Amazon WorkLink

Administration Guide

Amazon WorkLink: Administration Guide

Table of Contents

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, such as 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

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 (DX) – 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.
- AWS Transit Gateway – Provision a dedicated VPC to route Amazon WorkLink traffic and connect it to your company network with the AWS Transit Gateway.
- 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 (IAM) users, 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 as well as 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 web page 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

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

To sign up for an AWS account

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

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

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. Use your AWS account email address and password to sign in as the *AWS account root user* to the IAM console at https://console.aws.amazon.com/iam/.

   Note
   We strongly recommend that you adhere to the best practice of using the **`Administrator`** IAM user below 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 (ACM). 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.

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. 9).
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. 34).

Topics

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).

Note
You can use up to 48 characters, including letters, numbers, and "-". Don't use spaces.

4. (Optional) Under **Display name**, type a friendly name unique to your AWS account. This is used for internal searching purposes.
5. Choose **Create fleet**.

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.

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.

   Use the following instructions to set up a SAML 2.0 app using common identity providers:

   - To set up a SAML 2.0 app in Okta, see Setting Up a SAML Application in Okta.
   - To set up a SAML 2.0 app in AWS Single Sign-On, see Custom SAML 2.0 Applications.
   - To set up a SAML 2.0 app in Ping Identity, see Add or update a SAML application.
   - To set up a SAML 2.0 app in G Suite, see Set up your own custom SAML application.
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 the following:

   - 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 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/.
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. 7), 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. 9).
    - If the content of the webpage is displayed, your domain is successfully associated. Also, you have configured your company network to route Amazon WorkLink requests to this domain.
    - If the webpage doesn't display or shows a different error message, search for **AWS support** in the AWS Management Console. Choose **Create case** to contact us for help.

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**.
3. Choose **Company Network**, **Link network**.
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.
5. Choose **VPN** and enter the following **Connection info** settings:

   - **Connection Name** – Amazon WorkLink
   - **Connection Type** – L2TP/IPSec RSA
   - **Server** – 54.190.62.41
   - **Identity Certificate** – The device certificate that you configured

Option 3: 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.

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**.
3. Choose **Audit logs - optional**, **Configure audit logs**.
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

You can view detailed information about your fleets, including 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. Choose the button on any of the following categories to view detailed information about the fleet:
   - **Identity provider (IdP)**
   - **Company network**
   - **Device policies - optional**
   - **Domains**
   - **Audit logs - optional**
   - **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. Choose the button on any of the following categories to edit the category:
   - **Identity provider (IdP)**
   - **Company network**
   - **Device policies - optional**
   - **Domains**
   - **Audit logs - optional**
   - **User invites**
4. After making your edits, save your changes to update the fleet.

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

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

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. 8), you can view details, download or delete them, or upload more CAs.

Topics

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. 9), you can view and edit details about the network.

Topics

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

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

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. 11) 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

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

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**

Logging Amazon WorkLink API Calls with AWS CloudTrail

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 and 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"
}
```

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.

Troubleshooting

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

Issue	Solution
I can't download the Amazon WorkLink app.	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.
I can't find my company code.	From the Amazon WorkLink console, choose **Fleets**, and find the **Company code** column.
The company code I entered is invalid.	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.
After I enter my company code in the app, I don't see a login page. Instead, I see the following message: "WorkLink is unable to connect to your company's Identity Provider."	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).
After logging into my Identity Provider, I see an error message.	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.
After the Identity Provider sign-in in the Amazon WorkLink app, Amazon WorkLink shows as being not ready.	Search for **AWS support** in the AWS Management Console, and choose **Create case** to contact us for help.

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.

update-history-change	update-history-description	update-history-date
Attach an AWS managed policy to allow users to access Amazon WorkLink. (p. 35)	For more information, see Managing Access to Amazon WorkLink in the Amazon WorkLink Administration Guide.	September 10, 2019
If your domains use additional authorization providers, you can associate them to your fleet. (p. 35)	For more information, see Associate Website Authorization Providers in the Amazon WorkLink Administration Guide.	May 22, 2019
Manage TLS certificates used to associate your domains with AWS Certificate Manager (ACM). You can upload your existing certificate or create a new one. (p. 35)	For more information, see Prepare TLS Certificates for Company Domains in AWS Certificate Manager in the Amazon WorkLink Administration Guide.	April 18, 2019
Use service-linked role AWSServiceRoleForAmazonWorkLink to access resources linked to your fleets. (p. 35)	For more information, see Using Service-Linked Roles for Amazon WorkLink in the Amazon WorkLink Administration Guide.	April 1, 2019
Added support for Android and Google Chrome (p. 35)	For more information, see Deploy a Device Certificate on an iOS Device in the Amazon WorkLink Administration Guide.	February 25, 2019
Initial release (p. 35)	Initial release of Amazon WorkLink	January 23, 2019

AWS Glossary

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