Policies - optional, choose the button to view the certificate chain that you uploaded.

Edit your device policies

You can edit information about your device policies at any time.

To edit your device policies

1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. Under Device Policies - optional, choose the button to upload a new Device certificate authority.
4. Choose Configure device policies to save your changes.

Remove a device certificate

If you followed the steps in the section called “Deploy a device certificate on an iOS Device” (p. 12) or the section called “Deploy a device certificate on an Android device” (p. 13), you can remove the device certificate if you need to.

Note
At this time, you can't remove certificates that were manually deployed with a USB cable.

To remove a device certificate from an iOS or Android device

• Choose one of the following options:
  • If you created a profile with VMWare AirWatch, see "Revoking Digital Certificates" in AirWatch Securing Mobile Devices with Certificates.
• If you created a profile with Microsoft Intune, see "PKCS certificates" in Remove SCEP and PKCS certificates in Microsoft Intune.
Managing users

After you've invited users to use Amazon WorkLink in the section called “Invite users” (p. 14), you can view details about the users. You can also sign out users for security purposes.

Topics
  • View user details (p. 27)
  • Sign out a user (p. 27)

View user details

You can view details about a user, including their user name and number of devices.

To view user details
  1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
  2. On the Fleets page, select the check box next to the fleet, and choose View details.
  3. In the left navigation, choose Users.
  4. View the User name and Number of devices for each user.

Sign out a user

If a user’s device is lost or stolen, you can sign a user out of their devices for security purposes. This may take up to 1 hour to take effect.

To sign out a user
  1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
  2. On the Fleets page, select the check box next to the fleet, and choose View details.
  3. In the left navigation, choose Users.
  4. Select the check box next to the user you want to sign out, and choose Sign user out.
Managing devices

After you've invited users to use Amazon WorkLink in the section called "Invite users" (p. 14), you can view details about their devices.

Topics
• View device details (p. 28)

View device details

You can view details about user devices, including the Device ID, status, and manufacturer.

To view device details
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. On the Fleets page, select the check box next to the fleet, and choose View details.
3. In the left navigation, choose Devices.
4. View the following information:
   • Device ID
   • Status
   • Manufacturer
   • Model
   • User
   • Enrolled Date
5. To view the following information about a specific device, select the check box next to the device and choose Actions, View details:
   • Device model
   • Device manufacturer
   • Patch level
   • Status
   • Last sync
   • Enrolled date
Using service-linked roles for Amazon WorkLink

Amazon WorkLink uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Amazon WorkLink. Service-linked roles are predefined by Amazon WorkLink and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Amazon WorkLink more efficient because you don’t have to manually add the necessary permissions. Amazon WorkLink defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon WorkLink can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting their related resources. This protects your Amazon WorkLink resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see AWS Services That Work with IAM. In that topic, look for the services that have Yes in the Service-Linked Role column. Choose a Yes service with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Amazon WorkLink

Amazon WorkLink uses the service-linked role named AWSServiceRoleForAmazonWorkLink to access resources linked to your fleets.

The AWSServiceRoleForAmazonWorkLink service-linked role trusts the following services to assume the role:

* worklink.amazonaws.com

The role permissions policy allows Amazon WorkLink to complete the following actions on the specified resources:

* Action: ec2:CreateNetworkInterface on *
  
  Action: ec2:DeleteNetworkInterfacePermission on *
  
  Action: ec2:CreateNetworkInterfacePermission on *
  
  Action: ec2:ModifyNetworkInterfaceAttribute on *
  
  Action: ec2:DeleteNetworkInterface on *
  
  Action: kinesis:PutRecord on "arn:aws:kinesis:*::*:stream/AmazonWorkLink-*"
  
  Action: kinesis:PutRecords on "arn:aws:kinesis:*::*:stream/AmazonWorkLink-*"
You must configure permissions to allow an IAM entity to create, edit, or delete a service-linked role. An entity can be a user, group, or role. For more information, see Service-Linked Role Permissions in the IAM User Guide.

Creating a service-linked role for Amazon WorkLink

You don't need to manually create a service-linked role. If needed, Amazon WorkLink creates the service-linked role when you create an Amazon WorkLink fleet in the AWS Management Console, the AWS CLI, or the AWS API. All Amazon WorkLink fleets share a single service-linked role.

Important
This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. Also, Amazon WorkLink began supporting service-linked roles on March 25, 2019. If you were using Amazon WorkLink before that date, Amazon WorkLink created the AWSServiceRoleForAmazonWorkLink role in your account. For more information, see A New Role Appeared in My IAM Account.

If you delete this service-linked role, then a new service-linked role is created for you when you create new a new Amazon WorkLink fleet.

Editing a service-linked role for Amazon WorkLink

Amazon WorkLink does not allow you to edit the AWSServiceRoleForAmazonWorkLink service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the IAM User Guide.

Deleting a service-linked role for Amazon WorkLink

If you are no longer using a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don’t have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

Note
If the Amazon WorkLink service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To delete Amazon WorkLink resources used by the AWSServiceRoleForAmazonWorkLink
1. Open the Amazon WorkLink console at https://console.aws.amazon.com/worklink/.
2. Select each fleet and choose Delete to delete all Amazon WorkLink fleets in all AWS Regions.
3. Make sure that all fleets are in the Deleting state.
4. Delete the service-linked role using IAM.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForAmazonWorkLink service-linked role. For more information, see Deleting a Service-Linked Role in the IAM User Guide.
Supported regions for Amazon WorkLink service-linked roles

Amazon WorkLink supports using service-linked roles in all of the regions where the service is available. For more information, see AWS Regions and Endpoints.
Security in Amazon WorkLink

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, as follows:

- **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. For more information about the compliance programs that apply to Amazon WorkLink, see AWS Services in Scope by Compliance Program.

- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors, including the sensitivity of your data, your company’s requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon WorkLink. The following topics show you how to configure Amazon WorkLink 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 WorkLink resources.

**Topics**

- Data protection in Amazon WorkLink (p. 32)
- Identity and access management for Amazon WorkLink (p. 33)
- Logging and monitoring in Amazon WorkLink (p. 43)
- Compliance validation for Amazon WorkLink (p. 44)
- Resilience in Amazon WorkLink (p. 45)
- Infrastructure security in Amazon WorkLink (p. 45)
- Configuration and vulnerability analysis in Amazon WorkLink (p. 45)

Data protection in Amazon WorkLink

Amazon WorkLink only stores customer content that is required for Amazon WorkLink, including user names and device (phone) identifiers. No action is required for users to secure their content. Amazon WorkLink secures content by default. All data retention policies and protection standards follow AWS compliance standards.

**Data encryption**

All customer-specific data within Amazon WorkLink is encrypted at rest and in transit.

**Encryption at rest**

Encryption at rest is configured by default with KMS keys.

**Encryption in transit**

Encryption in transit is configured by default with TLS 1.2. Amazon WorkLink only supports secure connections.
Key management

There are currently no options for customers to manage encryption keys.

Interwork traffic privacy

An end user's connection to the Amazon WorkLink rendering service is TLS. However, the customer controls the encryption on the connection between the Amazon WorkLink rendering service and a customer's site. Although we currently don't support non-HTTPS domains, Amazon WorkLink doesn't have specific requirements for the certificate provided on the customer side.

Amazon WorkLink also uses TLS to secure connections between Availability Zones within a region, secure connections between regions, and secure connections between accounts.

Identity and access management for Amazon WorkLink

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 WorkLink resources. IAM is an AWS service that you can use with no additional charge.

Topics

- Audience (p. 33)
- Authenticating with identities (p. 34)
- Managing access using policies (p. 35)
- How Amazon WorkLink works with IAM (p. 37)
- Amazon WorkLink identity-based policy examples (p. 40)
- Troubleshooting Amazon WorkLink identity and access (p. 41)

Audience

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

Service user – If you use the Amazon WorkLink service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon WorkLink 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 WorkLink, see Troubleshooting Amazon WorkLink identity and access (p. 41).

Service administrator – If you're in charge of Amazon WorkLink resources at your company, you probably have full access to Amazon WorkLink. It's your job to determine which Amazon WorkLink features and resources your employees should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Amazon WorkLink, see How Amazon WorkLink works with IAM (p. 37).

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 WorkLink. To view example Amazon WorkLink identity-based policies that you can use in IAM, see Amazon WorkLink identity-based policy examples (p. 40).
Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. For more information about signing in using the AWS Management Console, see Signing in to the AWS Management Console as an IAM user or root user in the IAM User Guide.

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

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

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

AWS account root user

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

IAM users and groups

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

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

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

IAM roles

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

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

- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.

- **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as federated users. AWS assigns a role to a federated user when access is requested through an identity provider. For more information about federated users, see Federated users and roles in the IAM User Guide.

- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the IAM User Guide.

- **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 Actions, Resources, and Condition Keys for Amazon WorkLink 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 IAM identities or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. You can sign in as the root user or an IAM user, or you can assume an IAM role. When you then make a request, AWS evaluates the related identity-based or resource-based policies. 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. In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

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

**Identity-based policies**

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, 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 (ACLs)**

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 entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the Principal field are not limited by the permissions boundary. An explicit deny
in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the IAM User Guide.

• **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see How SCPs work in the AWS Organizations User Guide.

• **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see Session policies in the IAM User Guide.

### Multiple policy types

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

### How Amazon WorkLink works with IAM

Before you use AWS Identity and Access Management (IAM) to manage access to Amazon WorkLink, you should understand what IAM features are available to use with Amazon WorkLink. To get a high-level view of how Amazon WorkLink and other AWS services work with IAM, see AWS Services That Work with IAM in the IAM User Guide.

#### Topics

- Amazon WorkLink identity-based policies (p. 37)
- Amazon WorkLink resource-based policies (p. 39)
- Access control lists (ACLs) (p. 39)
- Authorization based on Amazon WorkLink tags (p. 39)
- Amazon WorkLink IAM roles (p. 39)

### Amazon WorkLink identity-based policies

With IAM identity-based policies, you can specify allowed or denied actions and resources, and also the conditions under which actions are allowed or denied. Amazon WorkLink supports specific actions, resources, and condition keys. For more information about all of 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 WorkLink use the following prefix before the action: worklink:. For example, to grant someone permission to run an Amazon EC2 instance with the Amazon EC2 RunInstances API operation, you include the ec2:RunInstances action in their policy. Policy statements must include either an Action or NotAction element. Amazon WorkLink 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": [
  "ec2:action1",
  "ec2:action2"
]
```

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

```
"Action": "ec2:Describe*"
```

To see a list of Amazon WorkLink actions, see Actions Defined by Amazon WorkLink in the IAM User Guide.

Resources

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 Resource JSON policy element specifies the object or objects to which the action applies. Statements must include either a Resource or a NotResource element. As a best practice, specify a resource using its Amazon Resource Name (ARN). You can do this for actions that support a specific resource type, known as resource-level permissions.

For actions that don’t support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*
```

The Amazon EC2 instance resource has the following ARN:

```
arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}
```

For more information about the format of ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces.

For example, to specify the i-1234567890abcdef0 instance in your statement, use the following ARN:

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

To specify all instances that belong to a specific account, use the wildcard (*):

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/**"
```

Some Amazon WorkLink actions, such as those for creating resources, cannot be performed on a specific resource. In those cases, you must use the wildcard (*).

```
"Resource": "*
```
Many Amazon EC2 API actions involve multiple resources. For example, AttachVolume attaches an Amazon EBS volume to an instance, so an IAM user must have permissions to use the volume and the instance. To specify multiple resources in a single statement, separate the ARNs with commas.

```
"Resource": [
    "resource1",
    "resource2"
]
```

Amazon WorkLink has one resource (fleet), and policies can restrict at the fleet level. To see a list of Amazon WorkLink resource types and their ARNs, see Resources Defined by Amazon WorkLink in the IAM User Guide. To learn with which actions you can specify the ARN of each resource, see Actions Defined by Amazon WorkLink.

**Condition keys**

Amazon WorkLink does not support any global condition keys.

**Examples**

To view examples of Amazon WorkLink identity-based policies, see Amazon WorkLink identity-based policy examples (p. 40).

**Amazon WorkLink resource-based policies**

Amazon WorkLink does not support resource-based policies.

**Access control lists (ACLs)**

Amazon WorkLink does not support Access Control Lists (ACLs).

**Authorization based on Amazon WorkLink tags**

You can attach tags to Amazon WorkLink resources or pass tags in a request to Amazon WorkLink. To control access based on tags, you provide tag information in the condition element of a policy using the worklink:ResourceTag/key-name, aws:RequestTag/key-name, or aws:TagKeys condition keys. For more information about tagging Amazon WorkLink resources, see the section called "Create a fleet" (p. 6).

**Amazon WorkLink IAM roles**

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

**Using temporary credentials with Amazon WorkLink**

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 WorkLink 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 WorkLink supports service-linked roles. For details about creating or managing Amazon WorkLink service-linked roles, see Using service-linked roles for Amazon WorkLink (p. 29).
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 WorkLink supports service roles.

Amazon WorkLink identity-based policy examples

By default, AWS Identity and Access Management (IAM) users and roles don't have permission to create or modify Amazon WorkLink 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.

For more information about 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. 40)
- Allow users to view their own permissions (p. 40)

Policy best practices

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

- Get started using AWS managed policies – To start using Amazon WorkLink quickly, use AWS managed policies to give your employees the permissions they need. These policies are already available in your account and are maintained and updated by AWS. For more information, see Get started using permissions with AWS managed policies in the IAM User Guide.

- Grant least privilege – When you create custom policies, grant only the permissions required to perform a task. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. For more information, see Grant least privilege in the IAM User Guide.

- Enable MFA for sensitive operations – For extra security, require IAM users to use multi-factor authentication (MFA) to access sensitive resources or API operations. For more information, see Using multi-factor authentication (MFA) in AWS in the IAM User Guide.

- Use policy conditions for extra security – To the extent that it's practical, define the conditions under which your identity-based policies allow access to a resource. For example, you can write conditions to specify a range of allowable IP addresses that a request must come from. You can also write conditions to allow requests only within a specified date or time range, or to require the use of SSL or MFA. For more information, see IAM JSON policy elements: Condition in the IAM User Guide.

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.

{
Troubleshooting Amazon WorkLink identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Amazon WorkLink and AWS Identity and Access Management (IAM).

Topics
- I am not authorized to perform iam:PassRole (p. 41)
- I want to view my access keys (p. 42)
- I'm an administrator and want to allow others to access Amazon WorkLink (p. 42)
- I want to allow people outside of my AWS account to access my Amazon WorkLink resources (p. 42)

I am not authorized to perform iam:PassRole

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

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 WorkLink. However, the action requires the service to have permissions granted by a service role. Mary does not have permissions to pass the role to the service.
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole

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

I want to view my access keys

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

Access keys consist of two parts: an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret
access key (for example, wJalrXUtznFEfMI/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 WorkLink

To allow others to access Amazon WorkLink, 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 WorkLink.

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 WorkLink 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 WorkLink supports these features, see How Amazon WorkLink works with
  IAM (p. 37).
- 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 WorkLink

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

For more information, about CloudTrail, see the AWS CloudTrail User Guide.

Amazon WorkLink information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Amazon WorkLink, 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 WorkLink, 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 AWS 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 any of the following topics:

- 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 WorkLink actions are logged by CloudTrail and are documented in the Amazon WorkLink API Reference. For example, the CreateFleet, DescribeDevice, and ListFleets actions 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 whether the request was made:

- With root or AWS Identity and Access Management (IAM) user credentials.
- With temporary security credentials for a role or federated user.
- By another AWS service.

For more information, see the CloudTrail userIdentity Element.

Understanding Amazon WorkLink 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. An event includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.
The following example shows a CloudTrail log entry that demonstrates the `ListFleets` action.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "User",
    "principalId": "ABCDE12AB1ABCEXAMPLE",
    "arn": "arn:aws:iam::123456789012:user",
    "accountId": "123456789012",
    "accessKeyId": "ABCDEFGHIJKL7EXAMPLE",
    "userName": "user_name"
  },
  "eventTime": "2019-01-02T21:45:23Z",
  "eventSource": "worklink.amazonaws.com",
  "eventName": "ListFleets",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.0/24",
  "userAgent": "example-user-agent-string",
  "requestParameters": {
    "CompanyId": "company_id"
  },
  "responseElements": null,
  "requestID": "6d9c4bfc-148a-11e5-81b6-7577cEXAMPLE",
  "eventID": "4d293154-a15b-4c33-9e0a-ff5eeEXAMPLE",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

### Compliance validation for Amazon WorkLink

Third-party auditors assess the security and compliance of AWS services as part of multiple AWS compliance programs, such as SOC, PCI, FedRAMP, and HIPAA.

To learn whether Amazon WorkLink or other AWS services are in scope of specific compliance programs, see [AWS Services in Scope by Compliance Program](https://aws.amazon.com/about-aws/compliance/global-certifications-scope/). For general information, see [AWS Compliance Programs](https://aws.amazon.com/compliance/).

You can download third-party audit reports using AWS Artifact. For more information, see [Downloading Reports in AWS Artifact](https://aws.amazon.com/about-aws/whats-new/articles/2019/aws-artifact-download/).

Your compliance responsibility when using AWS services 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 baseline environments on AWS that are security and compliance focused.
- **Architecting for HIPAA Security and Compliance Whitepaper** – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
  
  **Note**
  
  Not all services are compliant with HIPAA.
- **AWS Compliance Resources** – This collection of workbooks and guides might apply to your industry and location.
- **Evaluating Resources with Rules** in the [AWS Config Developer Guide](https://docs.aws.amazon.com/config/latest/developerguide/config-rule-examples.html) – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
Resilience in Amazon WorkLink

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 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.

In addition to the AWS global infrastructure, Amazon WorkLink offers several features to help support your data resiliency and backup needs.

Amazon WorkLink generates service metadata and writes it to an Amazon Kinesis stream that customers choose. By default, Amazon WorkLink metadata isn't stored. Customers have full control over how they choose to store the data. Amazon WorkLink supports connections through multiple subnets. Customers who have high availability environments can choose to connect through multiple subnets in a region.

Infrastructure security in Amazon WorkLink

As a managed service, Amazon WorkLink 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 WorkLink 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 AWS Identity and Access Management (IAM) principal. Or, you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

Configuration and vulnerability analysis in Amazon WorkLink

Configuration and IT controls are a shared responsibility between AWS and you, our customer. For more information, see the AWS shared responsibility model.
## Troubleshooting

If you experience any of the following issues with Amazon WorkLink, try these solutions.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>I can't download the Amazon WorkLink app.</td>
<td>Confirm that your device is connected to the internet. If you're using a test device, make sure that your device has been registered. The App Store and Play Store don't allow unregistered devices to download apps.</td>
</tr>
<tr>
<td>I can't find my company code.</td>
<td>From the Amazon WorkLink console, choose Fleets, and find the Company code column.</td>
</tr>
<tr>
<td>The company code I entered is invalid.</td>
<td>Company codes are alphanumeric. Make sure that you entered it correctly. Or, you can download and email yourself the invite template. From the Amazon WorkLink console, choose User invites, View details, and Download email template. Then choose the link in step 2 to automatically format the company code in your Amazon WorkLink app.</td>
</tr>
<tr>
<td>After I enter my company code in the app, I don't see a login page.</td>
<td>Amazon WorkLink can't log in with your company's SAML 2.0 provider. Check your Identity Provider availability, and confirm you have correctly completed the steps in the section called “Configure your identity provider (IdP)” (p. 7).</td>
</tr>
<tr>
<td>After logging into my Identity Provider, I see an error message.</td>
<td>Make sure that you've completed the steps in the section called “Configure your identity provider (IdP)” (p. 7). If a user is able to log in with their SAML credentials, but unable to use the app, the user might not have access to the app in the Identity Provider portal.</td>
</tr>
<tr>
<td>After the Identity Provider sign-in in the Amazon WorkLink app,</td>
<td>Search for AWS Support in the AWS Management Console, and choose Create case to contact us for help.</td>
</tr>
<tr>
<td>Amazon WorkLink shows as being not ready.</td>
<td></td>
</tr>
</tbody>
</table>
Document history for Amazon WorkLink Administration Guide

The following table describes important changes to the Amazon WorkLink Administration Guide, beginning in January 2019. For notifications about updates to this documentation, you can subscribe to an RSS feed.

<table>
<thead>
<tr>
<th>update-history-change</th>
<th>update-history-description</th>
<th>update-history-date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use tags to assign an optional label to an AWS resource. You can use tags to search</td>
<td>For more information, see Create a Fleet in the Amazon WorkLink Administration Guide.</td>
<td>June 1, 2020</td>
</tr>
<tr>
<td>and filter your resources, or track your AWS costs. (p. 47)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure Amazon WorkLink to meet your security and compliance objectives, and learn</td>
<td>For more information, see Security in Amazon WorkLink in the Amazon WorkLink Administration Guide.</td>
<td>April 30, 2020</td>
</tr>
<tr>
<td>how to use other AWS services that help you to secure your Amazon WorkLink resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create an end user account for each end user authorized to access Amazon WorkLink.</td>
<td>For more information, see Configure your Identity Provider (IdP) in the Amazon WorkLink Administration Guide.</td>
<td>February 25, 2020</td>
</tr>
<tr>
<td>(p. 47)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attach an AWS managed policy to allow users to access Amazon WorkLink. (p. 47)</td>
<td>For more information, see Managing Access to Amazon WorkLink in the Amazon WorkLink Administration Guide.</td>
<td>September 10, 2019</td>
</tr>
<tr>
<td>If your domains use additional authorization providers, you can associate them to</td>
<td>For more information, see Associate Website Authorization Providers in the Amazon WorkLink Administration Guide.</td>
<td>May 22, 2019</td>
</tr>
<tr>
<td>your fleet. (p. 47)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage TLS certificates used to associate your domains with AWS Certificate Manager.</td>
<td>For more information, see Prepare TLS Certificates for Company Domains in AWS Certificate Manager in the Amazon WorkLink Administration Guide.</td>
<td>April 18, 2019</td>
</tr>
<tr>
<td>You can upload your existing certificate or create a new one. (p. 47)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use service-linked role AWSServiceRoleForAmazonWorkLink to access resources linked</td>
<td>For more information, see Using Service-Linked Roles for Amazon WorkLink in the Amazon WorkLink Administration Guide.</td>
<td>April 1, 2019</td>
</tr>
<tr>
<td>to your fleets. (p. 47)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Added support for Android and Google Chrome (p. 47)</td>
<td>For more information, see Deploy a Device Certificate on an iOS Device in the Amazon WorkLink Administration Guide.</td>
<td>February 25, 2019</td>
</tr>
</tbody>
</table>
AWS glossary

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