Amazon Monitron

IT Manager's Guide

Amazon Monitron: IT Manager's Guide

Table of Contents

What Is Amazon Monitron?

Amazon Monitron is a machine learning (ML) end-to-end condition monitoring solution system that detects potential failures within equipment, enabling you to implement a predictive maintenance program and reduce lost productivity from unplanned machine downtime. Amazon Monitron includes purpose-built sensors to capture vibration and temperature data; gateways to automatically transfer data to the AWS Cloud; and a mobile application for system setup, analytics, and notification when tracking equipment condition. Reliability managers can quickly deploy Amazon Monitron to easily track the machine health of industrial equipment—such as bearings, motors, gearboxes, and pumps—without any development work or specialized training.

Using sensors mounted on your equipment and industry-recognized vibration standards and machine learning techniques, Amazon Monitron analyzes data for indications of potential equipment failure. It notifies you about developing faults so you can resolve them before they become more serious problems. With Amazon Monitron, you can schedule corrective maintenance activities more effectively to limit productivity losses and minimize repair costs that can result from catastrophic failure of your equipment.

The sensors capture both temperature and vibration data and send it to the AWS Cloud using gateways that fit unobtrusively on factory walls and use your Wi-Fi network. Amazon Monitron analyzes and interprets the data, then sends the information to the Amazon Monitron mobile app, where your team monitors the condition of your machines. When there is a problem with one of your machines, Amazon Monitron immediately sends a notification on the mobile app to let you know.

This guide covers IT Manager tasks, including

- Performing tasks that you need to do as AWS account user.
- Creating an Amazon Monitron project to contain the monitoring activities of the rest of your monitoring team (reliability managers and technicians). The *Amazon Monitron User Guide* describes how to install and operate the Amazon Monitron devices using the mobile app.
- Creating or attaching the project to an AWS Single Sign-On (AWS SSO) directory. End users will log into the app not as AWS account users, but through the credentials of the AWS SSO directory.

Topics

Features of Amazon Monitron

Amazon Monitron provides the following key features:

- **Works out of the box** – Amazon Monitron sensors and gateways are preconfigured to work with Amazon Monitron software. Reliability managers can install these devices easily and quickly using the

mobile app and can start monitoring equipment in just a matter of few hours. Amazon Monitron is simple to set up and requires no development work, knowledge of ML, or integration.

- **Immediate notifications in the Amazon Monitron mobile app** – When it detects abnormal machine patterns, Amazon Monitron sends notifications to users in the mobile app. Technicians can view, track, and provide feedback on these abnormal machine states within the mobile app.
- **ISO- and ML-based analytics** – Amazon Monitron automatically detects abnormal machine operating states by analyzing vibration and temperature signals and comparing them to International Standards Organization (ISO 20816) standard thresholds and ML enabled models.
- **Support for adding feedback in the app** –Amazon Monitron offers simple workflows for technicians to enter feedback on the accuracy and nature of the alerts in the mobile app. Amazon Monitron learns from that feedback and continually improves over time.

Amazon Monitron Devices and Software

Devices

Amazon Monitron includes two types of devices: a sensor, for collecting data from your equipment, and a gateway, for sending that data to Amazon Monitron. You can purchase both from Amazon.com or Amazon Business. You mount the sensors directly on the machines (or *assets*) that you want to monitor. You can place up to 20 sensors on an asset.

An Amazon Monitron sensor

Each sensor measures temperature and vibration data from the asset and sends it to the AWS Cloud using a gateway that is mounted nearby. If it's a Wi-Fi gateway, it is plugged into a standard outlet. If it's an Ethernet gateway, it gets power from the Ethernet cord plugged into its RJ-45 socket.

An Amazon Monitron Wi-Fi gateway

An Amazon Monitron Ethernet gateway

Software

Most Amazon Monitron tasks are performed by your team using the Amazon Monitron mobile app, which is installed on smartphones. The reliability manager uses this mobile app to set up assets, sensors, gateways, and so on. Technicians use the mobile app to monitor data from the sensors. For more information about these tasks, see the *Amazon Monitron User Guide*.

Amazon Monitron also includes a console, which is used by the IT Manager to create a project and add admin users to manage it. This project is the framework for all the Amazon Monitron tasks that the rest of the team performs to monitor your equipment. Until you set up the project, no other equipment monitoring can be done using Amazon Monitron. IT Manager tasks include the following:

- Setting up a user directory to provide users for Amazon Monitron
- Creating a project to contain all of your team's Amazon Monitron monitoring tasks, such as creating sites, pairing sensors, adding assets, and so on
- Adding an admin user to manage the project

This guide describes how to perform these tasks.

Getting Started with Amazon Monitron

Amazon Monitron divides tasks by whether they require the Amazon Monitron console or the mobile app. This guide shows you how to create a project and initially assign admin users to manage it. These are the tasks that require using the console. Tasks that use the Amazon Monitron mobile app include managing a project, creating assets, setting up sensors, and monitoring the condition of your equipment. For more information about these tasks, see the Amazon Monitron User Guide.

Before you can start the tasks in this guide, it's necessary to set up an AWS account and an admin user for the account, and provide permissions for that user. For more information, see Sign Up for AWS and Create an IAM User in the Amazon Monitron Getting Started Guide. The required permissions are listed in Using the Amazon Monitron Console (p. 34) in this guide.

For an overview of Amazon Monitron, we recommend that you begin by reading the following sections:

- How Amazon Monitron Works (p. 5) – To learn essential Amazon Monitron concepts.
- Managing Projects in Amazon Monitron (p. 7) – To learn how to set up a project for your team. This is the foundation for all Amazon Monitron tasks.

- Measurements and Machine Abnormalities – To learn how to monitor your equipment and understand the data you collect.

Related Resources

The Amazon Monitron documentation set includes three guides:

- **Amazon Monitron Getting Started Guide** – For IT managers, reliability managers, and technicians, this guide gets you started using Amazon Monitron.
- **Amazon Monitron User Guide** – For reliability managers (admin users) and technicians, this guide describes how to use Amazon Monitron to monitor your equipment for machine abnormalities. It also describes how to use the mobile app, your primary Amazon Monitron tool.
- **Amazon Monitron IT Manager's Guide** – This guide provides the IT manager more in-depth information about using Amazon Monitron than the *Amazon Monitron Getting Started Guide*. It also shows you how to use Amazon Monitron to set up projects and assign admin users to manage the project.

In addition to reading the guides, we also recommend that you visit the Amazon Monitron Discussion Forum. This community-based forum provides the chance for developers to discuss technical questions related to Amazon Monitron.

Pricing for Amazon Monitron

For information, see Amazon Monitron Pricing.

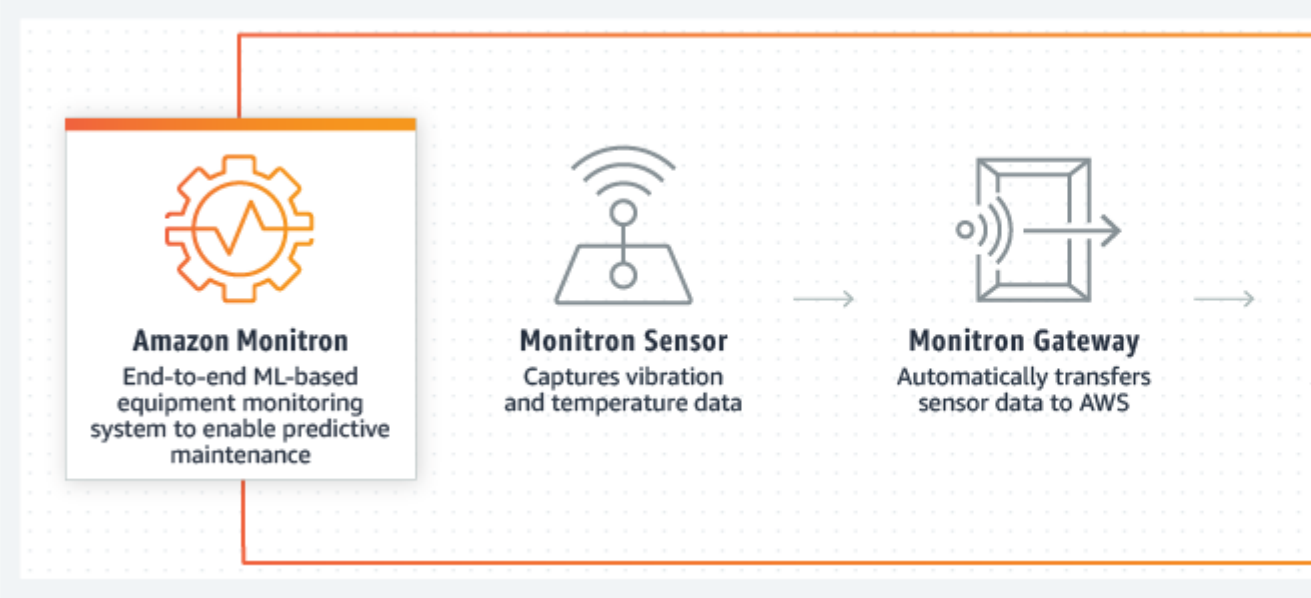
How Amazon Monitron Works

Amazon Monitron is an end-to-end system that detects abnormal machine behavior so you can enable predictive maintenance and reduce lost productivity from unplanned machine downtime. It includes sensors to capture vibration and temperature data, gateways to automatically transfer data to the AWS Cloud, machine learning-based software that analyzes the data for abnormal machine patterns, and a companion mobile app for simple system setup and immediate notifications of abnormal machine behavior. Reliability managers can quickly deploy Amazon Monitron to track machine health for industrial equipment, such as bearings, motors, gearboxes, and pumps, without any development work or specialized training.

.

The Amazon Monitron Workflow

The following diagram shows the basic workflow of Amazon Monitron.



1. An Amazon Monitron sensor captures temperature and vibration data from the equipment (the asset) and transmits it to the gateway.
2. An Amazon Monitron gateway transmits the data to the AWS Cloud using the factory's internet connection.
3. The Amazon Monitron ML model in the AWS Cloud analyzes the sensor data.
   a. Amazon Monitron looks for abnormalities in the data that could indicate developing faults.
   b. If Amazon Monitron finds potential equipment abnormalities, it notifies reliability managers and technicians through the Amazon Monitron mobile app so they can take appropriate action.
   c. Technicians investigate based on the alerts, and resolve the developing fault. They then enter feedback on the accuracy of the alerts, and report the mode, cause, and action taken in the mobile app. Amazon Monitron learns from this feedback and continually improves over time.
4. The mobile app displays current and past temperature and vibration data in charts that are easy to understand and can be used while investigating an issue.

Next Steps

If you are new to Amazon Monitron, we recommend that you read the following topics in order:

- Getting Started with Amazon Monitron in the *Amazon Monitron Getting Started Guide*.
- Quotas in Amazon Monitron (p. 19)
- Managing Measurements and Anomalies in the *Amazon Monitron User Guide*

Managing Projects in Amazon Monitron

Projects are the foundation for using Amazon Monitron. A project is where your team sets up the gateways, assets, and sensors that Amazon Monitron uses to detect the abnormal conditions that can lead to equipment failure.

A project is structured like this:

Project → site or sites → assets → positions → sensors

You can't share these resources between projects. Before you begin creating a project, we recommend that you carefully consider your project's needs. Make sure that it contains all of the resources required to predict the maintenance needs for all of your assets.

Only the IT manager can create, update, and delete projects and use the Amazon Monitron console for those tasks.

Topics

Creating a Project

Although an AWS account can have multiple Amazon Monitron projects, typically you have just one per account. The project name must be unique in your AWS account and AWS Region.

To create a project

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron.
2. Choose **Create Project**.
3. Under **Project Details**, for **Project name**, enter a name that:
   - Is unique in the current account
   - Consists of uppercase and lowercase letters, numbers, punctuation marks, and spaces
   - Is between 1 and 60 characters
4. By default, Amazon Monitron uses an AWS owned key to encrypt your project through the AWS Key Management Service (AWS KMS). If you want to use a different KMS key, choose **Custom encryption settings (advanced)** under **Data encryption** and do one of the following:
   - If you already have a KMS key that you want to use, under **Choose an AWS KMS key**, choose the key or enter the key's Amazon Resource Name (ARN).
   - If you want to create a key, choose **Create an AWS KMS key**. This takes you to the AWS KMS console so you can set up a custom key.

   For more information about encrypting a project, see KMS and Data Encryption in Amazon Monitron (p. 26).

5. (Optional) To add a tag to the project, enter a key-value pair under **Tags** and then choose **Add tag**. To remove this tag before creating the project, choose **Remove tag**.

   For more information, see Using Tags With Your Amazon Monitron Project (p. 8).
6. Choose **Next** to create the project.

Now you are ready to add users to the project. See User Directory Setup (p. 14).

Using Tags With Your Amazon Monitron Project

A *tag* is a key-value pair that you can use to categorize your projects. For example, if you have multiple projects, you might categorize them by purpose, owner, location, or any other factor.

Use tags to:

- Organize your projects. You can search and filter by tag. For example, you could add tags such as 'test lab' or 'paint shop' to easily find those projects.
- Identify and organize your AWS resources. Many AWS services support tagging, so you can assign the same tag to resources in different services to indicate that the resources are related. For example, you can tag a project and the Amazon Simple Storage Service (Amazon S3) bucket that stores related data with the same tag.
- Control access to your resources. You can use tags in AWS Identity and Access Management (IAM) polices that control access to Amazon Monitron projects. You can attach these policies to an IAM role or user to enable tag-based access control. For more information, see Controlling access using tags in the *IAM User Guide*.

Each tag key must be unique within a project.

The following restrictions also apply to Amazon Monitron project tags:

- The maximum number of tags per project is 50.
- The maximum length of a tag key is 128 characters.
- The maximum length of a tag value is 256 characters.
- Valid characters for keys and values are a–z, A–Z, space, _ . : / = + - and @.
- Tag keys and values are case sensitive.
- The `aws:` prefix is reserved for AWS use.
- If you plan to use your tagging schema across multiple services and resources, remember that other services might have different restrictions for valid characters. Refer to the documentation for that service.

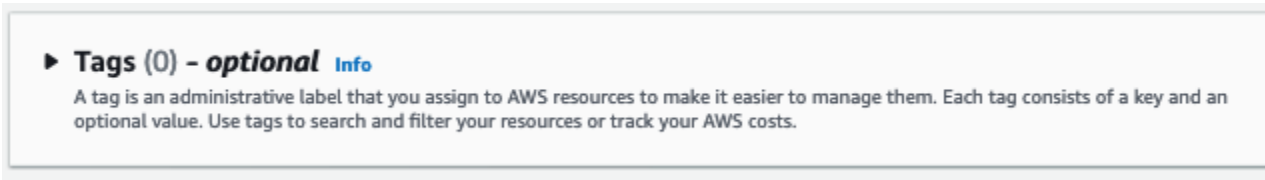
Topics

Adding a Tag to a Project When You Create It

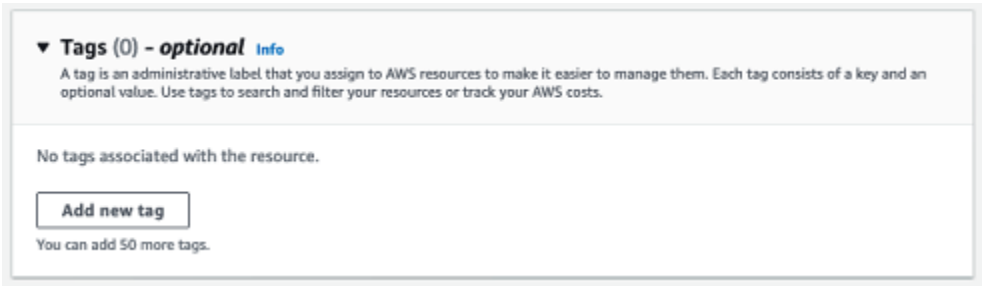
To add a tag to a project when creating it

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron .
2. Choose **Create Project**.

3. In the navigation pane, choose the project you want
4. Expand the **Tags** section.

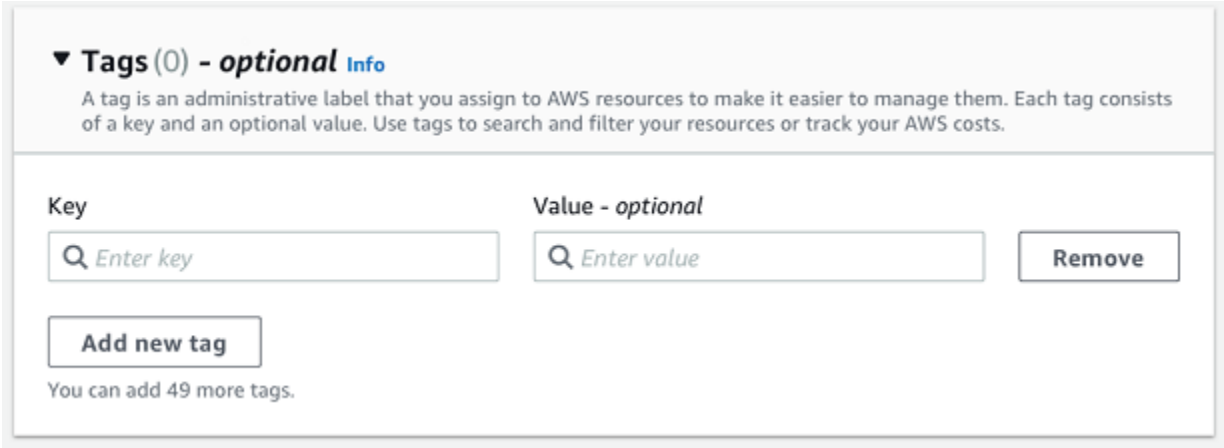


5. Choose **Add new tag**.

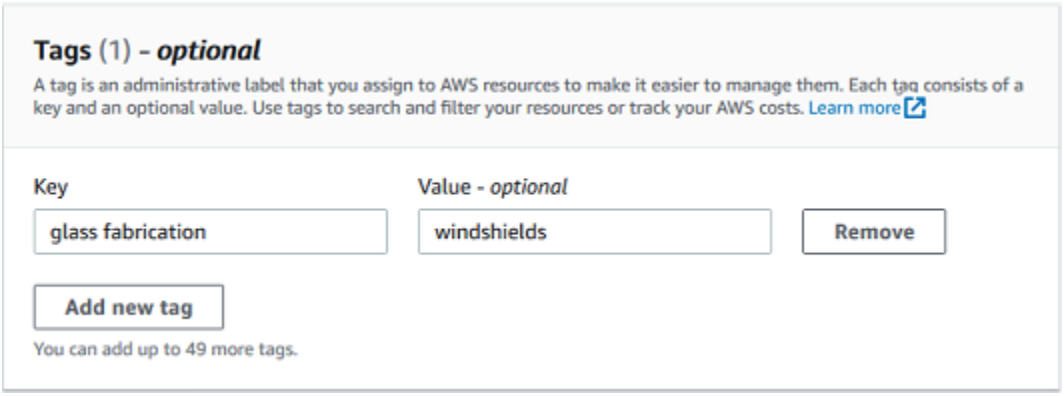


6. Enter the key-value pair for your tag.

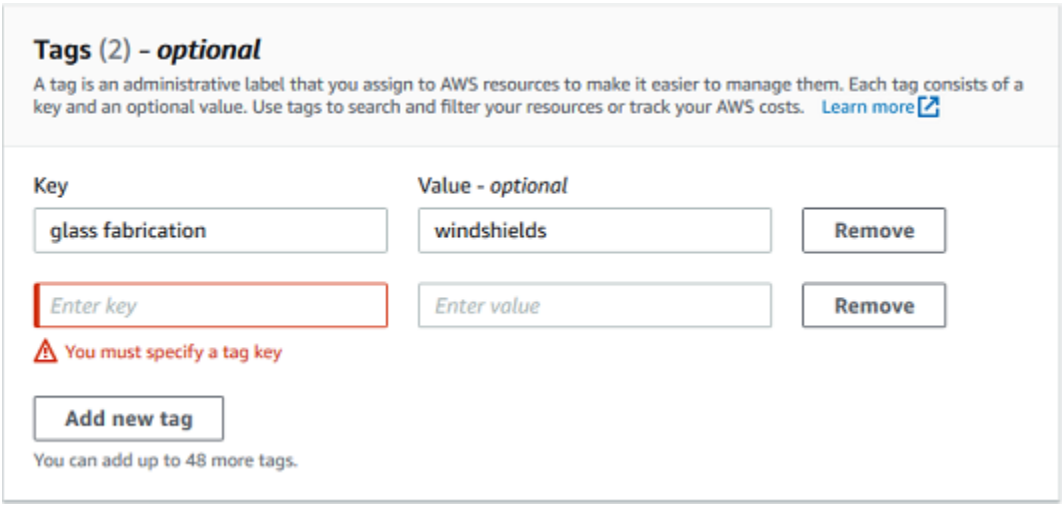
   The key must be unique for the project. The value is optional.



7. Choose **Add new tag**.
8. To add more tags, repeat steps 2 and 3.
9. To remove a tag, choose **Remove**.



10. Remove blank tag entries and then choose **Next**.

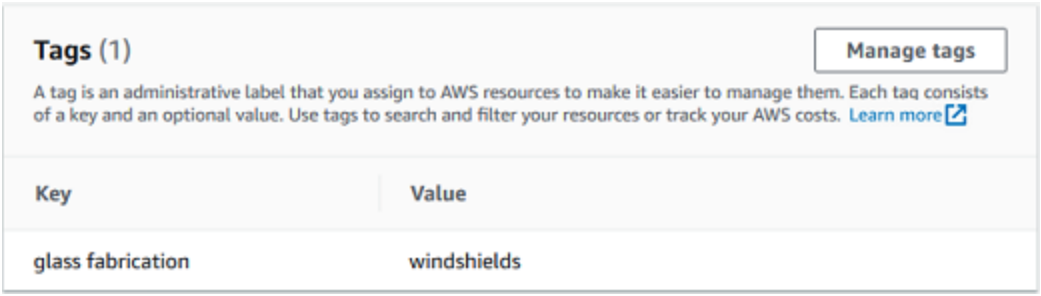


Adding a Tag to a Project After It's Been Created

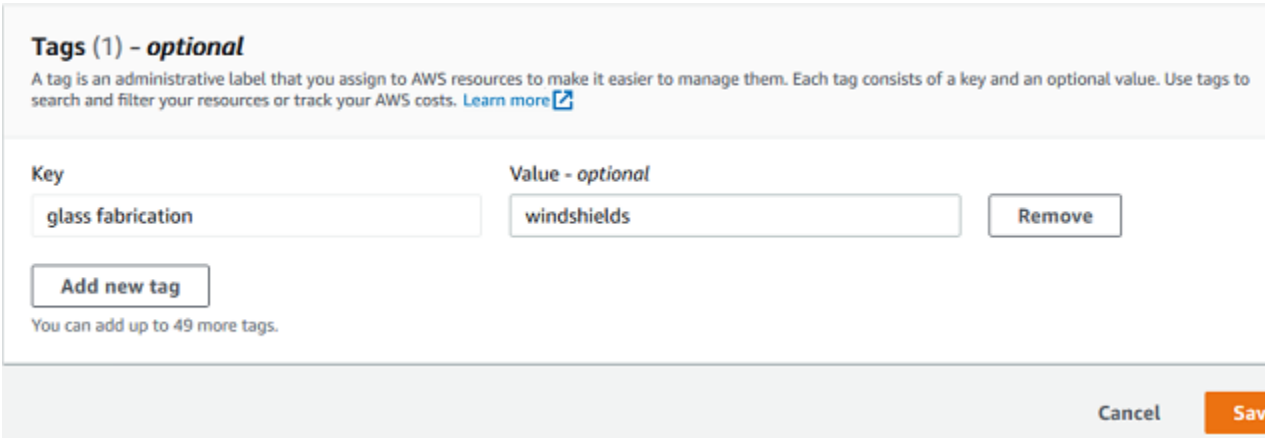
You can add a tag to a project on the project detail page.

To add a tag to an existing project

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron .
2. Choose **Create Project**.
3. In the navigation pane, choose **Projects**, and then choose the project you want.
4. Under **Tags**, choose **Manage tags**.

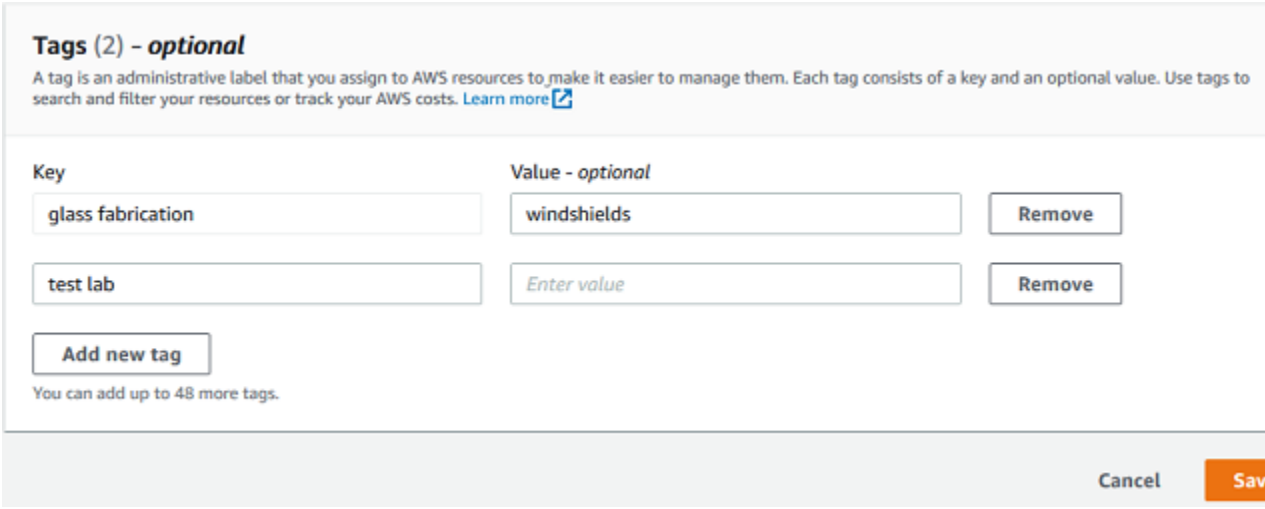


5. Choose **Add new tag**



6. Enter the key-value pair for your tag.

   Note
   Remember that the key must be unique for the project. The value is optional.



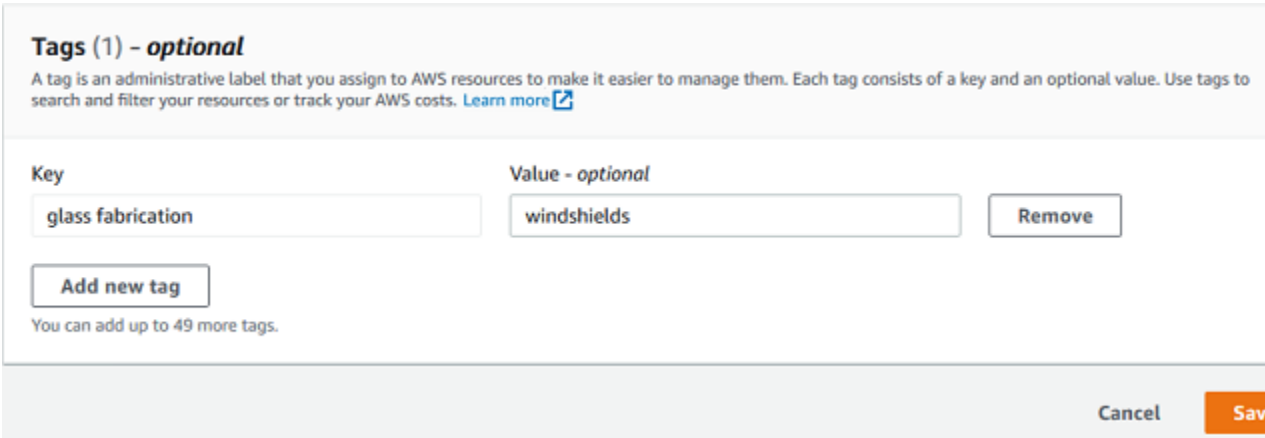
7. Choose **Save**.

Modifying or Removing a Tag

You can modify a tag value, but not a tag key. To change a tag key, remove the tag, then create a new tag with a different key. You can also remove any tag. You modify or remove tags on the project detail page.

To modify or remove a tag

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron.
2. Choose **Create Project**.
3. In the navigation pane, choose **Projects**, and then choose the project you want.
4. Under **Tags**, choose **Manage tags**.
5. To modify the tag value, make the change. To remove the tag, choose **Remove** next to the tag.



6. Choose **Save**.

Updating a Project

Only the project name can be edited using this procedure. The list of Admin users can also be changed, but you do this using the edit users process.

To edit a project

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron .
2. Choose **Create Project**.
3. In the navigation pane, choose the project you want to change.
4. From the **Projects** list, choose the project you want to edit.
5. Choose **Edit project**.
6. Edit the project name.
7. Choose **Save**.

Deleting a Project

With the `deleteProject` operation, you must have the AWS Single Sign-On (SSO) permissions for deletion. Without these permissions, the console's delete project functionality will still remove the project. However, it will not remove the resources from SSO and you may end up with dangling references on SSO.

To delete a project

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron .
2. Choose **Create Project**.
3. In the navigation pane, choose **Projects**.
4. From the **Projects** list, choose the project you want to delete.
5. Choose **Delete Project**.
6. Enter **Delete** in the confirmation box to confirm the deletion.

   If the project contains any active assets or sensors, you have to remove them before deleting the project. If this is the case, the confirmation box and option to delete don't appear.

   If there are active assets or sensors that need to be removed to delete this project, ask an Admin user do this or do it yourself by logging into the *Amazon Monitron mobile app*.
7. Choose **Delete**.

Additional Project Tasks

Two common project-related tasks that you might frequently encounter are listing all of your projects and retrieving the details on one specific project. You accomplish both of these tasks using the Amazon Monitron console.

To list all projects

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron .
2. Choose **Create Project**.
3. In the navigation pane, choose **Projects**.

The list of projects is displayed under **Projects**.

To get details about a project

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron .
2. Choose **Create Project**.
3. In the navigation pane, choose **Projects**.

   The list of projects is displayed under **Projects**.
4. Choose the project that you want to get details on.

Managing Admin Users

After creating a project, you need to assign at least one Admin user to help manage it. You can also add Admin users to a project or remove them from a project later. After using the console to add the first Admin user, you can add additional Admin users with the Amazon Monitron mobile app.

Topics

User Directory Setup

Amazon Monitron uses AWS Single Sign-On (AWS SSO) to manage user access. Users are added from this AWS SSO user directory.

When you create a project, Amazon Monitron automatically detects whether AWS SSO has been enabled and configured on your account and whether all prerequisites for using AWS SSO with Amazon Monitron are satisfied. If not, Amazon Monitron produces an error and provides a list of prerequisites that are needed. You must meet all prerequisites before you can add Admin users. For more information about enabling and configuring AWS SSO for your organization, see AWS Single Sign-On.

How you add an Admin user depends on how AWS SSO has been set up for your organization.

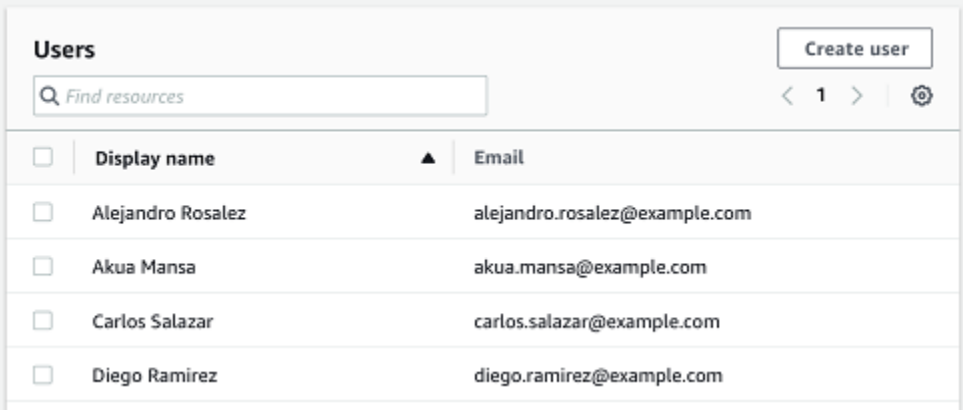
Topics

Adding Admin Users Using the Native AWS SSO Directory

The simplest way to add Admin users to your project is by using the AWS SSO native directory. You can use it by starting to use Amazon Monitron and letting it configure AWS SSO at a basic level for you. You can also set up AWS SSO prior to using Amazon Monitron and set it to use the native directory. Either way, you can add users manually and without potentially exposing user identity information to other Admin users beyond name and email.

To add an Admin user when using the native AWS SSO directory

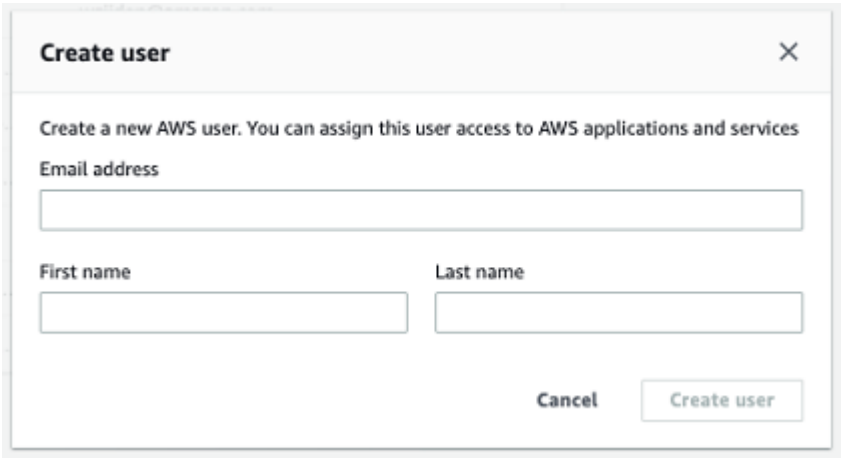
1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron .
2. Choose **Create Project**.
3. In the navigation pane, choose the project you want.
4. On the **Users** page, choose the users that you want to assign as Admin users. If you can't see a user, search for them.



The users you choose are displayed in the **Selected users** section.

5. If the user you want isn't in the directory, choose **Create user** to add the user.

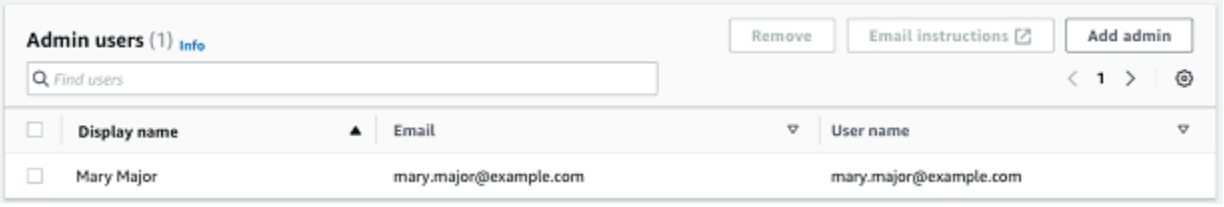
   1. Under **Create a user**, for **Email**, enter the new Admin user's email address.



   2. For **First name** and **Last name**, enter the admin's name.
   3. Choose **Create User**.

6. When the user's name appears in the directory list, choose **Add** to add the Admin users you've selected.
7. Email the Admin users an invitation to the project that includes a link to download the Amazon Monitron mobile app. For more information, see Sending an Email Invitation (p. 18).

   Amazon Monitron takes you to the project page for your project, where it lists all Admin users.



8. To add additional Admin users, choose **Add Admin**.

   Any Admin user can add other users using the Amazon Monitron mobile app. For more information, see Adding a User in the *Amazon Monitron User Guide*.

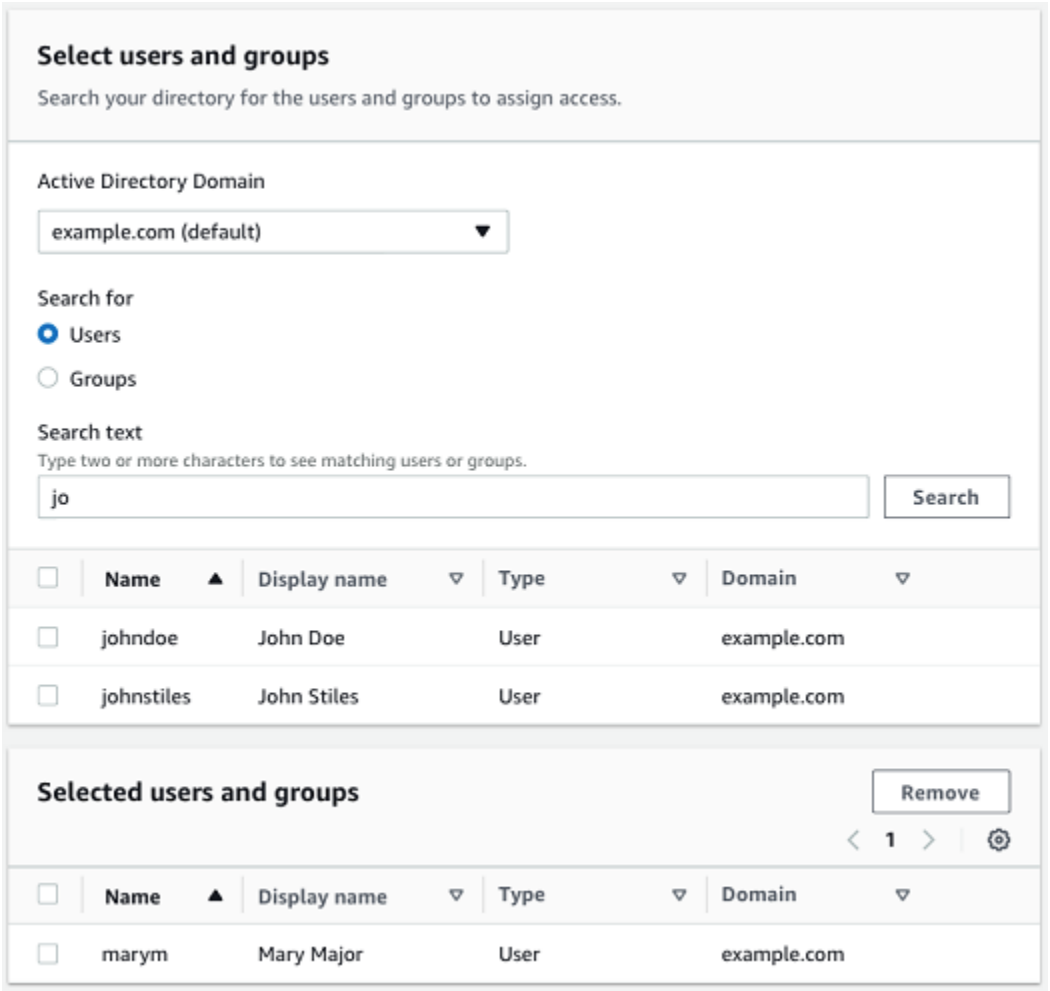
Adding Admin Users Using Microsoft Active Directory

If you use Microsoft Active Directory (AD) for your organization's primary user directory, you can configure AWS SSO to use it. AWS SSO enables you to connect your self-managed Active Directory as your AWS Managed Microsoft AD directory using AWS Directory Service. This Microsoft AD directory provides you with the pool of identities that you can pull from when using the Amazon Monitron console (or Amazon Monitron mobile app) to assign user roles.

All Amazon Monitron Admin users have access to identity information in the user directory that is configured in AWS SSO for Amazon Monitron. We strongly recommend using an isolated directory if you want to limit access to user organization information.

To add an Admin user using Microsoft Active Directory

1. Configure AWS SSO to connect with your Microsoft Active Directory. The steps involved in this differ depending on whether you're using a self-managed Active Directory or an AWS Managed Microsoft AD directory. For more information, see Connect to Microsoft AD Directory.
2. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron .
3. Choose **Create Project**.
4. In the navigation pane, choose the project you want.
5. For **Active directory domain**, choose the directory domain from which you want to add identities.



6. Choose **Users** or **Groups**, depending on how you want to search the user directory.

7. Enter a string in the search box to find the identity you want to add and then choose **Search**.

   To limit the number of users returned, enter a longer string in the search box. For example, if you enter "olg" in the search box, the list returns all users with the letters "olg" in their names, such as "Olga Kurth" and "Jamie Folgman."
8. Choose the users you want to assign as Admin users.
9. Choose **Add** to add the Admin users.

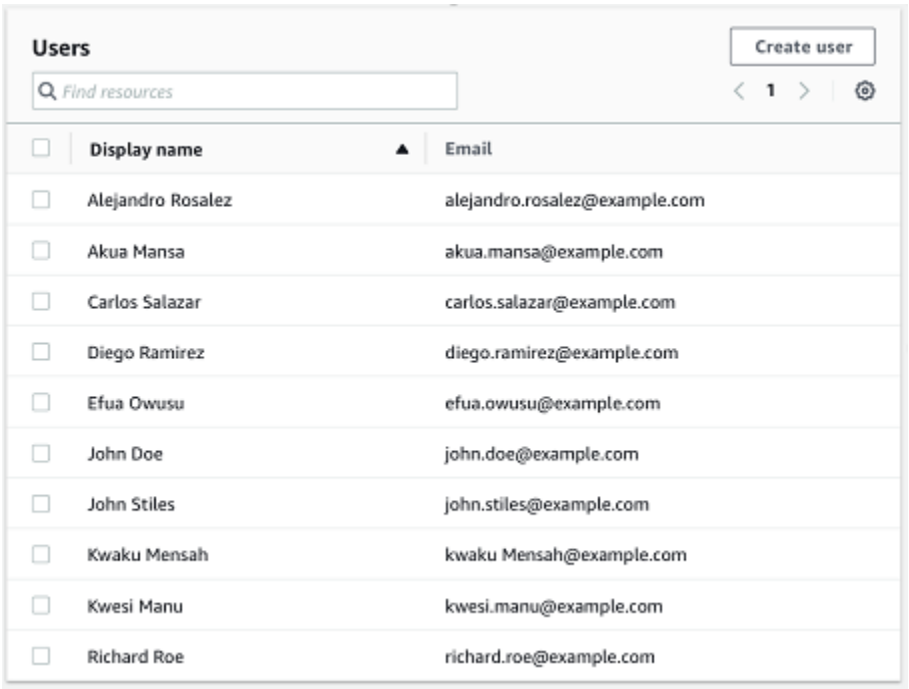
Adding Admin Users Using an External ID Provider

If you're using an external Identity provider (IdP), you can configure AWS SSO to use that provider through the Security Assertion Markup Language (SAML) 2.0 standard. This provides you with the pool of identities in your IdP directory. You can pull this pool when using the Amazon Monitron console (or Amazon Monitron mobile app) and assign them as Admin users. This also enables your users to sign in to Amazon Monitron with their corporate credentials.

All Amazon Monitron Admin users have access to identity information in the user directory that is configured in AWS SSO for Amazon Monitron. We strongly recommend using an isolated directory if you want to limit access to user organization information.

To add an Admin user using an external ID provider (IdP)

1. Configure AWS SSO to connect with your external IdP. The steps involved in this differ based on the provider you're using. For more information, see Connect to Your External ID Provider.
2. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron .
3. Choose **Create Project**.
4. In the navigation pane, choose the project you want.
5. On the **Users** page, choose the users that you want to assign as Admin users. If you can't see a user, search for them.



6. Choose **Add** to add the Admin users.

Removing an Admin User

Every project must have at least one Admin user. Before removing an Admin user from a project, make sure that there is at least one other Admin user assigned to it.

To remove an Admin user

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron .
2. Choose **Create Project**.
3. In the navigation pane, choose the project you want.
4. From the **Admin Users** list, choose the user that you want to remove.
5. Choose **Remove**.
6. Choose **Remove** again.

   The user is removed from the list of Admin users for that project.

Sending an Email Invitation

When you add a user to an Amazon Monitron project or site, you need to send them an email and invite them to download and log in to the Amazon Monitron mobile app. This invitation should also contains instructions for connecting to the project to which the user was added.

To generate an email invitation to a site or project

1. Add the user to the site or project.
2. On the **Project Details** page, choose the user you added.
3. Choose **Email instructions**.

   A draft of the email invitation addressed to that user is displayed. It contains a link to download the Amazon Monitron mobile app from the Google Play Store and a link to open the project to which they've been added.
4. Verify that the email is correct, and then send it to the user.

Warning
Because of the danger of phishing attacks, for example, when an attacker sends an email impersonating an Amazon Monitron project invitation email to your users, warn the user to make sure that the directory name is visible on the login screen before entering sign-in credentials.

Quotas in Amazon Monitron

You can request an increase of many of the Amazon Monitron quotas if your applications require it. For information about service quotas and to request a quota increase, see AWS Service Quotas.

Supported Regions

Amazon Monitron is currently supported in the following AWS Region:

- US East (N. Virginia): us-east-1
- Europe (Ireland): eu-west-1

Quotas

The following table lists the quotas for Amazon Monitron resources, sensors, gateways, and users.

Description	Quota
Maximum number of projects per account	10
Maximum number of sites per project	50
Maximum number of assets per site	100
Maximum number of positions (or sensors) per asset	20
Maximum number of gateways per site	200
Maximum number of users per site	20

Logging Amazon Monitron Actions with AWS CloudTrail

Amazon Monitron is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon Monitron. CloudTrail captures API calls for Amazon Monitron as events. CloudTrail captures calls from both the Amazon Monitron console and the Amazon Monitron mobile app. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon Simple Storage Service (Amazon S3) bucket, including events for Amazon Monitron. 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 console or mobile app request that was made to Amazon Monitron, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, including how to configure and enable it, see the AWS CloudTrail User Guide.

Topics

Amazon Monitron Information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When supported event activity occurs in Amazon Monitron, 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 Monitron, 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 the following:

- 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

Amazon Monitron supports logging a number of actions as events. Although the operations are publicly accessible through the AWS console or the Amazon Monitron mobile app, the APIs themselves are not public and are subject to change. They are meant for logging purposes only, and applications should not be built with them.

Amazon Monitron supports the following actions as events in CloudTrail log files:

- CreateProject
- UpdateProject

- DeleteProject
- GetProject
- ListProjects
- AssociateProjectAdminUser
- DisassociateProjectAdminUser
- ListProjectAdminUsers
- GetProjectAdminUser
- TagResource
- UntagResource
- ListTagsForResource
- AmazonMonitronApp:CreateSensor
- AmazonMonitronApp:UpdateSensor
- AmazonMonitronApp:DeleteSensor
- AmazonMonitronApp:CreateGateway
- AmazonMonitronApp:DeleteGateway
- AmazonMonitronApp:CreateSite
- AmazonMonitronApp:UpdateSite
- AmazonMonitronApp:DeleteSite
- AmazonMonitronApp:CreateAsset
- AmazonMonitronApp:UpdateAsset
- AmazonMonitronApp:DeleteAsset
- AmazonMonitronApp:CreateAssetStateTransition
- AmazonMonitronApp:CreateUserAccessRoleAssociation
- AmazonMonitronApp:UpdateUserAccessRoleAssociation
- AmazonMonitronApp:DeleteUserAccessRoleAssociation

Every event or log entry contains information about who generated the request. This contains details about the type of IAM identity that made the request, and which credentials were used. If temporary credentials were used, the element shows how the credentials were obtained. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials
- Whether the request was made with temporary security credentials for a role or federated user
- Whether the request was made by another AWS service

For more information, see the CloudTrail userIdentity Element in the *AWS CloudTrail User Guide*.

Example: Amazon Monitron 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 examples show CloudTrail log entries that demonstrate the project deletion (`DeleteProject`) action.

Successful DeleteProject Action

The following example show what might appear in the CloudTrail log following a successful `DeleteProject` action.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principal ID",
    "arn": "ARN",
    "accountId": "account ID",
    "accessKeyId": "access key ID",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principal ID",
        "arn": "ARN",
        "accountId": "account ID",
        "userName": "user name"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "timestamp"
      }
    }
  },
  "eventTime": "timestamp",
  "eventSource": "monitron.amazonaws.com",
  "eventName": "DeleteProject",
  "awsRegion": "region",
  "sourceIPAddress": "source IP address",
  "userAgent": "user agent",
  "requestParameters": {
    "Name": "name"
  },
  "responseElements": {
    "Name": "name"
  },
  "requestID": "request ID",
  "eventID": "event ID",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "account ID"
}
```

Failed DeleteProject Action (Authorization Error)

The following example shows what might appear in the CloudTrail log following a failed `DeleteProject` action due to an error occurring. In this case, the error is an authorization error, where the user does not have permission to delete the specified project.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "principal ID",
        "arn": "ARN",
        "accountId": "account ID",
        "accessKeyId": "access key ID",
        "userName": "user name",
```

```
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "timestamp"
            }
        }
    },
    "eventTime": "timestamp",
    "eventSource": "monitron.amazonaws.com",
    "eventName": "DeleteProject",
    "awsRegion": "region",
    "sourceIPAddress": "source IP address",
    "userAgent": "user agent",
    "errorCode": "AccessDenied",
    "requestParameters": {
        "Name": "name"
    },
    "responseElements": {
        "Message": "User: user ARN is not authorized to perform: monitron:DeleteProject on
 resource: resource ARN"
    },
    "requestID": "request ID",
    "eventID": "event ID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "account ID"
}
```

Failed DeleteProject Action (Conflict Exception Error)

The following example shows what might appear in the CloudTrail log following a failed `DeleteProject` action due to an error occurring. In this case, the error is a conflict exception, where sensors are still present when Amazon Monitron attempts to delete a project.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principal ID",
    "arn": "ARN",
    "accountId": "account ID",
    "accessKeyId": "access key ID",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principal ID",
        "arn": "ARN",
        "accountId": "account ID",
        "userName": "user name"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "timestamp"
      }
    }
  },
  "eventTime": "timestamp",
  "eventSource": "monitron.amazonaws.com",
  "eventName": "DeleteProject",
  "awsRegion": "region",
  "sourceIPAddress": "source IP address",
```

```
  "userAgent": "user agent",
  "errorCode": "ConflictException",
  "requestParameters": {
    "Name": "name"
  },
  "responseElements": {
    "message": "This project still has sensors associated to it and cannot be deleted."
  },
  "requestID": "request ID",
  "eventID": "event ID",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "account ID"
}
```

Security in Amazon Monitron

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

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

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to Amazon Monitron, 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 Monitron. The following topics show you how to configure Amazon Monitron 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 Monitron resources.

Topics

Data Protection in Amazon Monitron

Amazon Monitron conforms to the AWS shared responsibility model, which includes regulations and guidelines for data protection. AWS is responsible for protecting the global infrastructure that runs all the AWS services. AWS maintains control over data hosted on this infrastructure, including the security configuration controls for handling customer content and personal data. AWS customers and APN partners, acting either as data controllers or data processors, are responsible for any personal data that they put in the AWS Cloud.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM), so that each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use TLS (Transport Layer Security) to communicate with AWS resources.

- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.

We strongly recommend that you never put sensitive identifying information, such as your customers' account numbers, into free-form fields such as a **Name** field. This includes when you work with Amazon Monitron or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into Amazon Monitron or other services might get picked up for inclusion in diagnostic logs. When you provide a URL to an external server, don't include credentials information in the URL to validate your request to that server.

For more information about data protection, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

Data at Rest

Your data is encrypted at rest in the cloud using one of two types of keys through AWS Key Management Service (AWS KMS). The data is encrypted in Amazon Simple Storage Service (Amazon S3) using an AWS owned key. Amazon Monitron also stores data in tables in Amazon DynamoDB. By default, these are encrypted using an AWS owned CMK. However, if a customer chooses **Custom encryption settings** when setting up a project, Amazon Monitron uses a customer managed CMK.

Data in Transit

Amazon Monitron uses TLS (Transport Layer Security) to encrypt data that is transferred between your sensors and Amazon Monitron.

KMS and Data Encryption in Amazon Monitron

Amazon Monitron encrypts your data and project information using one of two types of keys through AWS Key Management Service (AWS KMS). You can choose one of the following:

- An AWS owned key. This is the default encryption key and is used if you do not choose **Custom encryption settings** when setting up your project.
- A customer managed CMK. You can use an existing key in your AWS account or create a key in the AWS KMS console or using the API. If you're using an existing key, you choose **Choose an AWS KMS key** and then either choose a key from the list of AWS KMS keys, or enter the Amazon Resource Name (ARN) of another key. If you want to create a new key, you choose **Create an AWS KMS key**. For more information, see Creating Keys in the *AWS Key Management Service Developer Guide*.

When using AWS KMS to encrypt your data, keep the following in mind:

- Your data is encrypted at rest in the Cloud in Amazon S3 and Amazon DynamoDB.
- When data is encrypted using an AWS owned CMK, Amazon Monitron uses a separate CMK for each customer.
- IAM users must have the required permissions to call the AWS KMS API operations connected with Amazon Monitron. Amazon Monitron includes the following permissions in its managed policy for console use.

```
{
                "Effect": "Allow",
```

```
                "Action": [
                        "kms:ListKeys",
                        "kms:DescribeKey",
                        "kms:ListAliases",
                        "kms:CreateGrant"
                ],
                "Resource": "*"
        },
```

For more information, see Using IAM Policies with AWS KMS in the *AWS Key Management Service Developer Guide*.

- If you delete or disable your CMK, you won't be able to access the data. For more information, see Deleting AWS KMS keys in the *AWS Key Management Service Developer Guide*.

Identity and Access Management for Amazon Monitron

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

Topics

Audience

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

Service user – If you use the Amazon Monitron service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon Monitron 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 Monitron, see Troubleshooting Amazon Monitron Identity and Access (p. 35).

Service administrator – If you're in charge of Amazon Monitron resources at your company, you probably have full access to Amazon Monitron. It's your job to determine which Amazon Monitron 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 Monitron, see How Amazon Monitron Works with IAM (p. 31).

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 Monitron. To view example Amazon Monitron identity-based policies that you can use in IAM, see Amazon Monitron Identity-Based Policy Examples (p. 33).

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 Monitron 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*.

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 Monitron Works with IAM

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

Topics

Amazon Monitron Identity-Based Policies

To specify allowed or denied actions and resources and the conditions under which actions are allowed or denied, use IAM identity-based policies. Amazon Monitron supports specific actions, resources, and condition keys. To learn 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.

In Amazon Monitron, policy actions use the following prefix before the action: `monitron:`. For example, to grant someone permission to create a project with the Amazon Monitron `CreateProject` operation, you include the `monitron:CreateProject` action in their policy. Policy statements must include either an `Action` or `NotAction` element. Amazon Monitron defines its own set of actions that describe tasks that you can perform with this service.

> **Note**
> With the `deleteProject` operation, you must have the AWS Single Sign-On (SSO) permissions for deletion. Without these permissions, the delete functionality will still remove the project. However, it will not remove the resources from SSO and you may end up with dangling references on SSO.

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

```
"Action": [
      "monitron:action1",
      "monitron:action2"
]
```

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

```
"Action": "monitron:List*"
```

Resources

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

Condition Keys

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 `Condition` element (or `Condition` *block*) lets you specify conditions in which a statement is in effect. The `Condition` element is optional. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request.

If you specify multiple `Condition` elements in a statement, or multiple keys in a single `Condition` element, AWS evaluates them using a logical `AND` operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical `OR` operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see IAM policy elements: variables and tags in the *IAM User Guide*.

AWS supports global condition keys and service-specific condition keys. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

Amazon Monitron defines its own set of condition keys and also supports using some global condition keys. For a list of all AWS global condition keys, see AWS Global Condition Context Keys in the *IAM User Guide*.

To see a list of Amazon Monitron condition keys, see Condition Keys for Amazon Monitron in the *IAM User Guide*. To learn with which actions and resources you can use a condition key, see Actions Defined by Amazon Monitron.

Examples

To view examples of Amazon Monitron identity-based policies, see Amazon Monitron Identity-Based Policy Examples (p. 33).

Amazon Monitron Resource-Based Policies

Amazon Monitron does not support resource-based policies.

Authorization Based on Amazon Monitron Tags

You can associate tags with certain types of Amazon Monitron resources for authorization. To control access based on tags, provide tag information in the condition element of a policy using the `Amazon Monitron:TagResource/${TagKey}`, `aws:RequestTag/${TagKey}`, or `aws:TagKeys` condition keys.

Amazon Monitron IAM Roles

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

Using Temporary Credentials with Amazon Monitron

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

Amazon Monitron 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 Monitron supports service-linked roles.

Service Roles

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

Amazon Monitron supports service roles.

Amazon Monitron Identity-Based Policy Examples

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

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

Topics

Policy Best Practices

Identity-based policies are very powerful. They determine whether someone can create, access, or delete Amazon Monitron 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 Monitron quickly, use AWS managed policies to give your employees the permissions they need. These policies are already available in your account and are maintained and updated by AWS. For more information, see Get started using permissions with AWS managed policies in the *IAM User Guide*.
- **Grant least privilege** – When you create custom policies, grant only the permissions required to perform a task. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. For more information, see Grant least privilege in the *IAM User Guide*.
- **Enable MFA for sensitive operations** – For extra security, require IAM users to use multi-factor authentication (MFA) to access sensitive resources or API operations. For more information, see Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.

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

Using the Amazon Monitron Console

To set up Amazon Monitron using the console, please complete the initial setup process using a high privilege user (such as one with the `AdministratorAccess` managed policy attached).

To access the Amazon Monitron console for day-to-day operations after the initial setup, you must have a minimum set of permissions. These permissions must allow you to list and view details about the Amazon Monitron resources in your AWS account and include a set of permissions related to AWS SSO. If you create an identity-based policy that is more restrictive than these minimum required permissions, the console won't function as intended for entities (IAM users or roles) with that policy. For basic Amazon Monitron Console functionality, you need to attach the `AmazonMonitronFullAccess` managed policy. Depending on the circumstances, you may also need additional permissions to the Organizations and SSO service. Contact AWS support if you need more information.

Example: List All Amazon Monitron Projects

This example policy grants an IAM user in your AWS account permission to list all projects in your account.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "monitron:ListProject"
            "Resource": "*"
        }
    ]
}
```

Example: List Amazon Monitron Projects Based on Tags

You can use conditions in your identity-based policy to control access to Amazon Monitron resources based on tags. This example shows how you might create a policy that allows listing projects. However, permission is granted only if the project tag `location` has the value of `Seattle`. This policy also grants the permissions necessary to complete this action on the console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListProjectsInConsole",
            "Effect": "Allow",
            "Action": "monitron:ListProjects",
            "Resource": "*"

            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/location": "Seattle"
                }
            }
```

```
        }
    ]
}
```

For more information, see IAM JSON Policy Elements: Condition in the *IAM User Guide*.

Troubleshooting Amazon Monitron Identity and Access

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

Topics

I Am Not Authorized to Perform an Action in Amazon Monitron

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

The following example error occurs when the `mateojackson` IAM user tries to use the console to view details about a project but does not have `monitron:GetProject` permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 monitron:GetProject on resource: Dalla Fulfillment Center
```

In this case, Mateo asks his administrator to update his policies to allow him to access the `Dallas Fulfillment Center` resource using the `monitron:GetProject` action.

I Want to View My Access Keys

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

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

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

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

I'm an Administrator and Want to Allow Others to Access Amazon Monitron

To allow others to access Amazon Monitron, 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 Monitron.

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 Monitron 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 Monitron supports these features, see How Amazon Monitron Works with IAM (p. 31).
- 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 Monitron

Monitoring is an important part of maintaining the reliability, availability, and performance of your Amazon Monitron applications. To monitor Amazon Monitron console and mobile app actions, you can use AWS CloudTrail.

CloudTrail logs provide a record of actions taken by a user, role, or an AWS service in Amazon Monitron. Using the information collected by CloudTrail, you can determine the request that was made to Amazon Monitron, the IP address from which the request was made, who made the request, when it was made, and additional details. For more information, see Logging Amazon Monitron Actions with AWS CloudTrail (p. 20).

Compliance Validation for Amazon Monitron

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 Monitron or other AWS services are in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

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

Your compliance responsibility when using 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* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.
- AWS Audit Manager – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

Infrastructure Security in Amazon Monitron

As a managed service, Amazon Monitron 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 Monitron through the network. Clients must support Transport Layer Security (TLS) 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

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

Security Best Practices for Amazon Monitron

Amazon Monitron provides a number of security features to consider as you develop and implement your own security policies. The following best practices are general guidelines and don't represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions.

The following best practices for Amazon Monitron can help prevent security incidents:

- When creating an AWS Single Sign-On (AWS SSO) directory of users for Amazon Monitron enable multi-factor authentication (MFA) for the directory for better directory security.
- Be aware that all project and site admins using the Amazon Monitron mobile app will have read access to all users in your organization who are listed in the user directory you choose when setting up your project. We strongly recommend using an isolated directory if you want to limit access to user organization information.

- Because of the danger of phishing attacks, in which an attacker sends an email impersonating a Amazon Monitron project invitation email to your users, warn users to make sure that the directory name is visible on the login screen before they enter their sign-in credentials.
- Because the Amazon Monitron mobile app runs on a smartphone and has access to your project, have all users enable screen lock to protect access when not in use.

Document History for the Amazon Monitron IT Manager's Guide

The following table describes important changes in each release of the Amazon Monitron IT Manager's Guide. For notification about updates to this documentation, you can subscribe to an RSS feed.

- **Latest documentation update:** May 5, 2021

Change	Description	Date
New region supported	Amazon Monitron is now available in the Europe (Ireland) Region. For all supported Regions, see Supported Regions (p. 19).	May 5, 2021
New service and guide	This is the initial release of the Amazon Monitron IT Manager's Guide	December 1, 2020