aws

User Guide

# Amazon Monitron



Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# Amazon Monitron: User Guide

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

# Table of Contents


**..... x**

**What is Amazon Monitron? ..... 1**

Amazon Monitron devices ..... 1

Amazon Monitron software ..... 3

Benefits of Amazon Monitron ..... 7

Pricing for Amazon Monitron ..... 7

Related resources ..... 7

Are you a first-time user of Amazon Monitron? ..... 8

**How Amazon Monitron works ..... 12**

Amazon Monitron workflow ..... 12

Amazon Monitron concepts ..... 13

Amazon Monitron components ..... 17

Amazon Monitron alerts ..... 22

**Getting started ..... 25**

Setting up a project ..... 25

Step 1: Create an account ..... 26

Step 2: Create a project ..... 28

Step 3: Create admin users ..... 29

Step 4: (optional) Add Amazon Monitron users to your project ..... 30

Step 5: Invite users to your project ..... 34

Adding assets and installing devices ..... 35

Step 1: Add a Gateway ..... 35

Step 2: Adding Assets ..... 40

Step 3: Attach Sensors ..... 47

Step 4: Pairing Sensors to an Asset ..... 49

Understanding warnings and alerts ..... 52

Step 1: Understanding asset health ..... 53

Step 2: Viewing asset conditions ..... 57

Step 3: Viewing and acknowledging a machine abnormality ..... 59

Step 4: Resolving a machine abnormality ..... 63

Step 5: Muting and unmuting alerts ..... 63

**Projects ..... 75**

Creating a project ..... 75

Using tags with your project ..... 76

Adding a tag to a project when you create it ... 77
Adding a tag to a project after it's been created ... 79
Modifying or removing a tag ... 80
Updating a project ... 81
Switching between projects ... 82
Switching between projects in the web app ... 82
Switching between projects in the mobile app ... 85
Deleting a project ... 89
Additional project tasks ... 90
**Sites ... 92**
Organizing a project into sites ... 92
Controlling access to projects and sites ... 93
Creating a site ... 93
To add a site using the mobile app ... 93
To add a new site using the web app ... 94
Changing a site name ... 95
To change a site name using the mobile app ... 95
To change a site name using the web app ... 95
Deleting a site ... 96
To delete a site using the mobile app ... 96
To delete a site using the web app ... 97
Navigating between projects and sites in the mobile app ... 98
Switching from project level to site level ... 98
Switching from site level to project level ... 99
**Gateways ... 101**
Ethernet gateways ... 101
Reading the LED lights on an Ethernet gateway ... 103
Placing and installing an Ethernet gateway ... 105
Commissioning an Ethernet gateway ... 110
Troubleshooting Ethernet gateway detection ... 113
... 115
Resetting the Ethernet gateway to factory settings ... 115
Viewing the list of gateways ... 116
Viewing Ethernet gateway details ... 118
Editing Ethernet gateway name ... 122
Deleting an Ethernet gateway ... 126

Retrieving MAC address details ... 127
Wi-Fi gateways ... 132
Reading the LED lights on a Wi-Fi gateway ... 133
Placing and installing a Wi-Fi gateway ... 135
Commissioning a Wi-Fi gateway ... 143
Troubleshooting Wi-Fi gateway detection ... 145
Troubleshooting Bluetooth pairing ... 147
Resetting the Wi-Fi gateway to factory settings ... 147
Viewing the list of gateways ... 148
Viewing Wi-Fi gateway details ... 150
Editing Wi-Fi gateway name ... 154
Deleting a Wi-Fi gateway ... 158
Retrieving MAC address details ... 159
**Assets ... 165**
Creating asset classes ... 166
Creating a custom class ... 167
Updating a custom class ... 171
Deleting a custom class ... 174
Managing assets ... 178
Viewing the list of assets ... 180
To open the Assets list ... 180
Adding an asset ... 180
Adding assets using the mobile app ... 41
Adding assets using the web app ... 45
Changing an asset name ... 186
To change an asset's name in the mobile app ... 186
To change an asset's name in the web app ... 186
Moving an asset ... 187
To move an asset on the web app ... 188
To move an asset on the mobile app ... 190
Deleting an asset ... 196
To delete an asset ... 196
**Sensors ... 198**
Positioning a sensor ... 198
Mounting a sensor ... 202
Adding a sensor position ... 204

To add a sensor position on the web app ... 205
To add a sensor position on the mobile app ... 206
Pairing a sensor to an asset ... 212
To pair a sensor to an asset ... 212
Renaming a sensor position ... 218
Renaming a sensor position on the mobile app ... 219
Renaming a sensor position on the web app ... 219
Editing machine class ... 220
To edit machine class on the mobile app ... 221
To edit machine class on the web app ... 227
To edit machine class from the position detail page ... 228
Deleting a sensor ... 228
To delete a sensor in the mobile app ... 229
To delete a sensor in the web app ... 230
Deleting a sensor position ... 231
To delete a sensor position in the mobile app ... 231
To delete a sensor position in the web app ... 232
Understanding sensor details ... 233
Viewing sensor details ... 234
Sensor connectivity status ... 236
Sensor battery status ... 237
Identifying sensor position ... 239
Identifying paired sensor ... 239
Missing or unread sensor ... 243
Permissions and site commissioning issues ... 244
Scanning sensor from another site ... 246
Ex-rated sensors ... 247
**Measurements and machine abnormalities ... 251**
Choosing your measurement viewing platform ... 251
In-app updates ... 252
Viewing sensor measurements ... 256
Understanding sensor measurements ... 258
Understanding asset status ... 262
The Assets list ... 262
Asset and position status ... 264
Notifications ... 267

Acknowledging a machine abnormality ... 269
To view and acknowledge a machine abnormality ... 269
Resolving an abnormality ... 271
Failure modes ... 271
Failure causes ... 272
To resolve a machine abnormality using the mobile app ... 272
Taking a one-time measurement ... 273
To take a one-time measurement (mobile app only) ... 274
**Managing users ... 289**
Managing admin users ... 289
User directory setup ... 290
Adding users as an admin ... 299
Managing users as an admin user ... 301
Removing an admin user ... 305
Sending an email invitation ... 306
Managing non-admin users ... 307
Displaying a list of users ... 308
Adding a user ... 310
Changing a user role ... 314
Removing a user ... 316
**Networking ... 318**
Networking with your mobile device ... 318
Setting up your Monitron network foundation with your mobile app ... 318
Setting up your gateways ... 319
Setting up your sensors ... 319
Securing your network ... 320
**Accessing your data ... 322**
Exporting your data to Amazon S3 ... 322
Prerequisites ... 323
Exporting your data with AWS CloudFormation (recommended option) ... 323
Exporting your data with the console ... 330
Exporting your data with CloudShell ... 350
Exporting your data with Kinesis v1 ... 360
Exporting your data to a Kinesis stream ... 360
Editing live data export settings ... 361
Stopping a live data export ... 361

Viewing data export errors ... 362
Using server-side encryption for the Kinesis stream ... 362
Monitoring with Amazon CloudWatch Logs ... 362
Storing exported data in Amazon S3 ... 364
Processing data with Lambda ... 366
Understanding the v1 data export schema ... 372
Exporting your data with Kinesis v2 ... 379
Exporting your data to a Kinesis stream ... 380
Editing live data export settings ... 380
Stopping a live data export ... 381
Viewing data export errors ... 381
Using server-side encryption for the Kinesis stream ... 381
Monitoring with Amazon CloudWatch Logs ... 382
Storing exported data in Amazon S3 ... 384
Processing data with Lambda ... 385
Understanding the v2 data export schema ... 391
Migration from Kinesis v1 to v2 ... 410
**Monitoring costs ... 413**
Conceptual overview ... 413
Billing tag keys and tag values ... 414
Retrieving project tag values ... 414
Retrieving site tag values ... 415
Activating billing tags ... 416
Viewing cost reports ... 418
**App settings ... 420**
Localization settings ... 420
Changing localization settings ... 420
**Logging actions with AWS CloudTrail ... 425**
Amazon Monitron information in CloudTrail ... 425
Example: Amazon Monitron log file entries ... 427
Successful DeleteProject action ... 428
Failed DeleteProject action (authorization error) ... 429
Failed DeleteProject action (conflict exception error) ... 430
**Security ... 432**
Data Protection ... 432
Data at rest ... 434

Data in transit ... 434
AWS KMS and Data Encryption ... 434
Identity and Access Management ... 435
Audience ... 435
Authenticating with Identities ... 436
Managing Access Using Policies ... 439
How Amazon Monitron Works with IAM ... 441
Using service-linked roles ... 449
Logging and Monitoring ... 456
Compliance Validation ... 456
Infrastructure Security ... 457
Security Best Practices for Amazon Monitron ... 458
**Troubleshooting ... 459**
Troubleshooting Issues with Amazon Monitron Sensors ... 459
If you can't commission your sensors ... 459
If your sensor is offline ... 461
If your sensor falls off ... 462
... 462
... 463
If commissioning the gateway fails ... 464
... 464
**Available devices ... 467**
**Quotas ... 468**
Supported Regions ... 468
Quotas ... 468
**Document history ... 469**

Amazon Monitron is no longer open to new customers. Existing customers can continue to use the service as normal. For capabilities similar to Amazon Monitron, see our blog post.

# What is Amazon Monitron?

Amazon Monitron is a machine-learning based end-to-end condition monitoring system that detects potential failures within equipment. You can use it 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, and gateways to automatically transfer data to the AWS Cloud. Amazon Monitron analyzes data for indications of potential equipment failure and 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.

Amazon Monitron comes with an application in two versions. The mobile application handles system setup, analytics, and notification when tracking equipment conditions. The web application provides all the same functions as the mobile app except setup.

Reliability managers can quickly deploy Amazon Monitron to track the machine health of industrial equipment, such as bearings, motors, gearboxes, and pumps, without any development work or specialized training.

What is Amazon Monitron?

## Amazon Monitron 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 collects data from the asset and sends it through the AWS Cloud to Amazon Monitron using a gateway mounted on the factory wall and plugged into a standard outlet.

The Amazon Monitron Starter Kit, which is available at Amazon.com or Amazon Business, contains five sensors and one Wi-Fi gateway. You can add more sensors and gateways as needed.



*An Amazon Monitron gateway*

# Amazon Monitron software

Amazon Monitron includes a **console**, which is used by your IT account 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

Except for the initial project set up, your team performs all monitoring tasks using the Amazon Monitron **mobile app**, which they install on their smartphones, or the **web app**, which they can use in their browsers. Using the mobile app, reliability managers in your factory can set up sites, manage users, add assets, and install sensors. Using the web app, they can complete the same tasks, except for installing sensors and gateways. Technicians can use the apps to monitor the health of your equipment, and track and document potential failures.

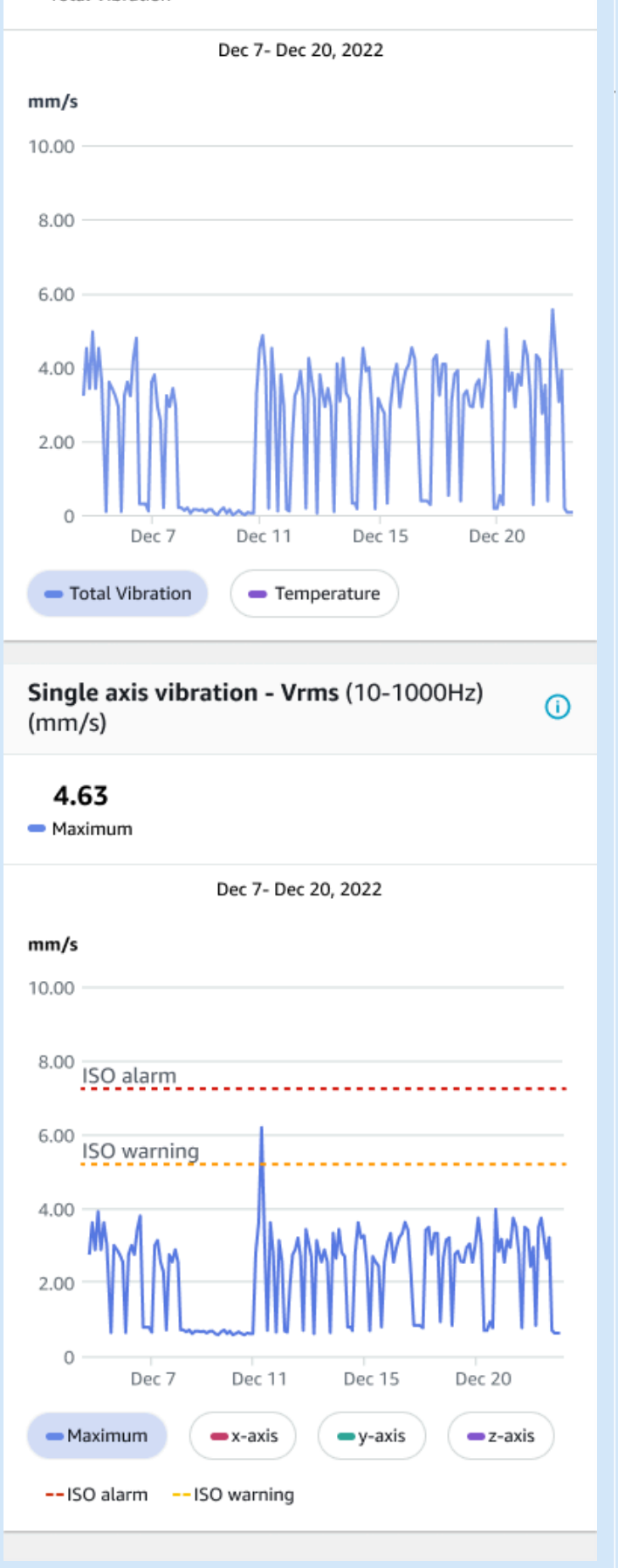
The mobile app displays an icon for each asset, so you can see its condition at a glance.

| Alert icon | Alert definition |
| --- | --- |
|  | **Healthy:** The machine is working normally. |
|  | **Alarm**: An alarm has been triggered for one of the positions of this asset, indicating that the machine vibration and temperature are out of the normal range at this position. We recommend that you investigate the issue at the earliest opportunity. An equipment failure might occur if the issue isn't addressed. |

| Alert icon | Alert definition |
| --- | --- |
|  | **Warning**: A warning has been triggered for one of the positions of this asset, indicatin g that Amazon Monitron has detected early signs of potential failure. Amazon Monitron identifies warning conditions by analyzing equipment vibration and temperature, using a combination of machine learning and ISO vibration standards. |
|  | **Maintenance**: Someone has acknowledged the alarm and is looking into the issue. |
|  | **Asset Healthy-offline:** Sensor is offline and the last recorded state was **Healthy**. No new alerts will be generated till the sensor returns online. |
|   | **Position Healthy-offline:** Sensor is offline and the last recorded state was **Healthy**. No new alerts will be generated till the position returns online. |
|  | **Asset Alarm-offline:** Sensor is offline and the last recorded state was an **Alarm**. No new alerts will be generated till the sensor returns online. |
|   | **Position Alarm-offline:** Sensor is offline and the last recorded state was an **Alarm**. No new alerts will be generated till the position returns online. |

| Alert icon | Alert definition |
| --- | --- |
|  | **Asset Warning-offline:** Sensor is offline and the last recorded state was a **Warning**. No new alerts will be generated till the sensor returns online. |
|  | **Position Warning-offline:** Sensor is offline and the last recorded state was a **Warning**. No new alerts will be generated till the position returns online. |
|  | **Asset Maintenance-offline:** Sensor is offline and the last recorded state was **Maintenance**. No new alerts will be generated till the sensor returns online. |
|  | **Position Maintenance-offline:** Sensor is offline and the last recorded state was **Maintenance**. No new alerts will be generated till the position returns online. |
| No sensor | **No sensor**: At least one position for the asset doesn't have a sensor paired to it. |

To find out more, you can drill down into the data.




Sensor reading of a healthy asset.




Sensor reading of an unhealthy asset.

As Amazon Monitron collects more data, it improves its machine learning (ML) model and learns to make more accurate estimates of potential machine abnormalities.

## Benefits of Amazon Monitron

Amazon Monitron provides the following key benefits:

- **Works out of the box** – Amazon Monitron sensors and gateways are pre-configured to work with Amazon Monitron software. Reliability managers can install these devices using the app and can start monitoring equipment in just a few hours. It's simple to set up and requires little or no development work, knowledge of ML, or integration.
- **Immediate notifications in the Amazon Monitron app** – Amazon Monitron sends users notifications in the app when it detects abnormal machine patterns. Technicians can view, track, and provide feedback on these abnormal machine states in the Amazon Monitron app.
- **ISO and ML-based analytics** – Amazon Monitron automatically detects abnormal machine operating states. To do this, Amazon Monitron analyzes vibration and temperature signals and compares them to International Standards Organization (ISO 20816) standard thresholds and ML-enabled models.
- **Support for adding ML feedback in the app**– Amazon Monitron offers simple workflows for technicians to enter feedback on the accuracy of the alerts in the app. Amazon Monitron learns from that feedback and continues to improves over time.

## Pricing for Amazon Monitron

Amazon Monitron includes both one-time, device purchase costs for the sensors and gateways, and an ongoing pay-as-you-go service fee per Amazon Monitron sensor in use. There are no additional upfront fees and no long-term commitments.

For information, see Amazon Monitron Pricing.

## Related resources

The following documentation and other resources are available for Amazon Monitron:

- Amazon Monitron Getting Started Guide – For IT managers, reliability managers, and technicians, this guide gets you started using Amazon Monitron. It shows you how to set up Amazon Monitron, create assets, set up sensors, and start monitoring your equipment.

- Amazon Monitron User Guide – This detailed guide provides reliability managers (admin users) and technicians with more in-depth information about using Amazon Monitron to monitor your equipment for machine abnormalities. It also describes how to use the app, your primary Amazon Monitron tool.

# Are you a first-time user of Amazon Monitron?

How you interact with Amazon Monitron depends on your role as an Amazon Monitron user. Select the role that fits you best from the options below to see a recommended set of topics to help you learn more about Amazon Monitron.

## IT Manager

An IT manager sets up an Amazon Monitron project, configures a user directory to add Amazon Monitron users, adds site admin users to manager projects, and can also check Amazon Monitron logs in AWS CloudTrail.

If you are a first-time IT Manager user of Amazon Monitron, we recommend that you read the following sections in order:

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| **How Amazon Monitron works** | **Setting up a project** | **Projects** | **Managing admin users** | **Understanding networking with Amazon Monitron** | ***Accessing your data*** | ***Security*** |
| Introduces Amazon Monitron components and describes how Amazon | Explains how to setup the AWS console for creating Amazon Monitron projects | Explains how to manage Amazon Monitron projects | Explains how to add and remove admin users to and from your Amazon | Explains Amazon Monitron hardware networking | Explains how to export your Amazon Monitron data with Kinesis or download | Explains how to configure Amazon Monitron to meet your security and |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| How Amazon Monitron works | Setting up a project | Projects | Managing admin users | Understanding networking with Amazon Monitron | *Accessing your data* | *Security* |
| Monitron works | | | Monitron projects | | it to Amazon S3 | compliance objectives |

## Reliability manager/Admin user

A reliability manager/admin user has full access to all resources within an Amazon Monitron project or site. As a reliability manager or site admin user, you can add other users, create assets, pair sensors to assets, monitor assets, acknowledge alerts, and resolve abnormalities.

If you are a first-time reliability manager or admin user of Amazon Monitron, we recommend that you read the following sections in order:

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| How Amazon Monitron works | Adding assets and installing devices | Sites | Ethernet gateways | Wi-Fi gateways | Assets | Managing users |
| Introduces Amazon Monitron components and describes how Amazon | Explains how to install Amazon Monitron gateways, add assets, and attach sensors | Describes how to create and manage sites | Explains how to set up and configure ethernet gateways | Explains how to set up and configure Wi-Fi gateways | Describes how to manage assets and sensors | Describes how to manage admin users |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| How Amazon Monitron works | Adding assets and installing devices | Sites | Ethernet gateways | Wi-Fi gateways | Assets | Managing users |
| Monitron works | | | | | | |

## Technician

A technician user has read-only permissions to a Amazon Monitron project or site to which they have been added. Technicians also have permissions for monitoring assets and acknowledging and resolving abnormalities.

If you are a first-time technician user of Amazon Monitron, we recommend that you read the following sections in order:

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| How Amazon Monitron works | Assets | Understanding sensor measurements and monitoring machine abnormalities | Ethernet gateways | Wi-Fi gateways | Troubleshooting Amazon Monitron device issues |
| Introduces Amazon Monitron components and describes how Amazon Monitron works | Describes how to manage assets and sensors | Explains how to understand sensor measurements and monitor machine | Explains how to set up and configure ethernet gateways | Explains how to set up and configure Wi-Fi gateways | Explains how to troubleshoot Amazon Monitron device issues |

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| How Amazon Monitron works | Assets | Understanding sensor measurements and monitoring machine abnormalities | Ethernet gateways | Wi-Fi gateways | Troubleshooting Amazon Monitron device issues |
| | | abnormalities | | | |

# How Amazon Monitron works

Amazon Monitron is a machine learning end-to-end condition monitoring solution system that detects developing faults within machinery, 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 an application for system set up, analytics, and notification when tracking equipment condition.

Amazon Monitron sensors use an ISO threshold model and a machine learning (ML) model to monitor vibration. The ISO model is used to analyze the magnitude of vibration (machine condition). The ML model is used to detect change in vibration (change in machine condition).

Reliability managers can deploy Amazon Monitron to track machine health of industrial equipment, such as bearings, motors, gearboxes, and pumps, without any development work or specialized training.

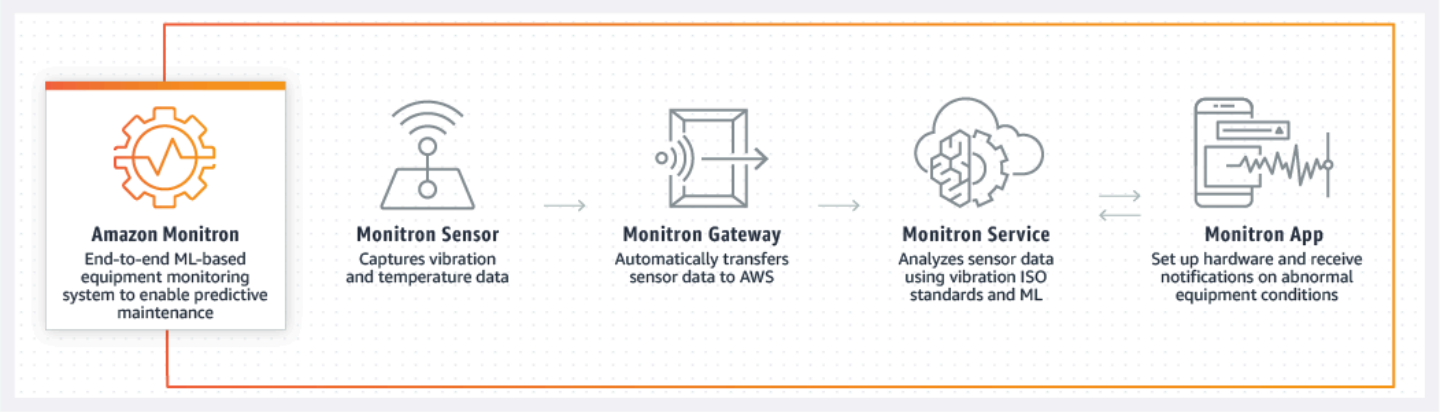
> **Tip**
>
> Check your Amazon Monitron app regularly for updates and access to the latest features.

**Topics**


- The Amazon Monitron workflow
- Amazon Monitron concepts
- Amazon Monitron components
- Amazon Monitron alerts


# 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-based service 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 failures, it notifies reliability managers and technicians through the Amazon Monitron app so they can take appropriate action.
   c. Technicians investigate based on the alerts, and resolve the developing fault. They enter feedback on the accuracy of the alerts, and report the failure mode, cause, and action taken in the app. Amazon Monitron learns from this feedback and continually improves.
4. The app displays current and past temperature and vibration data in charts that are easy to understand and can be used while investigating an issue.

# Amazon Monitron concepts

An Amazon Monitron implementation is structured in the following way:

**PROJECT → SITE → ASSET → SENSOR → POSITION**

The following table explains the Amazon Monitron concepts and terminology you need to know to get started with Amazon Monitron:

| Concept name | Concept definition | Key facts | Common users |
| --- | --- | --- | --- |
| **Project** | • Where you set up the gateways, assets, and sensors used by Amazon Monitron<br>• Captures details of Amazon Monitron detected machine abnormalities that can lead to equipment failure | • Resources can't be shared between projects<br>• Can only be created on the Amazon Monitron console<br>• Can only be created and managed by IT managers or users with access to the Amazon Monitron console | • IT administrators/ managers |
| **Site** | • A collection of assets, gateways, and sensors that share a purpose<br>• Used to organize projects to make them easier to manage | • Helpful for organization if your project has a large pool of assets, gateways, and sensors<br>• Can be used to control access and permissions<br>• Can create up to 50 sites within a project and add up to 100 assets and 200 gateways to each site<br>• Must be a project-level admin user | • IT administrators/ managers<br>• Reliability managers |

| Concept name | Concept definition | Key facts | Common users |
|---|---|---|---|
| | | to add a site to a project<br>• Can be configure d using both the mobile and web app | |
| Gateway | • Wi-Fi or Ethernet devices that transfer the data collected by Amazon Monitron senors to the AWS Cloud. | • Helpful for keeping track of whether sensor data is being correctly transferred to the Cloud.<br>• Must be commissio ned using the mobile app | • Reliability managers<br>• Technicians |
| Asset | • The pieces of equipment on your factory floor<br>• Can be:<br>  • individual machines<br>  • sections of a large piece of equipment<br>  • part of an industrial process<br>  • any element of your manufactu ring model | • Basis for viewing the health of your machines<br>• Amazon Monitron sensors are paired to assets and their parts<br>• Can place sensors on up to 20 positions on an asset<br>• Can be configured using both mobile and web app | • Reliability managers<br>• Technicians |

| Concept name | Concept definition | Key facts | Common users |
| --- | --- | --- | --- |
| **Sensor** | • Collects temperature and vibration data from your equipment<br>• Amazon Monitron uses the data to detect developing issues | • Can place sensors on up to 20 positions on each asset<br>• Can be assigned a machine class corresponding to the machine part it's placed on<br>• Can be configured using mobile app only | • Technicians<br>• Reliability managers |

| Concept name | Concept definition | Key facts | Common users |
| --- | --- | --- | --- |
| **Position** | • The place on the asset where you mount a sensor<br>• Important for collecting and analyzing data | • Can place sensors on up to 20 positions on each asset<br>• Positions on the same asset can be assigned different machine classes for a fine-grained view of machine health<br><br>**Important**<br>If you have complex machinery with more than one potential point of failure, we recommend that you collect data from multiple positions. | • Technicians<br>• Reliability managers |

# Amazon Monitron components

Amazon Monitron includes purpose-built sensors to capture vibration and temperature data, as well as gateways to automatically transfer data to the AWS Cloud. It also comes with an application in two versions. The mobile application handles system setup, analytics, and notification when

tracking equipment conditions. The web application provides all the same functions as the mobile app except setup.

The Amazon Monitron Starter Kit, which is available at Amazon.com or Amazon Business, contains five sensors and one Wi-Fi gateway. You can buy and add more sensors and gateways as needed. For more information, see Amazon Monitron FAQs.

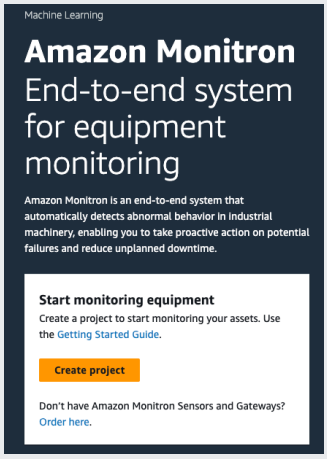
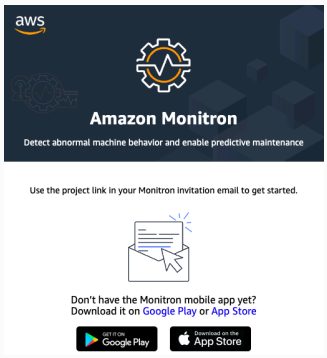
The following table shows Amazon Monitron components, their functions, and their use cases.

> **Note**
>
> Vibration is measured in milimeters (mm) and inches. Temperature is measured in Fahrenheit (F) and Celcius (C).

| Component name | Component details | Function | Common users |
|---|---|---|---|
| **Sensor**  | • **Hardware**<br>• **Temperature:** -20C – +80C/ -4F – +176F<br>• **Dimensions:** 52.8x43.0x24.9mm/2.08x1.69x0.98 inch<br>• **Weight:** 54 gms<br>• **IP Rating:** IP65<br>• **Wireless protocol:** Bluetooth Low Energy 5<br>• **Vibration sensor:** 3-axis MEMs accelerometer, range +/-16g, frequency response up to 6kHz, | • Captures vibration and temperature data directly from machines (assets)<br>• Sends collected data to the AWS Cloud using either Wi-Fi or Ethernet gateways<br>• Up to 20 can be placed on a machine (asset)<br>• Each sensor can be assigned a machine class corresponding to the machine (asset) part it's placed on | • Technicians<br>• Reliability managers |

| Component name | Component details | Function | Common users |
|---|---|---|---|
| | sampling frequency 26.7kHz<br>• **Power:** Lithium metal non-recha rgeable batteries<br>• **Battery life:** Estimated 5 years<br>• **Default data capture:** once an hour | | |
| **Ethernet gateway**<br>  | • **Hardware**<br>• **Temperature:** -20C – +60C/ -4F – +140F<br>• **Dimension s:** 13.9X10.7 X4.1cm/5. 5X4.2X1.6 inch<br>• **Weight:** 230 gms/8.20 oz<br>• **IP Rating:** IP65<br>• **Internet connectiv ity:** RJ45 10/100Mbps<br>• **Power:** IEEE 802.3at type1 (15.4 Watt class) | • Sends vibration and temperature data collected from machines (assets) to AWS Cloud<br>• Powered by a Ethernet Cat 5e or Cat 6 cord plugged into its RJ-45 socket<br>• Doesn't need to be directly attached to asset (machine)<br>• Needs a Power over Ethernet (POE) supported router or a POE power injector to work | • Technicians<br>• Reliability managers |

| Component name | Component details | Function | Common users |
| --- | --- | --- | --- |
| **Wi-Fi gateway**<br>  | • **Hardware**<br>• **Temperature:** 0C – 40C/ 32F – 104F<br>• **Dimensions:** 90x78x38 mm/3.6x3.1x1.5 inch<br>• **Weight:** 95gms<br>• **IP Rating:** IP65<br>• **Internet connectivity:** WiFi, 802.11b/g/n, ISM 2.4GHz only<br>• **Power:** 5.0V–2.0 DC, AC adapter included for USA, UK, and EU countries (indoors only) | • Sends vibration and temperature data collected from machines (assets) to AWS Cloud<br>• Wi-Fi (plugged into a standard socket)<br><br>**Note**<br>Wi-Fi gateways aren't supported in all sites. Amazon Monitron ethernet gateways are the global standard. | • Technicians<br>• Reliability managers |

| Component name | Component details | Function | Common users |
| --- | --- | --- | --- |
| **Console**<br>  | **Software** | • Signing up for AWS<br>• Creating an Amazon Monitron project<br>• Creating and initially assigning admin users to manage projects<br>**Important**<br>Must be set-up first for Amazon Monitron to work. | • IT managers<br>• IT administrators<br>• Reliability managers |
| **Mobile app**<br>  | **Software** | • Managing an Amazon Monitron project<br>• **(Project-level admin user only)** Creating sites<br>• Creating assets<br>• Monitoring equipment condition<br>• **(Mobile app only)** Setting up sensors and gateways | • Technicians<br>• Reliability managers |

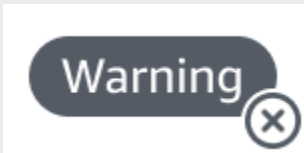
| Component name | Component details | Function | Common users |
| --- | --- | --- | --- |
| **Web app**<br>  | **Software** | • Managing an Amazon Monitron project<br>• **(Project-level admin user only)** Creating sites<br>• Creating assets<br>• Monitoring equipment condition<br><br>**Important**<br>The web app supports all tasks supported by the mobile app except installing sensors and gateways. | • Technicians<br>• Reliability managers |

# Amazon Monitron alerts

To track equipment health, the Amazon Monitron mobile app displays an icon for each asset, so you can see its condition at a glance.

The following table shows the status icons you may see for your asset.

| Alert icon | Alert definition |
| --- | --- |
|  | **Healthy:** The machine is working normally. |
|  | **Alarm**: An alarm has been triggered for one of the positions of this asset, indicating that the machine vibration and temperature are out of the normal range at this position. We recommend that you investigate the issue at the earliest opportunity. An equipment failure might occur if the issue isn't addressed. |
|  | **Warning**: A warning has been triggered for one of the positions of this asset, indicatin g that Amazon Monitron has detected early signs of potential failure. Amazon Monitron identifies warning conditions by analyzing equipment vibration and temperature, using a combination of machine learning and ISO vibration standards. |
|  | **Maintenance**: Someone has acknowledged the alarm and is looking into the issue. |
|  | **Asset Healthy-offline:** Sensor is offline and the last recorded state was **Healthy**. No new alerts will be generated till the sensor returns online. |
|  | **Position Healthy-offline:** Sensor is offline and the last recorded state was **Healthy**. No new alerts will be generated till the position returns online. |

| Alert icon | Alert definition |
| --- | --- |
|  | **Asset Alarm-offline:** Sensor is offline and the last recorded state was an **Alarm**. No new alerts will be generated till the sensor returns online. |
|  | **Position Alarm-offline:** Sensor is offline and the last recorded state was an **Alarm**. No new alerts will be generated till the position returns online. |
|  | **Asset Warning-offline:** Sensor is offline and the last recorded state was a **Warning**. No new alerts will be generated till the sensor returns online. |
|  | **Position Warning-offline:** Sensor is offline and the last recorded state was a **Warning**. No new alerts will be generated till the position returns online. |
|  | **Asset Maintenance-offline:** Sensor is offline and the last recorded state was **Maintenance**. No new alerts will be generated till the sensor returns online. |
|  | **Position Maintenance-offline:** Sensor is offline and the last recorded state was **Maintenance**. No new alerts will be generated till the position returns online. |

# Getting started

This chapter explains the basic steps to get started with Amazon Monitron:

1. **Setting up a project**—This provides the framework for the rest of your team to monitor your equipment. It uses the Amazon Monitron console and will probably only need to be done occasionally, or even just once, depending on the number of projects you choose to have. All other tasks are done through the Amazon Monitron mobile app.
2. **Adding assets and installing devices**—All of these tasks are done using the mobile app. It's a major activity at the beginning of the project. You can add a few assets and install just a few devices at first, and then come back to it with additional assets later on.
3. **Understanding alerts**—This is the daily use of Amazon Monitron and is done using the mobile app. It consists of daily monitoring, as well as the tasks that have to be dealt with when Amazon Monitron discovers a possible machine abnormality.

To learn more about Amazon Monitron, you can visit the Amazon Monitron product detail page.

**Topics**


- Setting up a project
- Adding assets and installing devices
- Understanding warnings and alerts


# Setting up a project

The first step with Amazon Monitron is to set up your project in the Amazon Monitron console. A project is where your team sets up gateways, assets, and sensors in the Amazon Monitron mobile app.

**Topics**


- Step 1: Create an account
- Step 2: Create a project
- Step 3: Create admin users
- Step 4: (optional) Add Amazon Monitron users to your project
- Step 5: Invite users to your project

# Step 1: Create an account

## Sign up for an AWS account

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 or text message and entering a verification code on the phone keypad.

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

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to https://aws.amazon.com/ and choosing **My Account**.

## Create a user with administrative access

After you sign up for an AWS account, secure your AWS account root user, enable AWS IAM Identity Center, and create an administrative user so that you don't use the root user for everyday tasks.

### Secure your AWS account root user

1. Sign in to the AWS Management Console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

   For help signing in by using root user, see Signing in as the root user in the *AWS Sign-In User Guide*.
2. Turn on multi-factor authentication (MFA) for your root user.

   For instructions, see Enable a virtual MFA device for your AWS account root user (console) in the *IAM User Guide*.

### Create a user with administrative access

1. Enable IAM Identity Center.

   For instructions, see Enabling AWS IAM Identity Center in the *AWS IAM Identity Center User Guide*.

2. In IAM Identity Center, grant administrative access to a user.

   For a tutorial about using the IAM Identity Center directory as your identity source, see Configure user access with the default IAM Identity Center directory in the *AWS IAM Identity Center User Guide*.

### Sign in as the user with administrative access

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

  For help signing in using an IAM Identity Center user, see Signing in to the AWS access portal in the *AWS Sign-In User Guide*.

### Assign access to additional users

1. In IAM Identity Center, create a permission set that follows the best practice of applying least-privilege permissions.

   For instructions, see Create a permission set in the *AWS IAM Identity Center User Guide*.

2. Assign users to a group, and then assign single sign-on access to the group.

   For instructions, see Add groups in the *AWS IAM Identity Center User Guide*.

> **Important**
>
> Amazon Monitron supports all IAM Identity Center regions except opt-in and government regions. For a list of supported regions, see Understanding SSO requirements.

# Step 2: Create a project

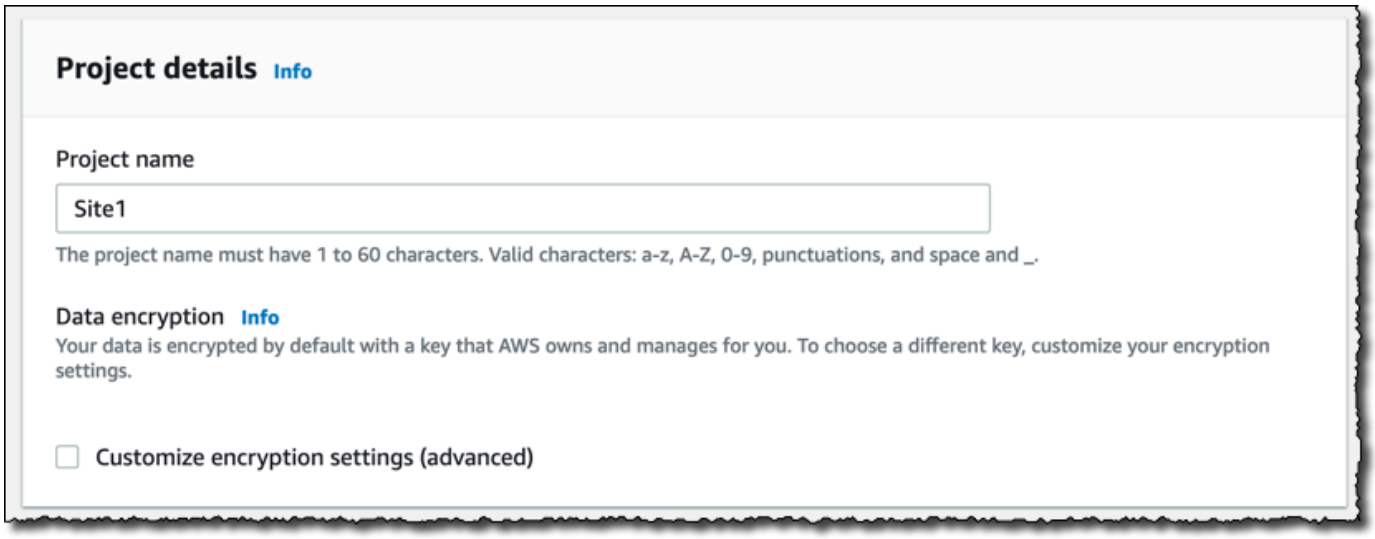
Now that you've signed in to the AWS Management Console, you can use the Amazon Monitron console to create your project.

**To create a project**

1. Choose the AWS Region that you want to use in the Region selector. Amazon Monitron is available only in the US East (N. Virginia), Europe (Ireland), and Asia Pacific (Sydney) Regions.
2. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron.
3. Choose **Create project**.
4. Under **Project Details**, for **Project name**, enter a name for the project.
5. (Optional) Under **Data encryption**, you can check **Custom encryption settings (advanced)** if you have an AWS KMS key in AWS Key Management Service. Amazon Monitron encrypts all data at rest and in transit. If you don't provide your own CMK, your data is encrypted by a CMK that Amazon Monitron owns and manages.

   For more information about encryption for your project, see KMS and Data Encryption in Amazon Monitron.
6. (Optional) To add a tag to the project, enter a key-value pair under **Tags** and then choose **Add tag**.

   For more information about tags, see Tags in Amazon Monitron.
7. Choose **Next** to create the project.



When you create your first project, the owner of the AWS account will get an email from *AWS Organizations*. No action needs to be taken based on this email.

## Step 3: Create admin users

Give access to one or more people in your organization (such as reliability managers) as *admin users*. An *admin user* is a person who belongs to an Amazon Monitron project and who can add other users to the project.

When you add an admin user, Amazon Monitron creates an account for that user in AWS IAM Identity Center. IAM Identity Center is a service that helps you manage SSO access to AWS accounts and applications in your organization. Amazon Monitron uses IAM Identity Center to authenticate users for the Amazon Monitron mobile app.

If you haven't enabled IAM Identity Center in your AWS account, Amazon Monitron enables it for you when you create your first Amazon Monitron admin user. If you are already using IAM Identity Center in your account, then your IAM Identity Center users are shown in the Amazon Monitron console.

Complete the steps in this section to add yourself to your project as an admin user. Repeat them for each additional admin user that you want to create.

**To create an admin user**

Unless you already use IAM Identity Center in your AWS account, use Amazon Monitron to create admin users. If these users are already in IAM Identity Center, you can skip creating the users, and you are ready to assign the admin role to them.

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron.
2. On the **Add project admin user** page, choose **Create user**.
3. In the **Create user** section, enter the admin user's email address and name.
4. Choose **Create user**.

   Amazon Monitron creates a user in IAM Identity Center. IAM Identity Center sends the user an email that contains a link to activate the account. The link is valid for up to seven days. Within this time, each user must open the email and accept the invitation.

**To assign the admin role to the admin users**

1. On the **Add project admin user** page, select the checkbox for each admin user that you created.
2. Choose **Add**.

   You can add admin users to your project even if those people have not yet accepted the invitations to their IAM Identity Center accounts.

## Step 4: (optional) Add Amazon Monitron users to your project

In addition to admin users, you can also add users who lack admin permissions. For example, these users might be technicians who only use the Amazon Monitron mobile app to monitor assets, acknowledge notifications and enter closure codes.

For users who are not admin users:

- You use IAM Identity Center, not Amazon Monitron, to create their user accounts.
- You use the Amazon Monitron mobile app to add the users to projects, not the Amazon Monitron console.

**Topics**


- To add users to IAM Identity Center
- To add a user using the mobile app
- How to add a user using the web app


### To add users to IAM Identity Center

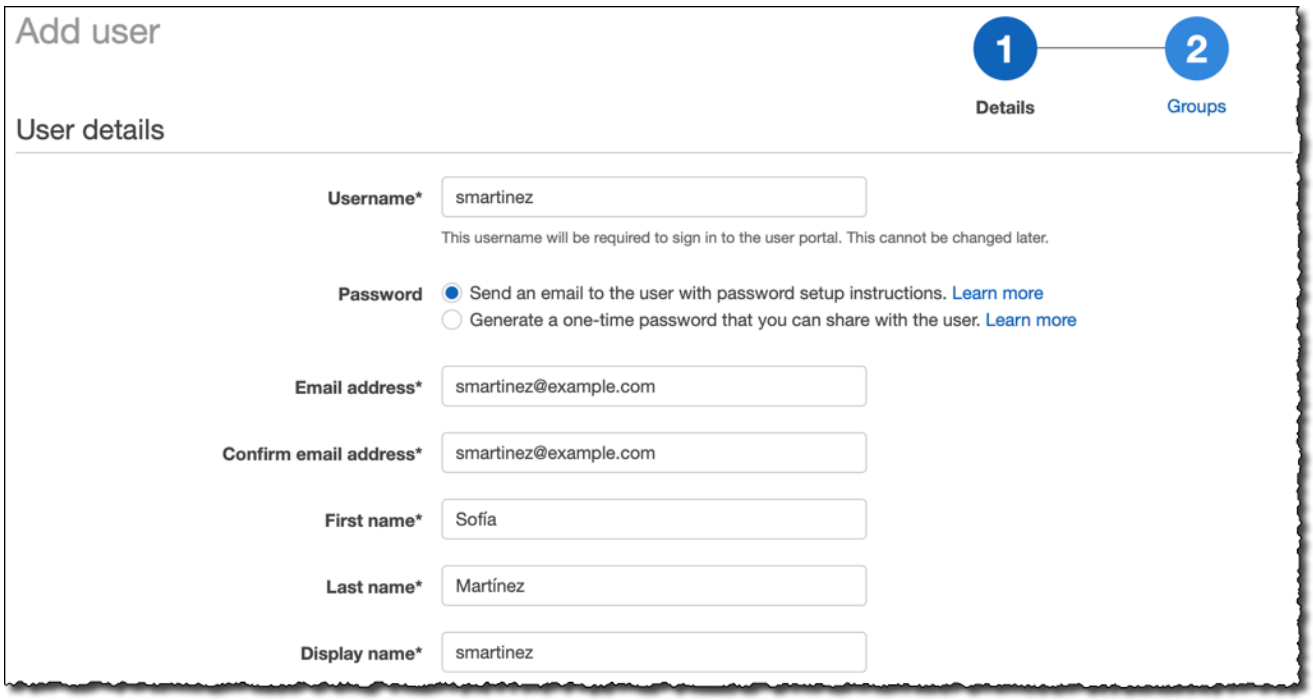
If your users already have accounts in IAM Identity Center in your AWS account, you can skip these steps. You are ready to add the users to your project in the mobile app. Otherwise, add your users to IAM Identity Center by completing the following steps.

> **Note**
>
> The following steps are not required if all of your users are admin users.

1. Open the AWS IAM Identity Center console at https://console.aws.amazon.com/singlesignon/.
2. In the IAM Identity Center console, choose **Users**.
3. Repeat the following steps for each user that will access your project in the Amazon Monitron mobile app.

    a. On the **Users** page choose **Add user**.

    b. In the **User details** section, provide the username and contact information. Leave **Password** set to **Send an email to the user with password setup instructions**.

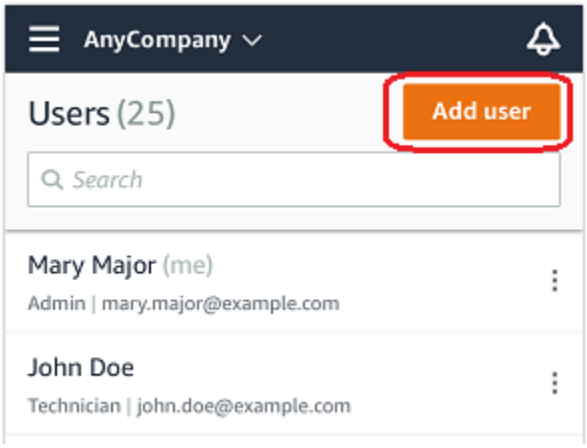



    c. Choose **Next: Groups**.

    d. Choose **Add user**. IAM Identity Center sends the user an email that contains a link to activate the IAM Identity Center user. The link is valid for up to seven days. Each user must open the email and accept the invitation before accessing your project in the Amazon Monitron mobile app.

## To add a user using the mobile app

1. Log into the Amazon Monitron mobile app on your smartphone.
2. Navigate to the project or site that you want to add a user to, and then to the **Users** list.
3. Choose **Add user**.




4. Enter a user name.

   Amazon Monitron searches the user directory for the user.

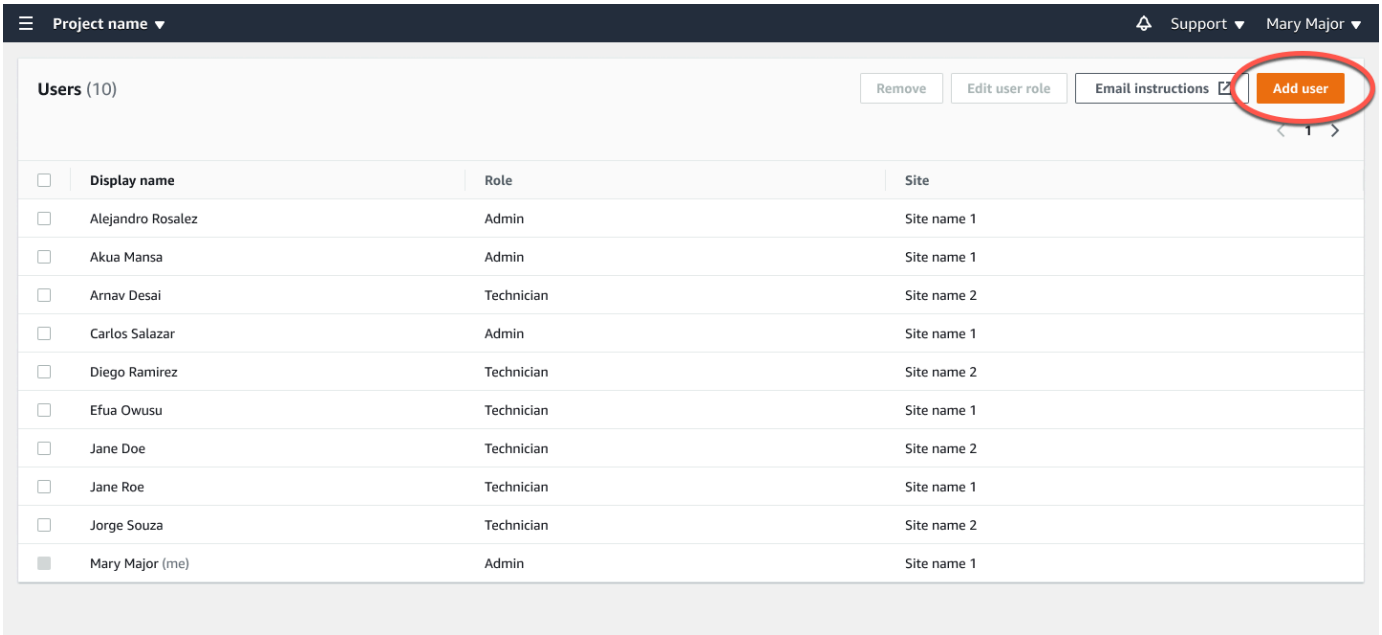
5. Choose the user from the list.
6. Choose the role that you want to assign the user: **Admin**, **Technician**, or **Viewer**.
7. Choose **Add**.

   The new user appears on the **Users** list.

8. Send the new user an email invitation with a link for accessing the project and downloading the Amazon Monitron mobile app. For more information, see Sending an email invitation.

## How to add a user using the web app

1. Select **Users** from the navigation pane.
2. Choose **Add user**.



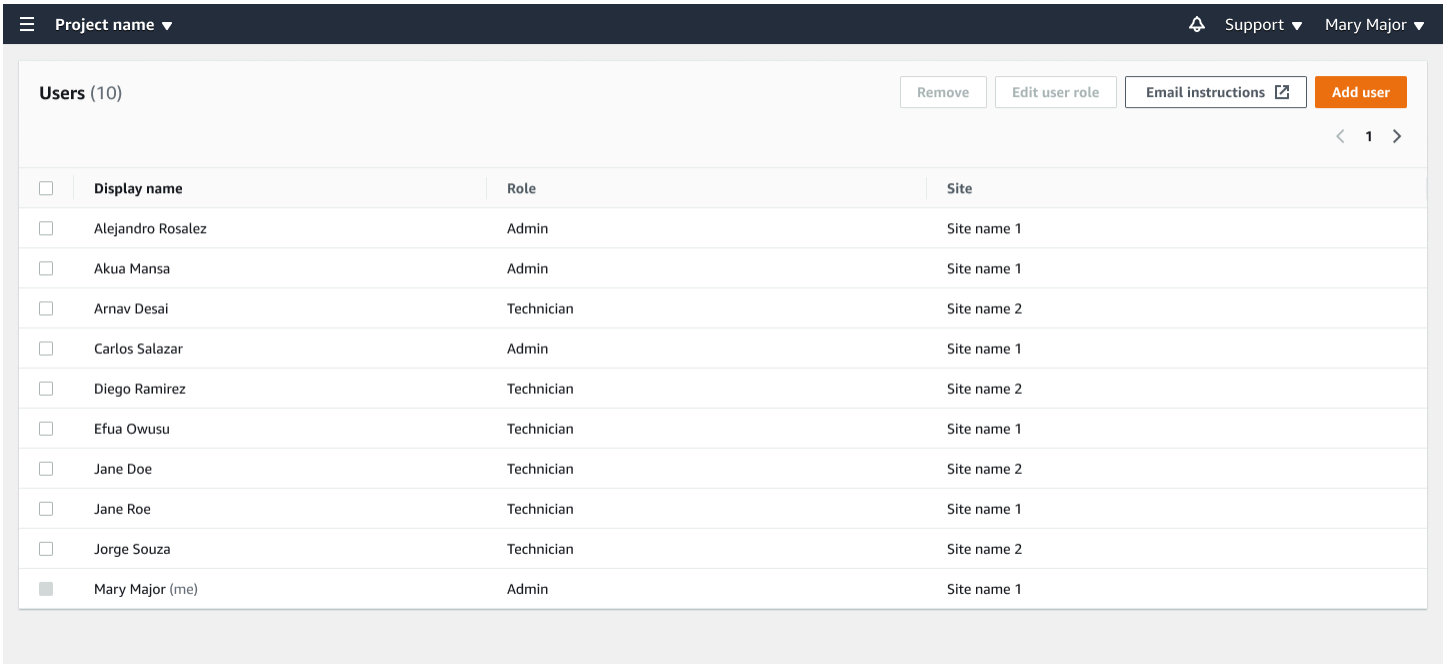

3. Enter a user name.

   Amazon Monitron searches the user directory for the user.

4. Choose the user from the list.
5. Choose the role that you want to assign the user: **Admin**, **Technician**, or **Read only**.
6. Choose **Add**.

   The new user appears on the **Users** list.

7. Send the new user an email invitation with a link for accessing the project and downloading the Amazon Monitron mobile app. For more information, see Sending an email invitation.

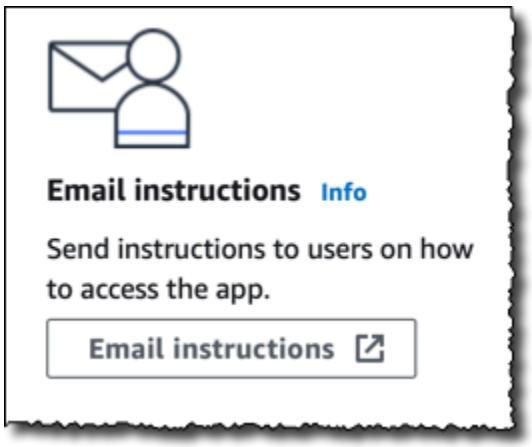



## Step 5: Invite users to your project

Invite the users you've added to your Amazon Monitron project.

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron.
2. In the navigation pane, choose **Projects**.
3. On the **Projects** page, choose your project name to open its details page.
4. Repeat the following steps for each user that you want to invite.

    a. Under **How it works**, choose **Email instructions**.



Your email client opens a draft that contains an invitation to your Amazon Monitron project. It contains both a link to download the Amazon Monitron mobile app from the Google Play Store and a link to open the project.

b. Email this message to the user.

# Adding assets and installing devices

Once you've created a project, you or reliability managers and technicians from your team can use the Amazon Monitron mobile app to add gateways, create assets and pair sensors to them, and start monitoring your equipment. Only smartphones using Android 8.0+ or iOS 14+ with Near Field Communication (NFC) and Bluetooth are supported by Amazon Monitron.

Your IT manager or reliability manager will generate an email describing how to log in for the first time and connect to your project and send this to you. Once you've logged in for the first time, you can follow the steps to add gateways and install devices.

**Topics**


- Step 1: Add a Gateway
- Step 2: Adding Assets
- Step 3: Attach Sensors
- Step 4: Pairing Sensors to an Asset


## Step 1: Add a Gateway

In Amazon Monitron, sensors collect data from machines and pass it to gateways, which transmit the data to the AWS Cloud and thus to Amazon Monitron for analysis. These gateways are usually mounted on the wall of a factory within 20 to 30 meters from the sensor and connect to the AWS Cloud using the local Wi-Fi network.

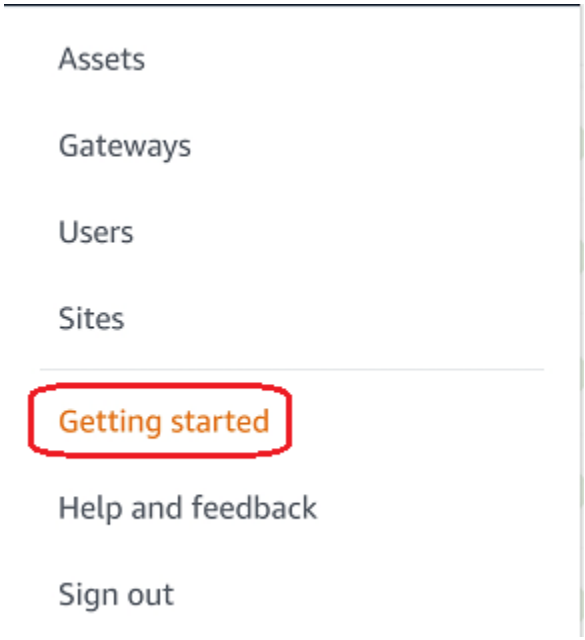
Before adding a gateway, make sure that Bluetooth is turned on for your smartphone. You can only add gateways using the mobile app.

**Topics**

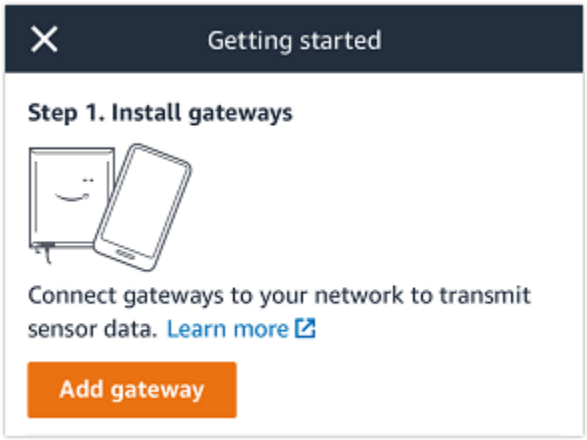

- To add a Wi-Fi gateway
- To add an Ethernet gateway

## To add a Wi-Fi gateway

1. Choose the menu icon (☰), and then choose **Getting Started**.



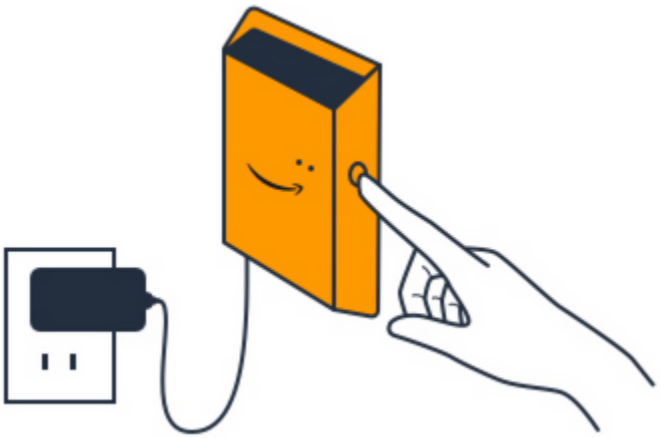

2. Choose **Add gateway**.




3. In your factory, position your gateway in the location that works best for communicating with your sensors.

   The best place to mount your gateway is higher than the sensors and no more than 20 to 30 meters away. For more information about locating gateways, see Where to Install Your Gateway in the *Amazon Monitron User Guide*.

4. Plug the gateway in and make sure that the LED lights on the top alternatively blink yellow and blue.

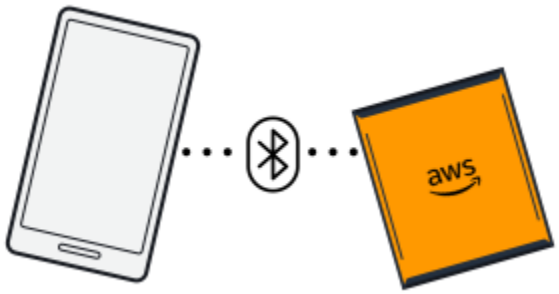


5. Push the button on the side of the gateway to put it into commissioning mode. The lights will start blinking rapidly.
6. In the mobile app, choose **Next**.
7. Choose **Add gateway**.

   Amazon Monitron searches for the gateway, which can take a few moments. When it finds it, the gateway appears in the gateway list.

   If it can't find the gateway, see Setting Up Gateways in the *Amazon Monitron User Guide* for possible solutions.
8. When you see the new gateway in the list, choose it.

   It can take a few moments for Amazon Monitron to connect to the new gateway.




9. After it connects to the gateway, Amazon Monitron scans for Wi-Fi networks. Choose the Wi-Fi network that you want to use.

> **Note**
>
> When the gateway is successfully connected, Amazon Monitron displays the gateway device ID and MAC ID in the mobile app.

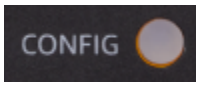
10. Enter your Wi-Fi password, and then choose **Connect**.

    It can take a few minutes for the gateway to be commissioned.

## To add an Ethernet gateway

1. If Bluetooth isn't already turned on for your smartphone, turn it on.
2. Position your gateway in the location that works best for communicating with your sensors.

   The best place to mount your gateway is higher than the sensors and no more than 20 to 30 meters away.For additional help with locating your gateway, see Placing and installing an Ethernet gateway.
3. Plug in the gateway and make sure the network light (yellow) and the Bluetooth light (blue) on the front of your gateway are blinking alternatively.
4. Push the **Config** button on the gateway to put it into commissioning mode. the Bluetooth and network LED lights will start flashing rapidly.

   
   
5. Open the mobile app on your smartphone.
6. On the **Getting started** page or the **Gateways** page, choose **Add gateway**.

   Amazon Monitron scans for the gateway. This can take a few moments. when Amazon Monitron finds the gateway, it displays it in the gateway list.
7. Choose the gateway.

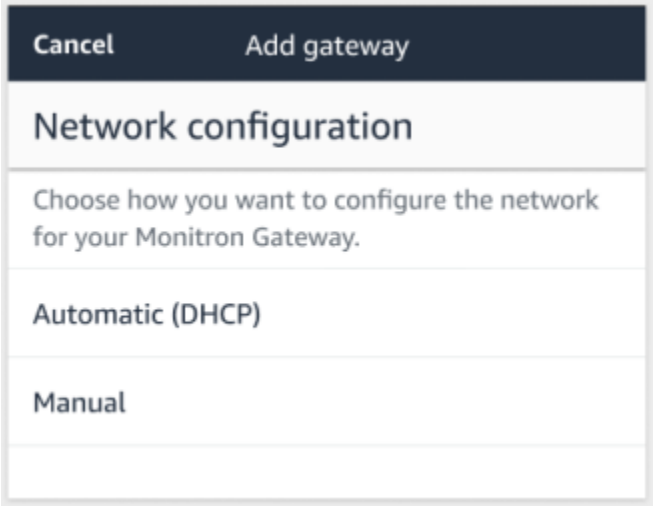
   It can take a few moments for Amazon Monitron to connect to the new gateway.




If the mobile app continues to try to connect to the gateway without success, see Troubleshooting Ethernet gateway detection.

> **Note**
>
> When the gateway is successfully connected, Amazon Monitron displays the gateway device ID and MAC ID in the mobile app.

8. After it connects to the gateway, Amazon Monitron will provide two options for you to configure the network connection for your gateway.

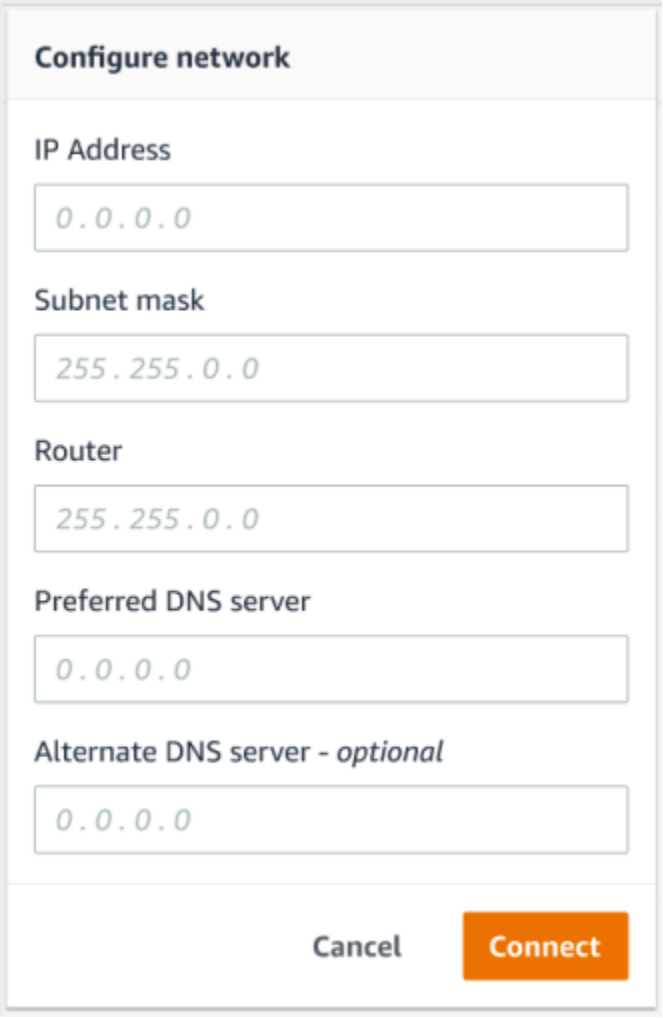



9. Choose your network configuation.

   It can take a few minutes for the gateway to be commissioned and to connect to the network.

If you have further difficulties making the gateway work, it might be helpful to reset it. For more information, see ???.

a. If you choose automatic (DHCP), Amazon Monitron will automatically configure the network to connect the gateway.
b. If you choose **manual**, enter your IP address, subnet mask, router, preferred DNS server, and alternate DNS server (optional) information. then choose **connect**.




## Step 2: Adding Assets

In Amazon Monitron, the machines you monitor are known as *assets*. Assets are usually individual machines, but they can also be specific sections of equipment. Assets are paired to sensors, which directly monitor temperature and vibration to check for potential failures. You can add assets using both the Amazon Monitron web app and the Amazon Monitron mobile app.

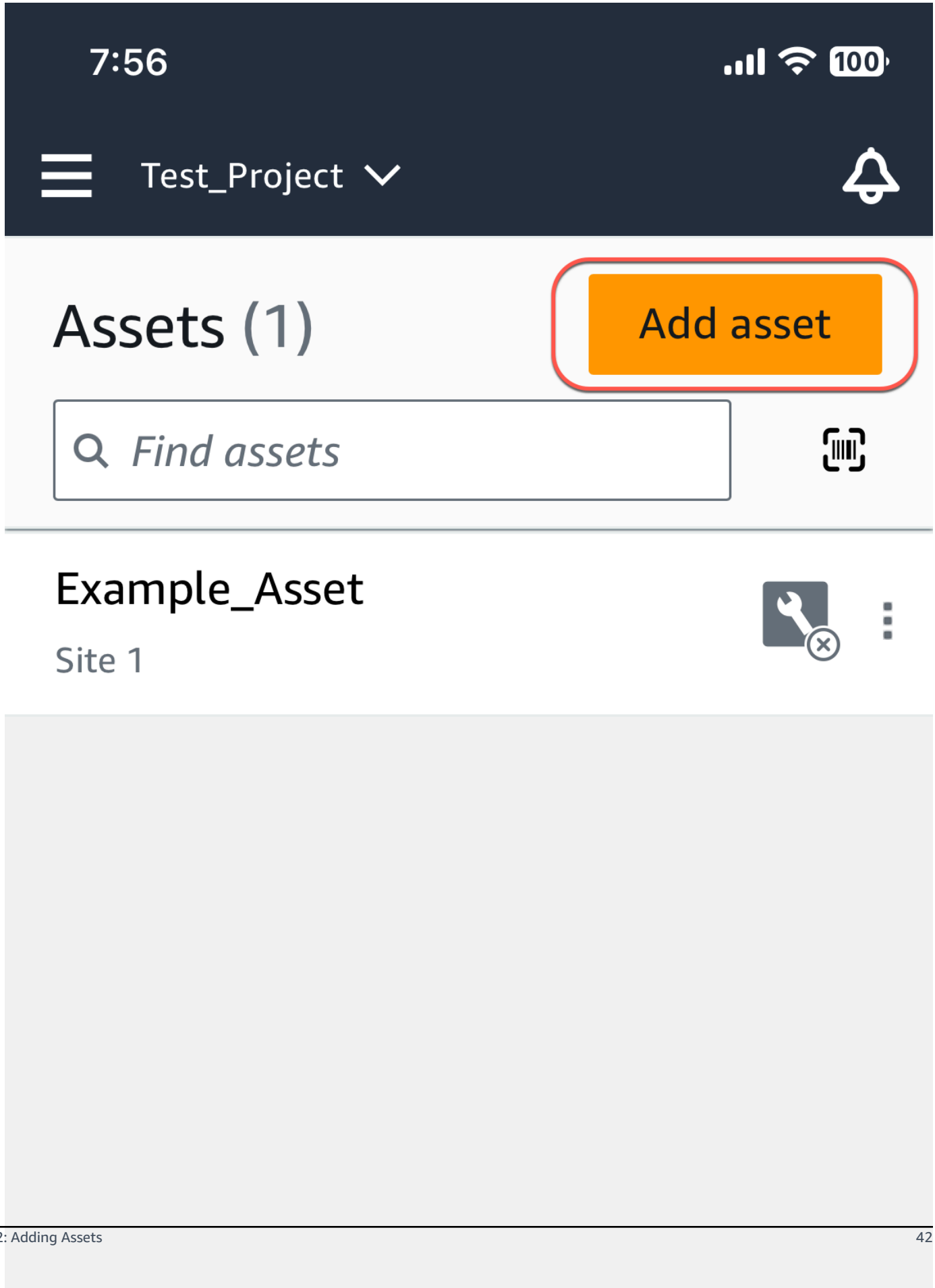
**Topics**


- Adding assets using the mobile app
- Adding assets using the web app


## Adding assets using the mobile app

### To add an asset using the mobile app

1. Sign in to your mobile app and select the project you want to add an asset to.

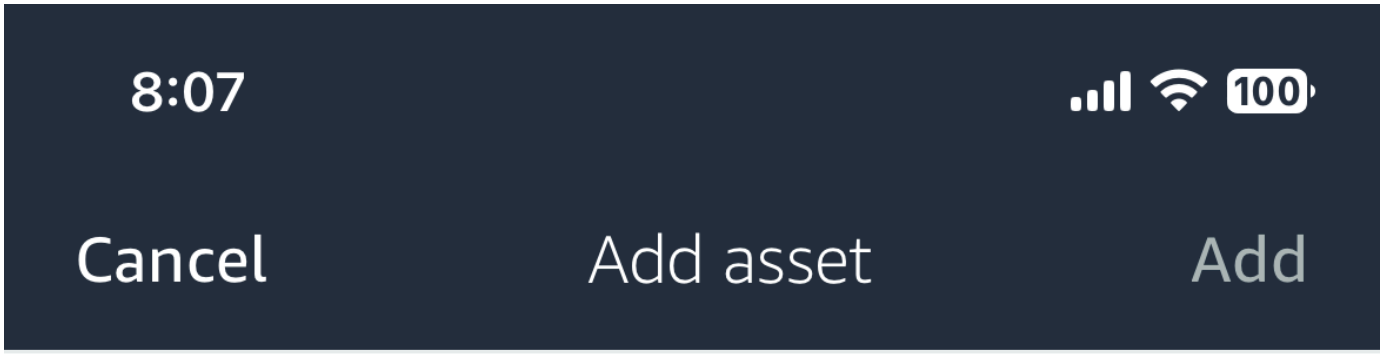

7:56
100
Test_Project
Assets (1)
Add asset
Find assets
Example_Asset
Site 1

2. Make sure you're on the correct site your project that you want to add the asset to. The project or site name indicates that you are at that level in the app.




   For more information about changing from site level to project level and vice versa, see Navigating between projects and sites in the mobile app.

3. From the **Assets** page, choose **Add asset**.
4. On the **Add asset** page, for **Asset name**, add a name for the asset you want to create and then select **Add**.




You are adding this asset to the project. We recommend you add it to a site. Once you add an asset you can't move it.
Learn more

## Asset name

Name for the asset to be monitored.

*Example: Pump*

Maximum 60 characters.

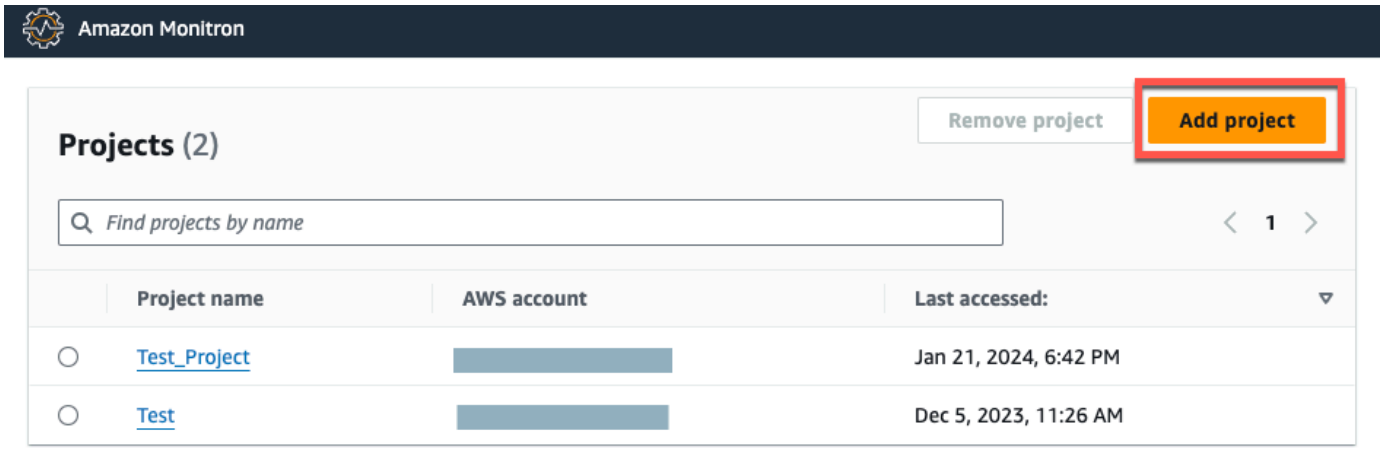
> **Note**
>
> If you have a QR code identifying the asset name, you can scan it by selecting the QR code.

When you've added your first asset, it's displayed on the **Assets list** page.

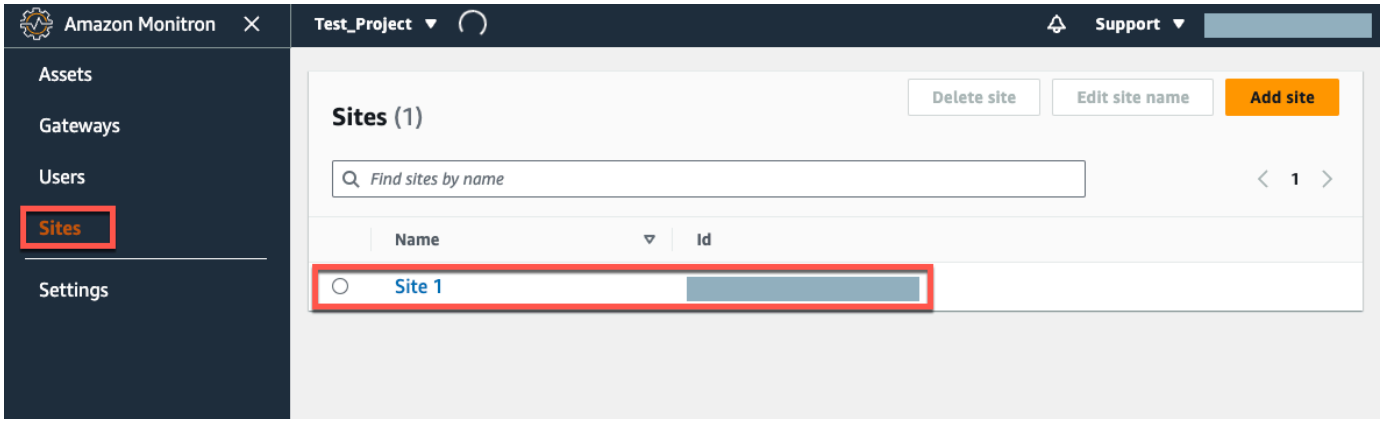
## Adding assets using the web app

### To add an asset using the web app

1. Sign in to your web app and select the project you want to add an asset to.

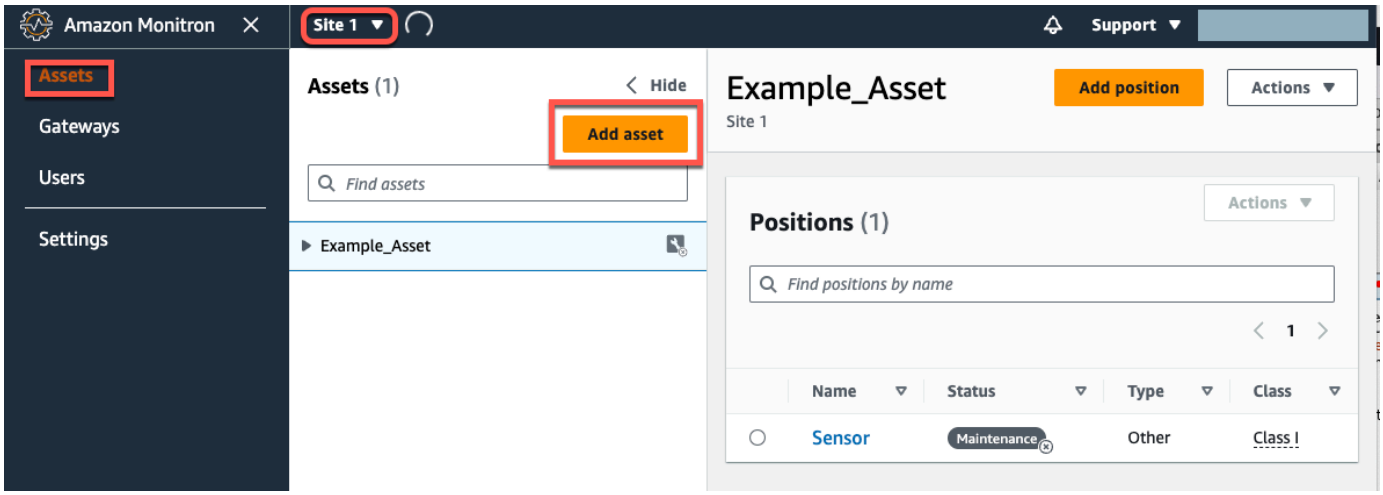



2. From the left navigation menu, choose **Sites**, and then select the site you want to the asset to.

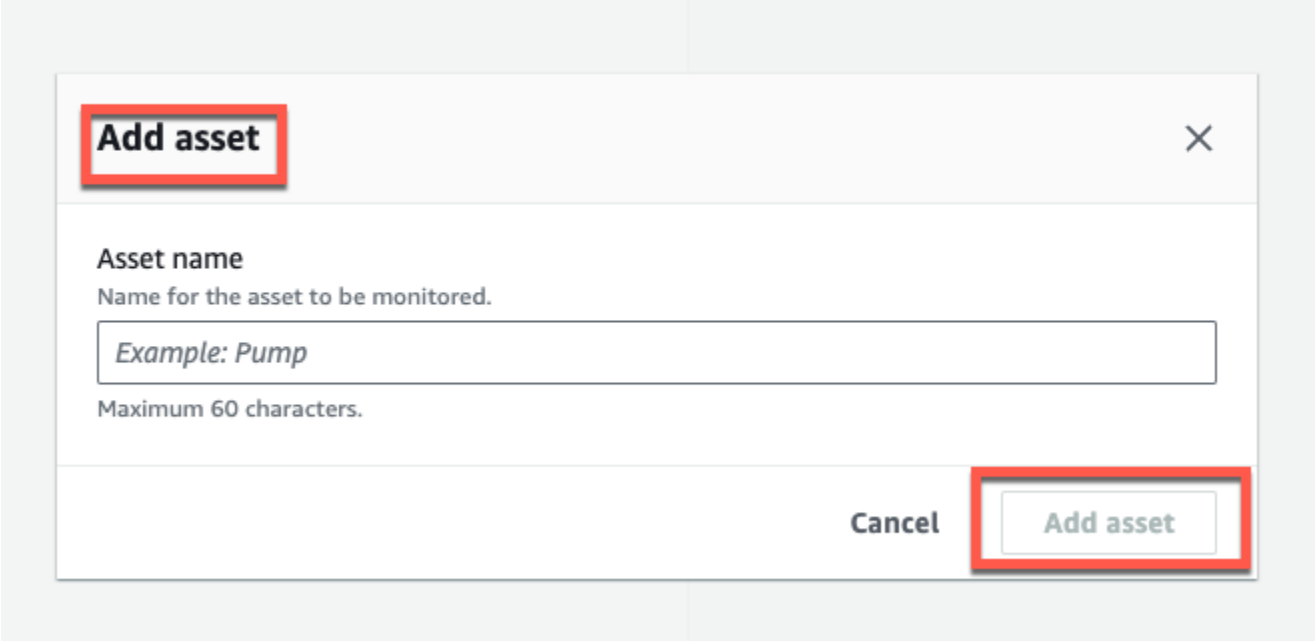


> **Note**
>
> You can also add the asset directly to a project.

3. From the **Assets** page, choose **Add asset**.




4. On the **Add asset** page, for **Asset name**, add a name for the asset you want to create and then select **Add asset**.




When you've added your first asset, it's displayed on the **Assets list** page.

# Step 3: Attach Sensors

Assets are paired to sensors, which directly monitor an asset's health. You place each sensor on the asset in a position that you want to monitor. You can place one or more sensors on each asset. Each sensor takes vibration and temperature measurements at the position to which it is paired and sends it to the AWS Cloud for analysis of machine health using the gateway.

## Where to Place Sensors

When placing a sensor, choose a location where it can accurately detect the machine's temperature or vibration.

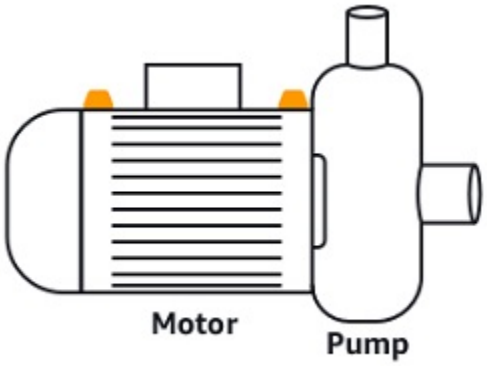
To achieve the greatest accuracy:

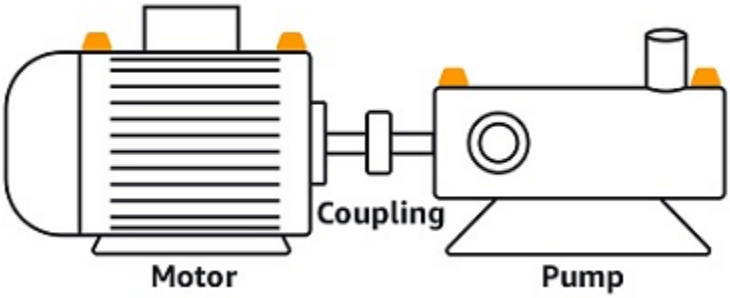
- Mount the sensor directly onto the housing of the target component.
- Minimize the length of the vibration transmission path, the distance between the source of vibration and sensor.
- Avoid mounting the sensor in a location that can oscillate due to natural frequencies, such as sheet metal covers.

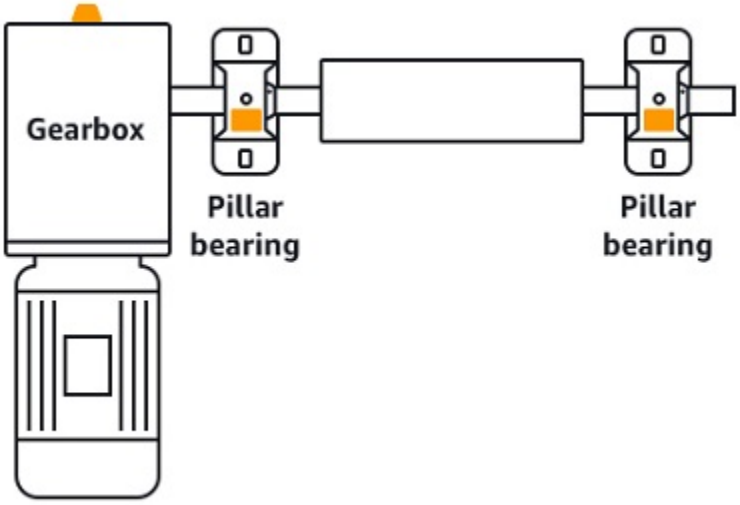
Vibration will attenuate up to 30-36"/75-90 cm) from the source. Attributes of the vibration transmission path length that can reduce the transmission path length include:

- The number of mounting surfaces, causing signal reflection
- Materials such as rubber and plastic that can absorb vibration

The following examples show where to place sensors. For more information and examples, see Where to Place Your Sensors in the *Amazon Monitron User Guide*.

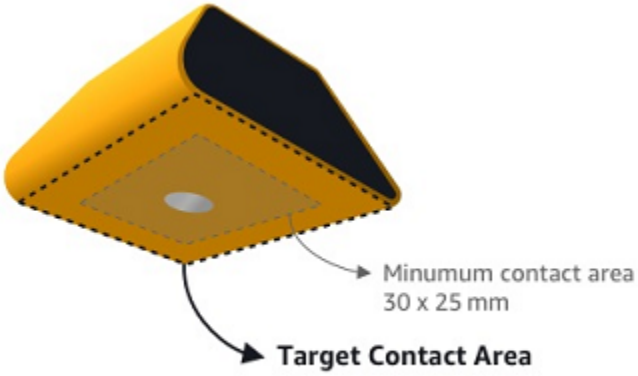





## How to Place Sensors

When you've decided where to place a sensor on an asset, make sure that a minimum of one-third of the sensor base is fixed to the asset. The sensors can pick up vibration and temperature measurements across the entire base of the sensor, but it's important to have the asset target area centered as much as possible on the sensor as shown in the following image.



Attach the sensor with an industrial adhesive. We recommend a cyanoacrylate-type epoxy. For additional information about attaching the sensor to your asset, see How to Place the Sensors in the *Amazon Monitron User's Guide*.

> **Warning**
>
> Amazon Monitron sensors can be attached to the equipment using industrial adhesive. We suggest you check the surface before selecting the adhesive. For surfaces up to 5 mm roughness/gaps, you can select an adhesive that fills the gap, such as LOCTITE® 3090 or LOCTITE® 4070. For flat surfaces (<0.1mm roughness), you can select a more generic adhesive, such as LOCTITE® 454. Always check and follow the processing guidelines outlined by the adhesive vendor.
> For more information about safely using the adhesive, see Loctite 454 Technical Information, Loctite 3090 Technical Information, or Loctite 4070 Technical Information, as appropriate.

**To attach the Amazon Monitron sensor**

1. Apply a thin layer of the adhesive on the bottom of the sensor, maximizing the contact area.
2. Hold the sensor to the mounting location on the machine part, pressing firmly for the length of time specified by the adhesive instructions.

## Step 4: Pairing Sensors to an Asset

Each sensor that you pair to an asset has a designated position and is set to monitor a specific part of the asset. For example, a sensor set up to monitor bearings on a conveyor belt might have the position of Left bearing 1 with a position type of Bearing.

Amazon Monitron uses Near Field Communications (NFC), a short-range (4 cm or less) wireless technology for communication between two electronic devices. To use Amazon Monitron, you need an iOS or Android 8.0+ smartphone with NFC installed natively.

> **Important**
>
> The equipment that you want to monitor must be in a healthy state before you pair it to a sensor. Amazon Monitron must establish a baseline for the equipment based on its normal state so that it can later determine abnormalities.

**To pair a sensor with an asset**

1. Attach your sensor in the correct position, as described in Step 3: Attach Sensors . You can also attach the sensor after pairing it to the asset in this step 4.
2. Make sure that the NFC feature on your smartphone is on and functioning.
3. Open your Amazon Monitron mobile app, and select the **Project** you want to add the sensors to.
4. From the navigation menu, make sure you're in the correct **Site**, and then choose **Assets**.
5. From the **Assets** list, choose the asset that you just created.
6. On your **Asset** page, choose **Add position**.
7. On the **Add position** page, do the following:

   a. For **Name**, add a name for your position.

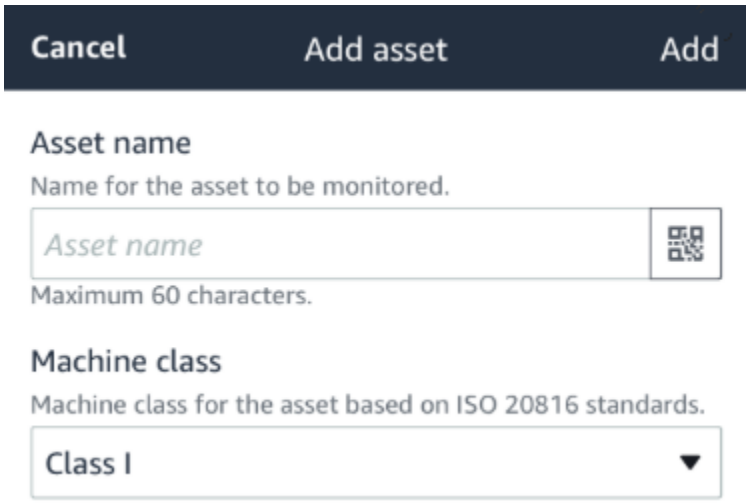
   b. For **Type**, choose the **Type of position** that best fits the location that you're going to monitor:

   - Bearing
   - Compressor
   - Fan
   - Gearbox
   - Motor
   - Pump
   - Other

   > **Note**
   >
   > After you pair the sensor, you can't change the position type.

c. For **Class**, choose the machine class of the asset from the four available.

> **Note**
>
> Asset machine class is based on ISO 20816 Standards. Amazon Monitron administrators can also create custom machine asset classes for all positions within a project. For more information about machine classes and customizing them, see Assets.




8. Choose **Next**. You'll be prompted to add sensors. For information on how to add sensors, see Sensors.
9. Choose **Pair sensor**.
10. Hold your phone close to the sensor to register it. A progress bar shows when registration is complete.



It can take a few moments for the sensor to be commissioned. If you have trouble pairing the sensor, see Pairing Your Sensor for more information.

> **Tip**
>
> If your smartphone fails to detect the sensor, try holding it so that the NFC antenna is close to the sensor. For iPhone models, the antenna is located at the top edge of the device. For Android models, the antenna location varies. The following resources might help you locate the NFC antenna on an Android device:
>
> - NFC detection area (Samsung)
> - Pixel phone hardware diagram

On the **Assets** page, the sensor is now paired to the asset and is identified by its position.

# Understanding warnings and alerts

> **Note**
>
> This section focuses on using the Amazon Monitron mobile app. To learn about the Amazon Monitron web app, see Understanding sensor measurements in the *Amazon Monitron User Guide*.

After a sensor is paired to an asset, Amazon Monitron starts monitoring the asset's condition. When it detects an abnormal machine condition, it sends you a notification (  ) and changes the asset state. The alert notification is generated using a combination of machine learning and ISO 20816 standards for machine vibration.

To monitor the data and respond to alerts about abnormalities, you use the Amazon Monitron mobile app.

Your administrator will send you an email with information about how to log in for the first time and connect to your project.

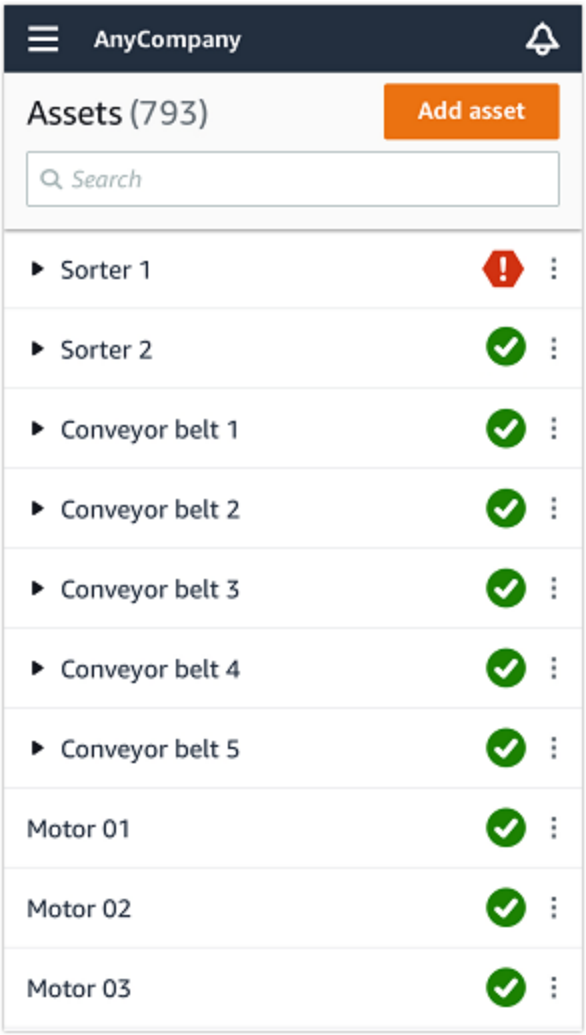
**Topics**

- Step 1: Understanding asset health

- Step 2: Viewing asset conditions
- Step 3: Viewing and acknowledging a machine abnormality
- Step 4: Resolving a machine abnormality
- Step 5: Muting and unmuting alerts

## Step 1: Understanding asset health

To monitor assets using the Amazon Monitron mobile app, start with the **Assets** list. This list is displayed when you open the mobile app.



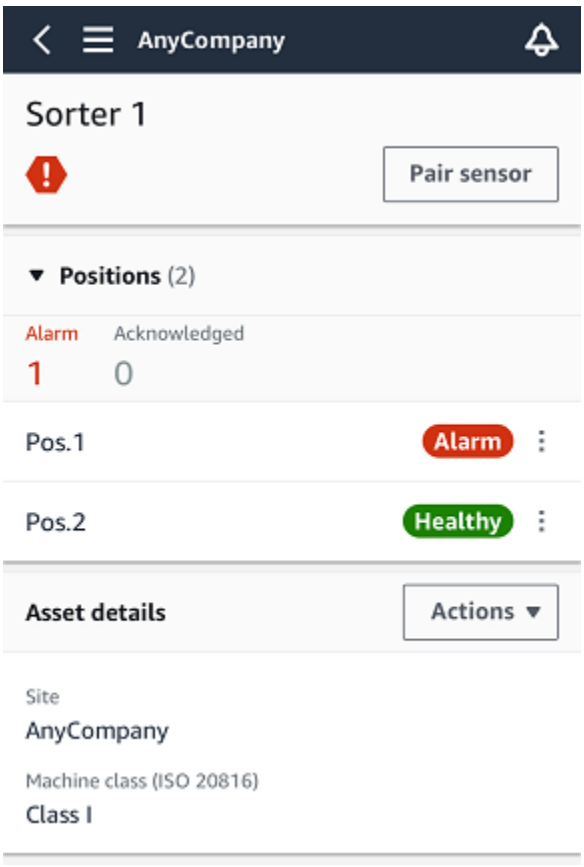

Each asset in your project or site is listed in the **Assets** list.

On the **Assets** list page, each asset shows an icon indicating its health. The following table describes these icons.

| Icon | Health state |
| --- | --- |
|  | **Healthy state**: The status of all sensor positions on the asset is healthy. |
|  | **Warning state**: A warning has been triggered for one of the positions of this asset, indicating that Amazon Amazon Monitron has detected early signs of potential failure. Amazon Amazon Monitron identifie s warning conditions by analyzing equipment vibration and temperatu re, using a combination of machine learning and ISO vibration standards. |
|  | **Alarm state**: Once an asset has been placed in a warning state, Amazon Monitron will continue to monitor it. Again, Amazon Monitron is using a combination of machine learning and vibration ISO standards. If the condition of the asset gets significa ntly worse, Amazon Amazon Monitron will escalate by sending an **Alarm** notificat ion when it detects that the equipment condition has significantly worsened. We recommend investigating the |

| Icon | Health state |
| --- | --- |
| | issue at the earliest opportuni ty. An equipment failure might occur if the issue isn't addressed. |
|  | **Maintenance state**: One of the asset's sensors is in the maintenance state. The alarm state of the asset has been acknowledged by a technicia n, but not yet addressed. |
| No sensor | **No sensor**: At least one position on the asset doesn't have a sensor paired to it. |

When you choose an asset, the app displays the health status of each underlying sensor position.




The following table describes the position status indicators.

| Status | State |
| --- | --- |
| Healthy | The position is healthy: All measured values are within their normal range. |
| Warning | A warning has been triggered for this position indicatin g early signs of a potential failure condition. We recommend that you monitor the equipment closely and initiate an investigation during an upcoming planned maintenance. |

| Status | State |
| --- | --- |
|  | An alarm has been triggered for this position, indicating that the machine vibration or temperature is out of the normal range at this position. We recommend investiga ting the issue at the earliest opportunity. An equipment failure might occur if the issue isn't addressed. |
|  | The alarm state of the position has been acknowled ged by a technician, but not yet addressed. |
| No sensor | The position doesn't have a sensor paired to it. |

When an issue is raised for an individual position, the status changes for that position and for the asset as a whole.

## Step 2: Viewing asset conditions

Viewing assets is more than simply understanding the icons that show the asset and position health status. It is often useful to see the data collected by the sensors yourself.

**To view sensor data in the Amazon Monitron mobile app**

1. In the **Assets** list, choose the asset you want to view.
2. Choose the position with the data that you want to view.
3. Under the **Vibration and Temperature** tabs, choose the chart of recent sensor data and the level of detail that you want to see.

   You can choose separate versions for different time periods (1 day, 1 week, 2 weeks, 1 month, and so on).

# Step 3: Viewing and acknowledging a machine abnormality

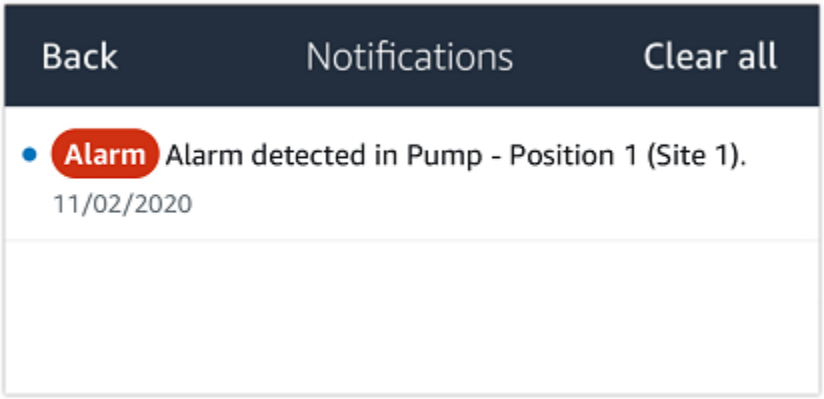
The longer Amazon Monitron monitors a position, the more it fine-tunes its baseline and increases its accuracy.

When an **Alarm** or a **Warning** is triggered, Amazon Monitron sends a notification to the mobile app that is displayed as an icon in the upper right of your screen (



).

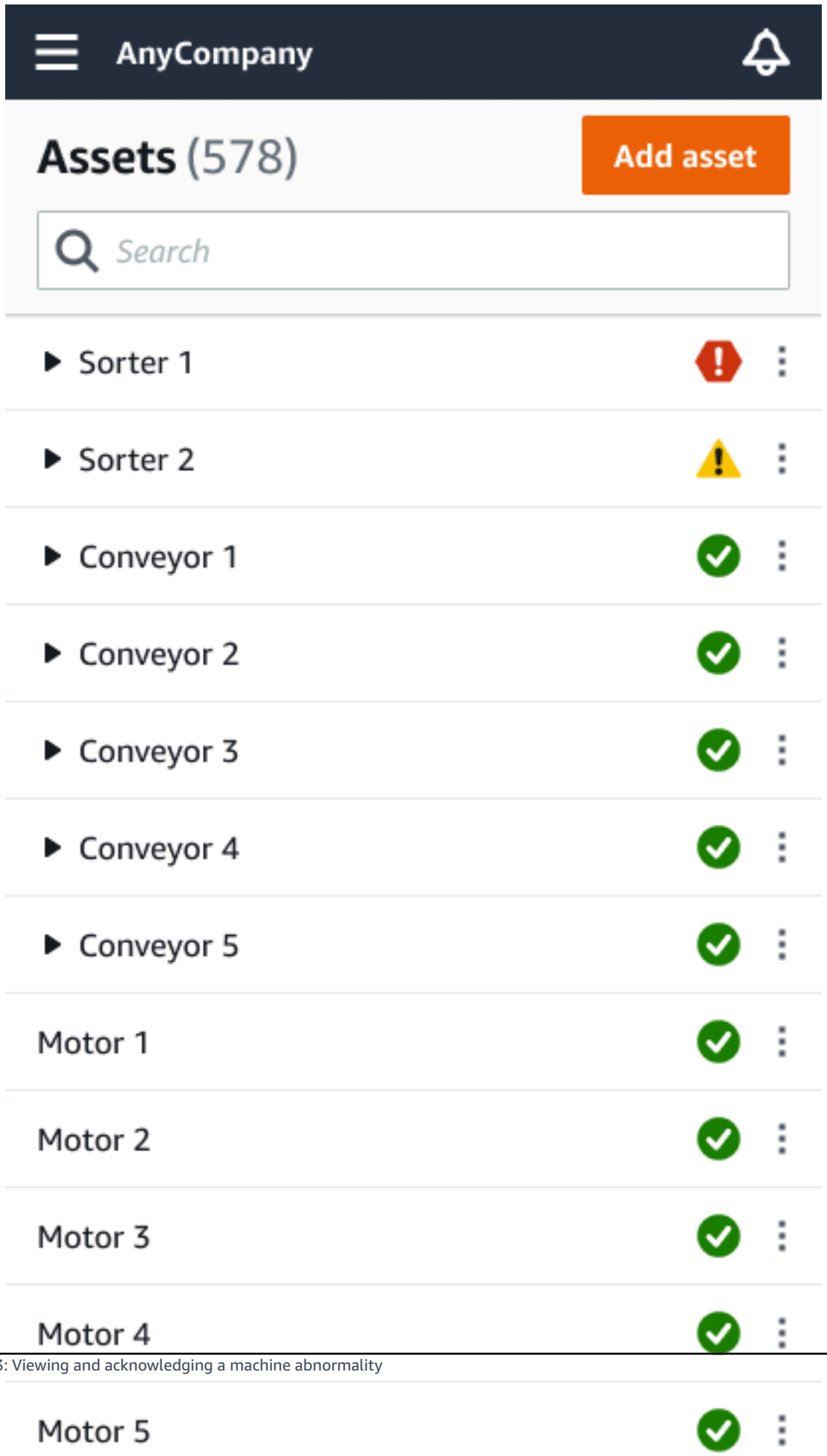
Choosing the notification icon opens the **Notifications** page, which lists all pending notifications.



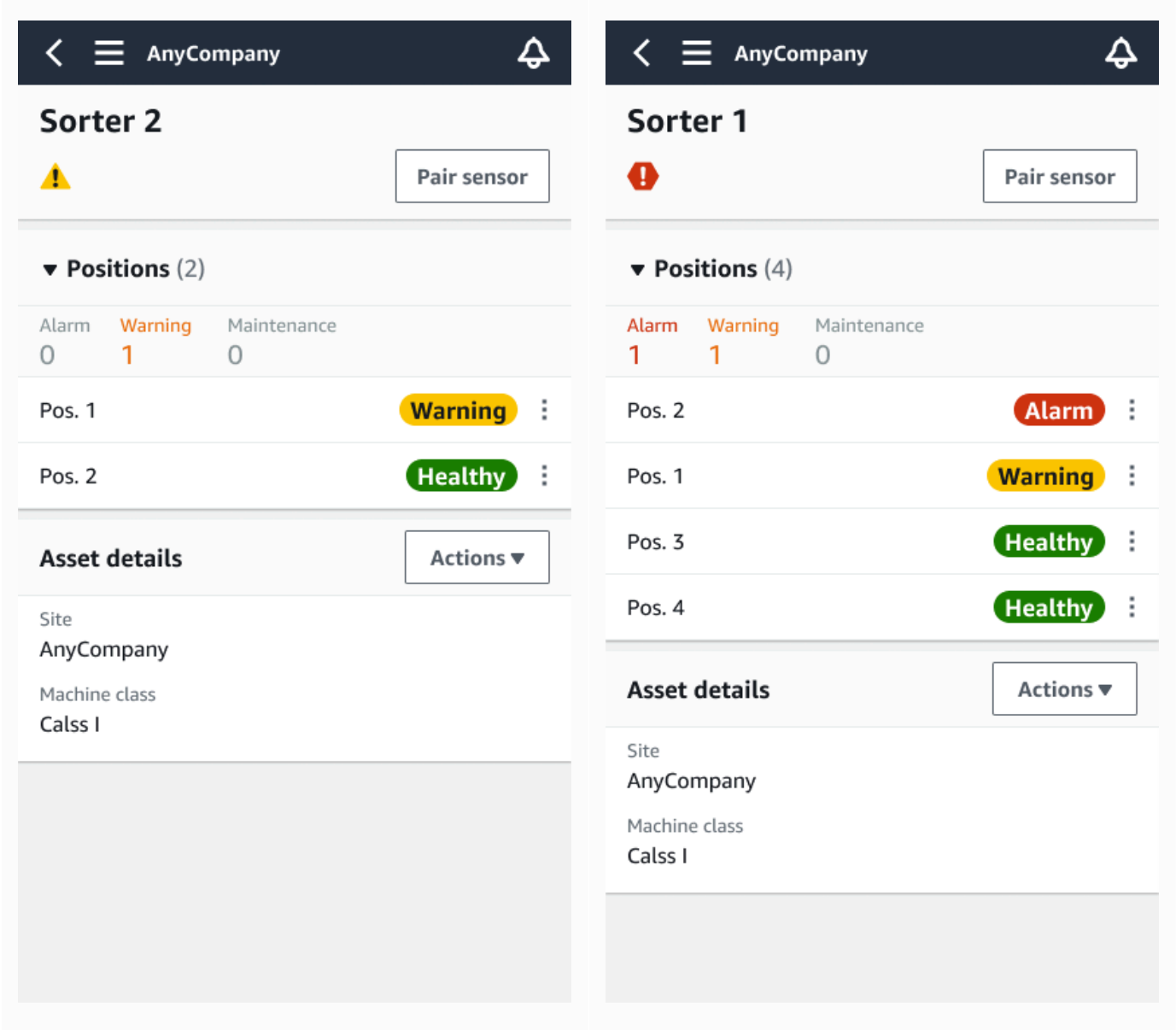

When you receive a notification, you must view and acknowledge it. This doesn't fix the issue with the asset, it just lets Amazon Monitron know that you are aware of it.

**To view and acknowledge an abnormality**

1. On the **Assets** list, choose the asset with the alarm.

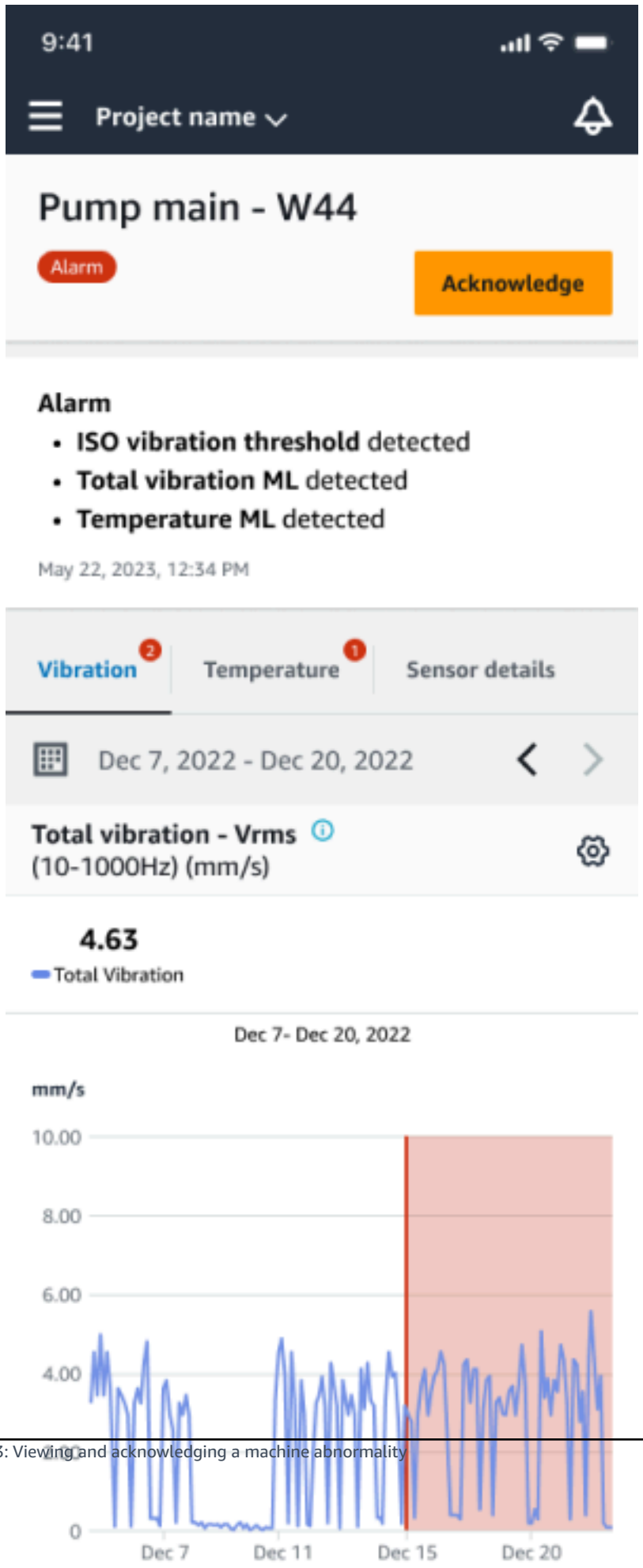

AnyCompany
Assets (578)
Add asset
Search
Sorter 1
Sorter 2
Conveyor 1
Conveyor 2
Conveyor 3
Conveyor 4
Conveyor 5
Motor 1
Motor 2
Motor 3
Motor 4
Motor 5

2. Choose the position with the alarm to view the issue.




3. To confirm that you are aware of the issue, choose **Acknowledge**.

   Note that the text on the following screens also indicates whether the alert notification was triggered based on the equipment's vibration or temperature, or by the vibration ISO thresholds or machine learning models. This information can be used by technicians to investigate and fix the issue. After an abnormality has been acknowledged and repaired, resolve the issue in the mobile app.


9:41
Project name
Pump main - W44
Alarm
Acknowledge
Alarm
ISO vibration threshold detected
Total vibration ML detected
Temperature ML detected
May 22, 2023, 12:34 PM
Vibration 2
Temperature 1
Sensor details
Dec 7, 2022 - Dec 20, 2022
Total vibration - Vrms
(10-1000Hz) (mm/s)
4.63
Total Vibration
Dec 7- Dec 20, 2022
mm/s
10.00
8.00
6.00
4.00
0
Dec 7
Dec 11
Dec 15
Dec 20

The status of the asset changes to:




After the alarm has been acknowledged, the abnormality can be examined and fixed as appropriate.

## Step 4: Resolving a machine abnormality

Resolving an abnormality returns the sensor to healthy status and provides information about the issue to Amazon Monitron so it can better determine when a failure might occur in the future.

For information about failure modes and causes, and how to resolve abnormalities, see Resolving a Machine Abnormality in the *Amazon Monitron User Guide*.

**To resolve an abnormality**

1. In the **Assets** list, choose the asset with the issue.
2. Choose the position with the resolved abnormality.
3. Choose **Resolve**.
4. For **Failure mode**, choose one of the available types.
5. For **Failure cause**, choose the cause.
6. For **Action taken** choose the action taken.
7. Choose **Submit**.

   In the **Assets** list, the asset status returns to **Healthy**.

## Step 5: Muting and unmuting alerts

You can choose to mute and unmute alerts (alarms and warnings) for a position.

**Topics**

- Muting alerts
- Unmuting alerts

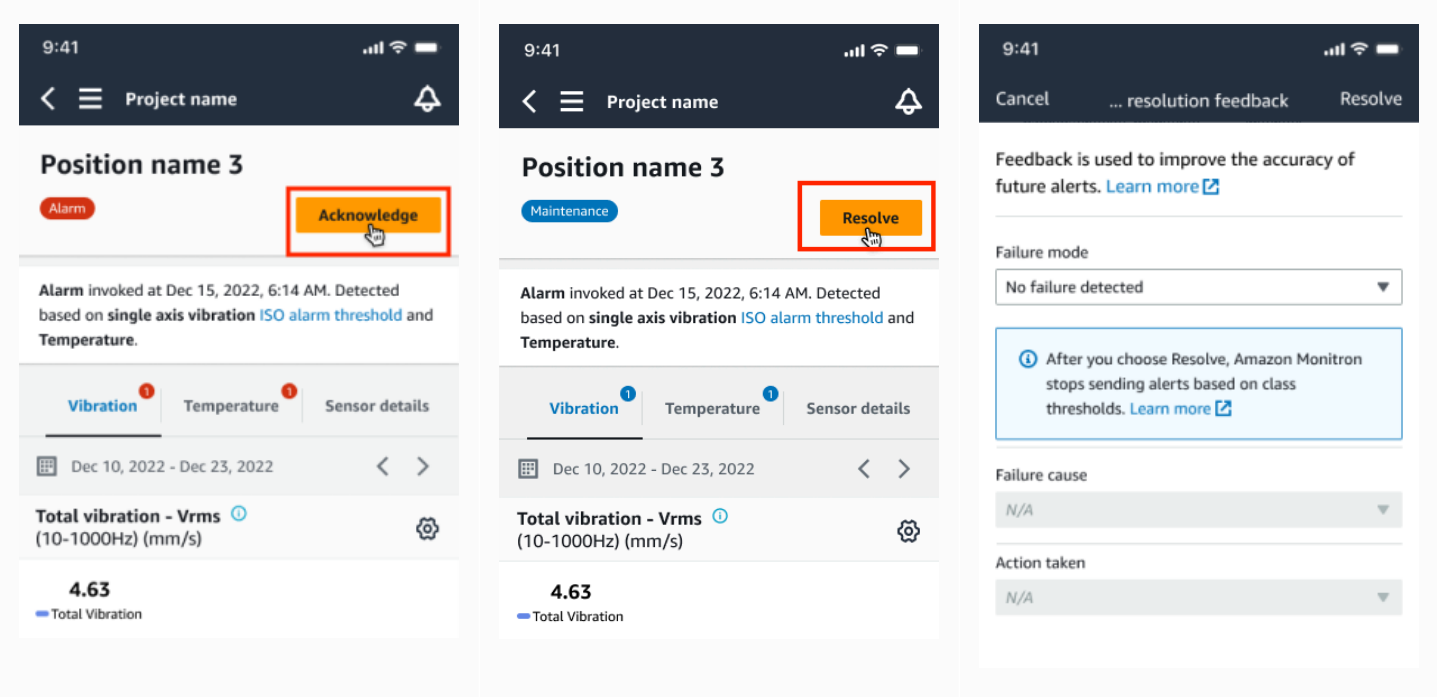
## Muting alerts

ISO thresholds apply broadly to large classes of equipment. Therefore, when detecting the potential failure of a specific asset, you may consider other factors as well. For example, you can mute a notification generated by ISO vibration thresholds if you assess that your equipment is still healthy when the alert is raised.

You also can mute alerts (alarms and warnings) by providing the 'No failure detected' feedback for the 'Failure mode' while closing the alert. Note that Amazon Monitron will continue to notify users of potential failures detected based on machine learning, even when notifications based on ISO thresholds are muted.

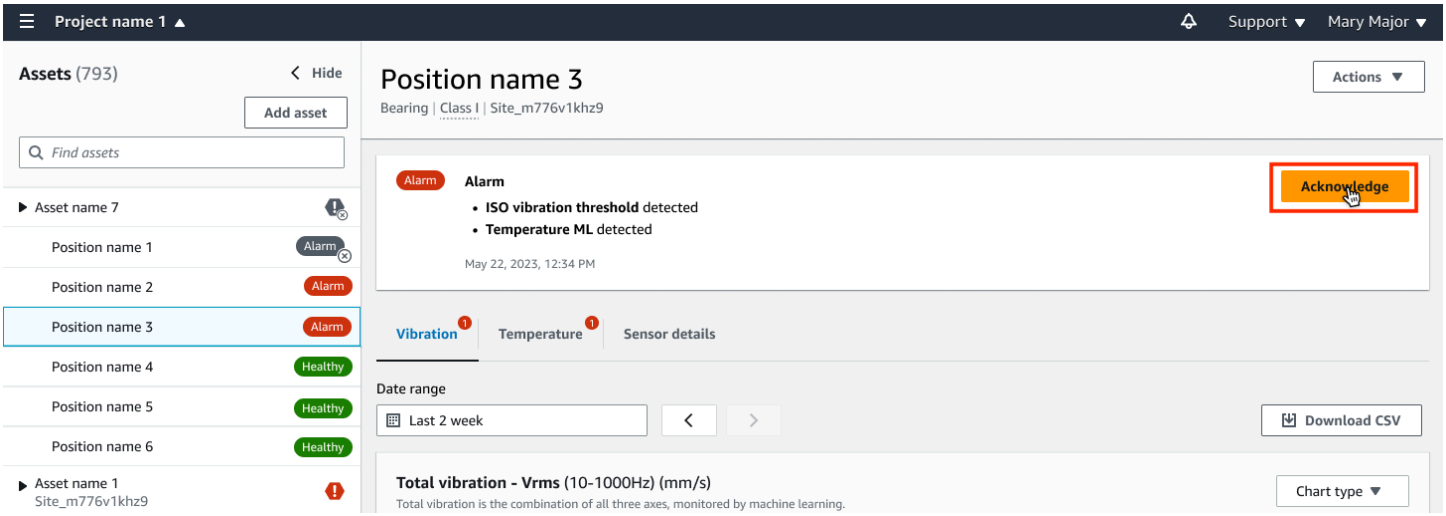
### Muting alerts on mobile app

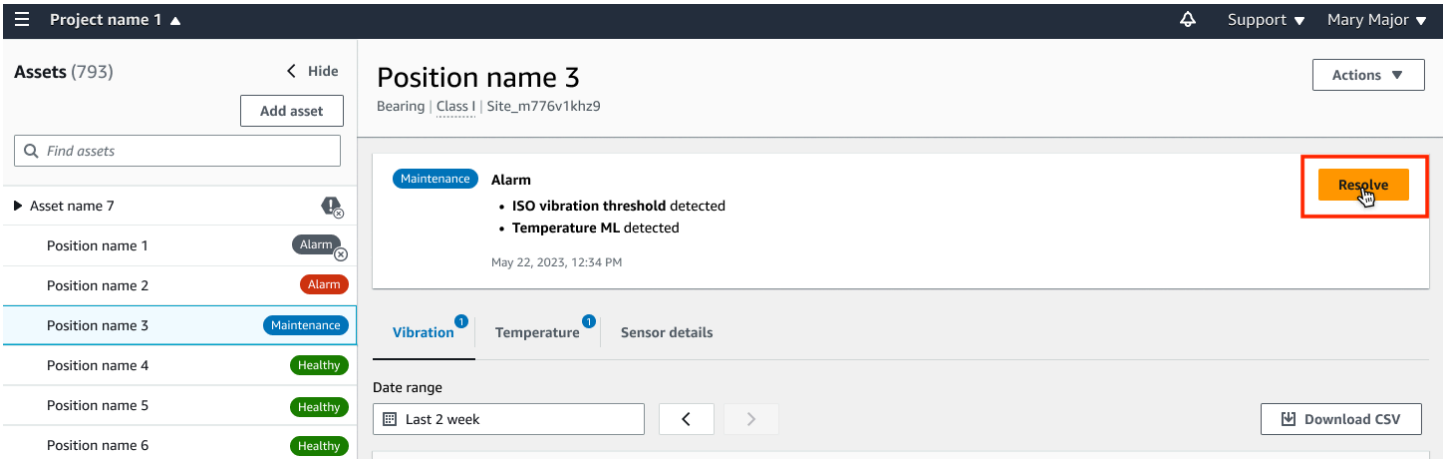
The following images show you how to mute alerts on the Amazon Monitron mobile app.

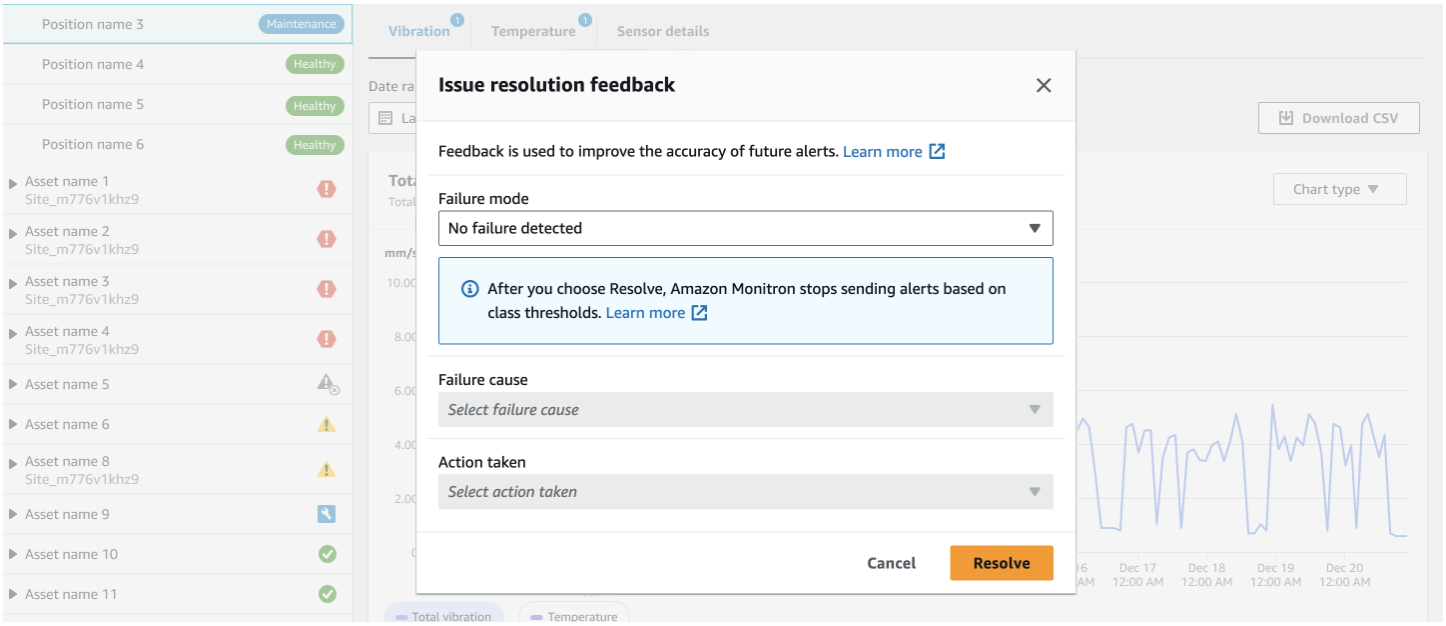



### Muting alerts on web app

The following images show you how to mute alerts on the Amazon Monitron web app.


Project name 1
Support
Mary Major
Assets (793)
Hide
Add asset
Find assets
Asset name 7
Position name 1
Alarm
Position name 2
Alarm
Position name 3
Alarm
Position name 4
Healthy
Position name 5
Healthy
Position name 6
Healthy
Asset name 1
Site_m776v1khz9
Position name 3
Bearing | Class I | Site_m776v1khz9
Actions
Alarm
Alarm
ISO vibration threshold detected
Temperature ML detected
May 22, 2023, 12:34 PM
Acknowledge
Vibration
Temperature
Sensor details
Date range
Last 2 week
Download CSV
Total vibration - Vrms (10-1000Hz) (mm/s)
Total vibration is the combination of all three axes, monitored by machine learning.
Chart type


Project name 1
Support
Mary Major
Assets (793)
Hide
Add asset
Find assets
Asset name 7
Position name 1
Alarm
Position name 2
Alarm
Position name 3
Maintenance
Position name 4
Healthy
Position name 5
Healthy
Position name 6
Healthy
Position name 3
Bearing | Class I | Site_m776v1khz9
Actions
Maintenance
Alarm
ISO vibration threshold detected
Temperature ML detected
May 22, 2023, 12:34 PM
Resolve
Vibration
Temperature
Sensor details
Date range
Last 2 week
Download CSV


Position name 3
Maintenance
Position name 4
Healthy
Position name 5
Healthy
Position name 6
Healthy
Asset name 1
Site_m776v1khz9
Asset name 2
Site_m776v1khz9
Asset name 3
Site_m776v1khz9
Asset name 4
Site_m776v1khz9
Asset name 5
Asset name 6
Asset name 8
Site_m776v1khz9
Asset name 9
Asset name 10
Asset name 11
Vibration
Temperature
Sensor details
Download CSV
Chart type
Issue resolution feedback
Feedback is used to improve the accuracy of future alerts. Learn more
Failure mode
No failure detected
After you choose Resolve, Amazon Monitron stops sending alerts based on class thresholds. Learn more
Failure cause
Select failure cause
Action taken
Select action taken
Cancel
Resolve
Dec 17 12:00 AM
Dec 18 12:00 AM
Dec 19 12:00 AM
Dec 20 12:00 AM
Total vibration
Temperature

# Unmuting alerts

You can choose to unmute alerts (alarms and warnings) at any time. When unmuting alerts, you can choose from the following options.

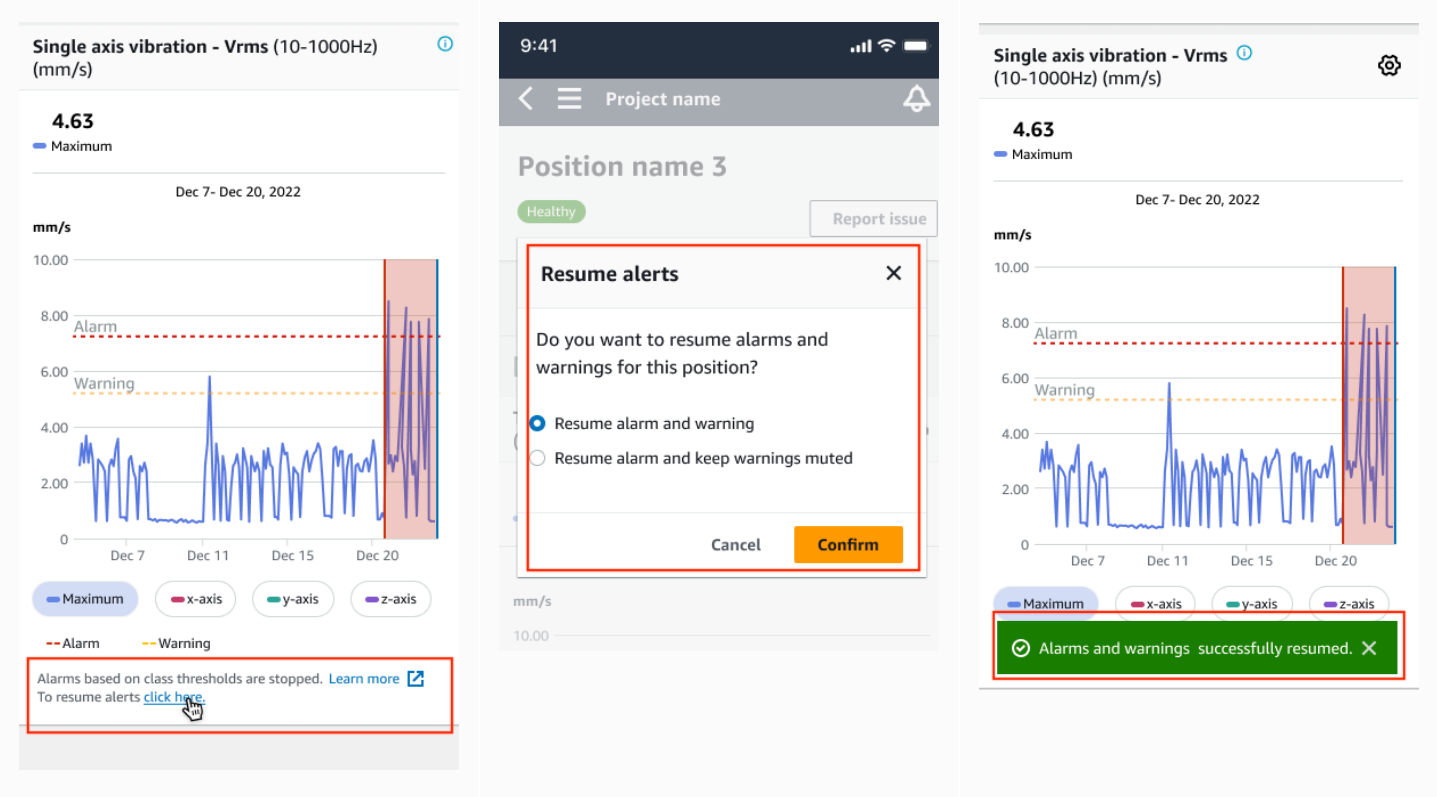
### Available options

- Resume all alerts (alarms and warnings)
- Resume alarms but keep warnings muted
- Resume only alarms
- Resume only warnings

### Resume all alerts (alarms and warnings)

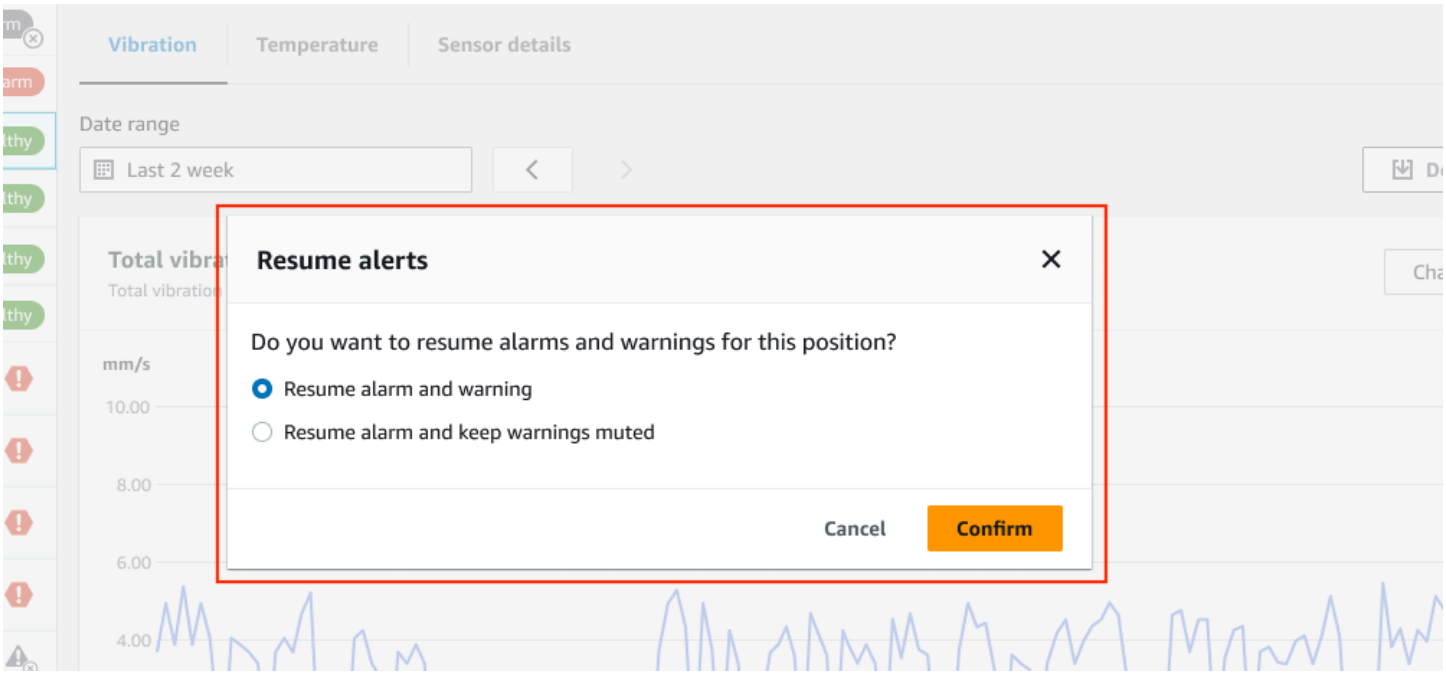
If you've muted both alarms and warnings, you can unmute them.

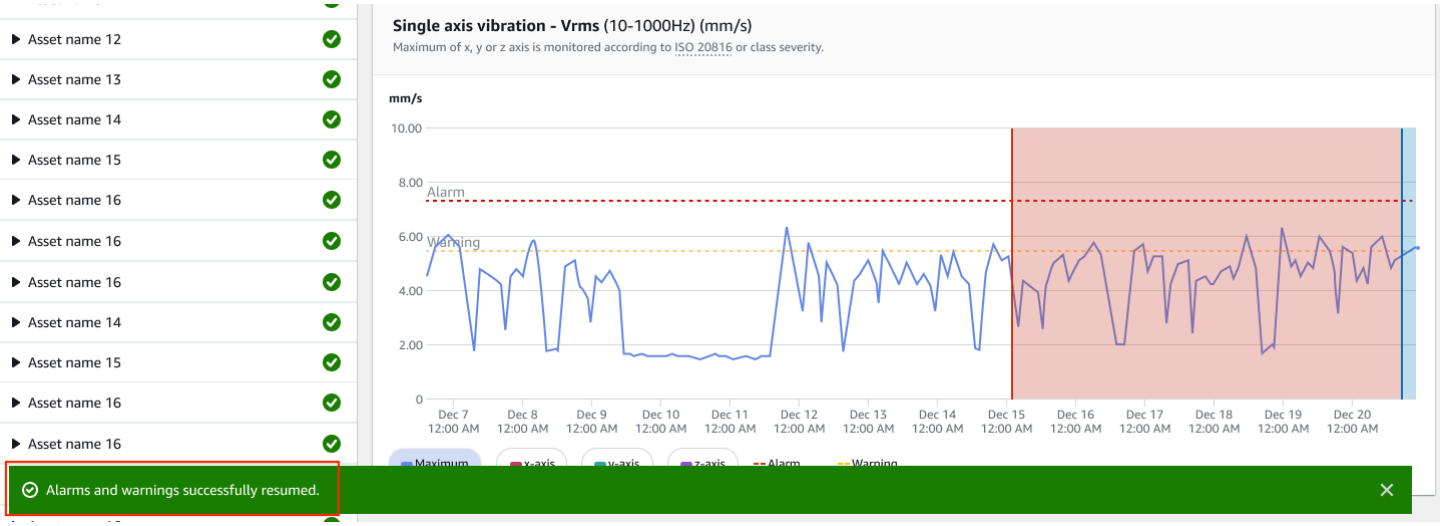
### Resume all alerts on mobile



## Resume all alerts on web



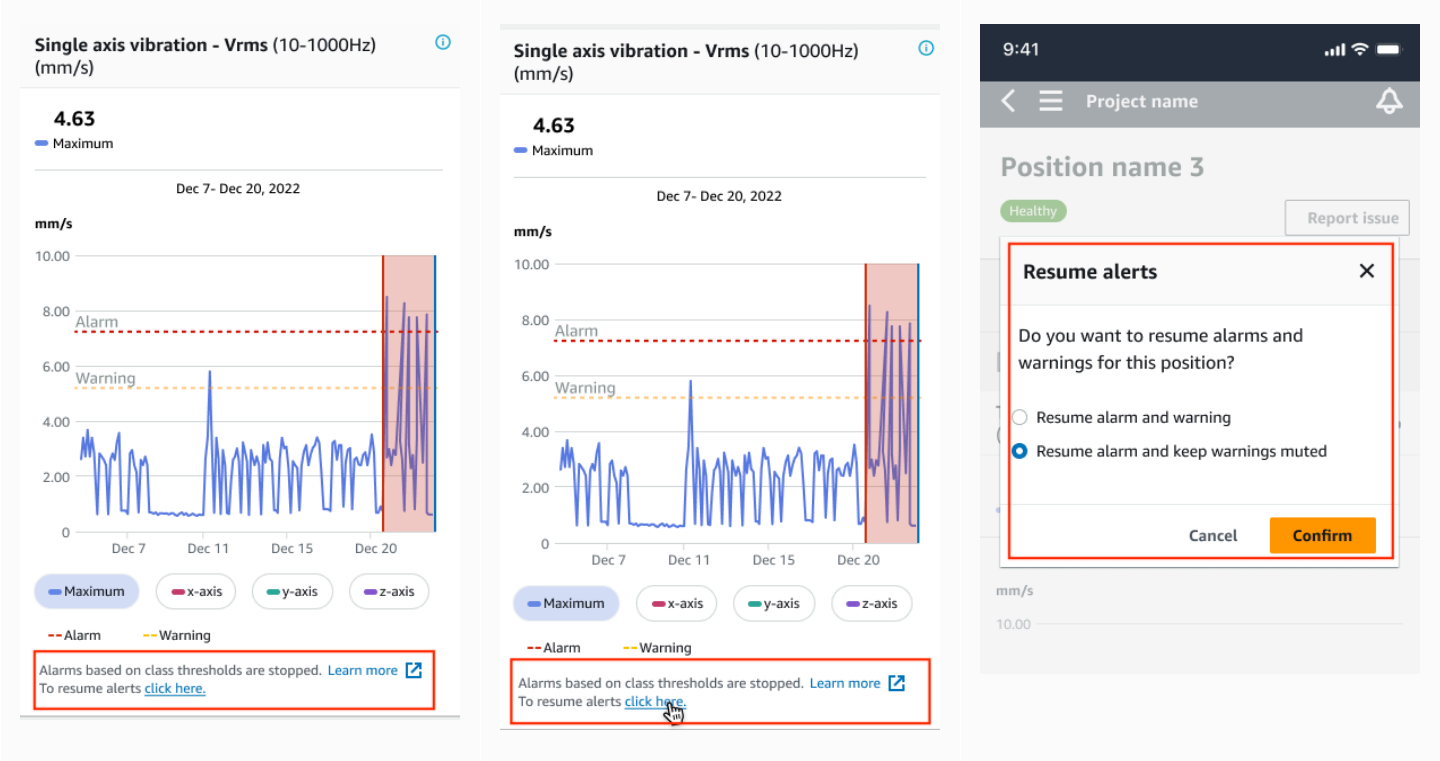





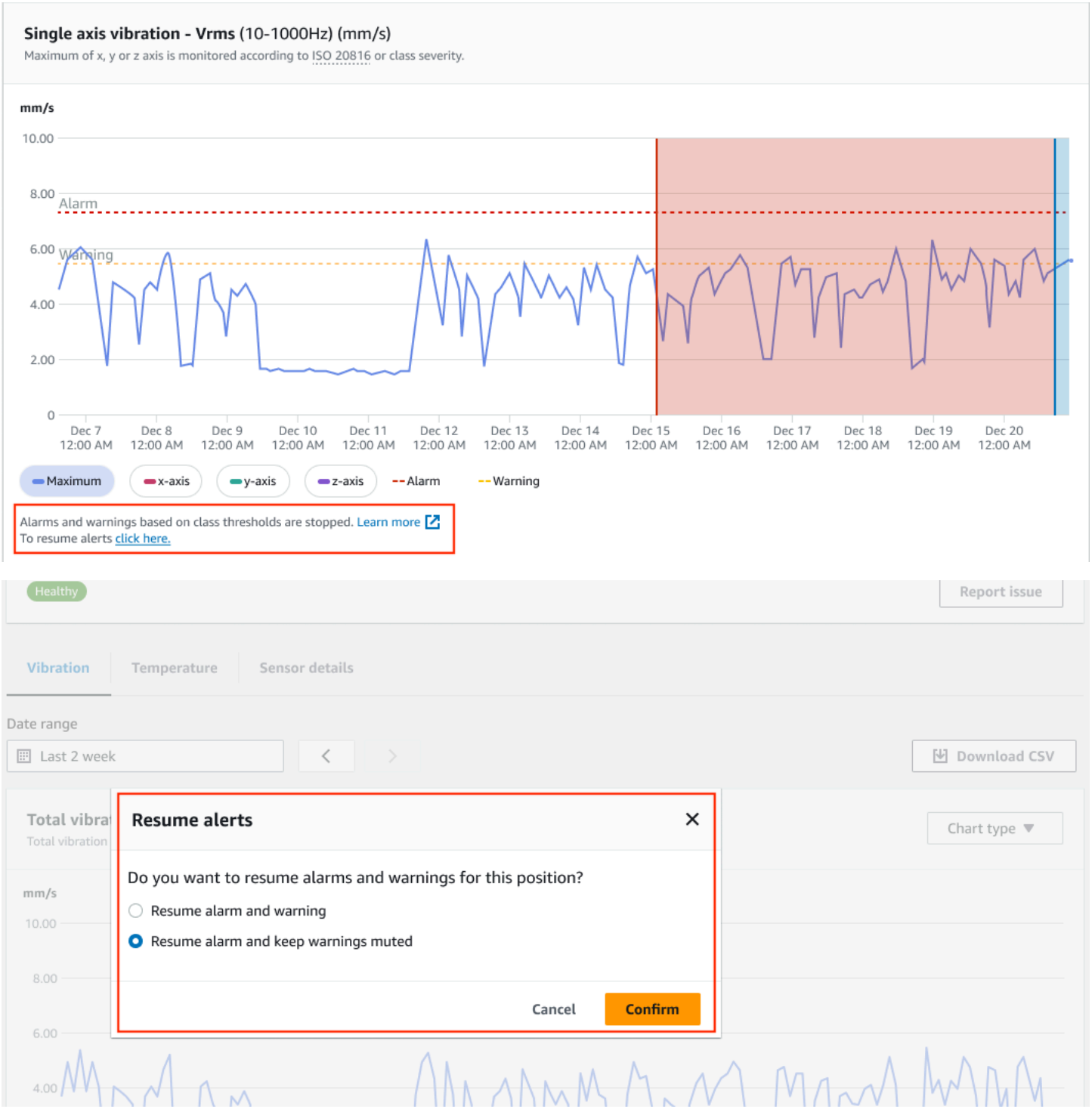

## Resume alarms but keep warnings muted

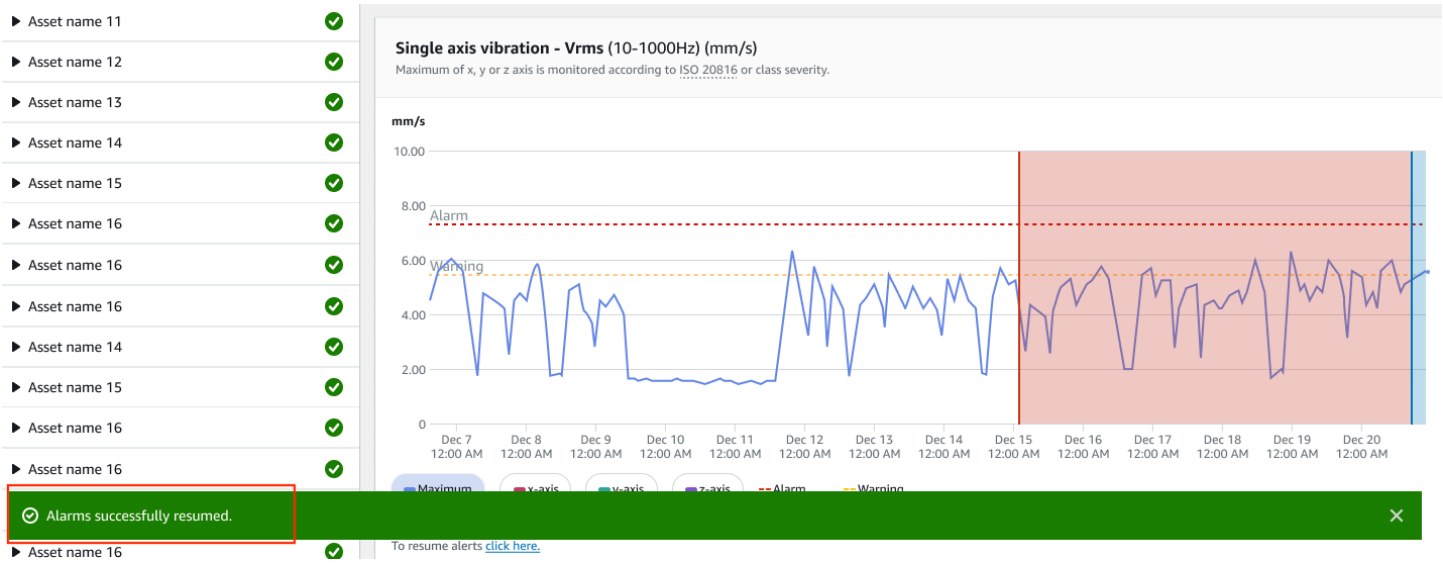
If you've muted both alarms and warnings, you can unmute alarms and keep warnings muted.

## Resume alarms keeping warnings muted on the mobile app



## Resume alarms keeping warnings muted on the web app

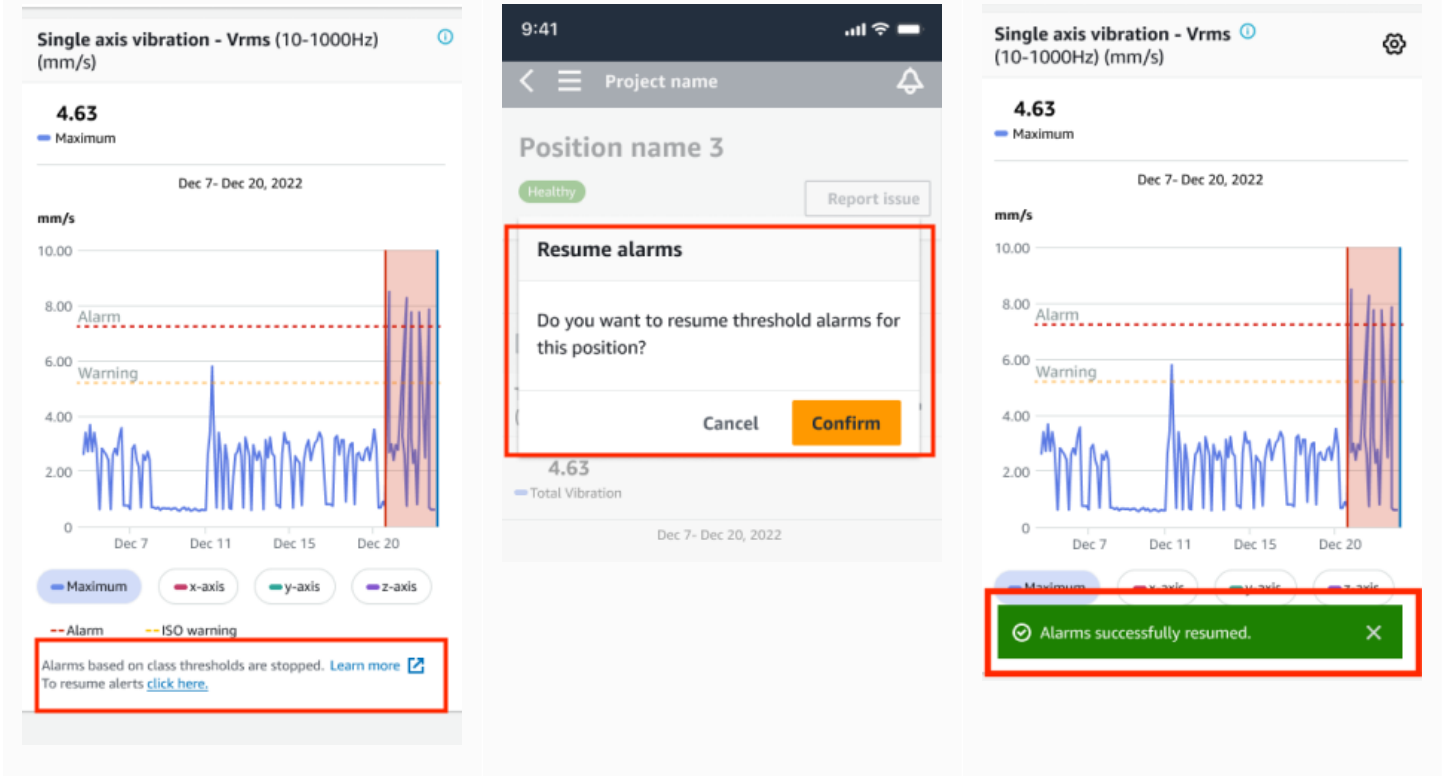




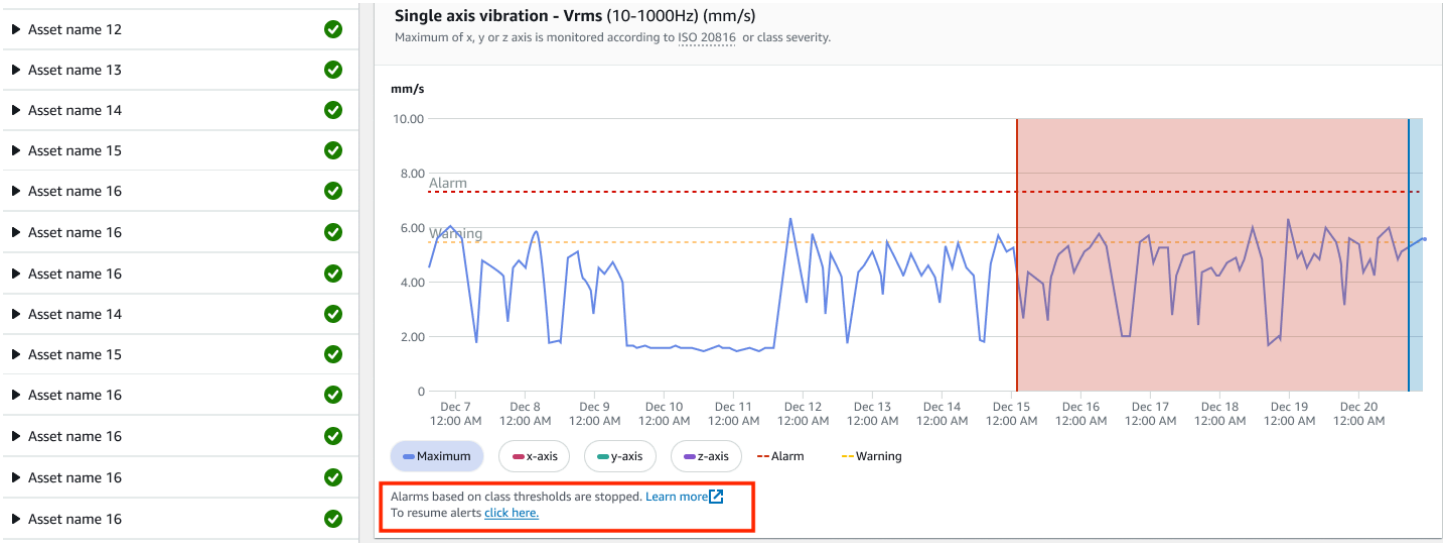

## Resume only alarms

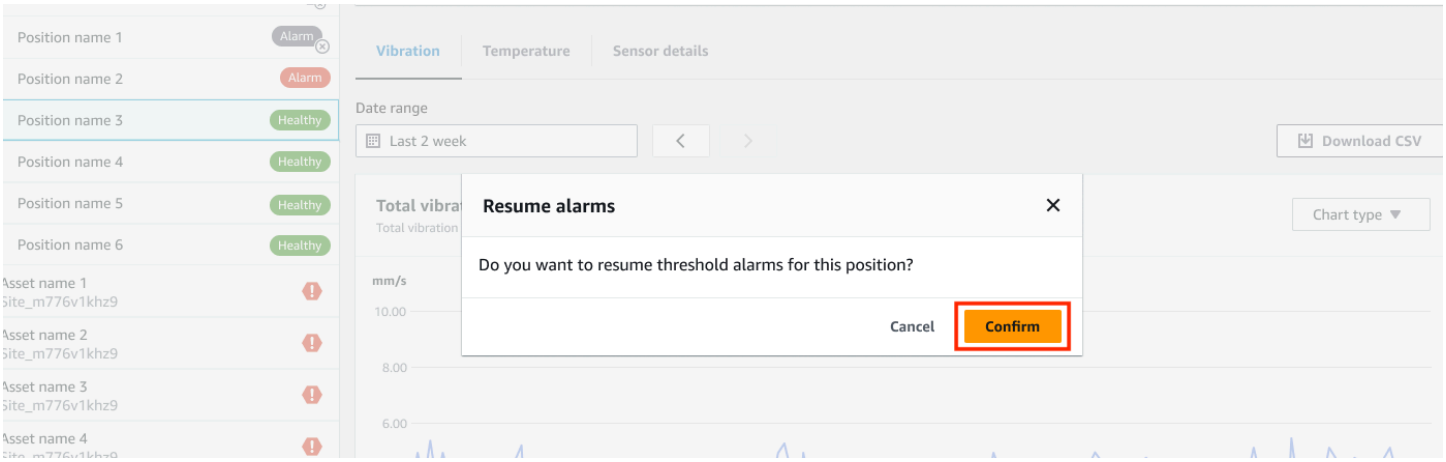
If you've muted alarms, you can unmute them.

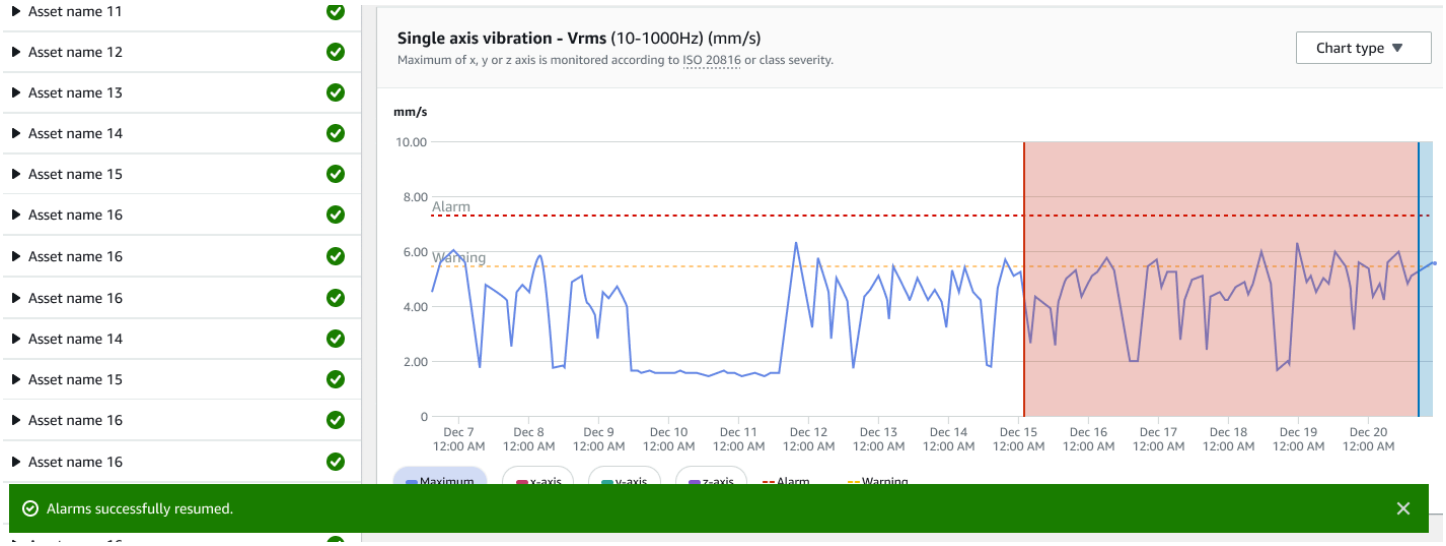
## Resume alarms on mobile app



# Resume alarms on web app



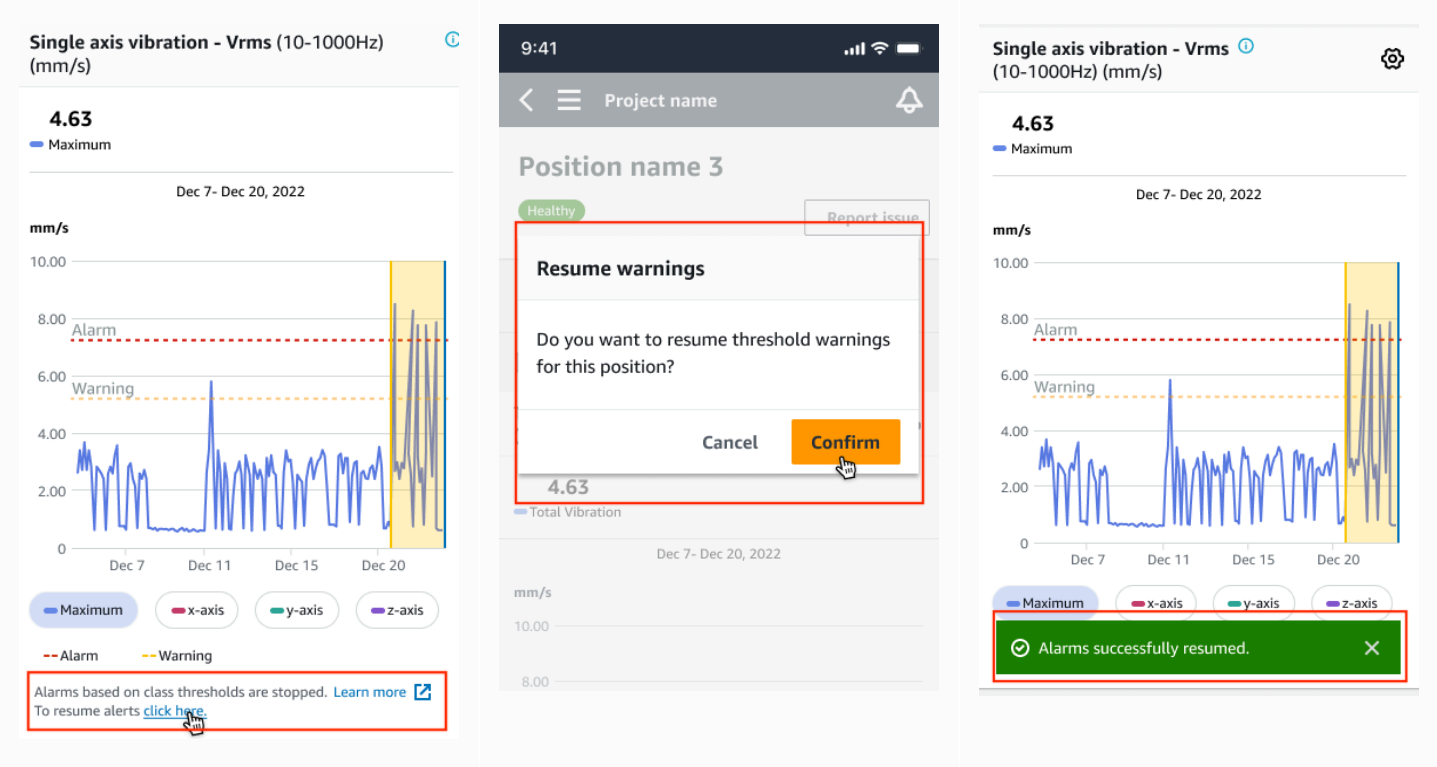



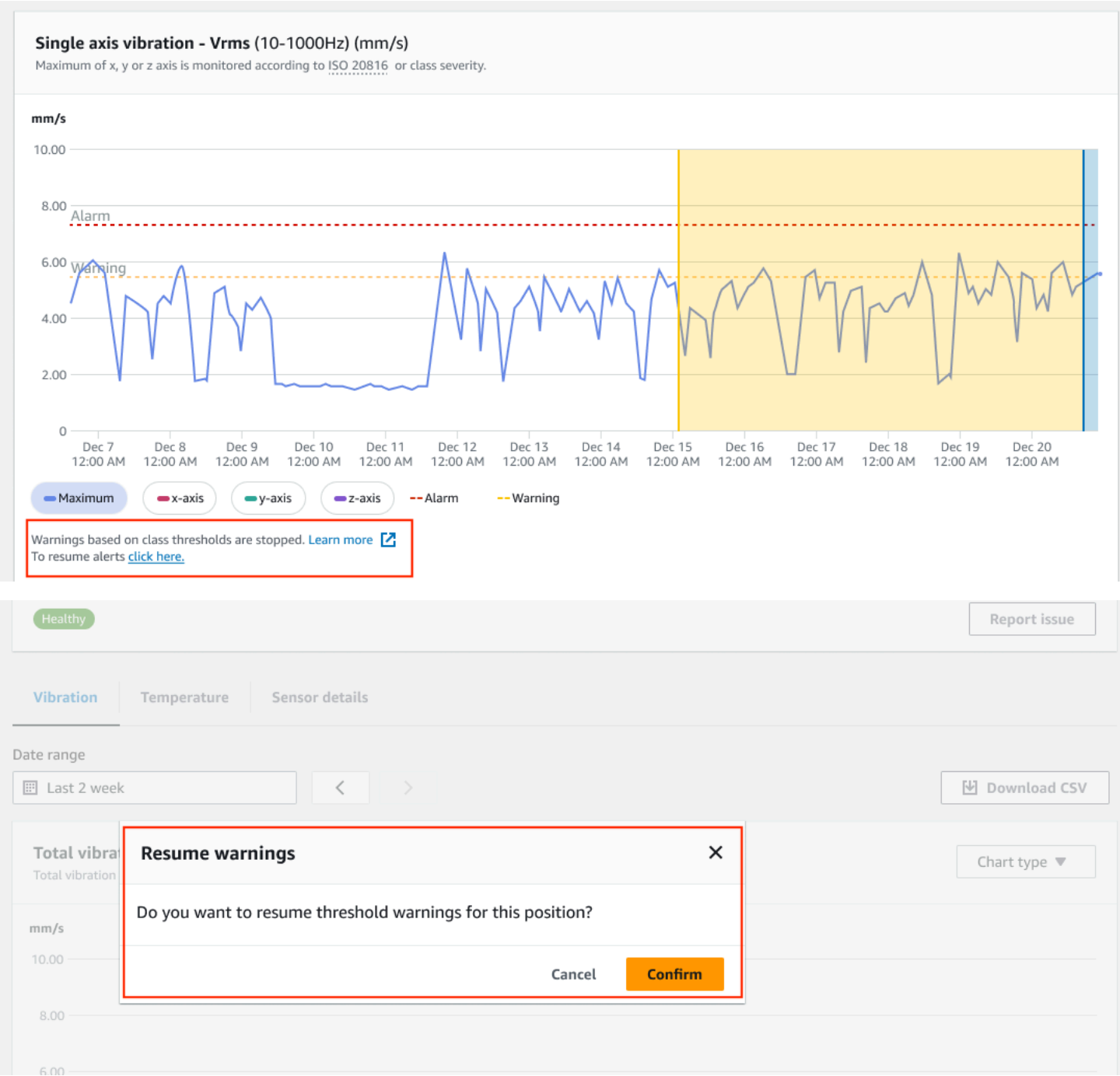
## Resume only warnings

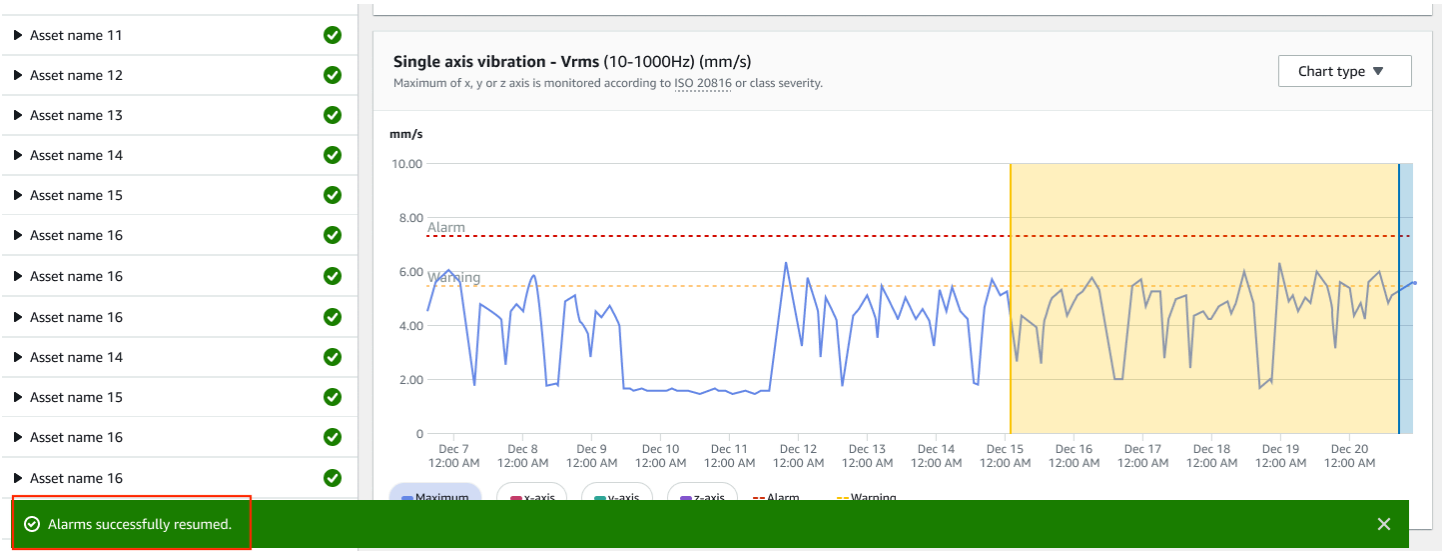
If you've muted warnings, you can choose to resume them.

## Resume warnings on mobile app



## Resume warnings on web app




Asset name 11
Asset name 12
Asset name 13
Asset name 14
Asset name 15
Asset name 16
Asset name 16
Asset name 16
Asset name 14
Asset name 15
Asset name 16
Asset name 16
Single axis vibration - Vrms (10-1000Hz) (mm/s)
Maximum of x, y or z axis is monitored according to ISO 20816 or class severity.
Chart type
mm/s
10.00
8.00
6.00
4.00
2.00
0
Alarm
Warning
Dec 7 12:00 AM
Dec 8 12:00 AM
Dec 9 12:00 AM
Dec 10 12:00 AM
Dec 11 12:00 AM
Dec 12 12:00 AM
Dec 13 12:00 AM
Dec 14 12:00 AM
Dec 15 12:00 AM
Dec 16 12:00 AM
Dec 17 12:00 AM
Dec 18 12:00 AM
Dec 19 12:00 AM
Dec 20 12:00 AM
Maximum
x-axis
y-axis
z-axis
Alarm
Warning
Alarms successfully resumed.

# Projects

A *Project* is 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.

An Amazon Monitron 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 consider your project's needs. Make sure that it contains all the resources required to predict the maintenance needs for all your assets.

Only a project-level admin user or IT manager can create, update, and delete projects and use the Amazon Monitron console for those tasks.

**Topics**


- Creating a project
- Using tags with your project
- Updating a project
- Switching between projects
- Deleting a project
- Additional project tasks


# Creating a project

Although an AWS account can have multiple Amazon Monitron projects, typically you have 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 AWS KMS key, choose **Custom encryption settings (advanced)** under **Data encryption** and do one of the following:

   - If you already have a AWS KMS key that you want to use, under **Choose an AWS 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 AWS KMS key**. This takes you to the AWS KMS console so you can set up a custom key.

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**.

6. Choose **Next** to create the project.

## Using tags with your 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.

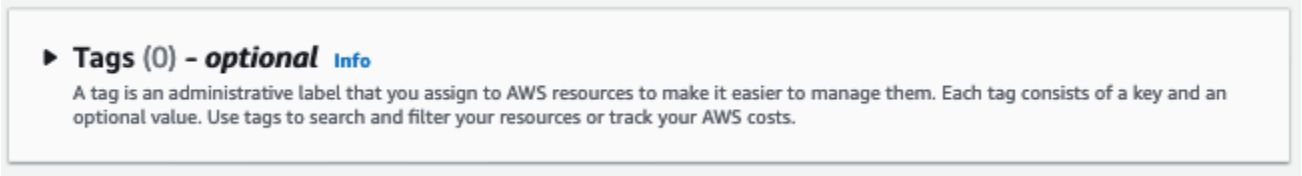
**Topics**


- Adding a tag to a project when you create it
- Adding a tag to a project after it's been created
- Modifying or removing a tag

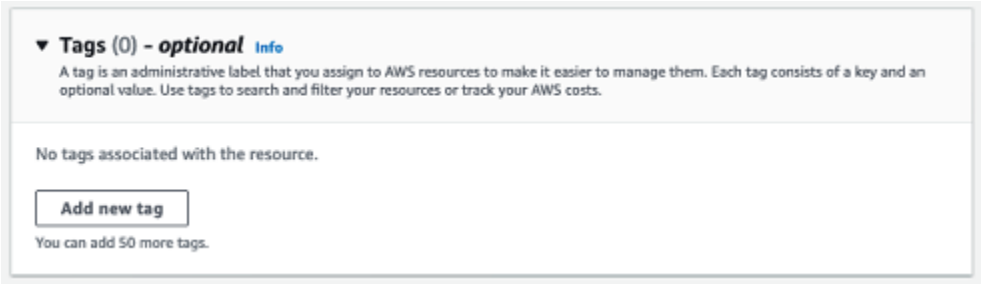

## Adding a tag to a project when you create it

**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.

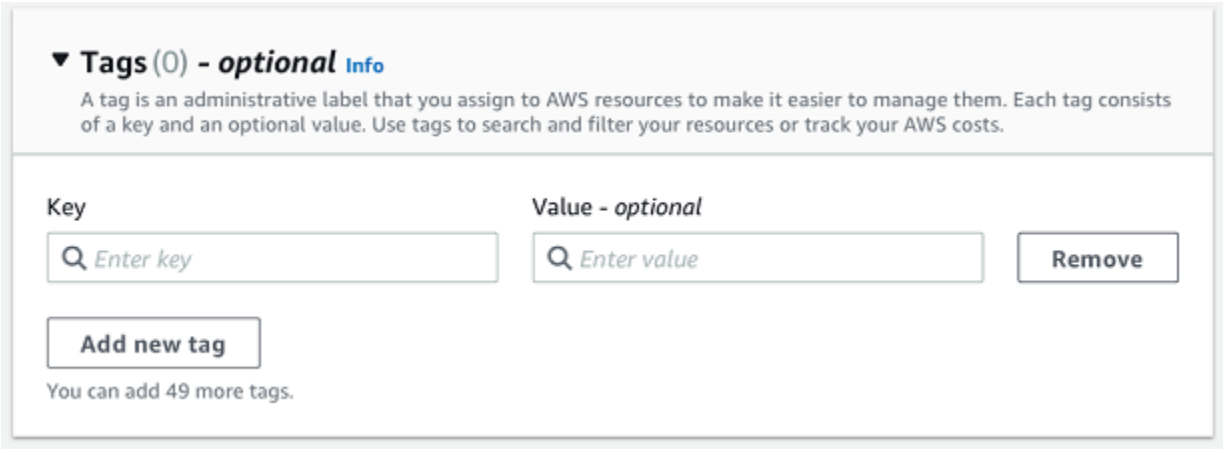



5. Choose **Add new tag**.

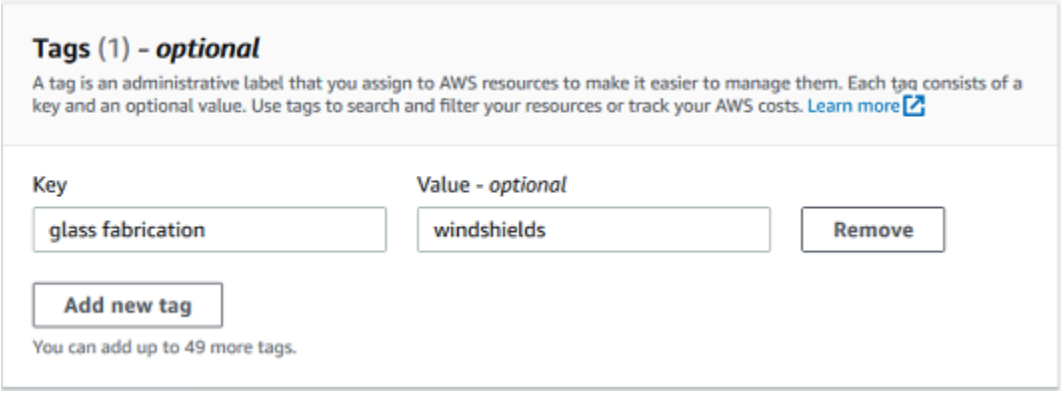



6. Enter the key-value pair for your tag.

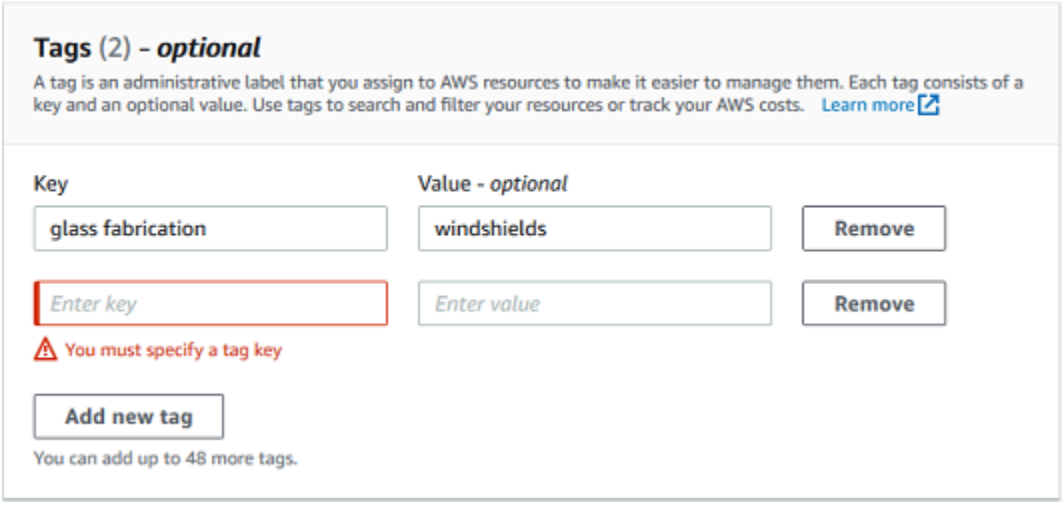
   The key must be unique for the project. The value is optional.




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**.

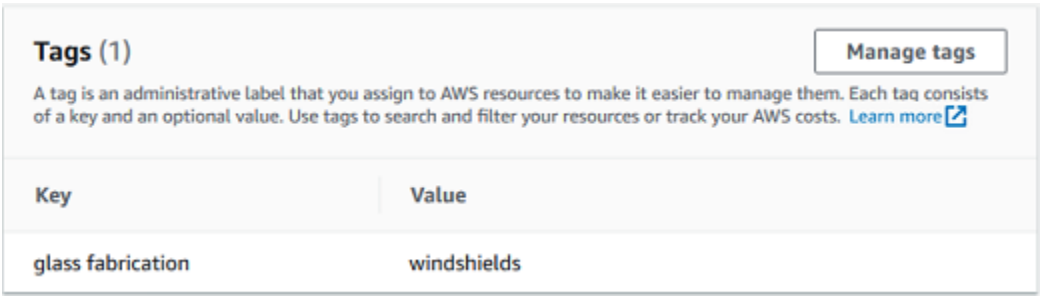



## Adding a tag to a project after it's been created

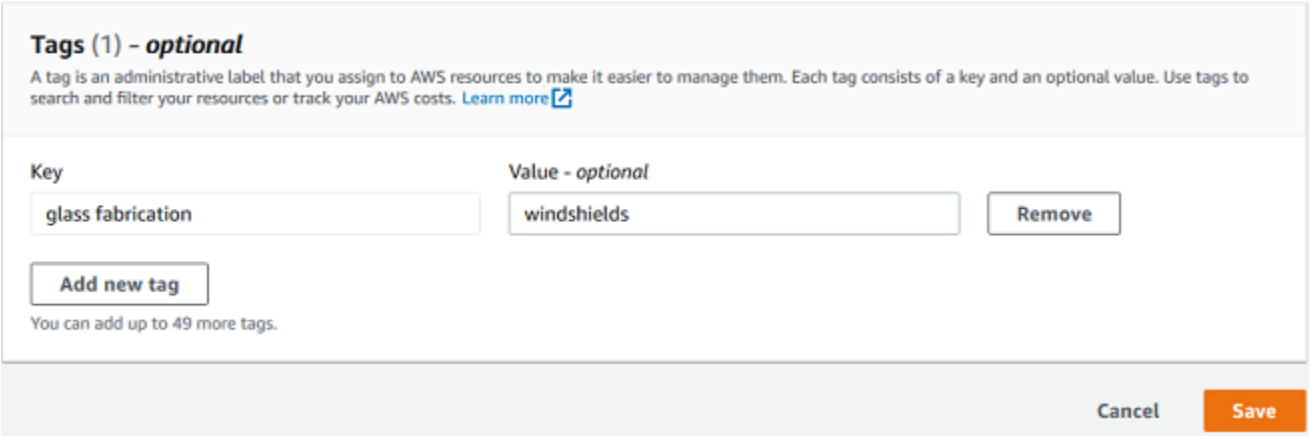
You can add a tag to a project on the project detail page.

### 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**.

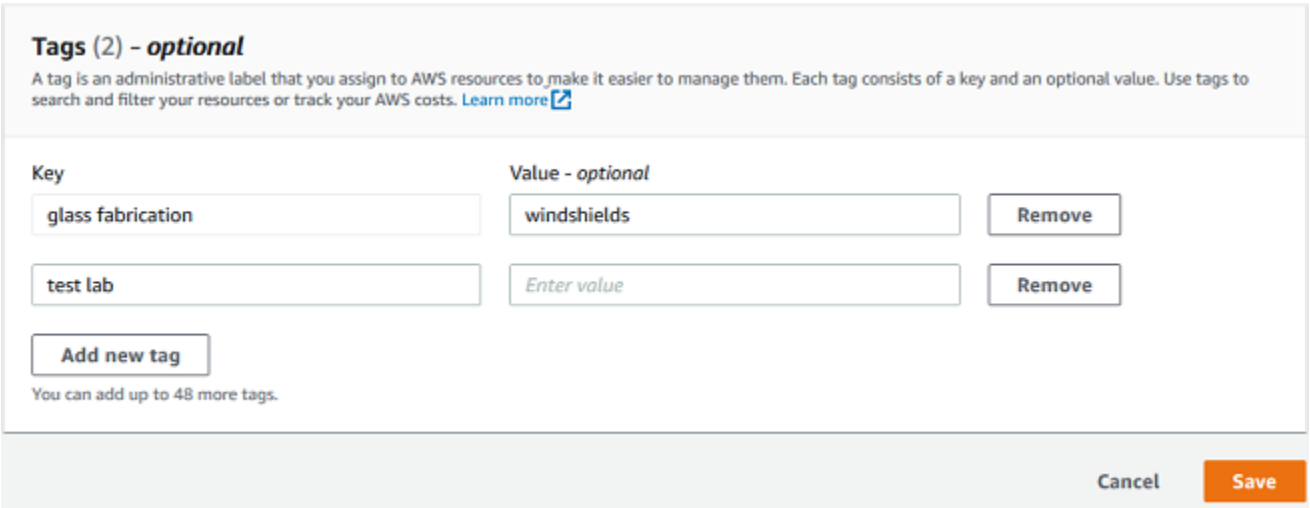



5. Choose **Add new tag**




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

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



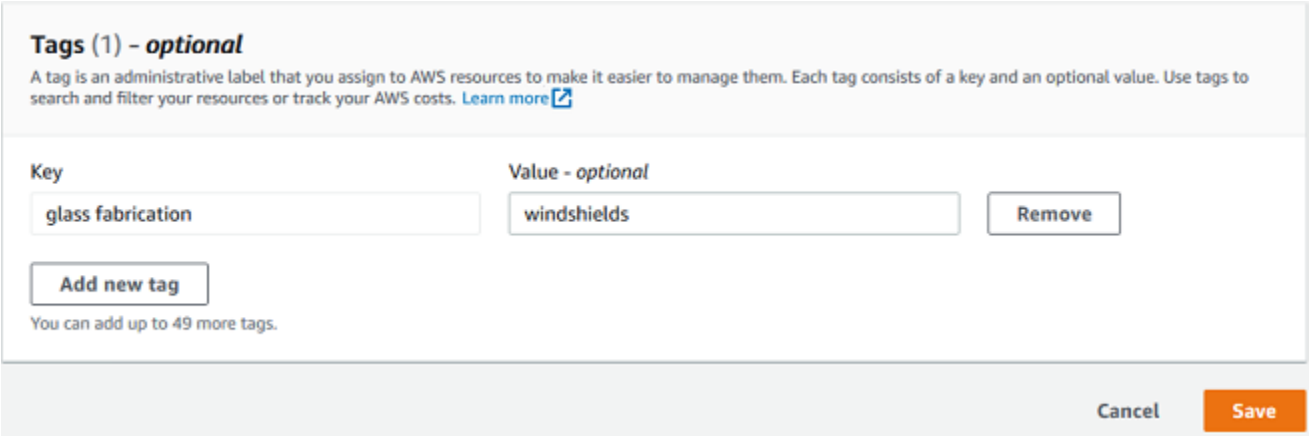

7. Choose **Save**.

## 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**.

# Switching between projects

You can switch between Amazon Monitron projects from both your mobile and web app to manage your resources.

> **Note**
>
> You can only be signed in to a single project at a time. When you switch projects you are automatically logged out from the project you were actively using.

When you log into a project using your account credentials, Amazon Monitron automatically adds your project to the Amazon Monitron projects page to make tracking easier. You can also choose to add projects manually to your projects page using the project URL in your Amazon Monitron invitation email.

When you add a project, it gets saved only on the platform you are adding it on. A project added or saved on the Amazon Monitron web app doesn't automatically get saved on the Amazon Monitron mobile app unless you also add it to the web app.

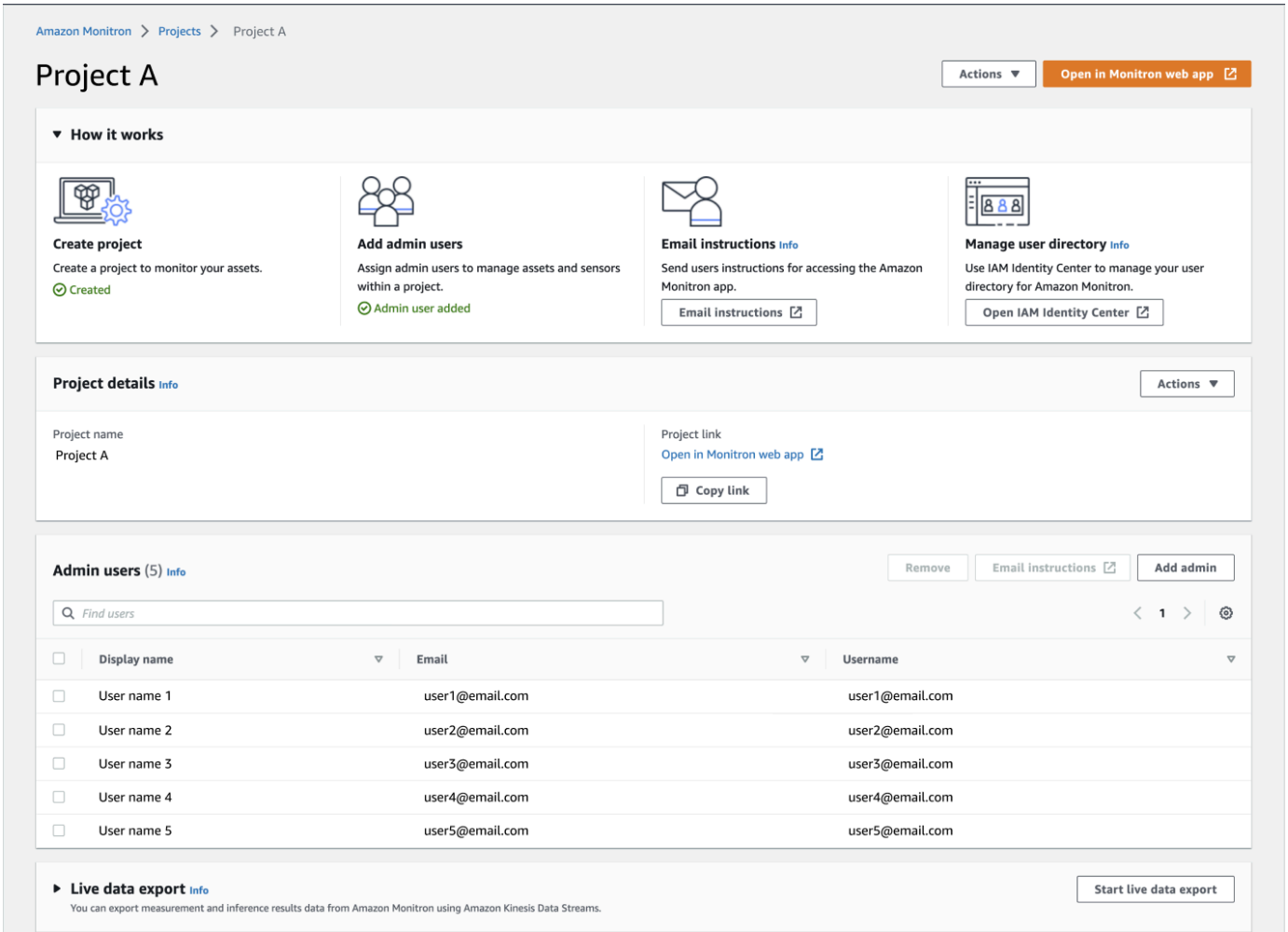
**Topics**


- Switching between projects in the web app
- Switching between projects in the mobile app

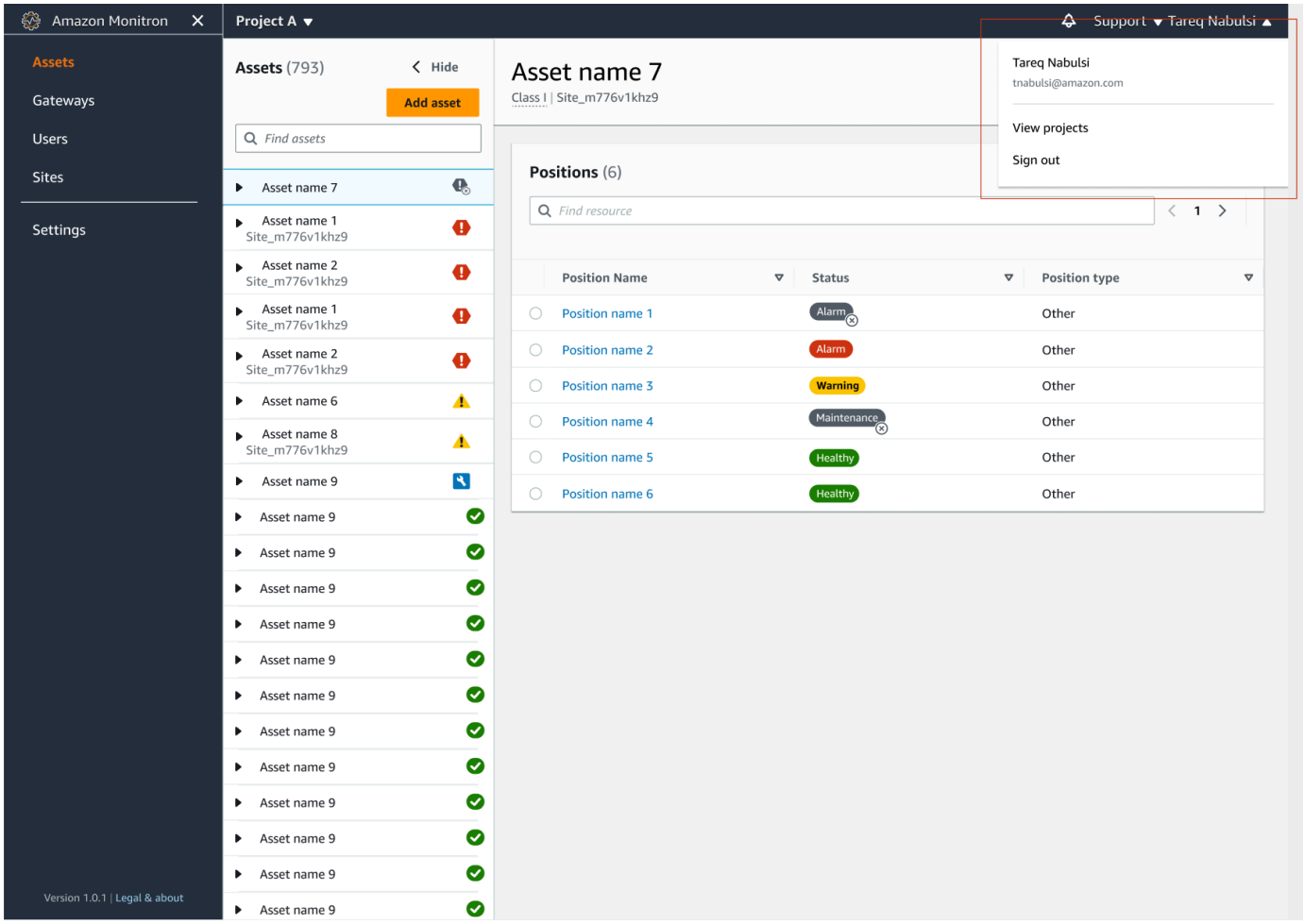

## Switching between projects in the web app

**To switch between projects in the web app**

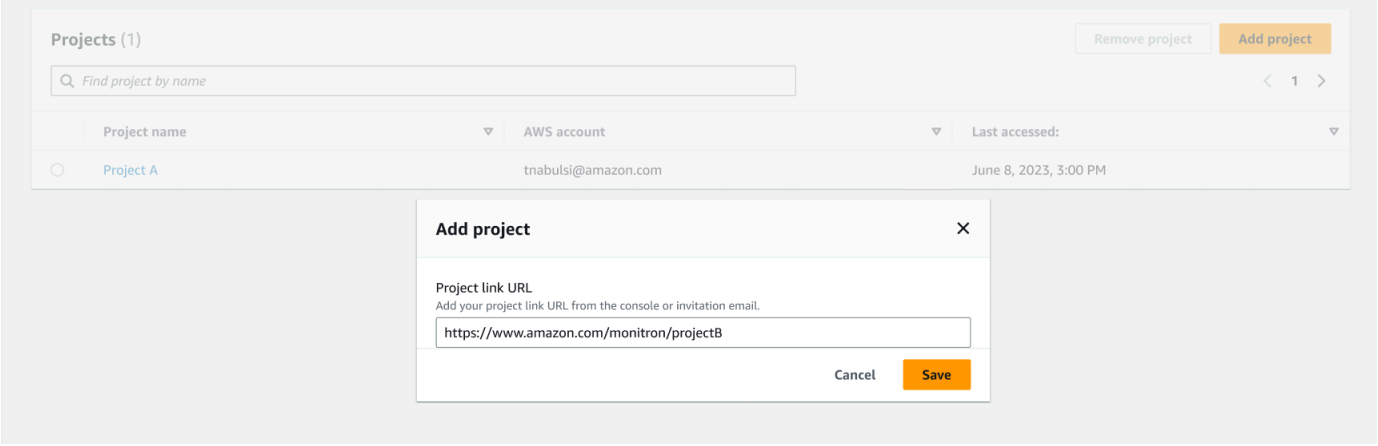
1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron .
2. Choose **Open in Amazon Monitron web app**.



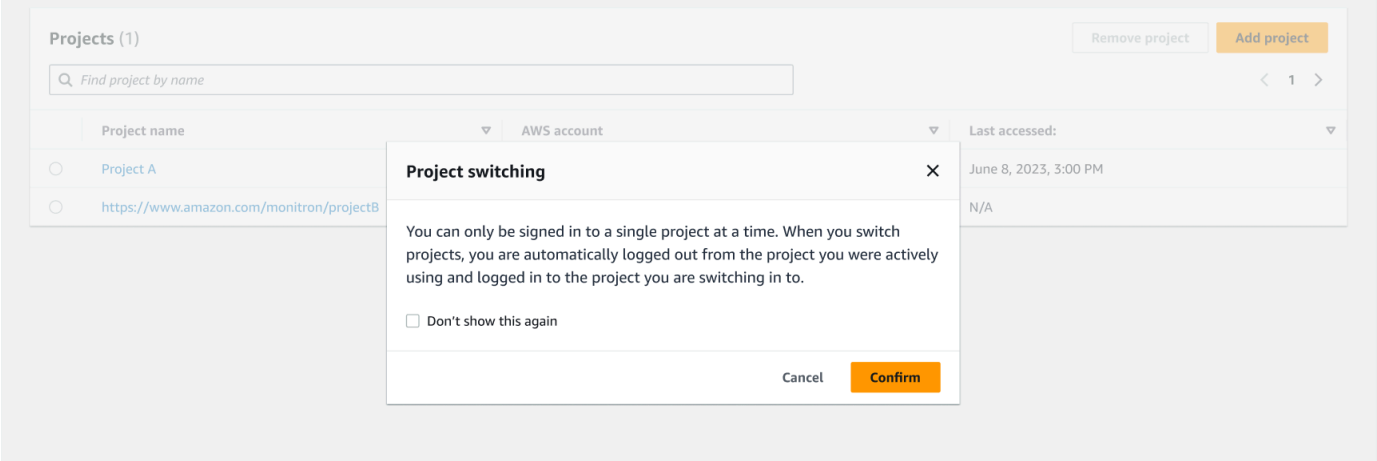

3. Enter your **Username** and **Password** on the **Sign in** screen.
4. From the **Assets** list page, select your account details dropdown menu, and then choose **View projects**.




5. If you want to add a project, choose **Add project** and enter your project link url.



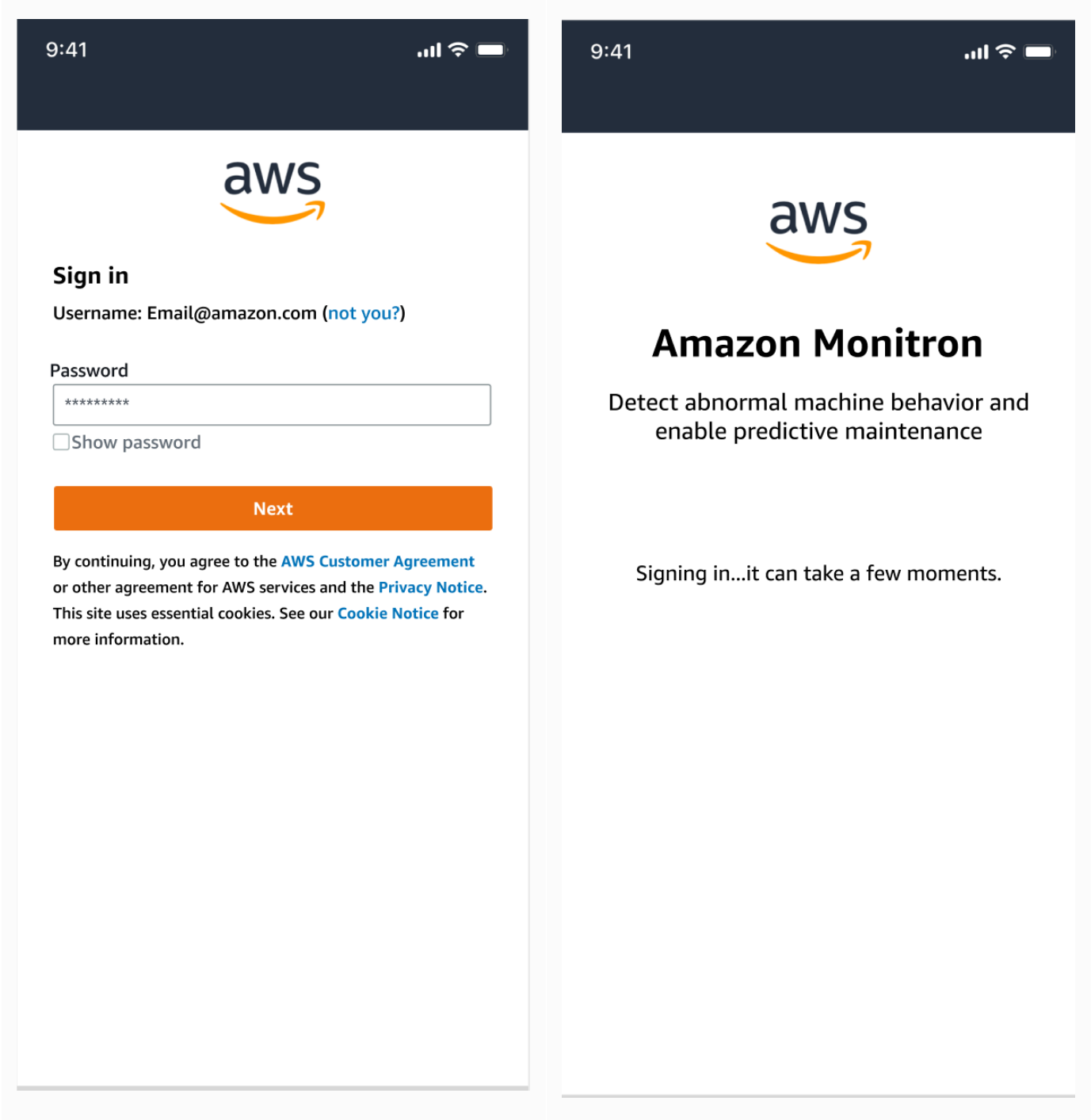

6. If you want to switch between projects, choose the project you want to view from the projects list. You will see this message before you switch.



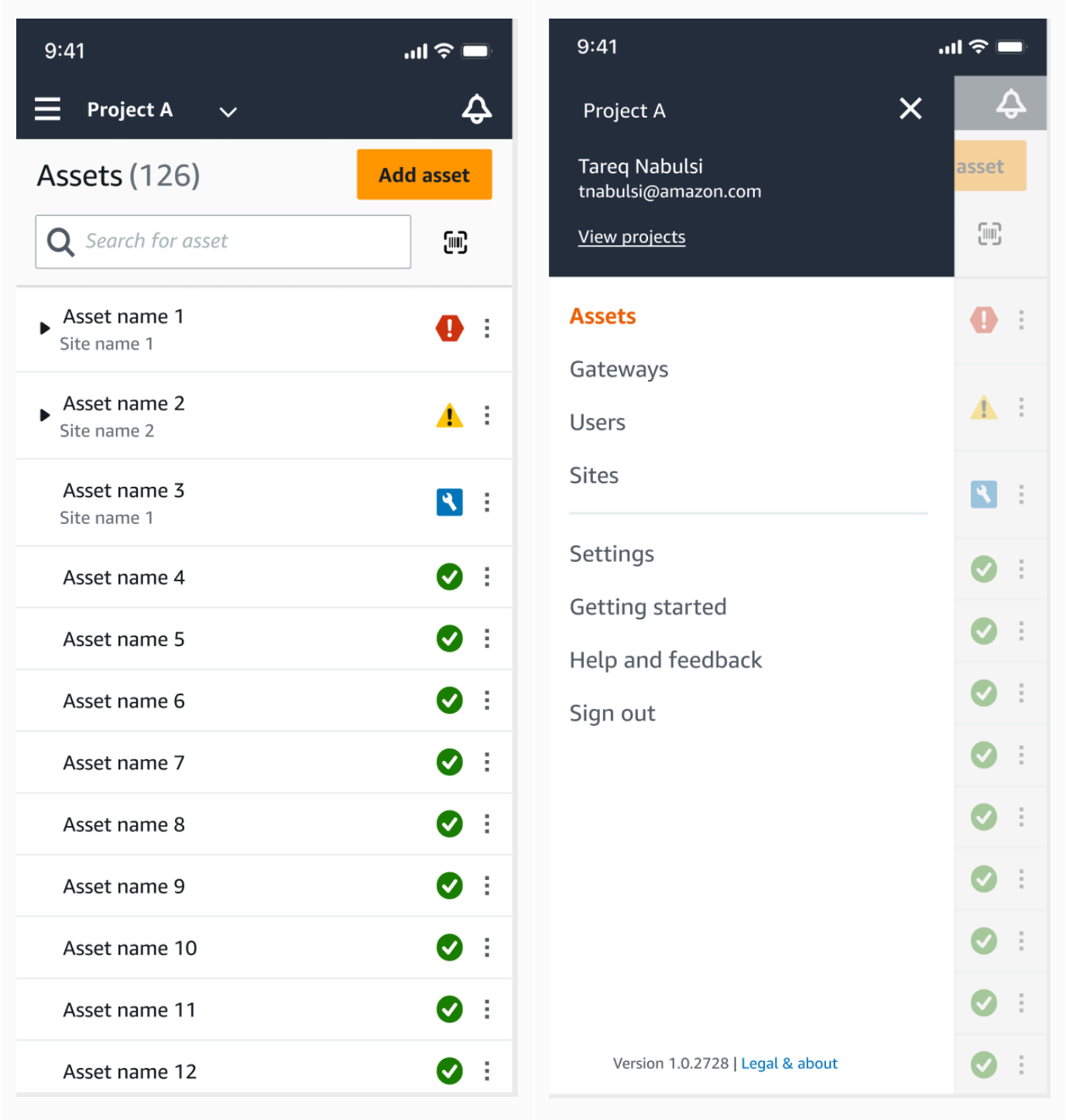

# Switching between projects in the mobile app

### To switch between projects in the mobile app

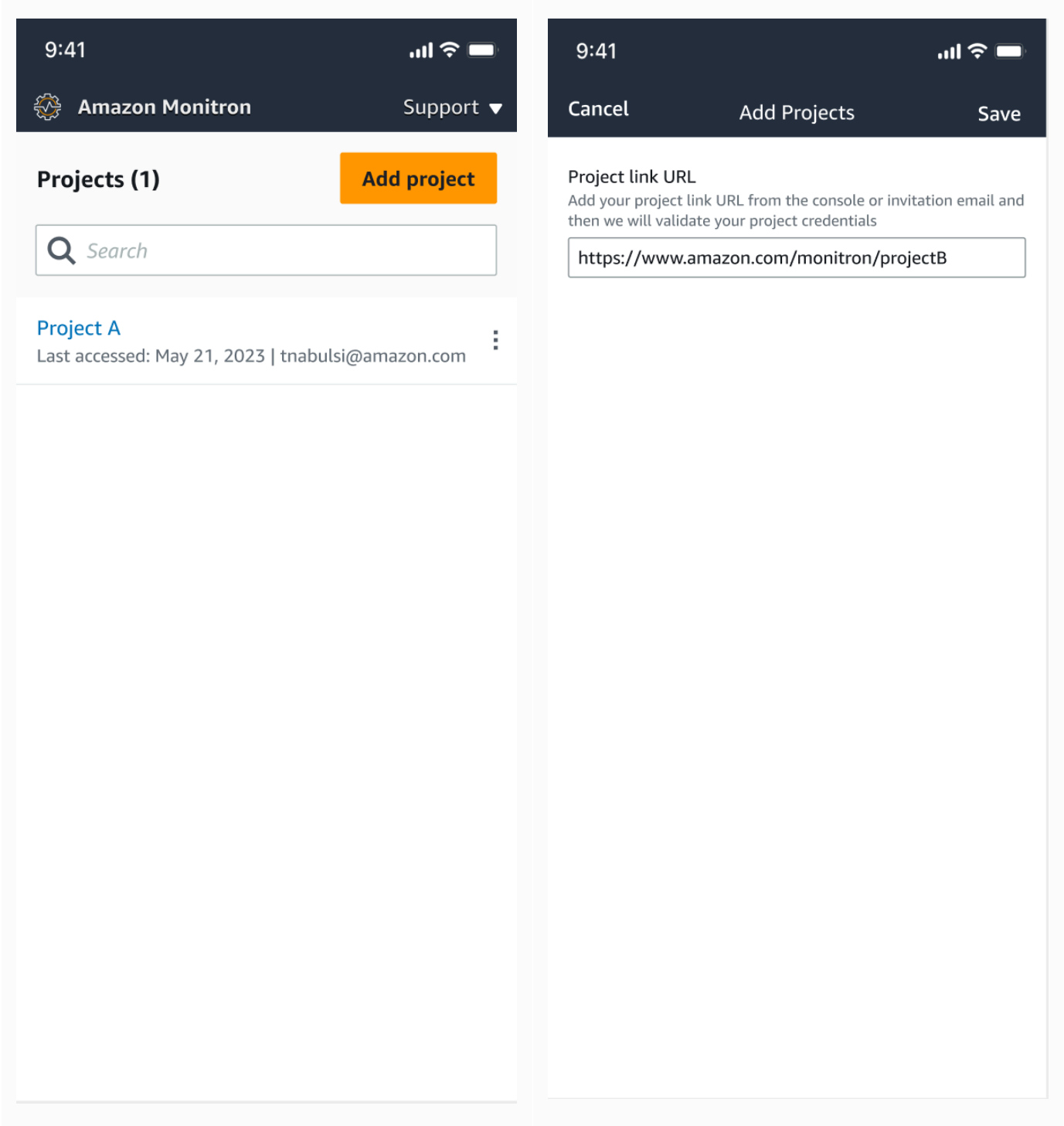
1. Open the Amazon Monitron mobile app and login using your username and password.



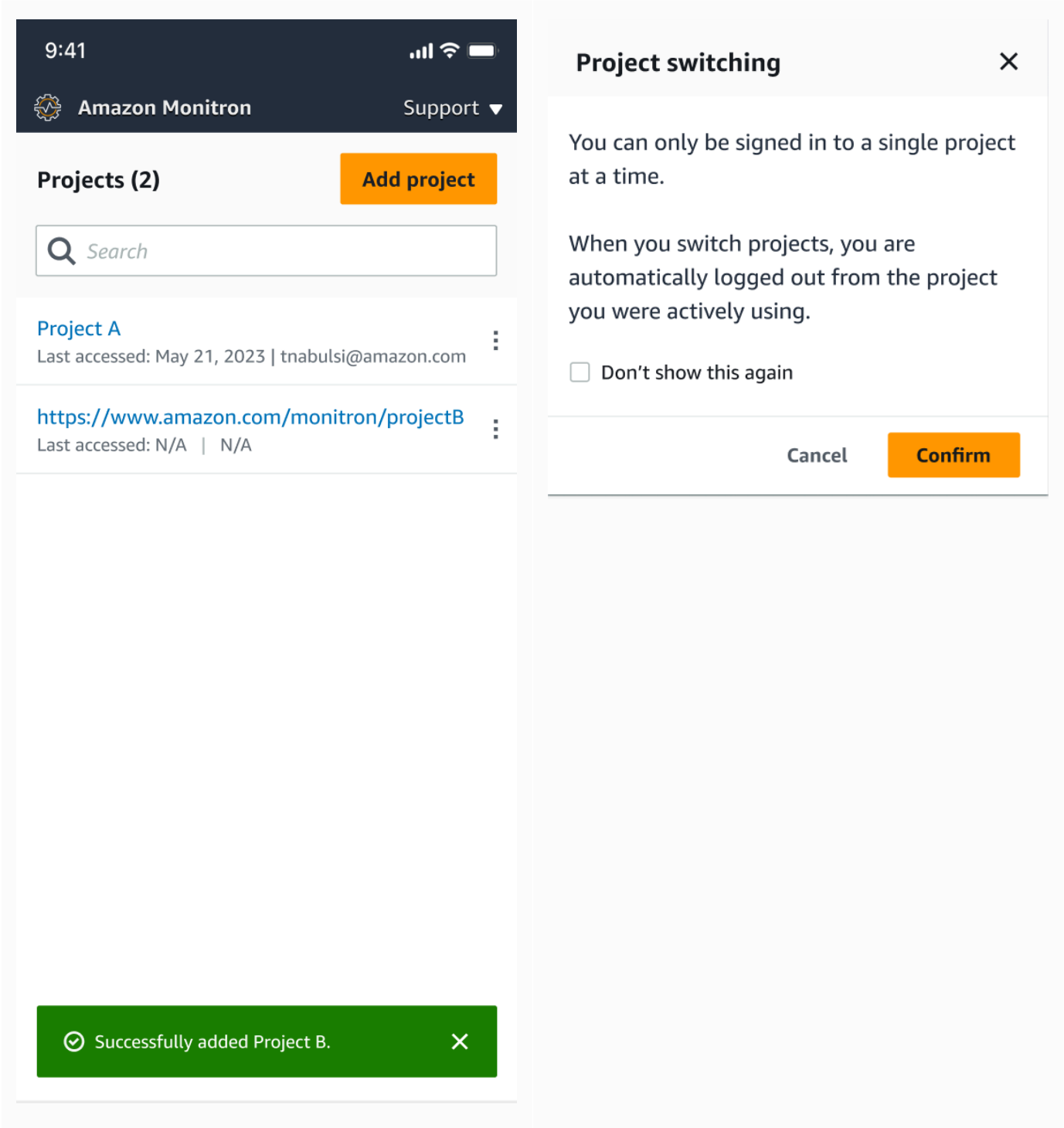

2. From the **Assets** list page, select your account details dropdown menu, and then choose **View projects**.




3. If you want to add a project, choose **Add project** and enter your project link url.




4. If you want to switch between projects, choose the project you want to view from the projects list. You will see this message before you switch.




# Deleting a project

With the `deleteProject` operation, you must have the AWS IAM Identity Center 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 IAM Identity Center and you may end up with dangling references on IAM Identity Center.

**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, sensors or gateways, 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.

# Sites

After setting up a project, you can organize it into sites to make it easier to manage. A *site* is a collection of assets, gateways, and sensors that share a purpose. Organizing a project into sites is helpful if your project has a large pool of assets, gateways, and sensors. You can use sites to control access and permissions to specific parts of that pool.

You can create up to 50 sites within a project, and add up to 100 assets and 200 gateways to each site.

**Topics**


- Organizing a project into sites
- Controlling access to projects and sites
- Creating a site
- Changing a site name
- Deleting a site
- Navigating between projects and sites in the mobile app


## Organizing a project into sites

You can organize a project into sites based on your business needs. For example, you can organize a project in one of the following ways:

- **No sites at all**. Everything is contained in a project, without any sites. This option is best for projects with a few assets and users that you can easily keep track of because it provides the greatest simplicity.
- **Sites based on geography**. Group resources and users by locale, such as by city, building, or areas within a building. For example, you might set up a site for the equipment in a factory test lab.
- **Sites based on function**. Group resources and users by functionality, either by machine functionality or by how they're used in your factory. For example, you might set up a site for all of the conveyor belts involved in moving an item from one side of the factory to the other.
- **Sites based on organization**. Sites represent a specific organizational structure in the company or factory. For example, you might want a single site that includes resources and users assigned to the shipping department.

# Controlling access to projects and sites

To give a user access to all of the resources in a project, including those in all of the project's sites, you add the user to the project. To give a user access to only the resources in a site, add the user to the site. Similarly, to make an asset or sensor available to all of the users who have access to an entire project, add it to the project. To make an asset or sensor available only to a specific site, add it to only that site. Gateways are always accessible to anyone or any sensor in the project.

For example: Olga is an admin user associated with the entire project. As a project-level admin user, she can manage users and resources anywhere within the project, including those within sites A, B, and C. Sam is an admin user associated with Site B. As a site-level admin user, he can manage users and resources within Site B but can't see or manage those within sites A and C. Sensors at Site B can use any gateway within the project.

Similarly, if Ed is a project-level technician, he can monitor any sensor in the project. However, Tom, who is a site-level technician for Site C, can see and monitor only sensors at that site.

# Creating a site

To add a site to a project, you must be a project-level admin user. You can create up to 50 sites within a project, and add up to 100 assets and 200 gateways to each site. You can make up to 20 users into admin users or technicians for a site.

**Topics**


- To add a site using the mobile app
- To add a new site using the web app


## To add a site using the mobile app

1. Log into the Amazon Monitron mobile app on your smartphone.

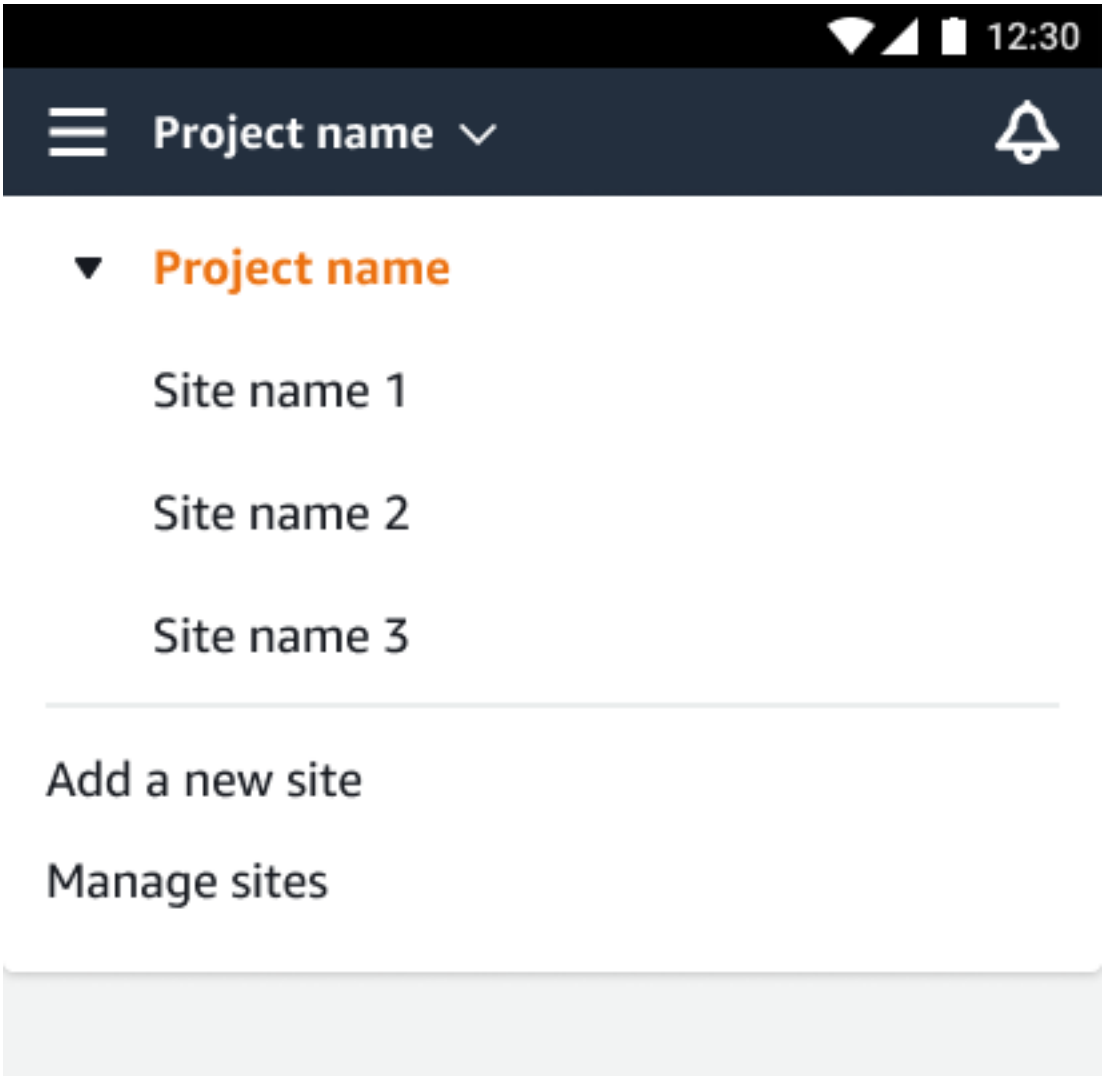
   Make sure that the project name is shown in the upper left of the screen. It is visible on all screens in the mobile app.
2. Choose the menu icon (☰).
3. Choose **Sites**.
4. Choose **Add site**.

5. For **Site name**, enter a name.
6. Choose **Add**.

   The **Sites** list displays the new site.

## To add a new site using the web app

1. Open the project selector dropdown menu from the upper left part of the app window.
2. Choose **Add a new site**




The project-level admin user who creates a site is automatically a site-level admin user for that site. To learn more about adding users, see Adding a user.

# Changing a site name

You can change only a site's name. When you change the name, nothing else (such as historical data or user permissions) changes.

**Topics**


- To change a site name using the mobile app
- To change a site name using the web app


## To change a site name using the mobile app

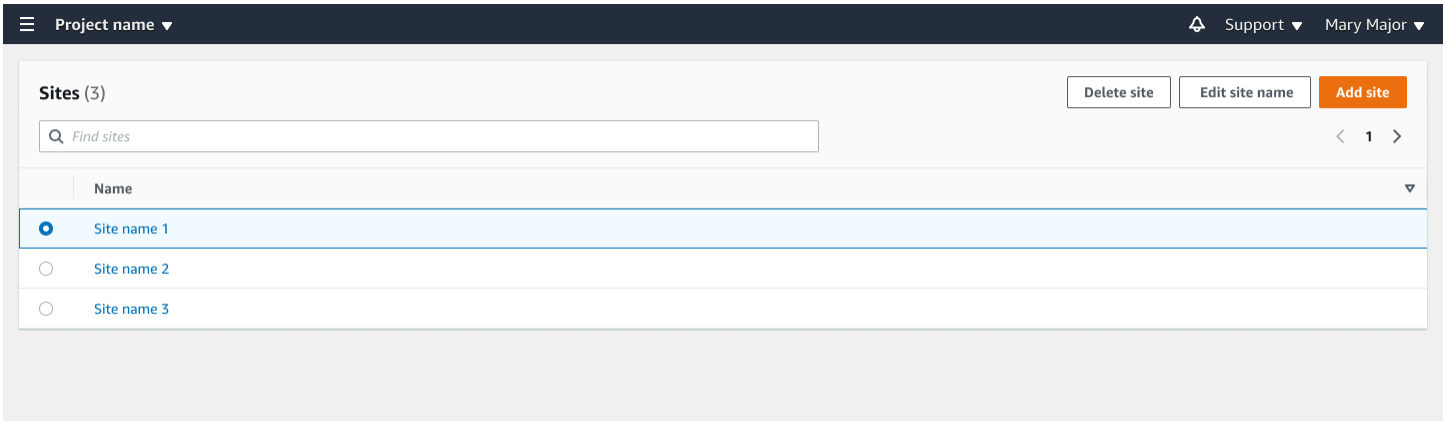
1. Log into the Amazon Monitron mobile app on your smartphone.

   Make sure that the project name is shown in the upper left of the screen.
2. Choose the menu icon (☰).
3. Choose **Sites**.
4. Next to the site that you want to rename, choose **Actions**.
5. Choose **Edit site name**.
6. Change the site name.

   The new name is displayed in the **Sites** list.

## To change a site name using the web app

1. Choose **Sites** from the left pane.
2. Select the site that you want to rename.
3. Choose the **Edit site name** button.




# Deleting a site

Before you can delete a site, you must delete all of the site's assets. The **Sites** list displays all of the devices and users associated with a site.

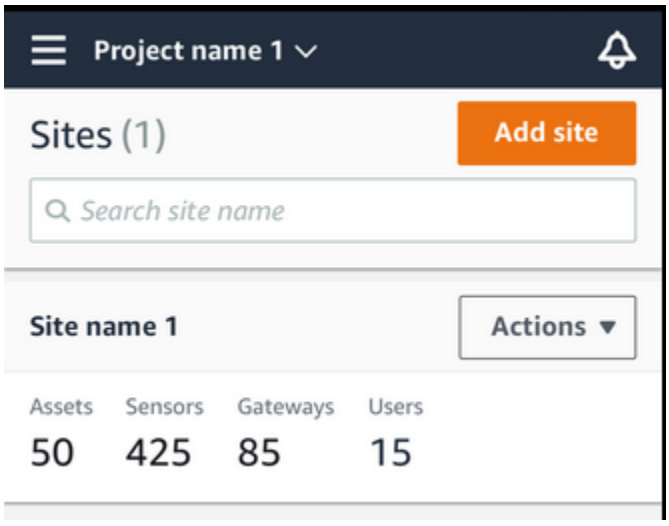
### Topics


- To delete a site using the mobile app
- To delete a site using the web app


## To delete a site using the mobile app

1. Log into the Amazon Monitron mobile app using your smartphone.

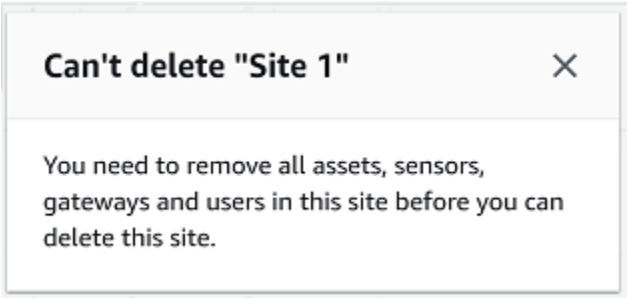
   Make sure that the project name is shown in the upper left of the screen.




2. Choose the menu icon (☰).

3. Choose **Sites**.
4. Next to the site that you want to delete, choose **Actions**.
5. Choose **Delete site**.
6. If assets, sensors, gateways, or users are associated with the site, choose **X**. Then delete those resources before proceeding.

   If there are no resources associated with the site, skip to the next step.

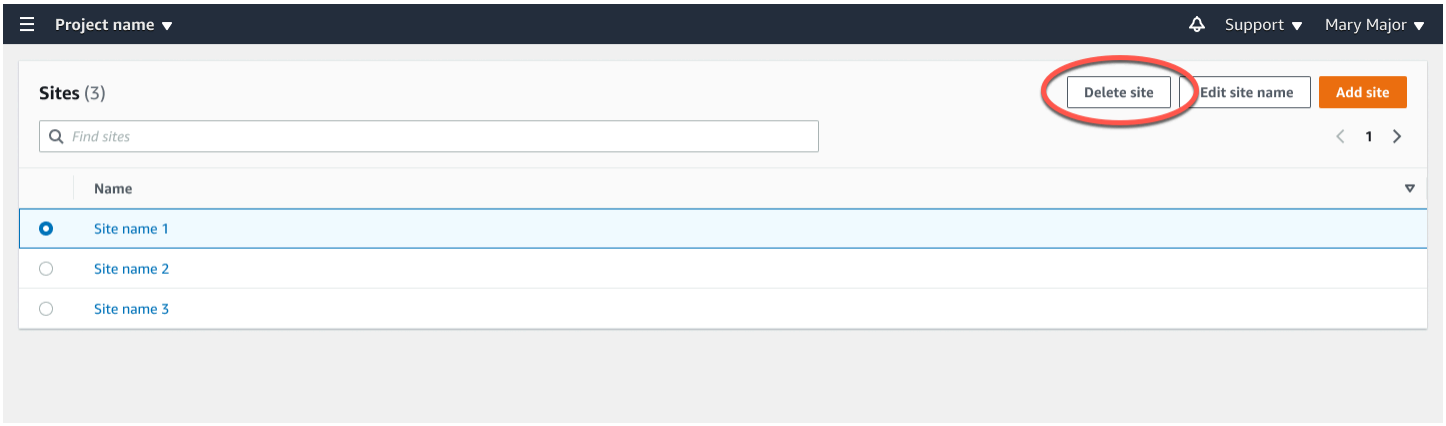



7. Choose **Delete**.

   The site is no longer listed in the **Sites** list.

## To delete a site using the web app

1. Choose **Sites** from the left pane.
2. Select the site that you want to delete.
3. Choose **Delete site**.



# Navigating between projects and sites in the mobile app

Project-level admin users and project-level technicians can access and manage either project-level or site-level resources. Project-level admin users can add resources and users at either the project or site level.

Site admins and site-level technicians have access only to their site.

To tell whether you're at the project level or in a specific site, note the name at the top of the app screen.




or




Project-level admin users and technicians can switch between the project level and the site level or between individual sites.

**Topics**

- Switching from project level to site level
- Switching from site level to project level

## Switching from project level to site level

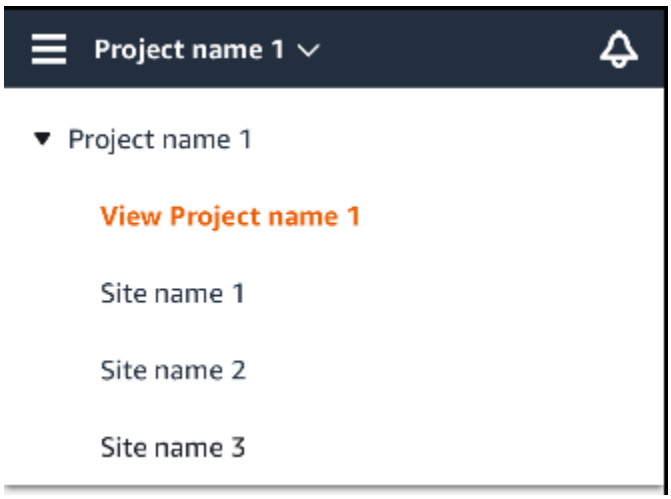
**To change from project level to site level**

1. Log into the Amazon Monitron mobile app on your smartphone.

   Navigate to the project you want.

2. Choose the project name.




3. Choose the site that you want to view.

## Switching from site level to project level

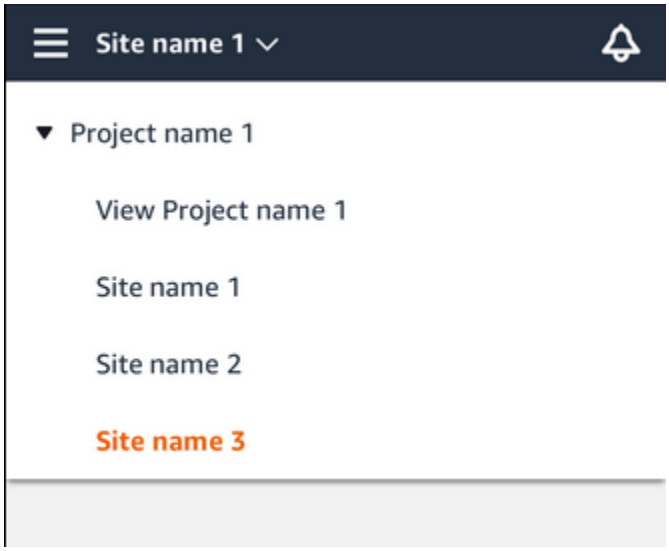
### To change from site level to project level

1. Log into the Amazon Monitron mobile app on your smartphone.

   The site name indicates that you are at the site level in the mobile app.




2. Choose the site name.




3. Choose the project name.

To change to a different site, choose the site name.

# Gateways

Amazon Monitron uses gateways to transfer the data collected by the Amazon Monitron Sensors to the AWS Cloud. Gateways are positioned in factories within 20 to 30 meters of the sensors. They communicate with the sensors over Bluetooth Low Energy (BLE), and with the AWS Cloud using either Wi-Fi or Ethernet.

This topic explains how to install your Ethernet and Wi-Fi gateways. It also explains how to delete an unnecessary gateways.

> **Note**
>
> Once you've added a gateway to your project, you can edit the gateway's name to help you find it fast.

**Topics**


- Ethernet gateways
- Wi-Fi gateways


# Ethernet gateways

The Amazon Monitron Ethernet Gateway comes equipped with an RJ-45 socket, so you can connect it to your Ethernet network using a Cat 5e or Cat 6 Ethernet cable. You power your gateway over the Ethernet cable, using Power over Ethernet (POE). Therefore, you need either a router that supports POE or a POE power injector.




After you have inserted an Ethernet cable into your gateway, put the gateway in commissioning mode by pressing the **Config** button.

To learn about using Amazon Monitron with Wi-Fi gateways, see Wi-Fi gateways.

**Topics**

- Reading the LED lights on an Ethernet gateway
- Placing and installing an Ethernet gateway

- Commissioning an Ethernet gateway
- Troubleshooting Ethernet gateway detection
- Troubleshooting Bluetooth pairing
- Resetting the Ethernet gateway to factory settings
- Viewing the list of gateways
- Viewing Ethernet gateway details
- Editing Ethernet gateway name
- Deleting an Ethernet gateway
- Retrieving MAC address details

## Reading the LED lights on an Ethernet gateway

The LED lights on the top of your Amazon Monitron Ethernet Gateway indicate the status of the gateway. Each gateway has one orange light, one blue light, and one green light. The green light indicates that the power is on. The orange light indicates that the gateway is connected to the Ethernet. The blue light indicates that the gateway's Bluetooth is connected to the sensors.

The sequence that the lights display indicates the status of the gateway, as described in the following table.

| | LED sequence | Description |
|---|---|---|
| 1 | Solid green light | The Ethernet gateway is powered on. |
| 2 | Solid orange light | The gateway is connected to the Ethernet network and the Amazon Monitron backend system. |
| 3 | Flashing orange light (slow) | The gateway is attempting to connect to the Ethernet network. |
| 4 | Flashing orange light (1 fast/ 1 slow) | The gateway is connected to the Ethernet network and is |

| | LED sequence | Description |
|---|---|---|
| | | attempting to connect to the Amazon Monitron backend system. |
| 5 | Solid blue light | At least one sensor is communicating with the gateway. |
| 6 | No blue light | No sensors are currently communicating with the gateway. |
| 7 | Orange and blue lights flashing (slowly) | The gateway is powered on, unconfigured (not commissio ned), and not in commissio ning mode (that is, not discoverable or configurable by the mobile app). |
| 8 | Orange and blue lights flashing (rapidly) | The gateway is on and in commissioning mode, but not yet linked to any sensors. In commissioning mode, the gateway is discoverable and configurable by Amazon Amazon Monitron, but no sensors can connect yet. |
| 9 | No lights | The gateway isn't connected to a power source or a firmware update is in progress. |
| 10 | Solid orange and blue lights | The gateway is starting up. |

# Placing and installing an Ethernet gateway

Unlike sensors, an Ethernet gateway doesn't need to be attached to the machines that are being monitored. However, it does need an available Ethernet network through which Amazon Monitron can connect to the AWS Cloud.




## Topics

- Where to place a gateway
- Installing an Ethernet gateway
- Turning on the gateway


## Where to place a gateway

You can install a gateway anywhere within your work area, depending on its layout. Typically, gateways are mounted on walls, but you can mount them on ceilings, pillars, or in any other location. A gateway must be within 20 to 30 meters of the sensors it will support, and an Ethernet gateway must be close enough to an Ethernet cable to plug in. Note that an Ethernet gateway draws power from the Ethernet cable.

Consider these other factors when mounting a gateway:

- Mounting the gateway higher than sensors (2 meters or above) can improve coverage.
- Keeping an open line of sight between the gateway and sensors improves coverage.
- Avoid mounting the gateway on building structures, such as exposed steel beams. They can cause interference with the signal.
- Try to work around any equipment that might produce electronic interference with the signal.
- If possible, install more than one gateway within transmission distance of your sensors. If a gateway becomes unavailable, the sensors will switch their data transmission to another gateway. Having multiple gateways helps to eliminate data loss. There is no minimum required distance between two gateways.

## Installing an Ethernet gateway

Almost everything you need to install your gateway in your work area is contained in the box that contains the gateway:

- The gateway
- A wall mounting bracket
- Double-sided tape
- Four mounting screws

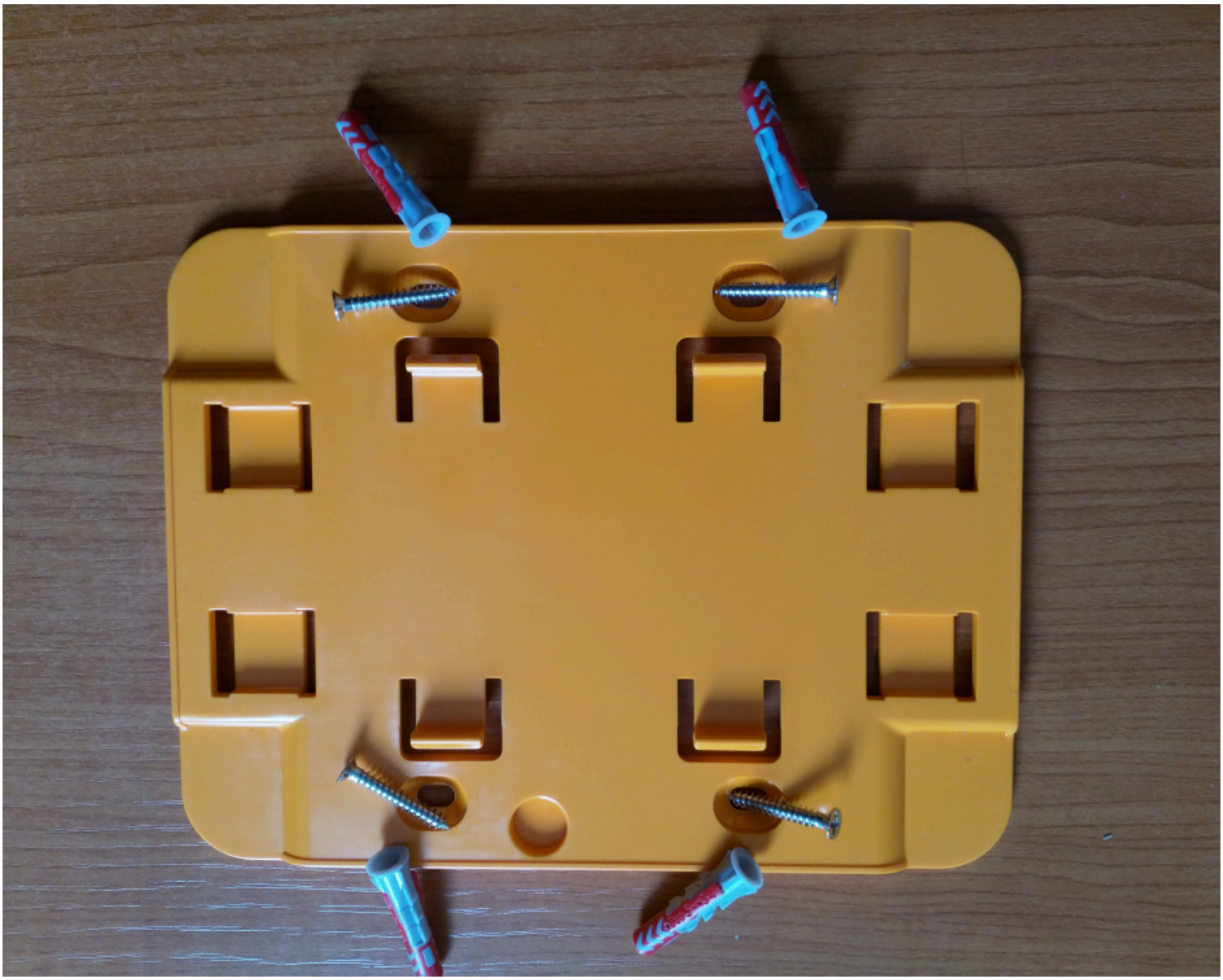
To install the gateway, position the wall mounting bracket on the wall or on another location, then mount the gateway on the bracket, Ethernet cable on the downwards side.

There are three ways to mount the mounting bracket: screw mounting, tape mounting, and plastic-tie mounting. The method you use depends on whether you're mounting the gateway on a wall or another location, and on the surface material.

To mount the bracket, choose one of the following.

**Screw mounting**

Typically, you mount the bracket directly to the wall using the mounting screws included in the gateway box. Mount the bracket from the front. You might need to use an expansion plug or toggle bolt (not included) to secure the screw in the wall.



### Tape mounting

A shaped piece of double-sided tape is included in the gateway box. Use it when you can't place a screw into the mounting surface. You can also use it in combination with the other methods of mounting for a more secure installation.



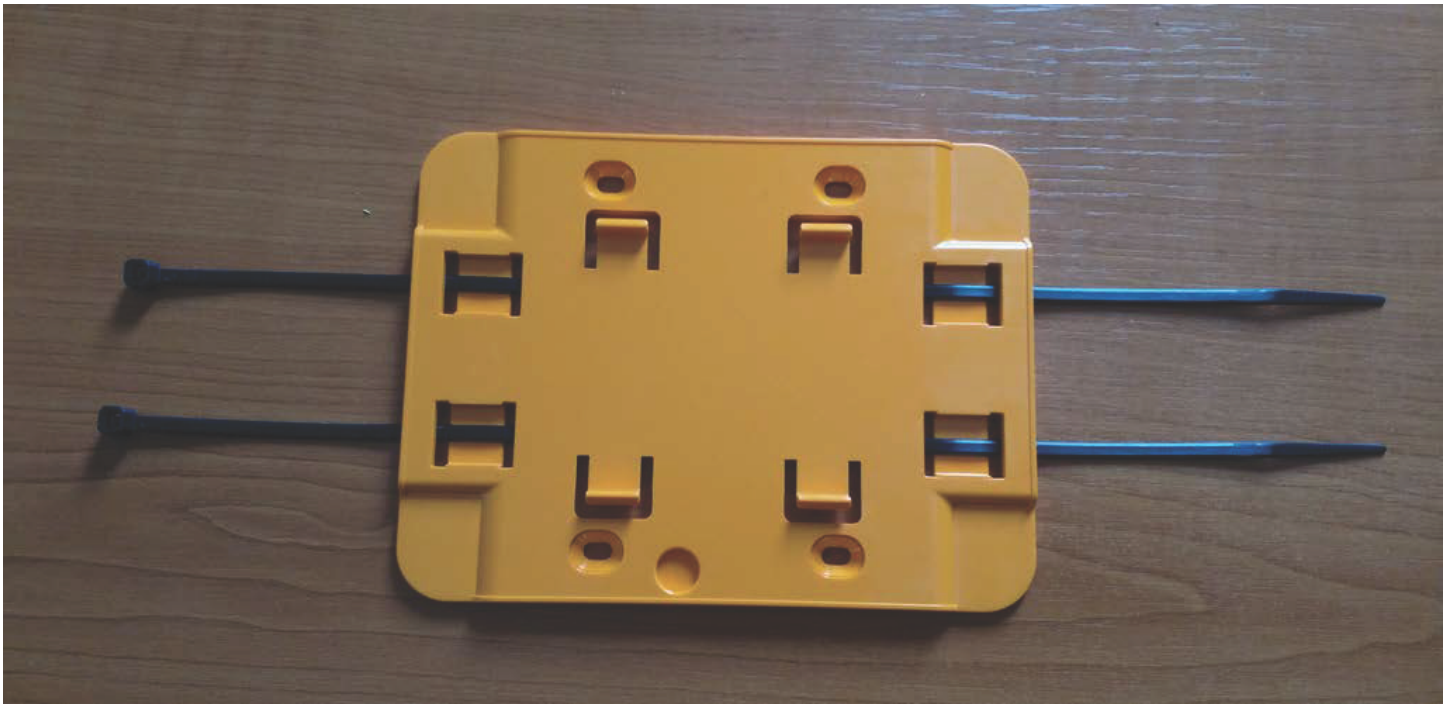

Remove the backing on one side of the tape and apply the tape to the back of the wall mounting bracket between the four raised sections.




Remove the remaining backing and apply the bracket to the mounting location. Press hard on the bracket to make sure that the tape firmly adheres to the surface.

**Plastic-tie mounting**

To mount a gateway to a smaller non-wall location, such as a pillar or fence, use cable ties (also known as zip ties) to fasten the wall mounting bracket. Put the ties through the holes in the four raised sections on the back of the bracket, wrap them around the mounting location, and pull tight.



After the bracket is mounted, attach the gateway to the bracket.

### Turning on the gateway

1. With the wall mounting bracket in place, place the gateway against the bracket, with the two plastic hooks on the back of the gateway inserted in the slots at the bottom of the bracket.
2. Press the top of the gateway against the bracket so that the plastic hooks on the back of the gateway latch into the top of the bracket.

> **Note**
>
> Install the gateway with the Ethernet cable going downwards.

If you have a problem with connecting to your gateway, see Troubleshooting Ethernet gateway detection.

## Commissioning an Ethernet gateway

When your gateway is mounted in your factory, you will need access to the Amazon Monitron mobile app to commission it. Amazon Monitron supports only smartphones using Android 8.0+ or iOS 14+ with near field communication (NFC) and Bluetooth.

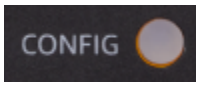
**Topics**


- To commission a gateway


## To commission a gateway

1. If Bluetooth isn't already turned on for your smartphone, turn it on.
2. Position your gateway in the location that works best for communicating with your sensors.

   The best place to mount your gateway is higher than the sensors and no more than 20 to 30 meters away. For additional help with locating your gateway, see Placing and installing an Ethernet gateway.
3. Plug in the gateway and make sure the network light (yellow) and the Bluetooth light (blue) on the front of your gateway are blinking alternately.
4. Push the **Config** button on the gateway to put it into commissioning mode. The Bluetooth and network LED lights will start flashing rapidly.

   
   
5. Open the mobile app on your smartphone.
6. On the **Getting started** page or the **Gateways** page, choose **Add gateway**.

   Amazon Monitron scans for the gateway. This can take a few moments. When Amazon Monitron finds the gateway, it displays it in the gateway list.
7. Choose the gateway.

   > **Note**
   >
   > If you are using an iOS mobile device, and you have previously paired with this particular gateway, then you may need to make your device "forget" the gateway before re-pairing. For more information, see Troubleshooting Bluetooth pairing.

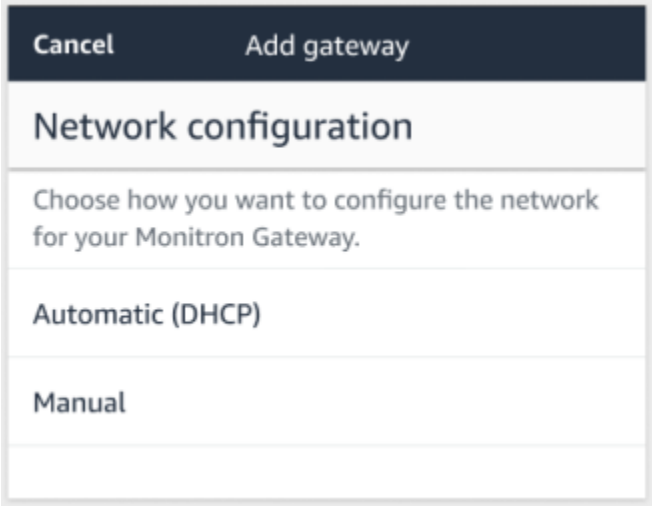
   It can take a few moments for Amazon Monitron to connect to the new gateway.




If the mobile app continues to try to connect to the gateway without success, see Troubleshooting Ethernet gateway detection.

> **Note**
>
> When the gateway is successfully connected, Amazon Monitron displays the gateway device ID and MAC ID in the mobile app.

8. After it connects to the gateway, Amazon Monitron will provide two options for you to configure the network connection for your gateway.



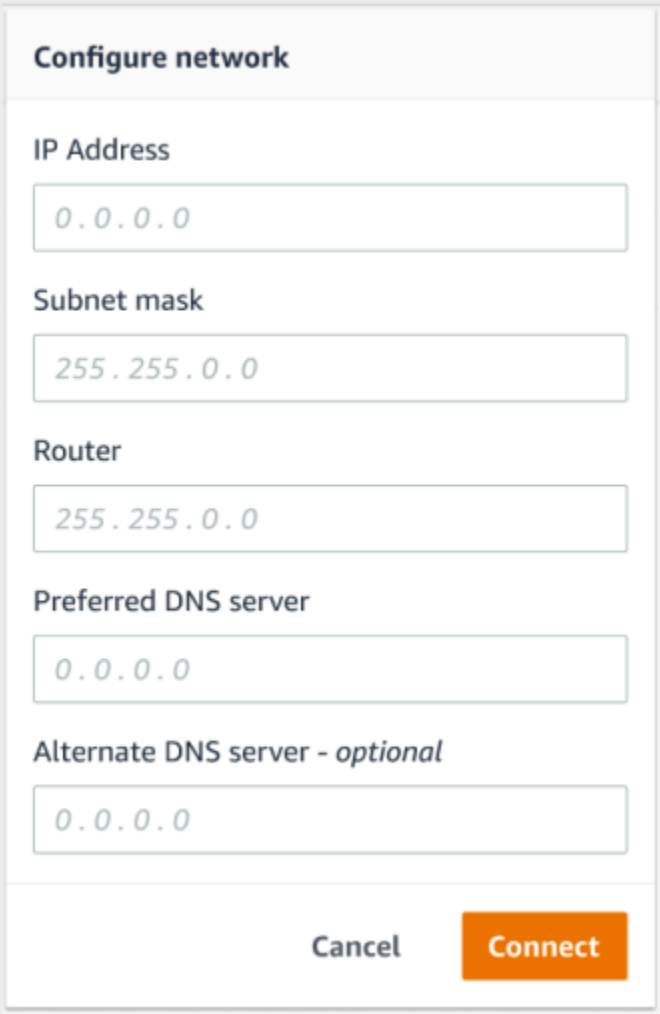

9. Choose your network configuation.

   It can take a few minutes for the gateway to be commissioned and to connect to the network.

If you have further difficulties making the gateway work, it might be helpful to reset it. For more information, see Resetting the Ethernet gateway to factory settings.

a. If you choose automatic (DHCP), Amazon Monitron will automatically configure the network to connect to the gateway.

b. If you choose **manual**, enter your IP address, subnet mask, router, preferred DNS server, and alternate DNS server (optional) information. Then choose **connect**.




## Troubleshooting Ethernet gateway detection

When you add a gateway to your project or site, as soon as you choose **Add Gateway**, the Amazon Monitron mobile app starts scanning for the gateway. If the app can't find the gateway, try the following troubleshooting tips.

- **Make sure that the gateway is powered up.** Check the small green light near the upper right corner of the gateway. If it's on, the gateway has power.

  If the gateway has no power, check the following:

  - Is the Ethernet cable firmly seated in the RJ-45 socket?
  - Is the router at the other end of the Ethernet cable functioning properly?
  - Is the Ethernet cable working? To test this, try using the cable with another gateway.
  - Is the RJ-45 socket clean? Be sure to also check the socket at the other end of the Ethernet cable.

- **Make sure the gateway is in configuration mode.** The Amazon Monitron mobile app finds a new gateway only when it's in configuration mode. When you turn a gateway on, the **Bluetooth** and **Network** LED lights blink slowly, alternating orange and blue. When you press the **Config** button to enter commissioning mode, they blink rapidly, again alternating orange and blue.




- If the LEDs show any sequence other than slow blinking before you press the button, the gateway might not go into configuration mode. In this case, reset the gateway by pressing the **Reset** button.
- **Make sure your smartphone's Bluetooth is working.** The gateway connects to your smartphone using Bluetooth, so it's a potential source of interruption. Check the following:
  - Is you smartphone's Bluetooth on and working? Try switching it off and on. If that doesn't help, restart your phone and check again.
  - Are you within your smartphone's Bluetooth range? Bluetooth range is relatively short, usually less than 10 meters, and its reliability can vary dramatically.

  - Is there anything that might be interfering electronically with the Bluetooth signal?
- **Make sure this gateway is not already commissioned to any of your projects.** The device must be deleted from all existing projects before commissioning.

If none of these actions resolves the issue, try the following:

- View and copy your gateway MAC address and get in touch with your IT admin. See Retrieving MAC address details.
- Log out of the mobile app and restart it.
- Perform a factory reset of the gateway by holding down **Config** and pressing **Reset**.

## Troubleshooting Bluetooth pairing

You may find yourself attempting to pair your iOS mobile device with a gateway that it has already paired with. This could happen because the gateway has changed locations, or because the general configuration of your Amazon Monitron site has been altered.

In that case, tell your iOS device to "forget" its Bluetooth connection with the gateway.

**Topics**

- To unpair a gateway from your device

### To unpair a gateway from your device

1. On your iOS device, choose **Settings**.
2. On your **Settings** screen, choose **Bluetooth**.
3. On the **Bluetooth** screen, choose the information icon next to the name of your Amazon Monitron Gateway.
4. On the next screen, choose **Forget This Device**.

## Resetting the Ethernet gateway to factory settings

If you re-use a gateway that was deleted from Amazon Monitron, use the commissioning button to reset the gateway to factory settings. This prepares the gateway to be used again for Amazon Monitron.

**Topics**


- Resetting the Ethernet gateway to factory settings (option 1)
- Resetting the Ethernet gateway to factory settings (option 2)


### Resetting the Ethernet gateway to factory settings (option 1)

1. Unplug the Ethernet cable from the gateway.
2. Hold down the **Config** button.
3. Plug the Ethernet cable back into the gateway.

   When the LED lights start slowly blinking, alternating orange and blue, release the **Config** button. The gateway is reset.

### Resetting the Ethernet gateway to factory settings (option 2)

1. Hold down the **Config** button.
2. Press the reset button.
3. When the led lights start slowly blinking, alternating orange and blue, release both buttons.

## Viewing the list of gateways

This page describes how to list your gateways in the Amazon Monitron app.

**Topics**


- To list your gateways list using the mobile app
- To list your gateways using the web app

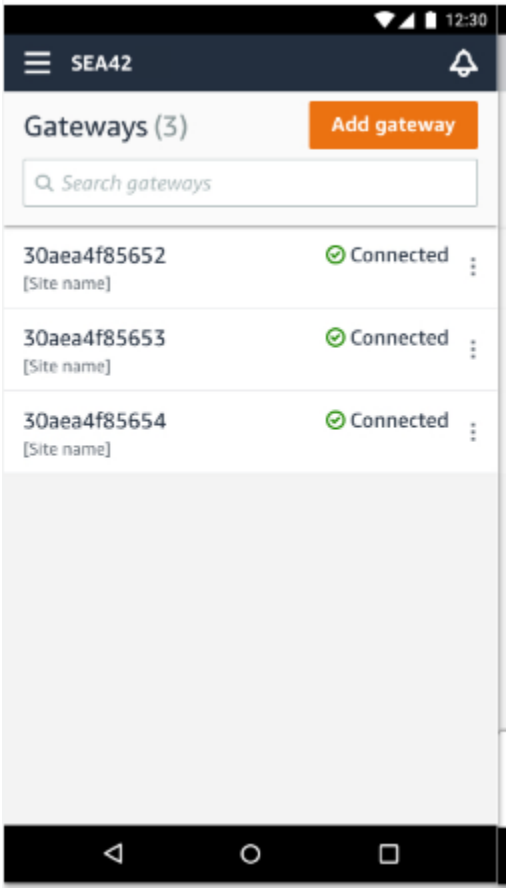

### To list your gateways list using the mobile app

1. Use your smartphone to log in to the Amazon Monitron mobile app.
2. Choose the menu icon in the upper left of the screen.

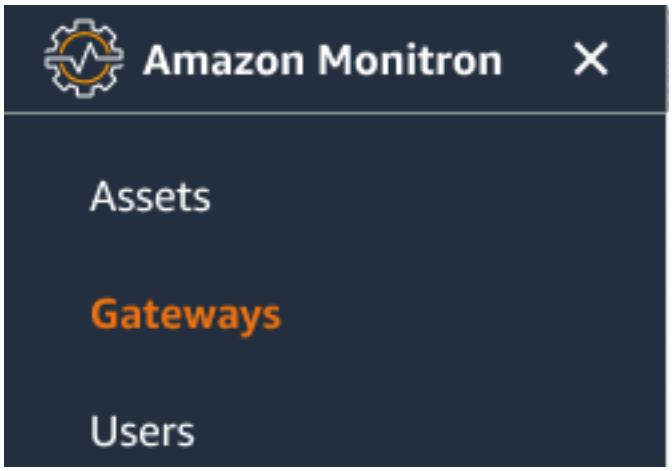
3. Choose **Gateways**.

A list of all gateways associated with the project is displayed.

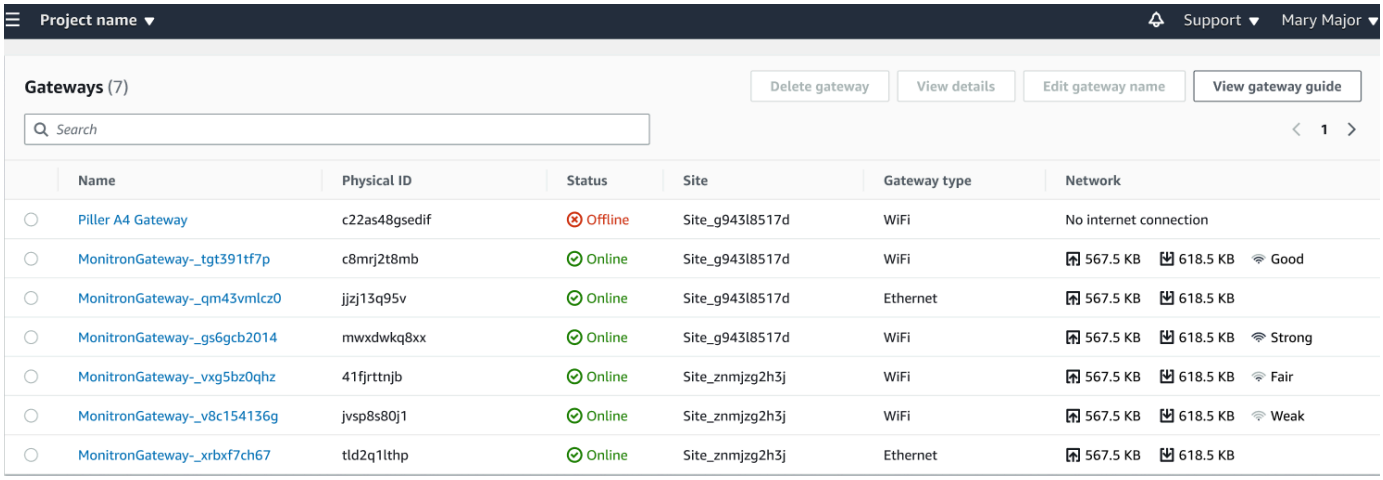



## To list your gateways using the web app

1. Choose **Gateways** from the left nav.




2. The gateway list appears in the right pane.




# Viewing Ethernet gateway details

You can view gateway details on your mobile or web app. The following gateway details are viewable:

- IP address
- Firmware version
- Last time commissioned

> **Note**
>
> You can also view and copy gateway MAC addresses. See Retrieving MAC address details.

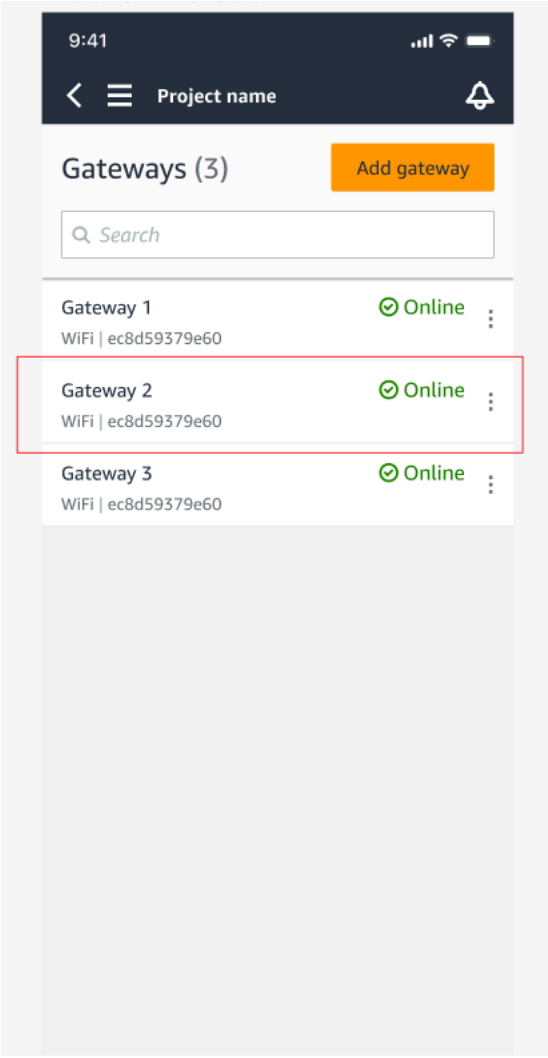
You can view sensor details on both the mobile and web app. The following section shows you how.

### Topics

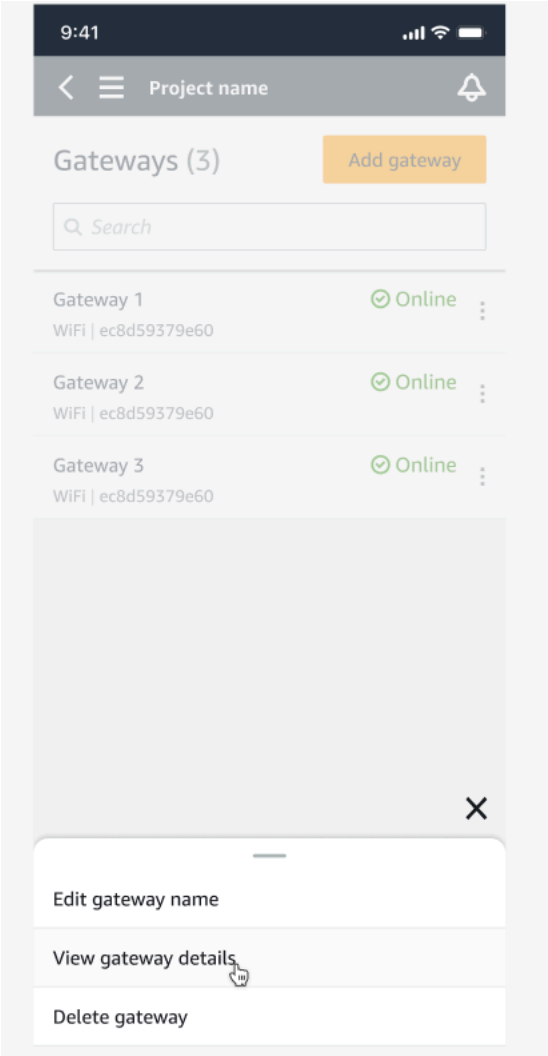

- To view Ethernet gateway details in the mobile app
- To view Ethernet gateway details in the web app


## To view Ethernet gateway details in the mobile app

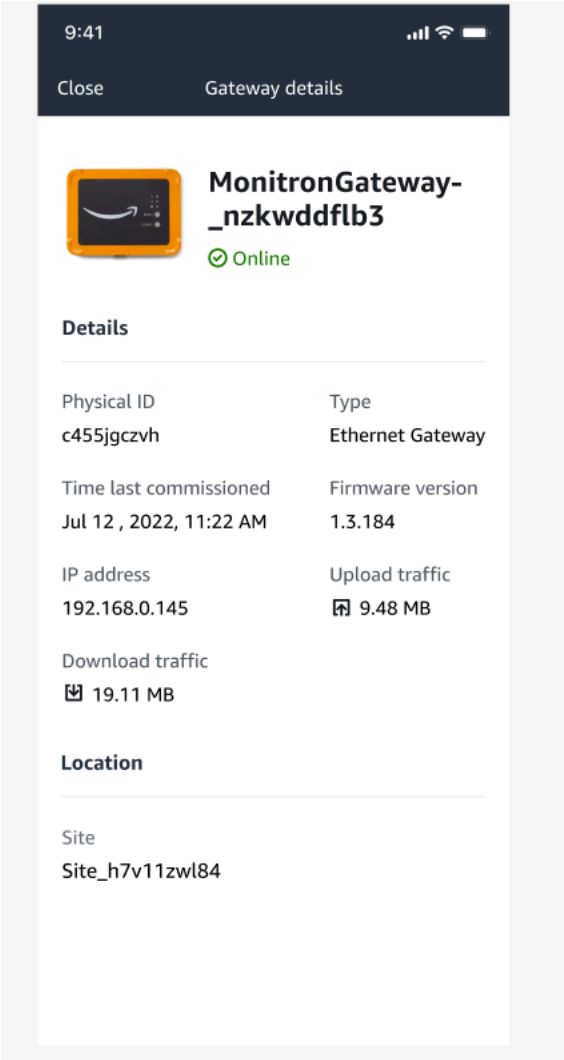
1. From the **Gateways** list, choose the gateway whose details you want to view.




2. From the options box that pops open, select **View gateway details**.

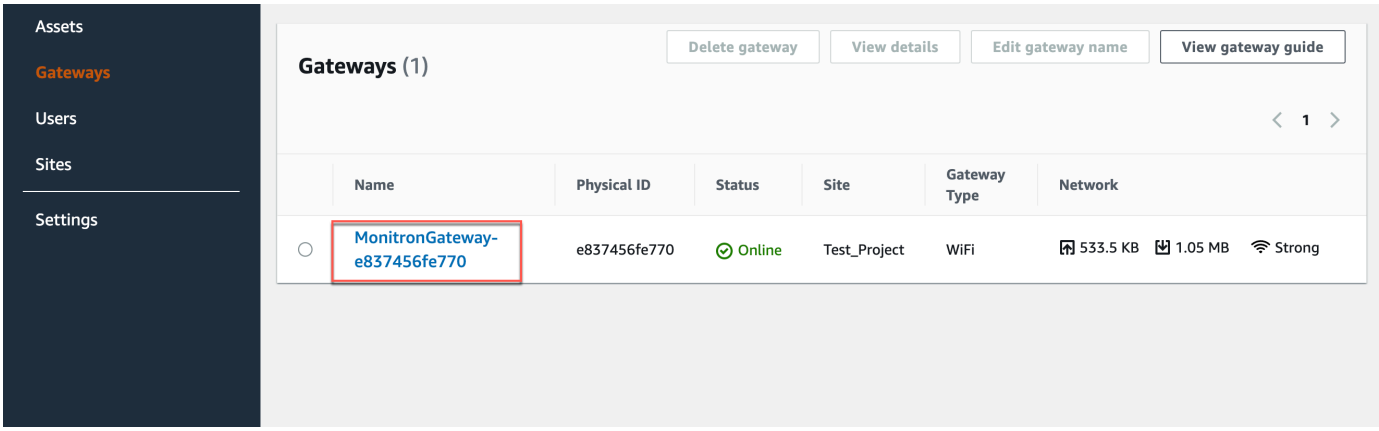



3. The **Gateway details** page is displayed.

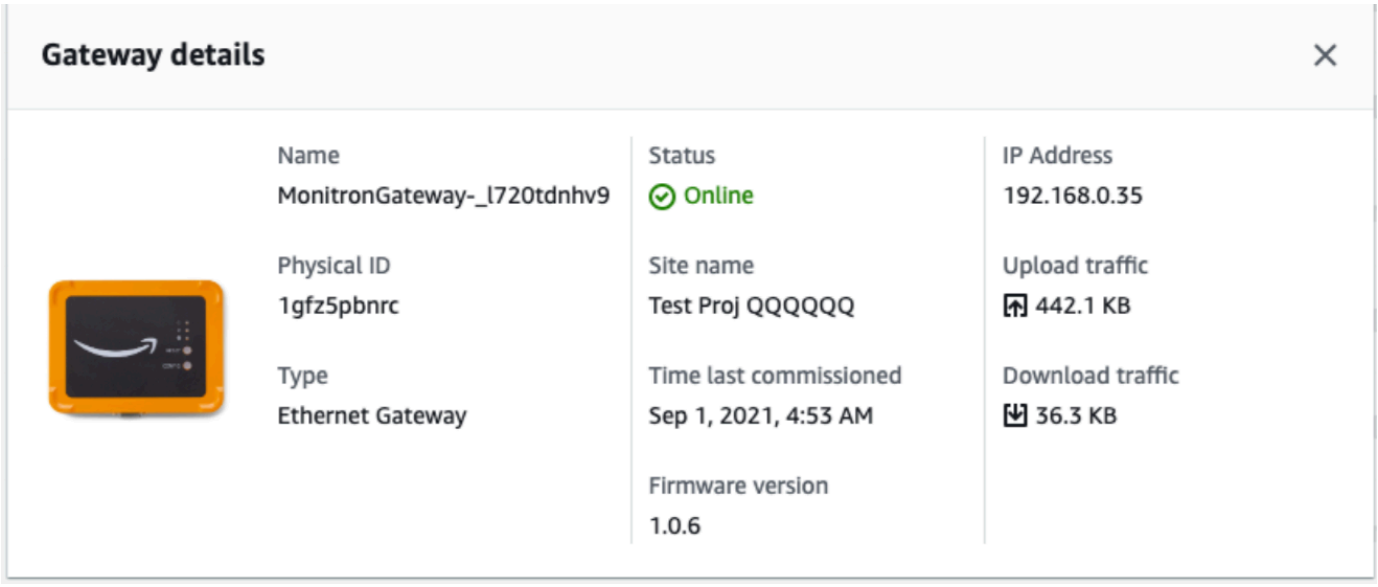



## To view Ethernet gateway details in the web app

1. From the **Gateways** list, choose the gateway whose details you want to view.



2. The **Gateway details** page is displayed.




## Editing Ethernet gateway name

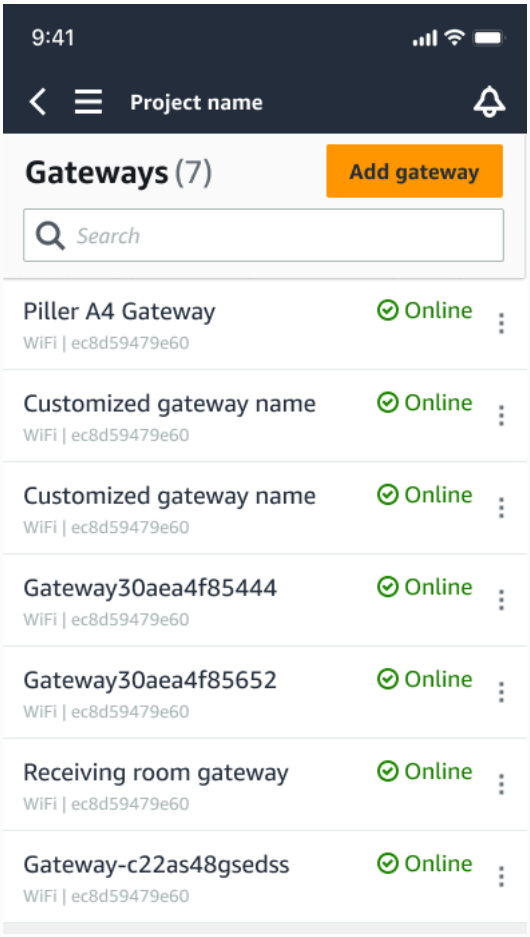
You can change the display name for your Ethernet gateway to find it faster. To edit a gateway name, open your web or mobile app and do the following.

### Topics

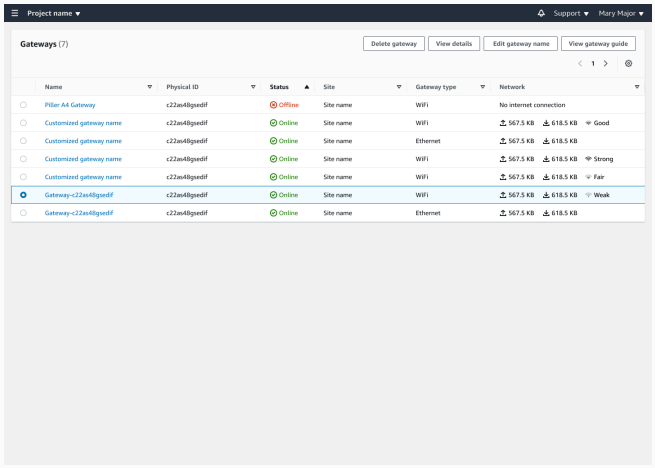
- To edit an Ethernet gateway name

### To edit an Ethernet gateway name

1. Select the gateway name you want to edit from the **Gateways** page.




Mobile app view

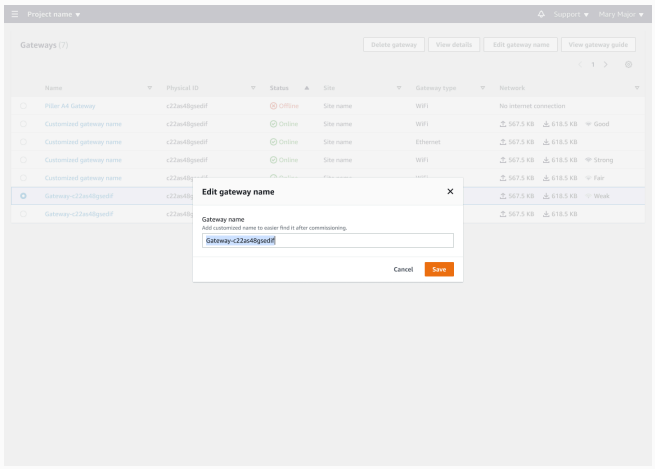



Web app view

2. A pop-up will appear prompting you to add a customized name for the gateway.




Mobile app view

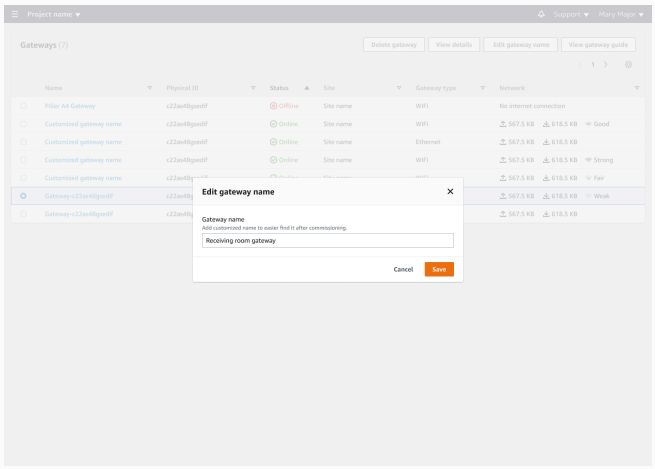



Web app view

3. Enter the new name for the gateway and choose **Save**.

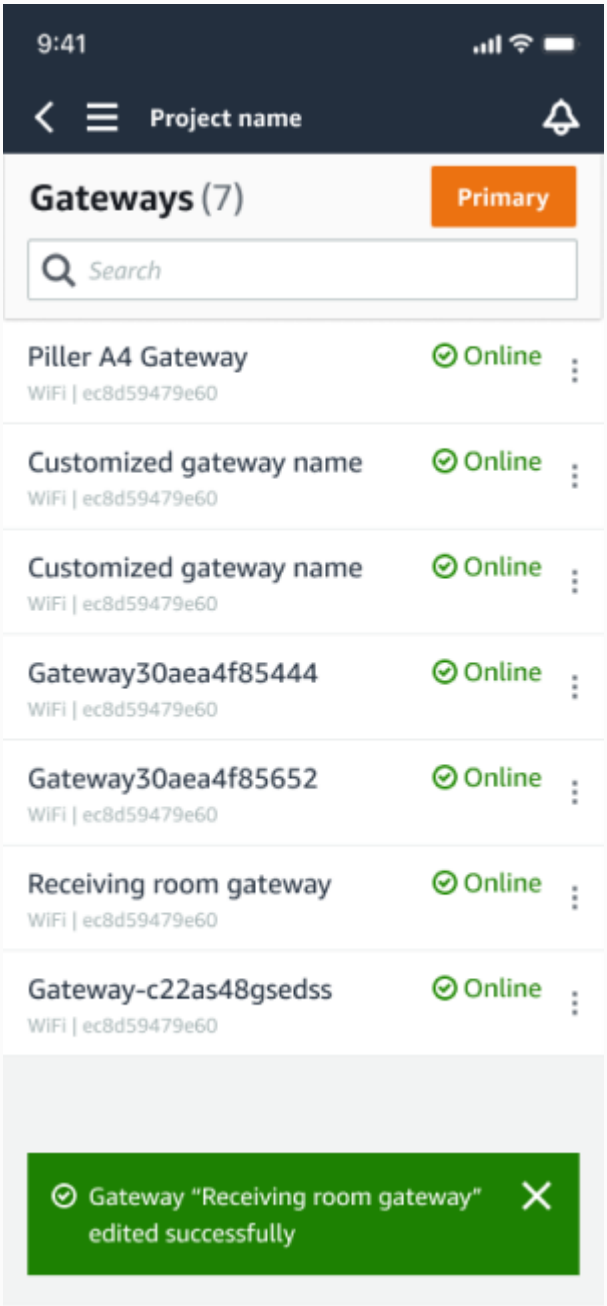



Mobile app view

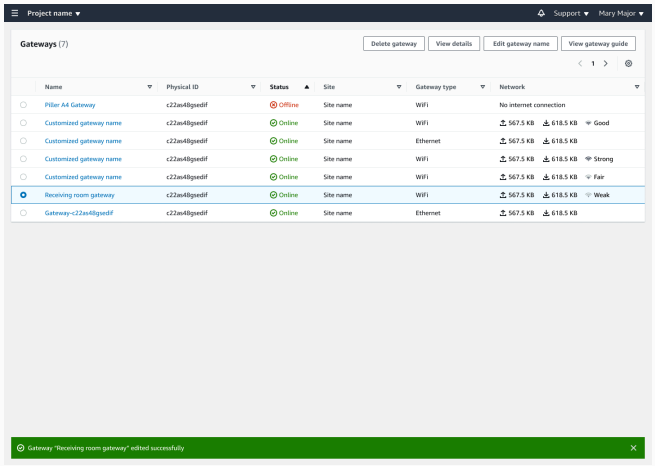



Web app view

4. You will see a success message confirming the new gateway name.




Mobile app view




Web app view

## Deleting an Ethernet gateway

Sensors need a gateway to relay their data to the AWS Cloud. Deleting a gateway might cause some sensors to lose their connection. Exercise caution before deleting a gateway.

When you delete a gateway, sensors switch their connection to another gateway that is within range, if there is one, and data transmission from the sensor continues uninterrupted. If no gateway is within range, data transmission is interrupted and the data might be lost.

When you delete a gateway which is currently offline, you must perform a factory reset of the device before commissioning it again.

**Topics**


- Deleting an Ethernet gateway using the mobile app
- Deleting an Ethernet gateway using the web app


### Deleting an Ethernet gateway using the mobile app

1. Using the mobile app, navigate to the **Gateways** page.
2. Choose the vertical ellipses icon (



)

   next to the gateway that you want to delete.
3. Choose **Delete Gateway**.
4. Choose **Delete** again.

### Deleting an Ethernet gateway using the web app

1. Navigate to the list of Wi-Fi gateways.
2. Select the gateway from the table.
3. Choose **Delete gateway**.

## Retrieving MAC address details

To retrieve your Amazon Monitron gateway's Media Access Control (MAC) address, you can scan the QR code on the gateway device with your mobile phone. Amazon Monitron returns both the MAC address and gateway ID when you scan the QR code.

If you are an IT admin, you can use the scanned MAC address to ensure gateway devices are configured with the correct network settings before they are commissioned. If you are a technician

commissioning gateways, you can use the scanned MAC address to troubleshoot any networking issues with your IT admin.

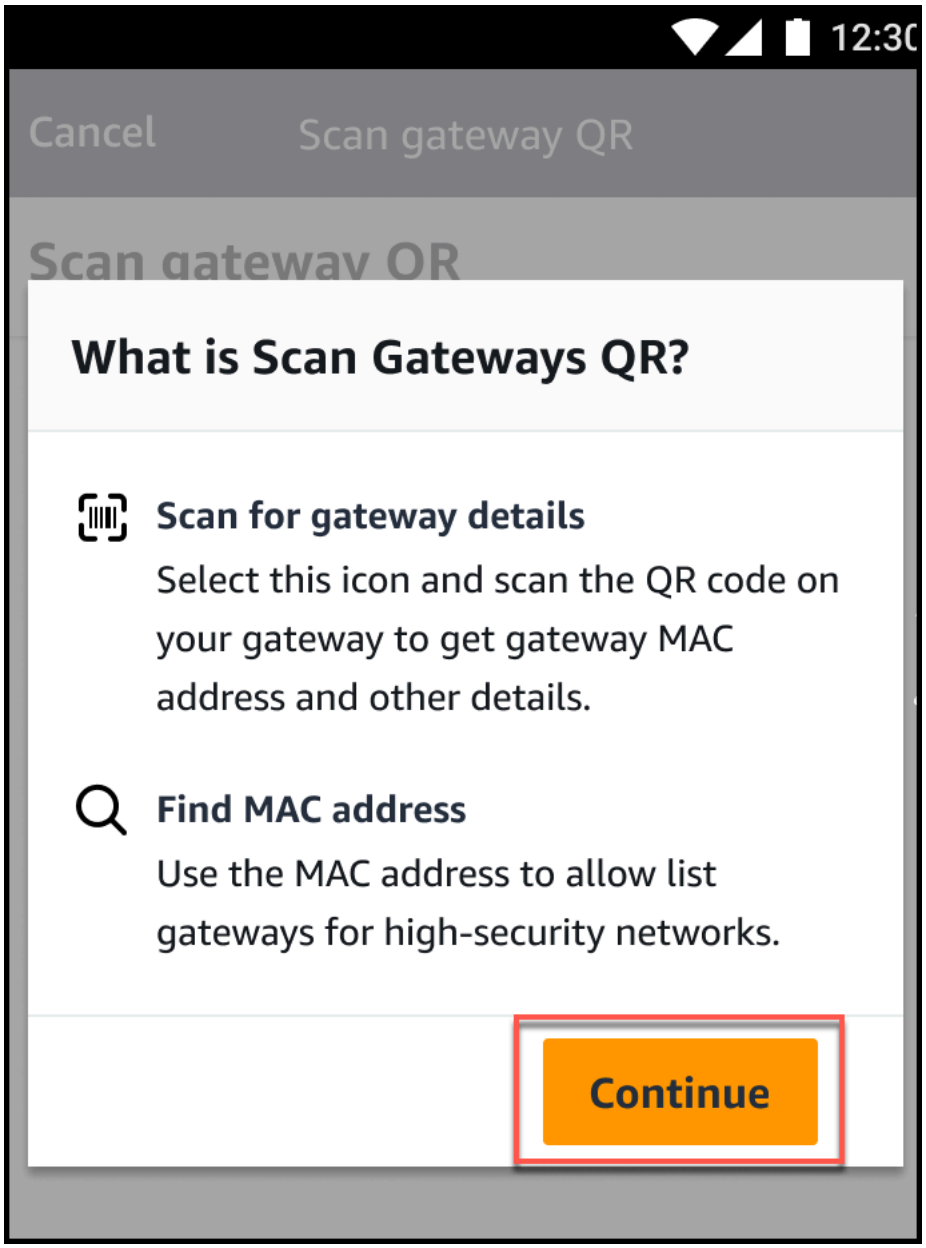
> **Note**
>
> Retrieving MAC addresses by scanning QR codes is only supported for the Amazon Monitron mobile app.

The following procedure shows you how to retrieve your gateway device's MAC address.

1. Navigate to the **Gateways** page.
2. Select the scan icon.

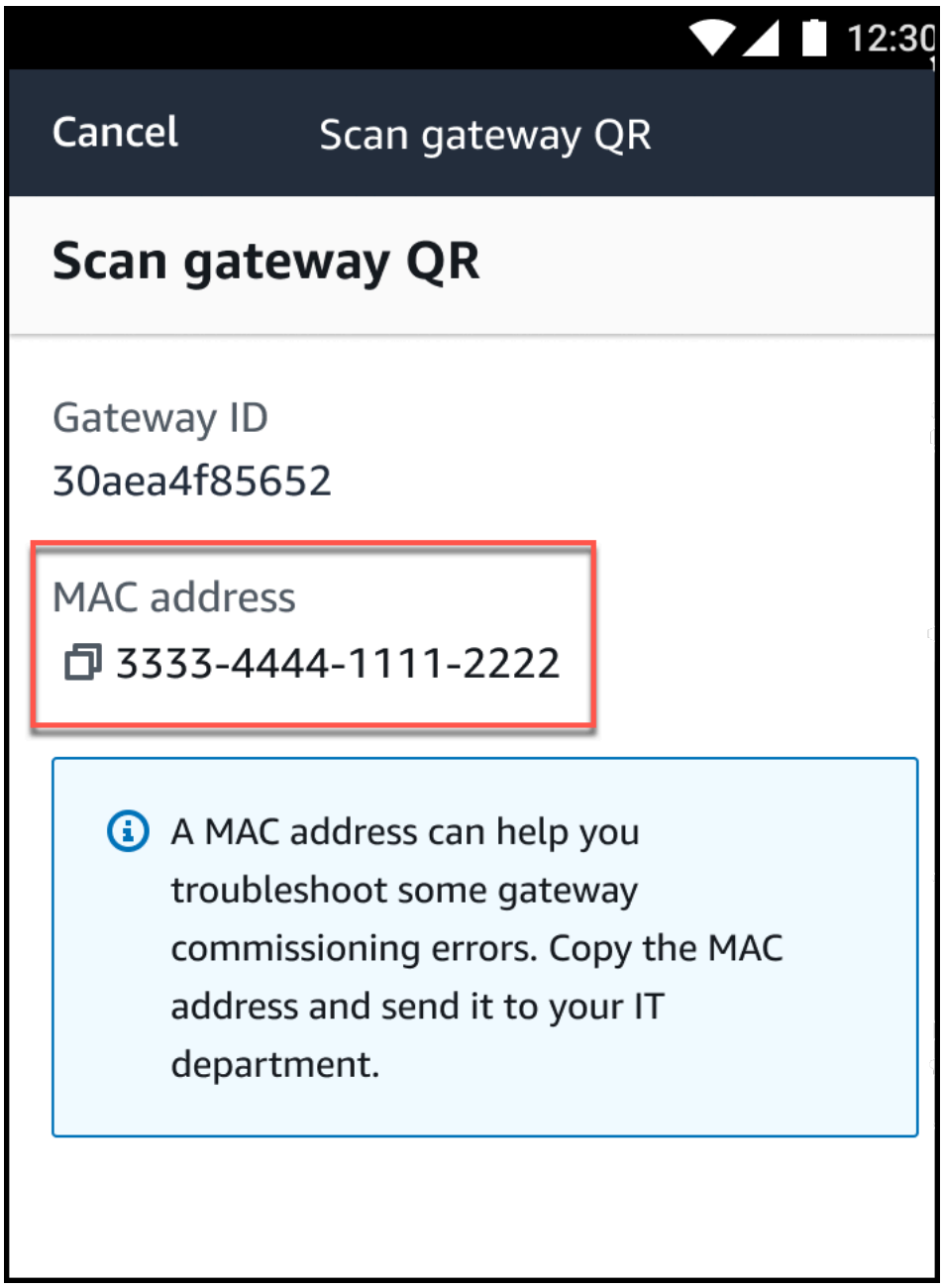


3. Amazon Monitron will display a message explaining what scanning a QR code will do. Select **Continue**.




4. On the **Scan QR Code** page, scan the gateway QR code using your mobile phone camera.

   When the scan successfully completes, Amazon Monitron displays the Gateway ID and MAC address on the **Scan QR Code** page in the mobile app.




You can also select the copy icon

( )

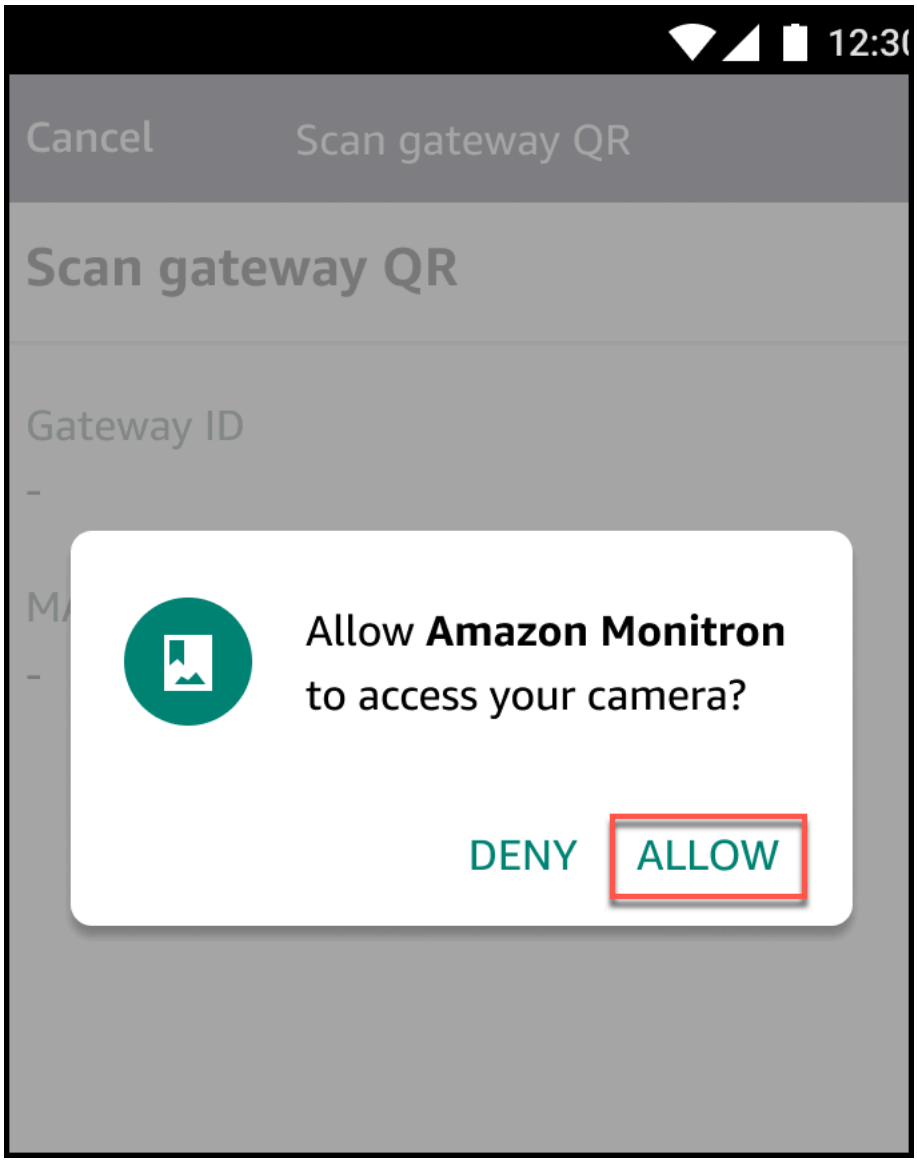
to copy the MAC address.

**Note**

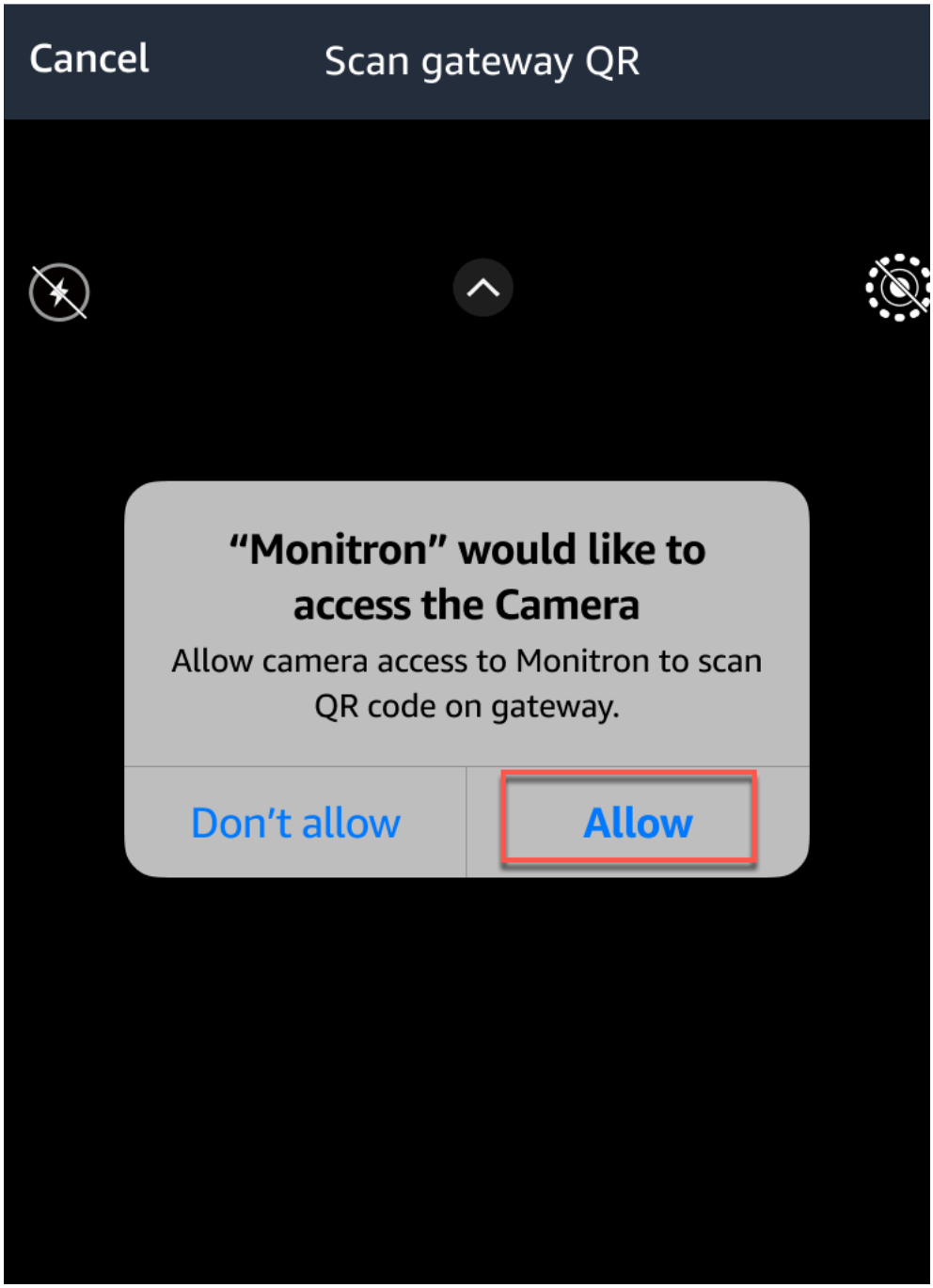
If not already enabled, Amazon Monitron may need permissions to access your camera to scan the QR code. These permissions must be enabled from the settings page

of your mobile device before you can successfully scan a device QR code. Amazon Monitron will prompt you to enable camera access during the scanning process if permissions haven't already been granted.

**On Android devices**




**On iOS devices**

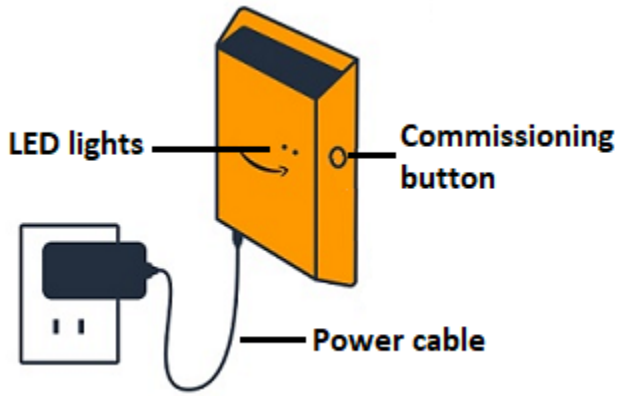



## Wi-Fi gateways

This topic explains how to install your Wi-Fi gateway. It also explains how to delete an unnecessary gateway.

To learn about using Amazon Monitron with Ethernet gateways, see Ethernet gateways.

The Amazon Monitron gateway is easy to install and operate. After plugging in the power cable, you can put the gateway in commissioning mode by pressing the commissioning button.

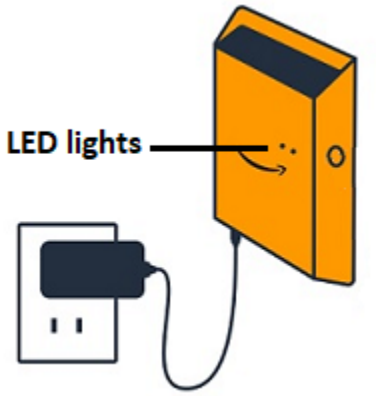



**Topics**


- Reading the LED lights on a Wi-Fi gateway
- Placing and installing a Wi-Fi gateway
- Commissioning a Wi-Fi gateway
- Troubleshooting Wi-Fi gateway detection
- Troubleshooting Bluetooth pairing
- Resetting the Wi-Fi gateway to factory settings
- Viewing the list of gateways
- Viewing Wi-Fi gateway details
- Editing Wi-Fi gateway name
- Deleting a Wi-Fi gateway
- Retrieving MAC address details


## Reading the LED lights on a Wi-Fi gateway

The LED lights on the top of your Amazon Monitron gateway indicate the status of the gateway. Each LED light has one orange light and one blue light. The orange light indicates that the gateway is connected to a Wi-Fi network. The blue light indicates that the gateway's Bluetooth is connected to the sensors.




The sequence that the lights display indicates the status of the gateway, as described in the following table.

| | LED sequence | Description |
|---|---|---|
| 1 | Solid green light | The Wi-Fi gateway is powered on. |
| 2 | Solid orange light | The gateway is connected to the Wi-Fi network and the Amazon Monitron backend system. |
| 3 | Flashing orange light (slow) | The gateway is attempting to connect to the Wi-Fi network. |
| 4 | Flashing orange light (1 fast/ 1 slow) | The gateway is connected to the Wi-Fi network and is attempting to connect to the Amazon Monitron backend system. |
| 5 | Solid blue light | At least one sensor is communicating with the gateway. |

| | LED sequence | Description |
|---|---|---|
| 6 | No blue light | No sensors are currently communicating with the gateway. |
| 7 | Orange and blue lights flashing (slowly) | The gateway is powered on, unconfigured (not commissio ned), and not in commissio ning mode (that is, not discoverable or configurable by the mobile app). |
| 8 | Orange and blue lights flashing (rapidly) | The gateway is on and in commissioning mode, but not yet linked to any sensors. In commissioning mode, the gateway is discoverable and configurable by Amazon Amazon Monitron, but no sensors can connect yet. |
| 9 | No lights | The gateway is not connected to a power source or a firmware update is in progress. |
| 10 | Solid orange and blue lights | The gateway is starting up. |

## Placing and installing a Wi-Fi gateway

Unlike sensors, a Wi-Fi gateway doesn't need to be attached to the machines that are being monitored. However, it does need an available Wi-Fi network through which Amazon Monitron can connect to the AWS Cloud.



**Topics**


- Choosing a location for your gateway
- Mounting the bracket
- Mounting the gateway on the bracket


## Choosing a location for your gateway

You can install a gateway almost anywhere within your factory, depending on its layout. Typically, gateways are mounted on a wall, but you can mount them on the ceiling, on pillars, or in almost any other location. A gateway must be within 20 to 30 meters of the sensors it supports. It also must be close enough to a power outlet that it can be plugged in.

Consider these other factors when mounting a gateway:

- Mounting the gateway higher than sensors (2 meters or more) can improve coverage.
- Keeping an open line of sight between the gateway and sensors improves coverage.
- Avoid mounting the gateway on building structures, such as exposed steel beams. They can cause interference with the signal.
- Try to work around any equipment that might produce electronic interference with the signal.
- If possible, install more than one gateway within transmission distance of your sensors. If a gateway becomes unavailable, the sensors will switch their data transmission to another gateway. Having multiple gateways helps to reduce data loss. There is no minimum required distance between two gateways.

## Mounting the bracket

To install a gateway, position the wall mounting bracket on the wall or on another location, then mount the gateway on the bracket.

Almost everything you need comes in the box that contains the gateway:

- The gateway
- An AC adapter
- AC adapter plugs for the EU, UK, and US
- The wall mounting bracket
- Double-sided tape
- Two mounting screws
- One small screw to attach the gateway to the bracket

There are three ways to mount the mounting bracket: screw mounting, tape mounting, and plastic-tie mounting. The method you use depends on whether you're mounting the gateway on a wall or another location, and on the surface material. You mount the gateway on the wall mounting bracket through the small screw hole in the center of one of the short sides.

To mount the bracket, choose one of the following techniques.

**Screw mounting**

Typically, you mount the bracket directly to the wall using the mounting screws included in the gateway box. Mount the bracket from the front. You might need to use an expansion plug or toggle bolt to secure the screw in the wall. An expansion plug or toggle bolt is not included.



### Tape mounting

A shaped piece of double-sided tape is included in the gateway box. Use it when you can't place a screw into the mounting surface. You can also use it in combination with the other methods of mounting for a more secure installation.




Remove the backing on one side of the tape and apply the tape to the back of the wall mounting bracket between the four raised sections.



Remove the remaining backing and apply the bracket to the mounting location. Press hard on the bracket to make sure that the tape firmly adheres to the surface.

**Plastic-tie mounting**

To mount a gateway to a smaller non-wall location, such as a pillar or fencing, use cable ties (also known as zip ties) to fasten the wall mounting bracket. Put the ties through the holes in the four raised sections on the back of the bracket. wrap them around the mounting location, and pull tight.



After the bracket is mounted, attach the gateway to the bracket.

## Mounting the gateway on the bracket

In the following procedure, we talk about the "top" and "bottom" of the gateway and the bracket. The two images below demonstrate this standard orientation. As noted below, the device does not have to be upright in order to function. This explanation is just to help you understand the mounting instructions.

When the gateway is upright, the Amazon logo on the front of the device is right-side up. The two holes that will reveal the LEDs are just above the logo, on the right side. The hole for the small screw that will attach the bracket to the gateway is at the top, in the center.



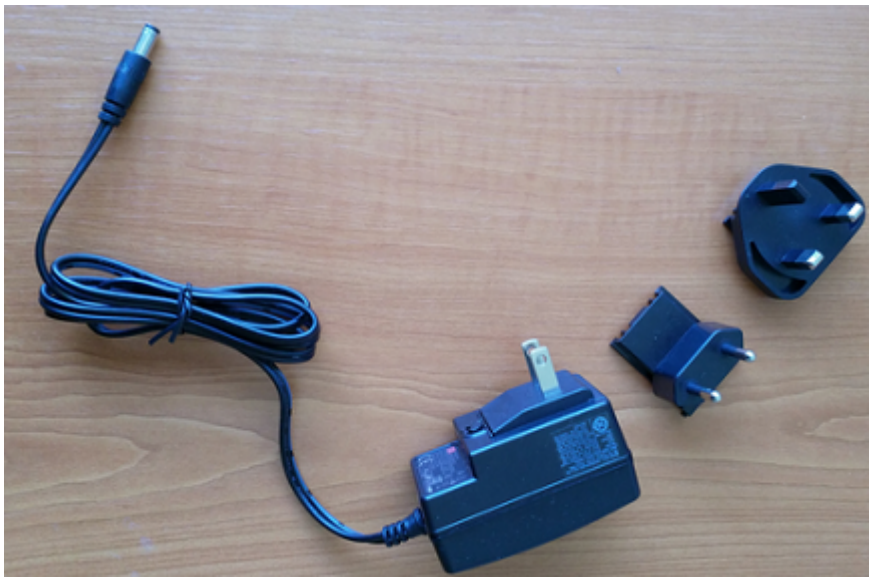
On the back of the device, there are two pairs of orange plastic hooks. The large hooks, near the bottom of the device, point downward. The small hooks, near the top of the device, point upward.



1. With the wall mounting bracket in place, place the gateway against the bracket. The two large plastic hooks on the back of the gateway should be in the slots at the bottom of the bracket.
2. Press the top of the gateway against the bracket so that the two small plastic hooks on the back of the gateway latch into the top of the bracket.
3. Using the small screw that came with the gateway, fasten the gateway to the bracket through the hole at the top of the gateway.



4. Insert the appropriate AC plug into the AC adapter. The following picture shows the US plug attached to the adapter.



5. Plug the AC adapter into the bottom of the gateway and a power outlet.

   When the LED lights on the gateway blink slowly, alternating orange and blue, the gateway is turned on and ready to be commissioned.

**Note**

The gateway is designed to be mounted with the small screw securing it at the top. However, installing it upside down doesn't affect its performance.

If you have problems connecting to your gateway, see Troubleshooting Wi-Fi gateway detection.

## Commissioning a Wi-Fi gateway

When your gateway is mounted in your factory, you will need access to the Amazon Monitron mobile app to commission it. Amazon Monitron supports only smartphones using Android 8.0+ or iOS 14+ with Near Field Communication (NFC) and Bluetooth.

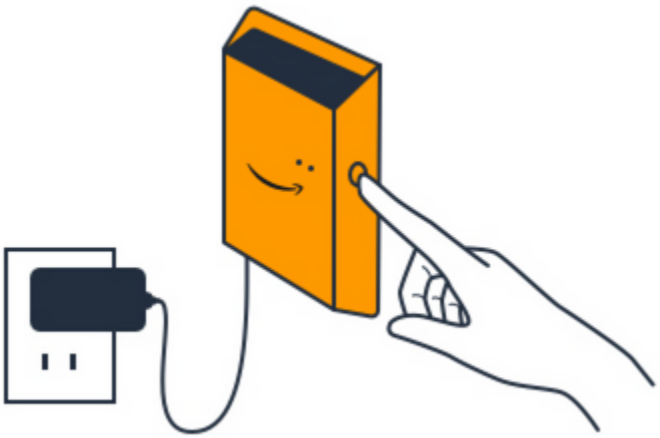
**Topics**


- To commission a gateway


### To commission a gateway

1. If Bluetooth isn't already turned on for your smartphone, turn it on.
2. Position your gateway in the location that works best for communicating with your sensors.

   The best place to mount your gateway is higher than the sensors and no more than 20 to 30 meters away. For additional help with locating your gateway, see Placing and installing a Wi-Fi gateway.
3. Plug in the gateway and make sure the LED lights on top are blinking alternatively yellow and blue.
4. Push the button on the side of the gateway to put it into commissioning mode. The lights will start rapidly blinking.

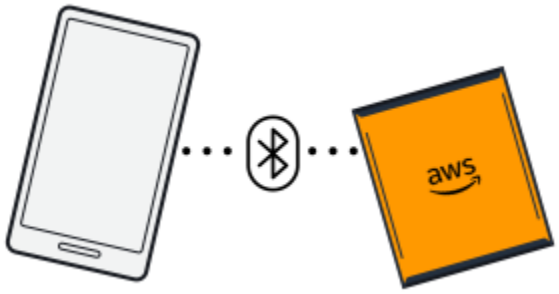


5. Open the mobile app on your smartphone.
6. On the **Getting Started** page or the **Gateways** page, choose **Add gateway**.

   Amazon Monitron scans for the gateway. This can take a few moments. When Amazon Monitron finds the gateway, it displays it in the gateway list.
7. Choose the gateway.

   > **Note**
   >
   > If you are using an iOS mobile device, and you have previously paired with this particular gateway, you may need to make your device "forget" the gateway before re-pairing. For more information, see Troubleshooting Bluetooth pairing.

   It can take a few moments for Amazon Monitron to connect to the new gateway.




   If the mobile app continues to try to connect to the gateway without success, see Troubleshooting Wi-Fi gateway detection.

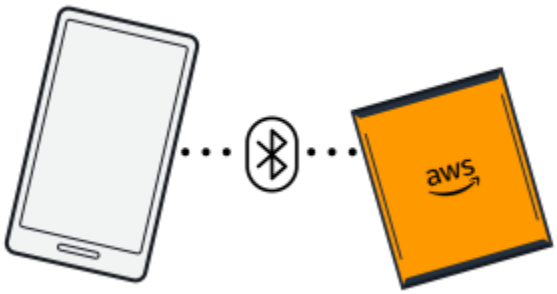
8. After it connects to the gateway, Amazon Monitron scans for Wi-Fi networks. Choose the Wi-Fi network that you want to use.
9. Enter your Wi-Fi password, and then choose **Connect**.

   It can take a few minutes for the gateway to be commissioned and to connect to the Wi-Fi network.

   If you have further difficulties, see Resetting the Wi-Fi gateway to factory settings.

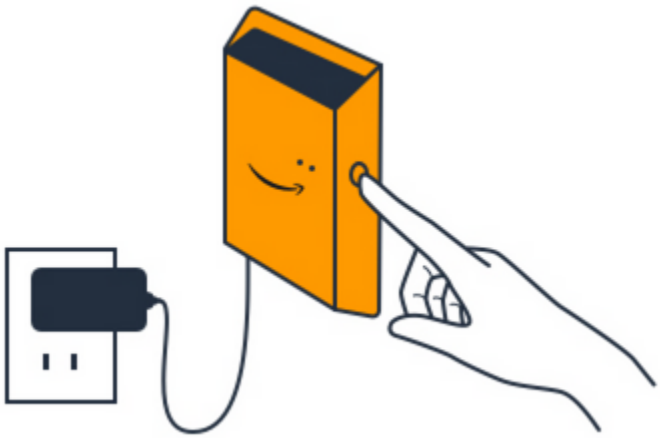
## Troubleshooting Wi-Fi gateway detection

When you add a gateway to your project or site, as soon as you choose **Add gateway** the Amazon Monitron mobile app starts scanning to find it. If the mobile app can't find the gateway, try the following troubleshooting tips.




- **Make sure that the gateway is turned on.** Check the LED lights—the two small orange and blue lights next to the Amazon symbol on the top of the gateway. If they're on, the gateway has power. If the gateway has no power, check the following:
  - Is the power cord firmly attached to both the back of the gateway and the power outlet?
  - Is the power outlet functioning properly?
  - Is the gateway power cable working? To test this, try using the cable with another gateway.
  - Is the outlet where the cable plugs into the gateway clean, with no debris stuck inside? Be sure to check both the outlet in the gateway and the connecting end of the cable.
- **Make sure that the gateway is in commissioning mode.** The Amazon Monitron mobile app finds a new gateway only when it's in commissioning mode. When you turn a gateway on, the LED lights blink slowly, alternating orange and blue. When you press the button on the side of the gateway and enter commissioning mode, they blink rapidly, also alternating orange and blue. If the LEDs show any sequence other than slow blinking before you press the button, the gateway

might not go into commissioning mode. In this case, perform a factory reset of the gateway by turning the power off, then pressing and holding down the commissioning button (located on the side) while you turn the power back on.



- **Make sure your smartphone's Bluetooth is working.** The gateway connects to your smartphone using Bluetooth.
  - Is you smartphone's Bluetooth on and working? Try switching it off and on. If that doesn't help, restart your phone and check again.
  - Are you within your smartphone's Bluetooth range? Bluetooth range is relatively short, usually less than 10 meters and its reliability can vary dramatically.
  - Is there anything that might be interfering electronically with the Bluetooth signal?
- **Make sure the gateway is not already commissioned to any of your projects.** The devide must be deleted from all existing projects before commissioning.

If none of these actions resolves the issue, try the following:

- View and copy your gateway MAC address and get in touch with your IT admin. See Retrieving MAC address details.
- Log out of the mobile app and restart it.
- Do a factory reset of the gateway by turning the power off, then pressing and holding down the commissioning button on the side while you turn the power back on.

# Troubleshooting Bluetooth pairing

You may find yourself attempting to pair your iOS mobile device with a gateway that it has already been paired with. This could happen because the gateway has changed locations, or because you have altered the general configuration of your Monitron site.

In that case, tell your iOS device to "forget" its Bluetooth connection with the gateway.

**Topics**


- To unpair a gateway from your device


## To unpair a gateway from your device

1. On your iOS device, choose **Settings**.
2. On your **Settings** screen, choose **Bluetooth**.
3. On the **Bluetooth** screen, choose the information icon next to the name of your Monitron Gateway.
4. On the next screen, choose **Forget This Device**.

# Resetting the Wi-Fi gateway to factory settings

If you reuse a gateway that was deleted from Amazon Monitron, you use the commissioning button to reset the gateway to factory settings. This prepares the gateway to be used again for Amazon Monitron.

If you delete a gateway that is currently offline, your must perform a factory reset of the device before commissioning it again.

**Topics**


- To reset a gateway to factory settings


## To reset a gateway to factory settings

1. Unplug the gateway.
2. Hold down the commissioning button.
3. Plug the gateway back in.

4. When the LED lights start slowly blinking, alternating orange and blue, release the commissioning button.
5. Unplug the gateway, wait 10 seconds, and then plug it back in. The gateway is reset.

# Viewing the list of gateways

This page describes how to list your Wi-Fi gateaways in the web or mobile app.

**Topics**


- To list your gateways list using the mobile app
- To list your gateways using the web app

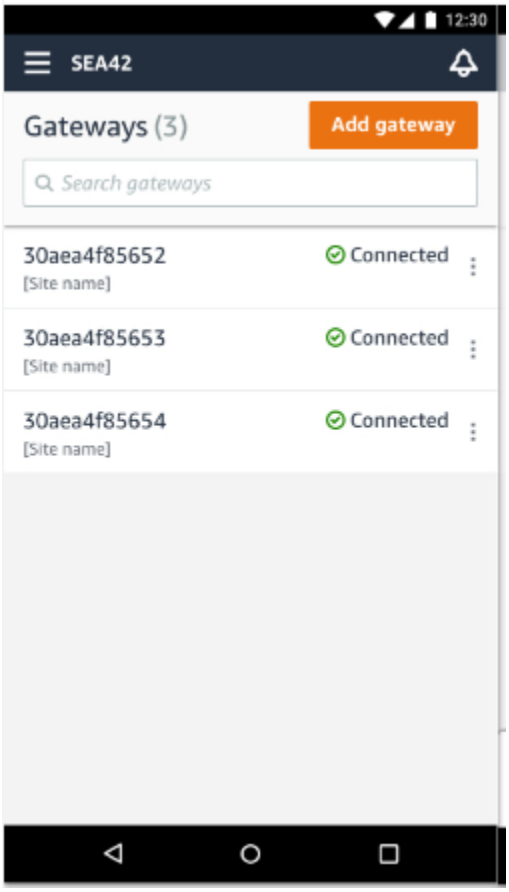

## To list your gateways list using the mobile app

1. Use your smartphone to log in to the Amazon Monitron mobile app.
2. Choose the menu icon in the upper left of the screen.



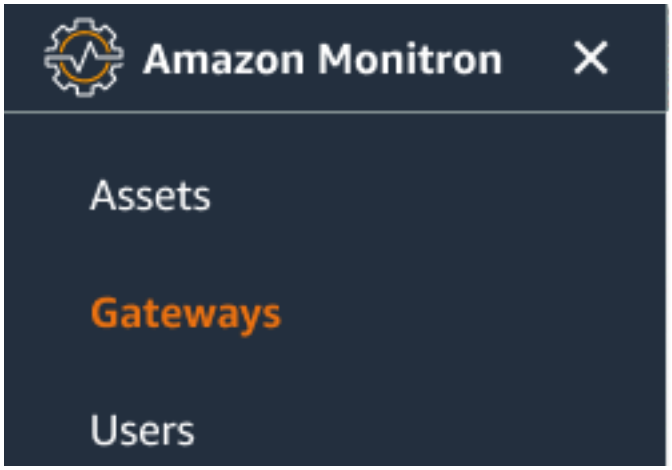

3. Choose **Gateways**.

   A list of all gateways associated with the project is displayed.

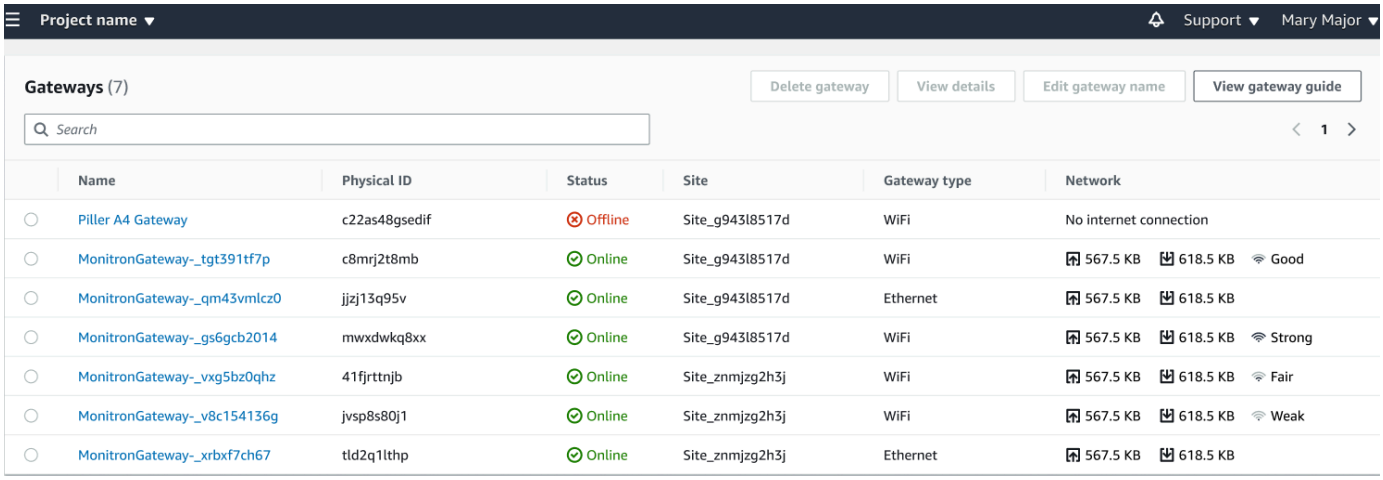



## To list your gateways using the web app

1. Choose **Gateways** from the left nav.




2. The gateway list appears in the right pane.




# Viewing Wi-Fi gateway details

You can view gateway details on your mobile or web app. The following gateway details are viewable:

- IP address
- Firmware version
- Last time commissioned

> **Note**
>
> You can also view and copy gateway MAC addresses. See Retrieving MAC address details.

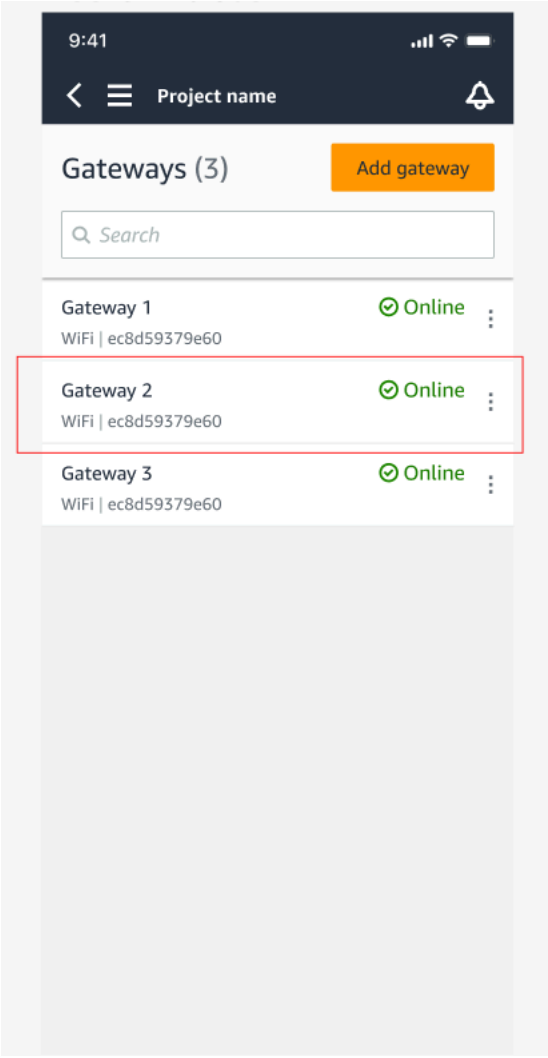
You can view sensor details on both the mobile and web app. The following section shows you how.

**Topics**

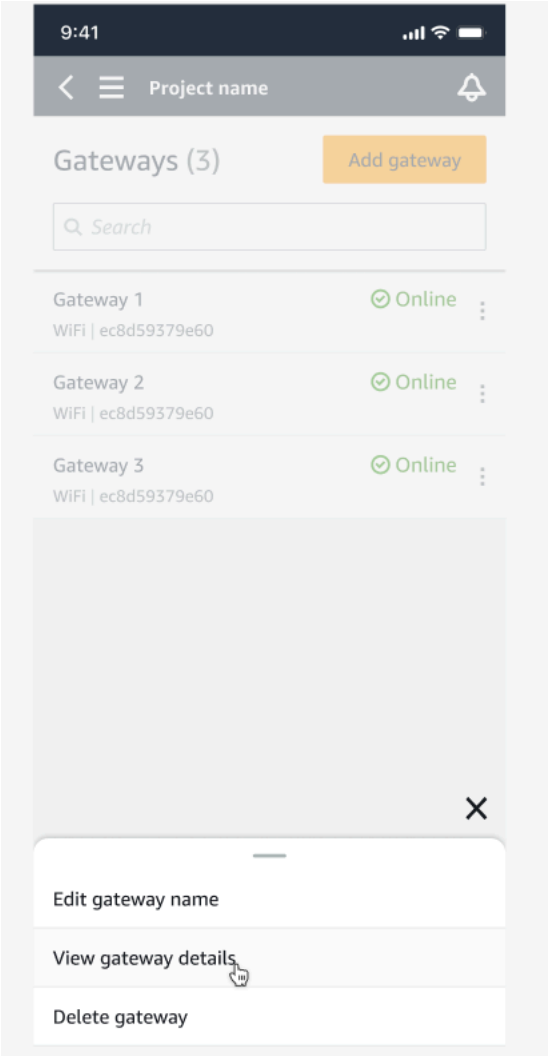

- To view Wi-Fi gateway details in the mobile app
- To view Wi-FI gateway details in the web app


## To view Wi-Fi gateway details in the mobile app

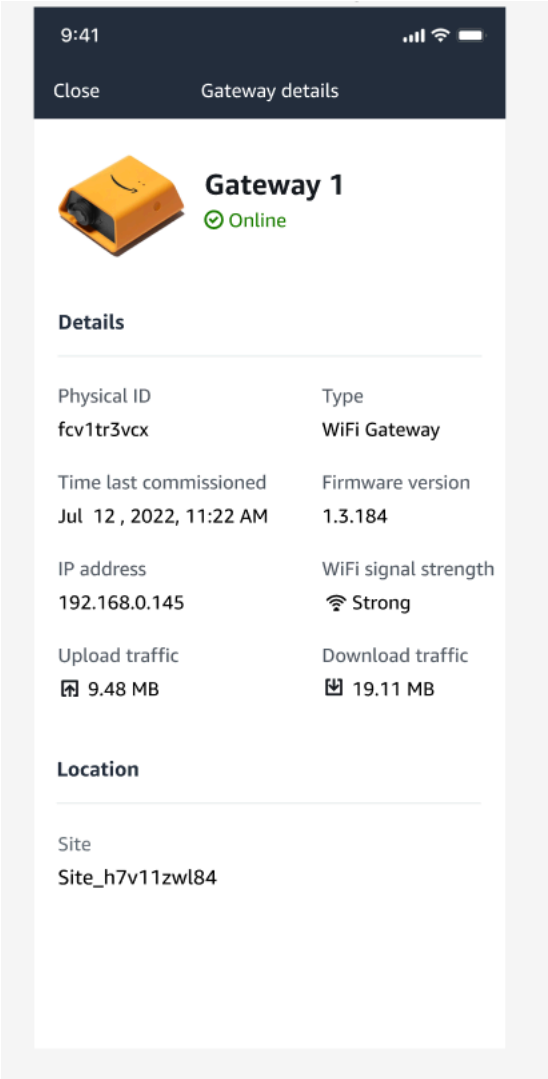
1. From the **Gateways** list, choose the gateway whose details you want to view.




2. From the options box that pops open, select **View gateway details**.

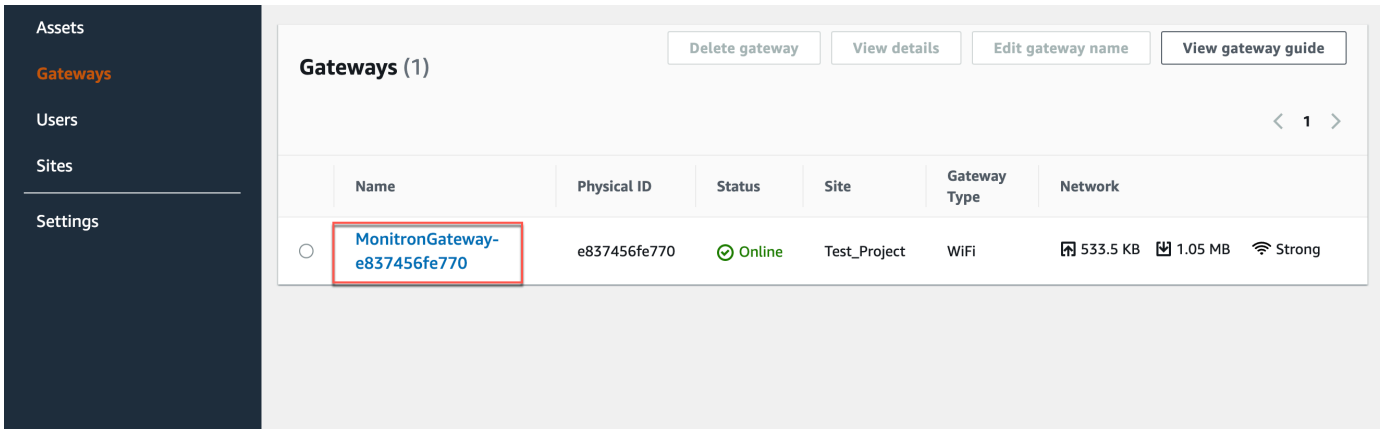



3. The **Gateway details** page is displayed.

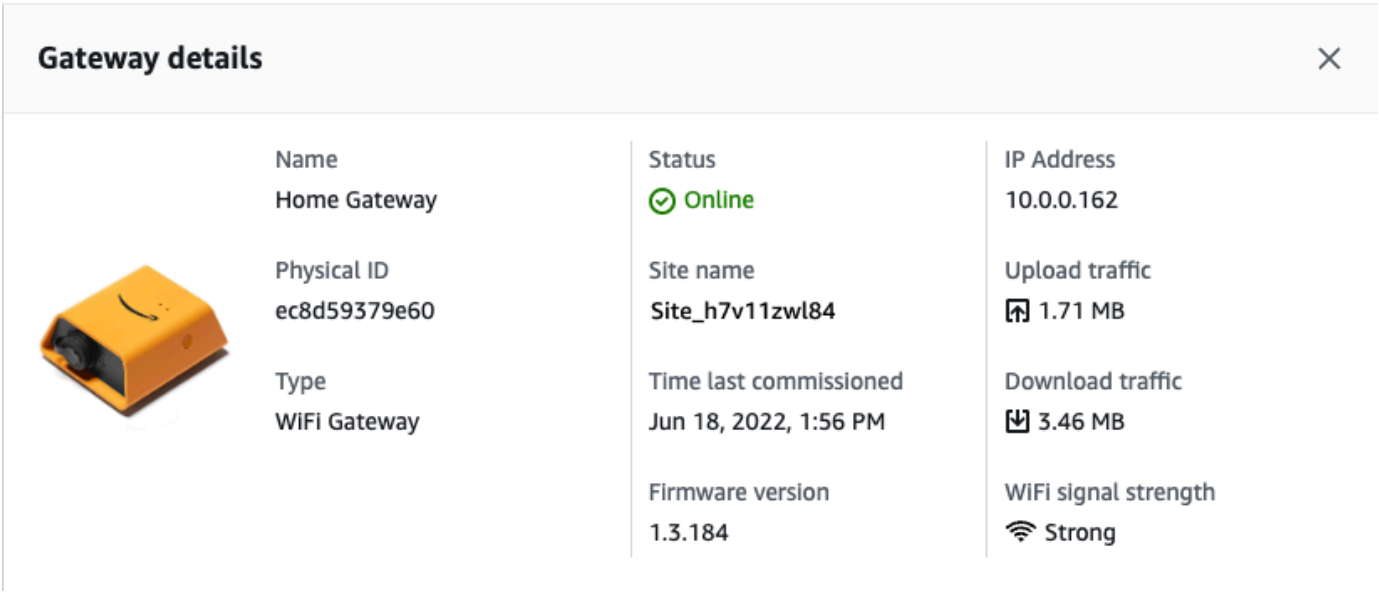



## To view Wi-FI gateway details in the web app

1. From the **Gateways** list, choose the gateway whose details you want to view.



2. The **Gateway details** page is displayed.




# Editing Wi-Fi gateway name

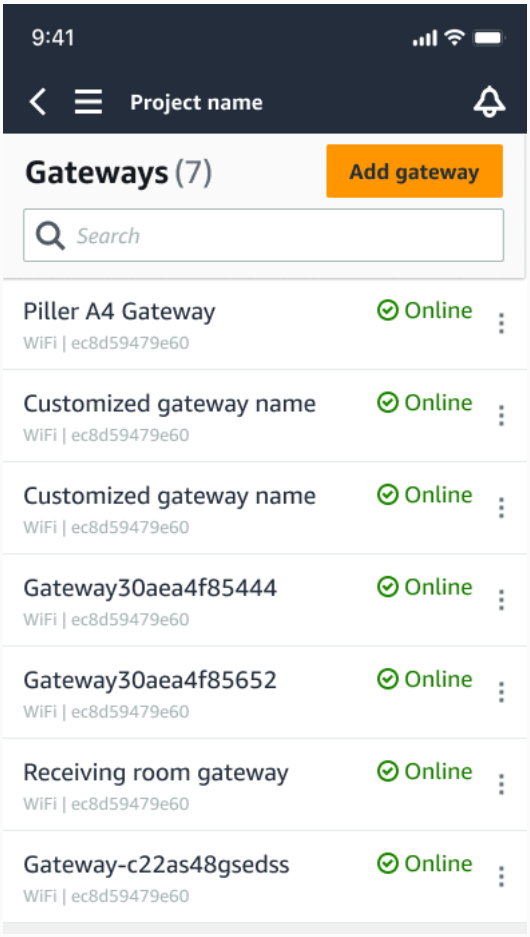
You can change the display name for your Wi-Fi gateway to find it faster. To edit a gateway name, open your web or mobile app and do the following.

**Topics**

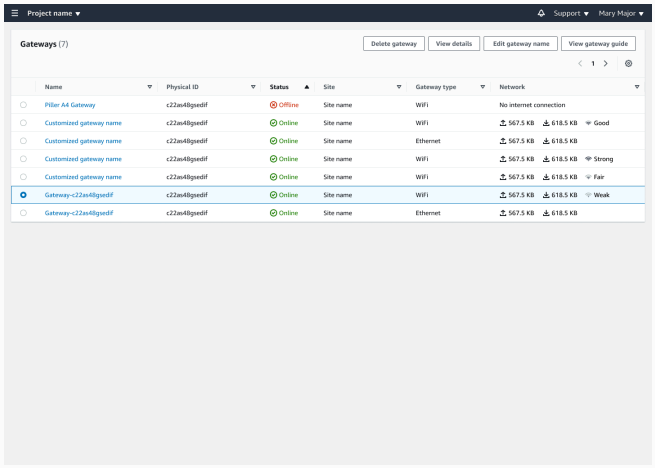

- To edit Wi-Fi gateway name


## To edit Wi-Fi gateway name

1. Select the gateway name you want to edit from the **Gateways** page.




Mobile app view

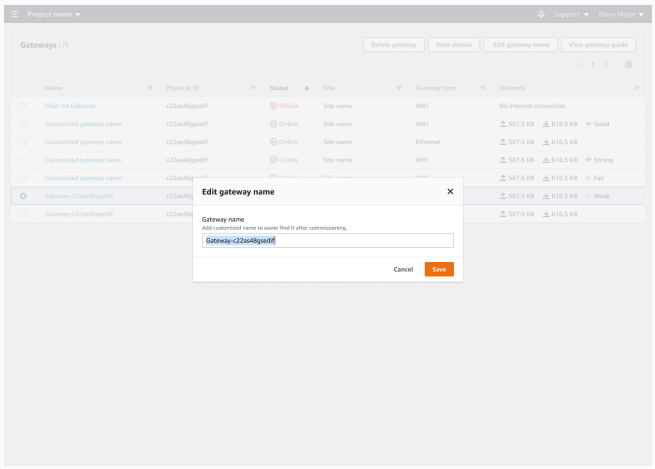



Web app view

2. A pop-up will appear prompting you to add a customized name for the gateway.




Mobile app view

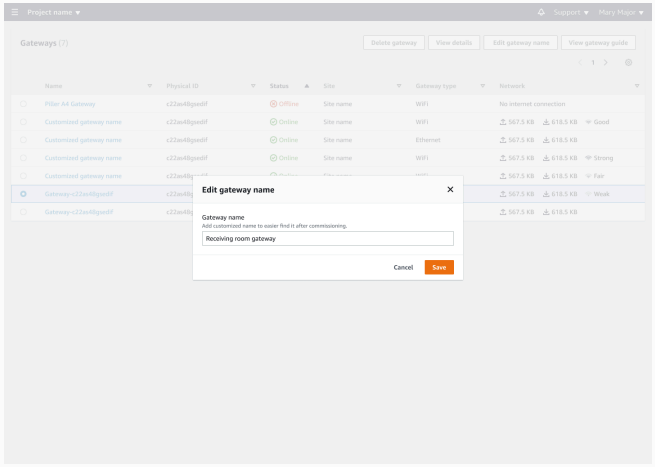



Web app view

3. Enter the new name for the gateway and choose **Save**.

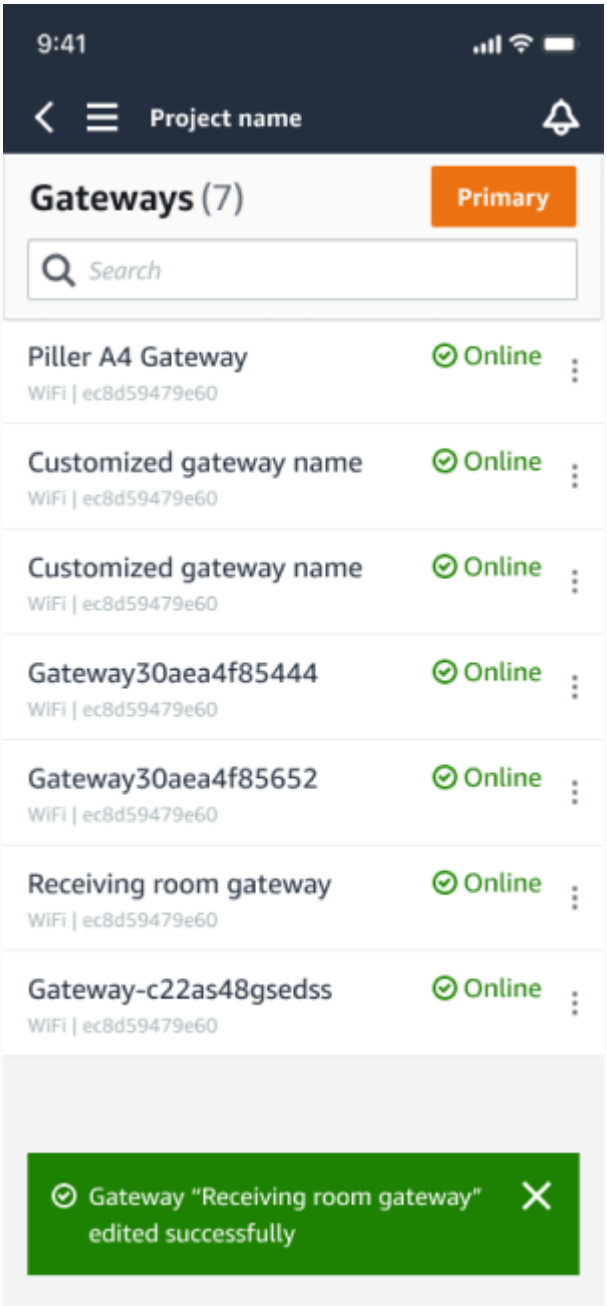



Mobile app view

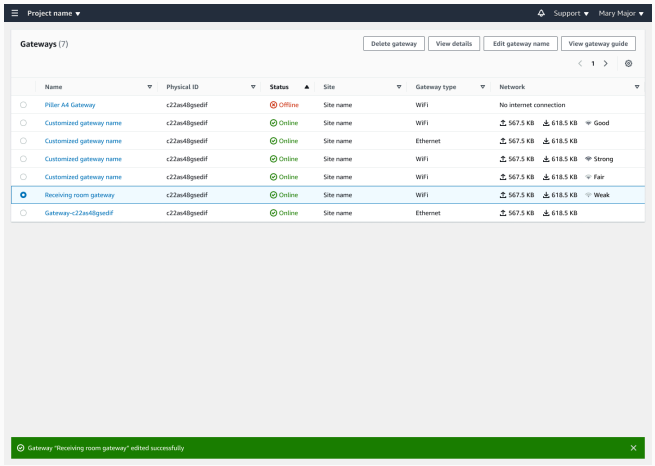



Web app view

4. You will see a success message confirming the new gateway name.




Mobile app view




Web app view

## Deleting a Wi-Fi gateway

Sensors need a gateway to relay their data to the AWS Cloud. Deleting a gateway might cause some sensors to lose their connection. Exercise caution before deleting a gateway.

When you delete a gateway, sensors switch their connection to another gateway that is within range, if there is one. Data transmission from the sensor continues uninterrupted. If no gateway is within range, data transmission is interrupted and the data might be lost.

**Topics**


- To delete a gateway using the mobile app
- To delete a gateway using the web app


### To delete a gateway using the mobile app

1. Navigate to the **Gateways** page.
2. Choose the vertical ellipses icon (



)

   next to the gateway that you want to delete.
3. Choose **Delete gateway**.
4. Choose **Delete** again.

### To delete a gateway using the web app

1. Navigate to the the section called “Viewing the list of gateways”.
2. Select the gateway from the table.
3. Choose **Delete gateway**.

## Retrieving MAC address details

To retrieve your Amazon Monitron gateway's Media Access Control (MAC) address, you can scan the QR code on the gateway device with your mobile phone. Amazon Monitron returns both the MAC address and gateway ID when you scan the QR code.

If you are an IT admin, you can use the scanned MAC address to ensure gateway devices are configured with the correct network settings before they are commissioned. If you are a technician commissioning gateways, you can use the scanned MAC address to troubleshoot any networking issues with your IT admin.

**Note**

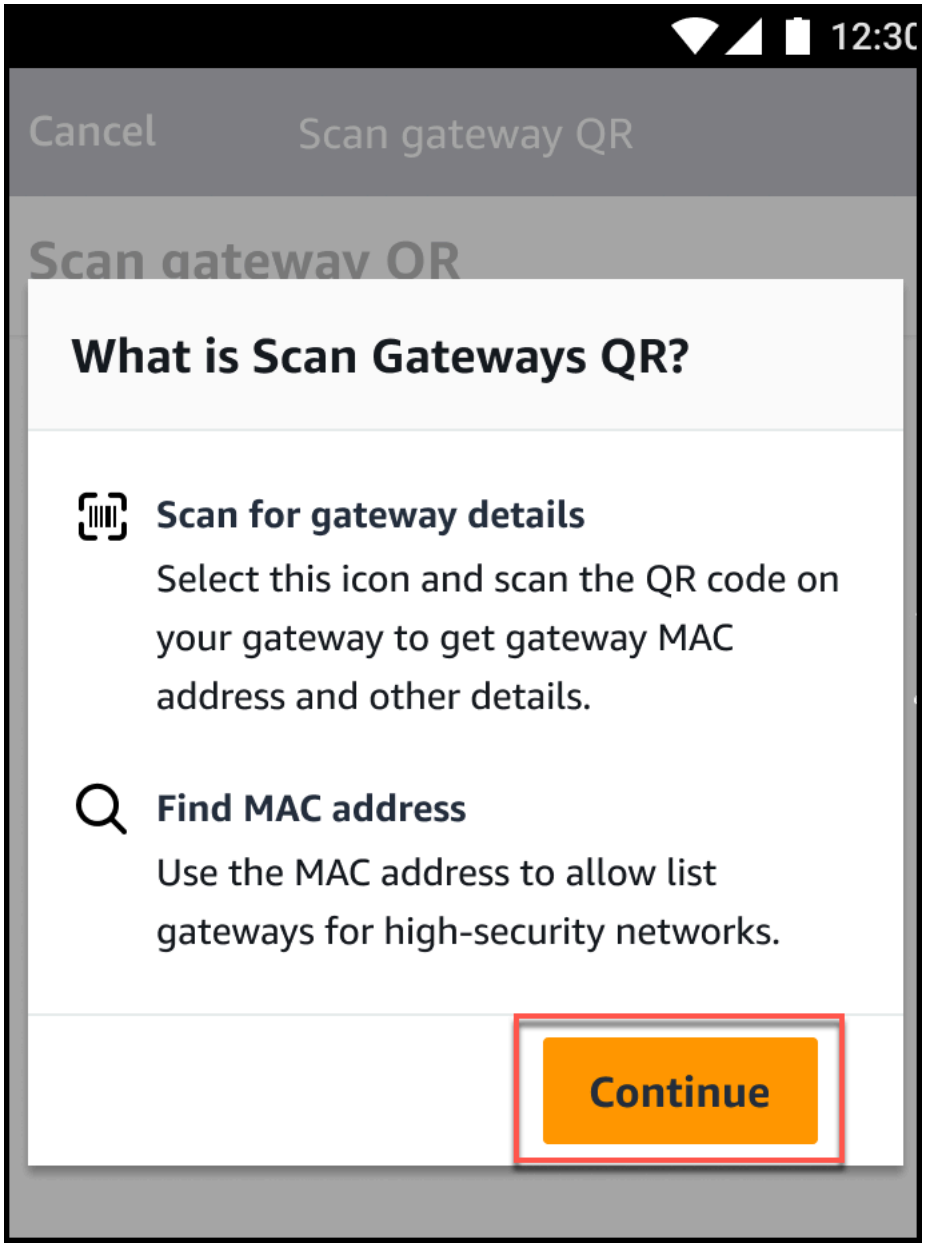
Retrieving MAC addresses by scanning QR codes is only supported for the Amazon Monitron mobile app.

The following procedure shows you how to retrieve your gateway device's MAC address.

1. Navigate to the **Gateways** page.
2. Select the scan icon.

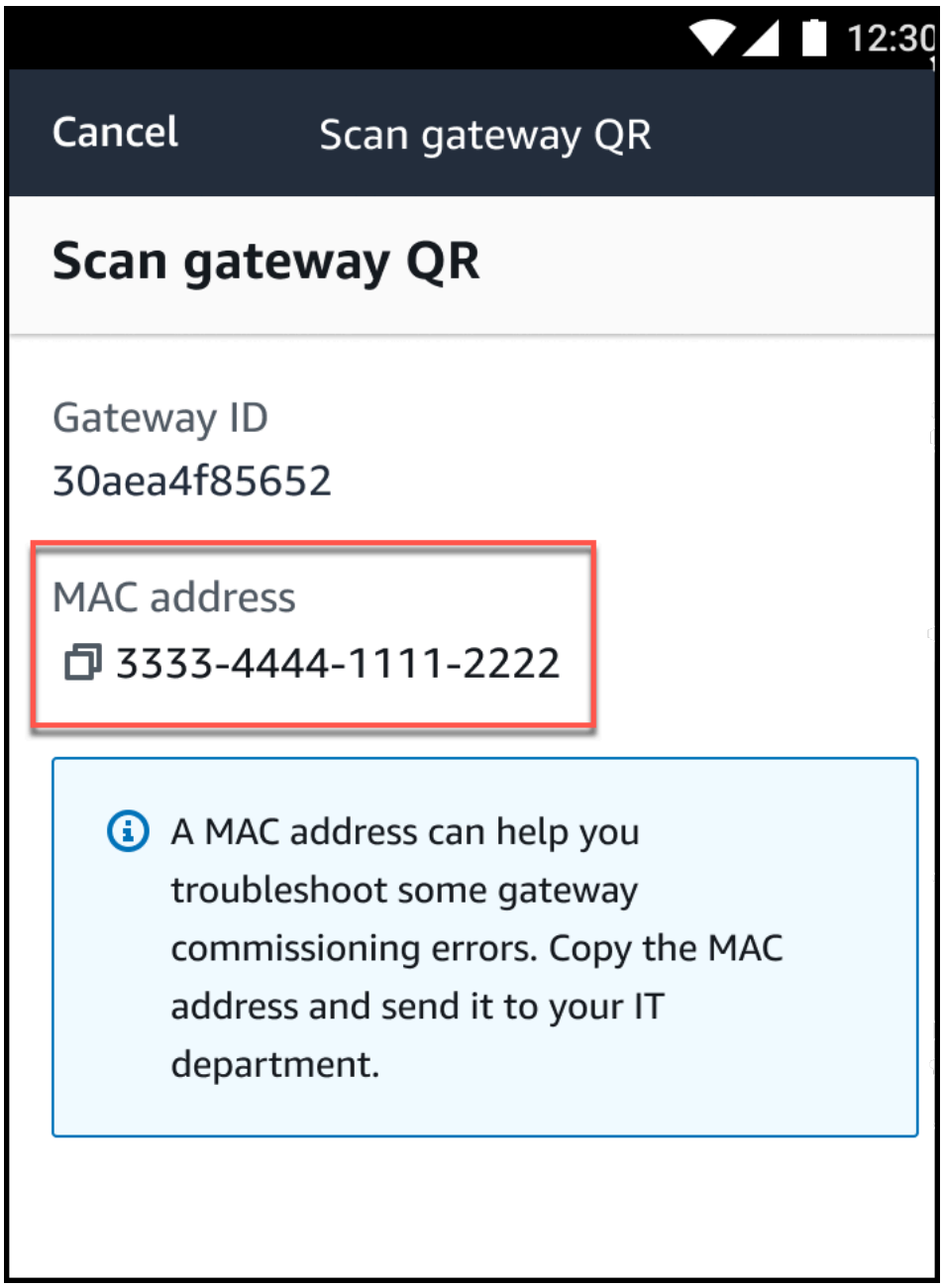



3. Amazon Monitron will display a message explaining what scanning a QR code will do. Select **Continue**.




4. On the **Scan QR Code** page, scan the gateway QR code using your mobile phone camera.

   When the scan successfully completes, Amazon Monitron displays the Gateway ID and MAC address on the **Scan QR Code** page in the mobile app.




You can also select the copy icon

( )

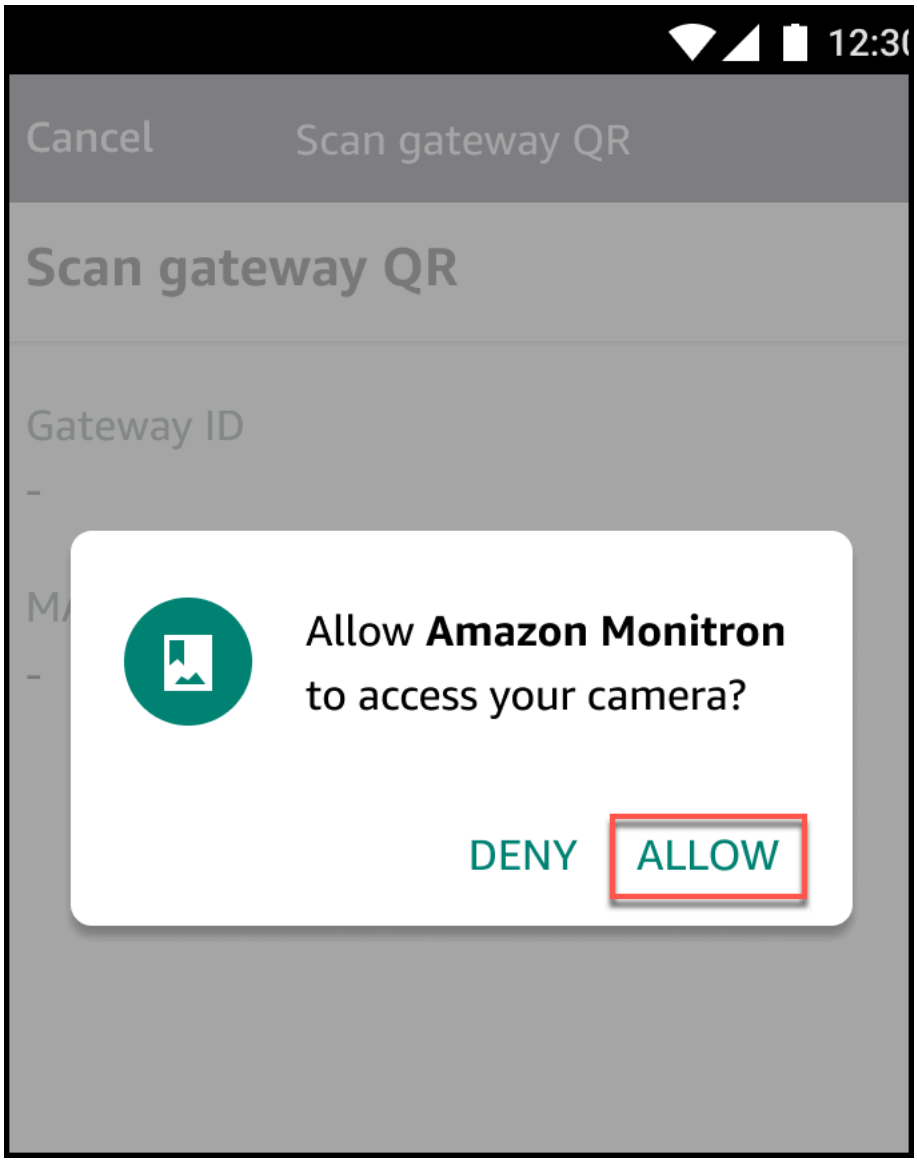
to copy the MAC address.

**Note**

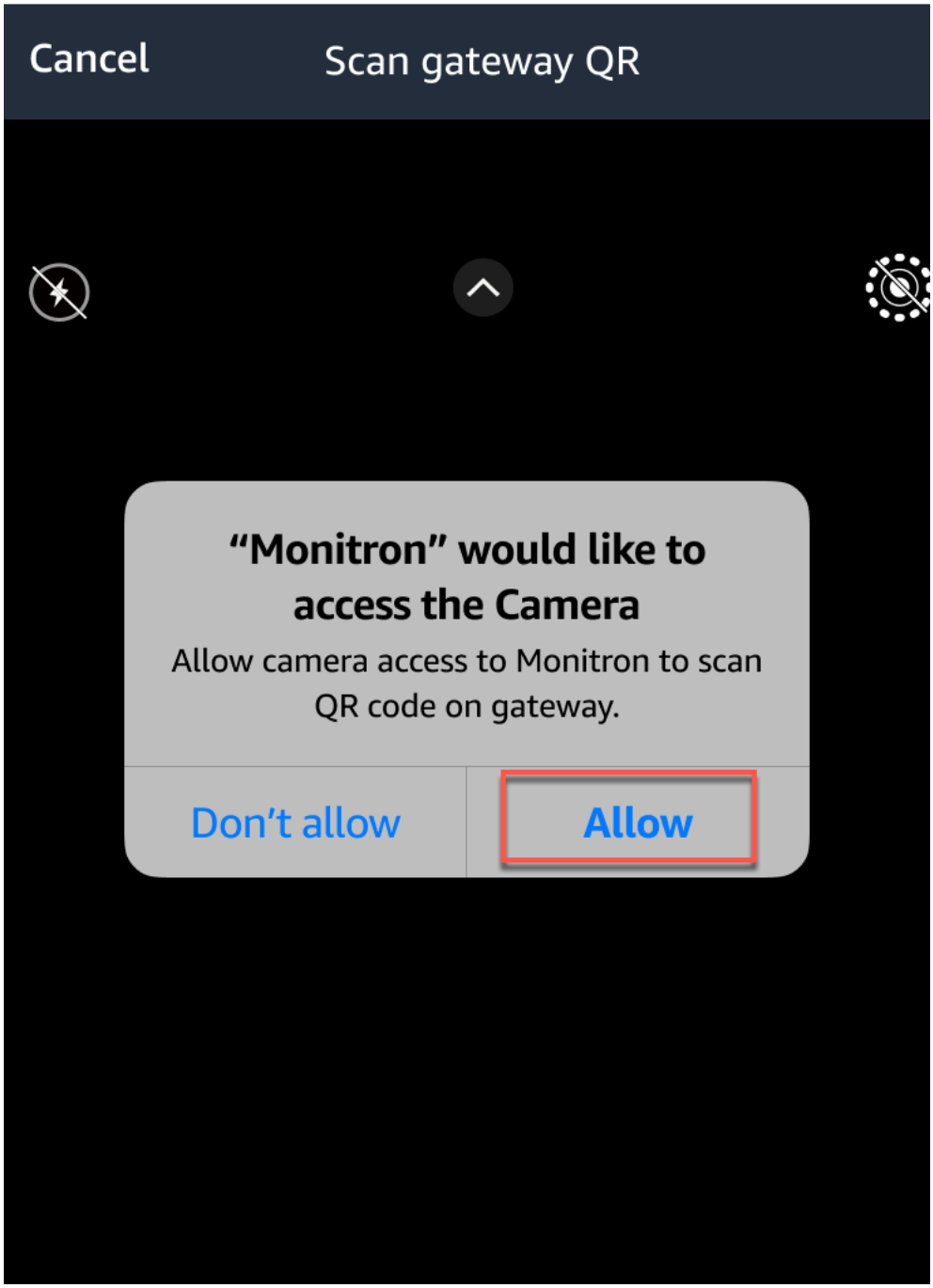
If not already enabled, Amazon Monitron may need permissions to access your camera to scan the QR code. These permissions must be enabled from the settings page

of your mobile device before you can successfully scan a device QR code. Amazon Monitron will prompt you to enable camera access during the scanning process if permissions haven't already been granted.

**On Android devices**




**On iOS devices**


Cancel
Scan gateway QR
"Monitron" would like to access the Camera
Allow camera access to Monitron to scan QR code on gateway.
Don't allow
Allow

# Assets

*Assets*, in Amazon Monitron, are the pieces of equipment on your factory floor. Typically, assets are individual machines, but they can also be sections of a larger piece of equipment, part of an industrial process, or any element of your manufacturing model.

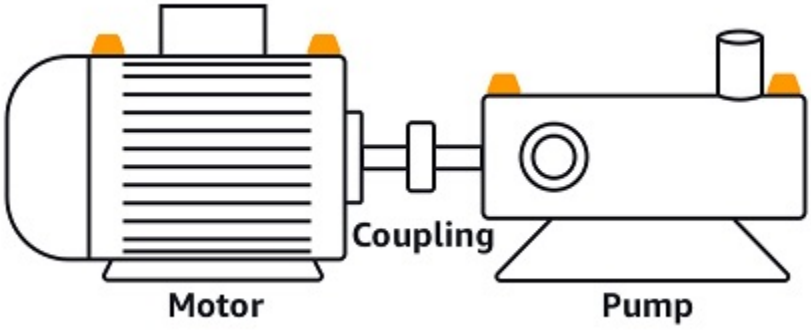
Amazon Monitron currently supports the following default ISO 20186 standard based machine classes:

- **Class I** – Individual parts of engines and machines, integrally connected to the complete machine in its normal operating condition, for example, production electrical motors of up to 15 kW.
- **Class II** – Medium-sized machines (typically electrical motors with 15 kW to 75 kW output) without special foundations, rigidly mounted engines or machines (up to 300 kW) on special foundations.
- **Class III** – Large prime-movers and other large machines with rotating masses mounted on rigid and heavy foundations that are relatively stiff in the direction of vibration.
- **Class IV** – Large prime-movers and other large machines with rotating masses mounted on rigid and heavy foundations that are relatively soft in the direction of vibration measurement, for example, turbo-generator sets and gas turbines with outputs greater than 10 MW.

You can also create custom classes for your assets to fit your use case better. For more information, see Creating custom classes.

An asset is also the basis for viewing the health of your machines. To monitor machine activity, you pair one or more sensors to the asset that you want to monitor. Each sensor gives you insight into how that part of the asset is functioning, and together they provide an overview of the entire asset. You can assign each sensor positioned on an asset can its own machine class.

The following diagram shows one asset, an electric motor pump set. It has four positions, each with a sensor, two on the motor and two on the pump. Each sensor collects data on the temperature and vibration levels of that specific position on the pump. Amazon Monitron then analyzes that data by comparing it to the baseline temperature and vibration levels of that position to determine when a change, or abnormality, occurs. When that happens, it sends a notification on the Amazon Monitron app.




This chapter explains how to manage your assets with Amazon Monitron, and how to pair them to the sensors that monitor their health.

**Topics**


- Creating asset classes
- Managing assets
- Viewing the list of assets
- Adding an asset
- Changing an asset name
- Moving an asset
- Deleting an asset


# Creating asset classes

Amazon Monitron offers four default machine classes based on ISO 20816 Standards. When you add an asset position, you can choose any of these four default classes as the machine class to use for detecting anomalies with your assets. Amazon Monitron then uses the assigned asset class to generate warnings and alarms on asset condition.

If your asset types don't align with the default machine classes offered by Amazon Monitron, you can create custom machine classes for your assets. Once created, these custom classes are available to be assigned to all asset positions in a project.

**Important**

Custom classes can only be created using the Amazon Monitron web app. Only the Amazon Monitron project admin can create, update, and delete custom asset classes.

**Topics**

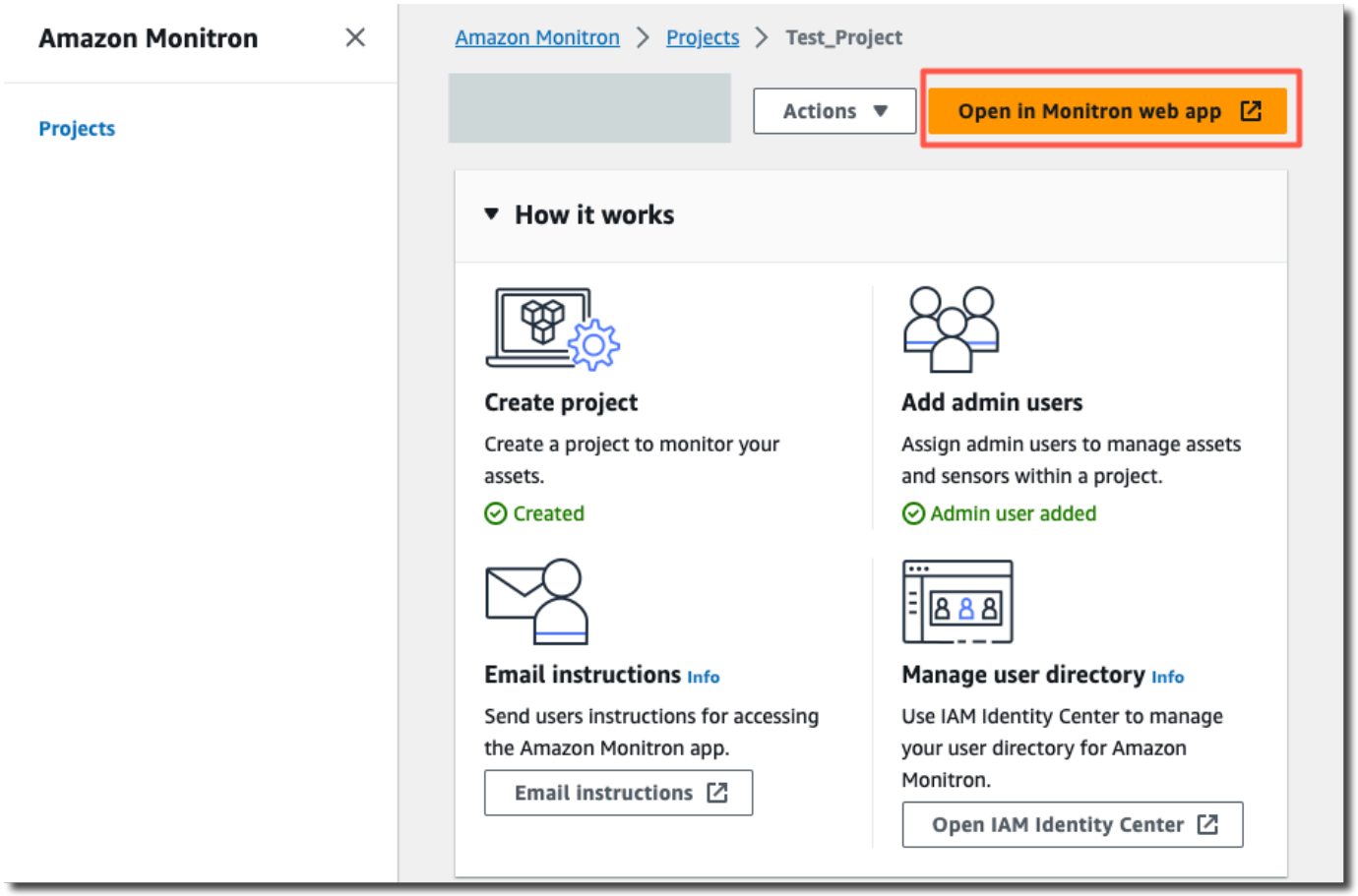

- Creating a custom class
- Updating a custom class
- Deleting a custom class


# Creating a custom class

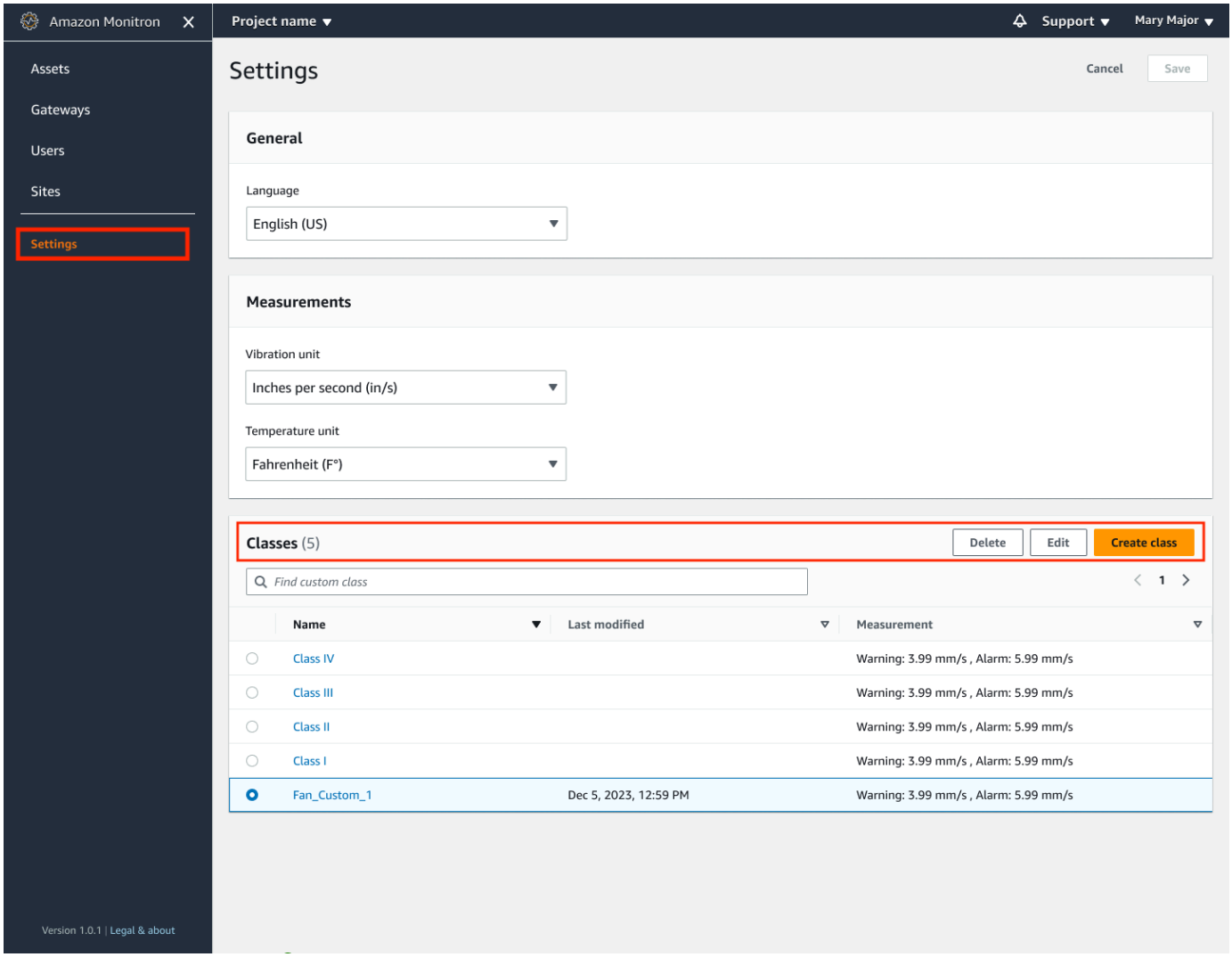
**To create a custom class**

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron.
2. Choose **Create project**.
3. If you're creating a project for the first time, follow the steps outlined in Creating a project.

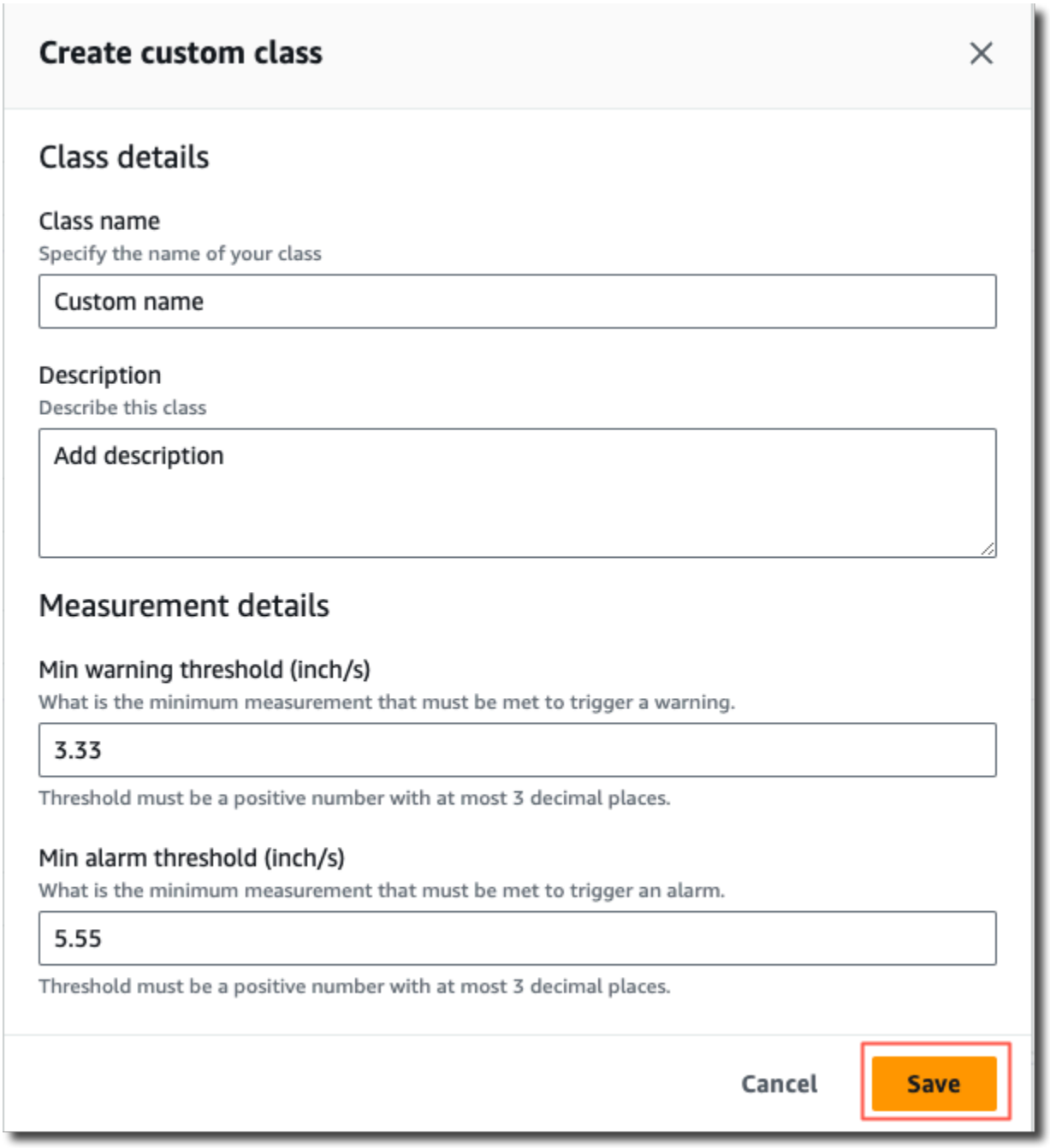
   If you're choosing an existing project, from the left navigation menu, select **Projects**, and then select the project you want to create custom classes for.
4. From the project details page, choose **Open in Amazon Monitron web app**.




5. In the Amazon Monitron web app page, from the left navigation pane, choose **Settings**.




6. Then, select from **Classes**, select **Create class**.




7. On the **Create custom class** page, do the following:

   - In **Class details**, for **Class name** – A name for your custom class.
   - **Description** – A description for your custom machine class.
   - In **Measurement details**, for **Measurement thresholds** – Custom measurement thresholds for your assets.

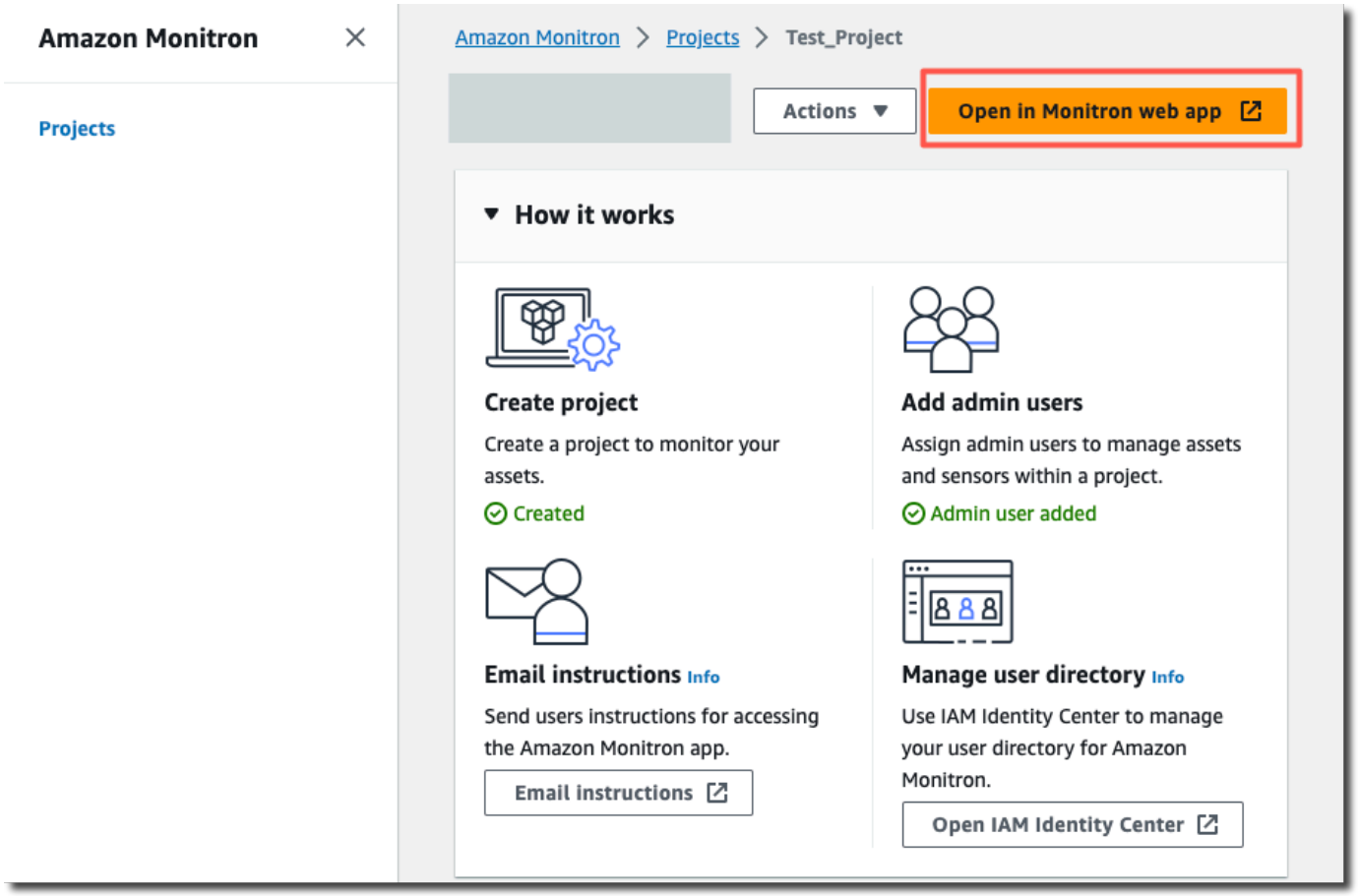
8. Choose **Save**.

# Updating a custom class

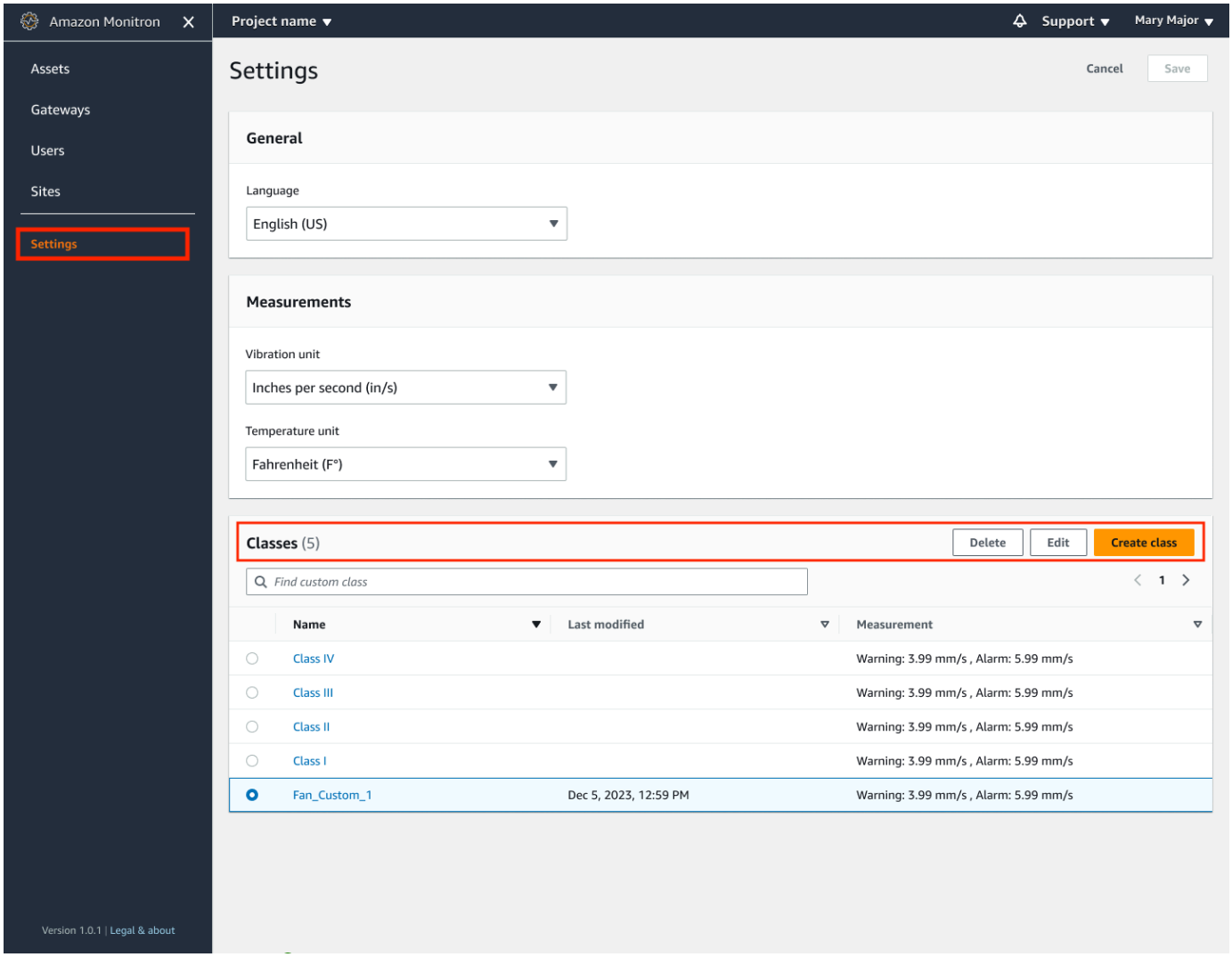
### To update a custom class

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron.
2. Choose **Create project**.
3. If you're creating a project for the first time, follow the steps outlined in Creating a project.

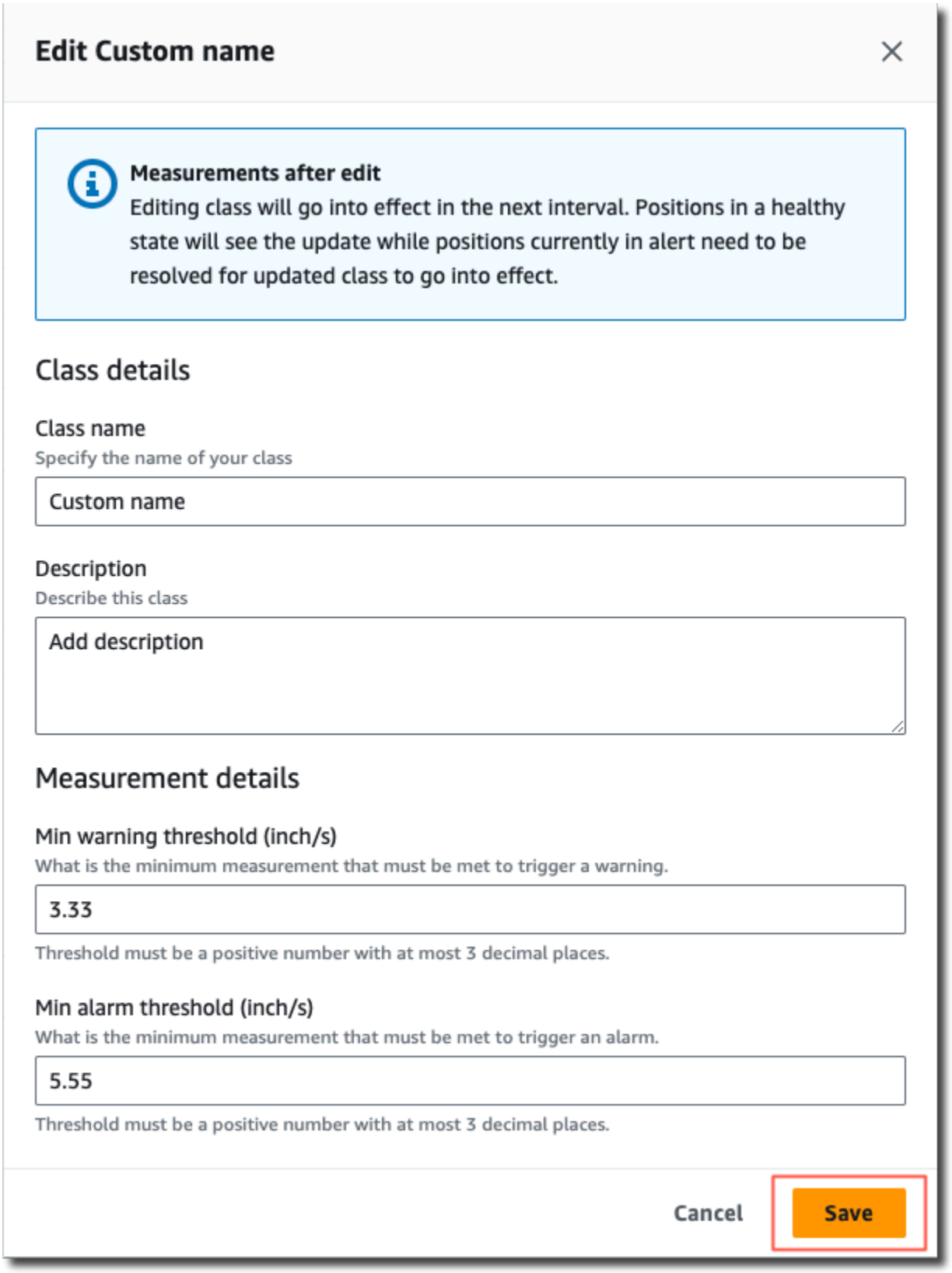
   If you're choosing an existing project, from the left navigation menu, select **Projects**, and then select the project you want to create custom classes for.
4. From the project details page, choose **Open in Amazon Monitron web app**.




5. In the Amazon Monitron web app page, from the left navigation pane, choose **Settings**.




6. Then, from **Classes**, select the class you would like to update, and select **Edit**.




7. On the **Edit class** page, do the following:

- In **Class details**, for **Class name** – A name for your custom class.
- **Description** – A description for your custom machine class.
- In **Measurement details**, for **Measurement thresholds** – Custom measurement thresholds for your assets.

8. Choose **Save**.

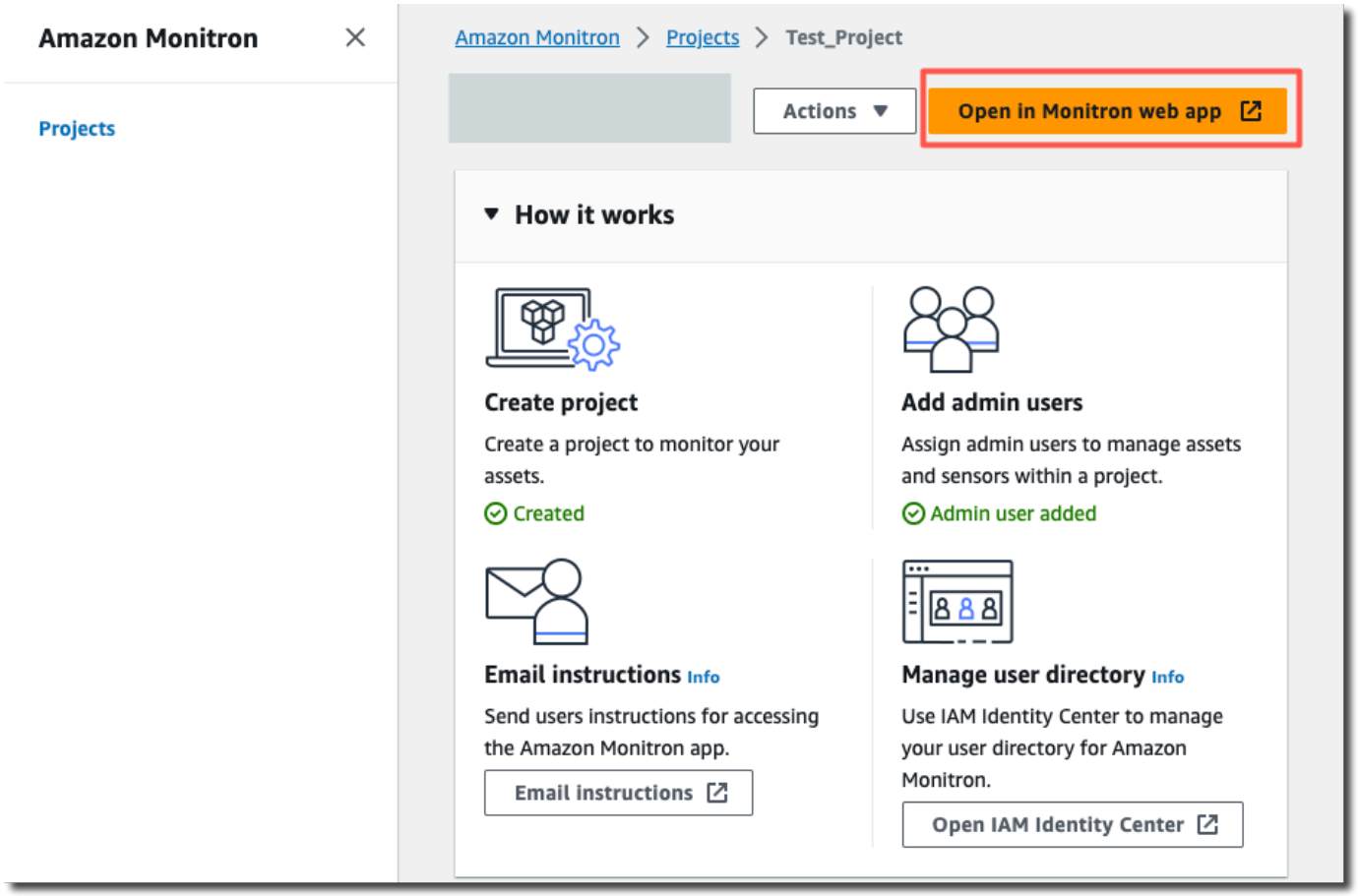
> **Note**
>
> The edited machine class will go into effect during the next Amazon Monitron measurement interval.

## Deleting a custom class

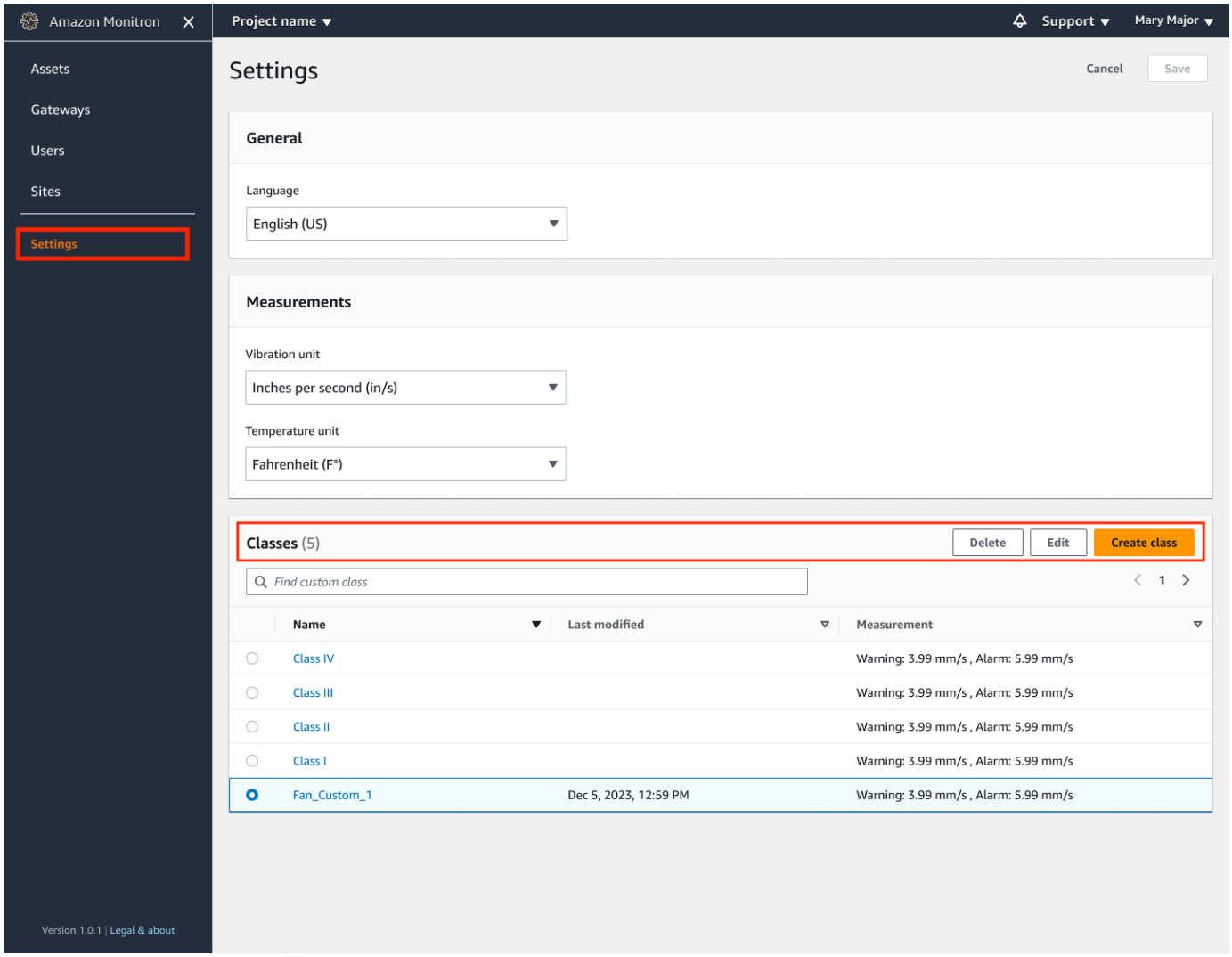
**To delete a custom class**

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron.
2. Choose **Create project**.
3. If you're creating a project for the first time, follow the steps outlined in Creating a project.

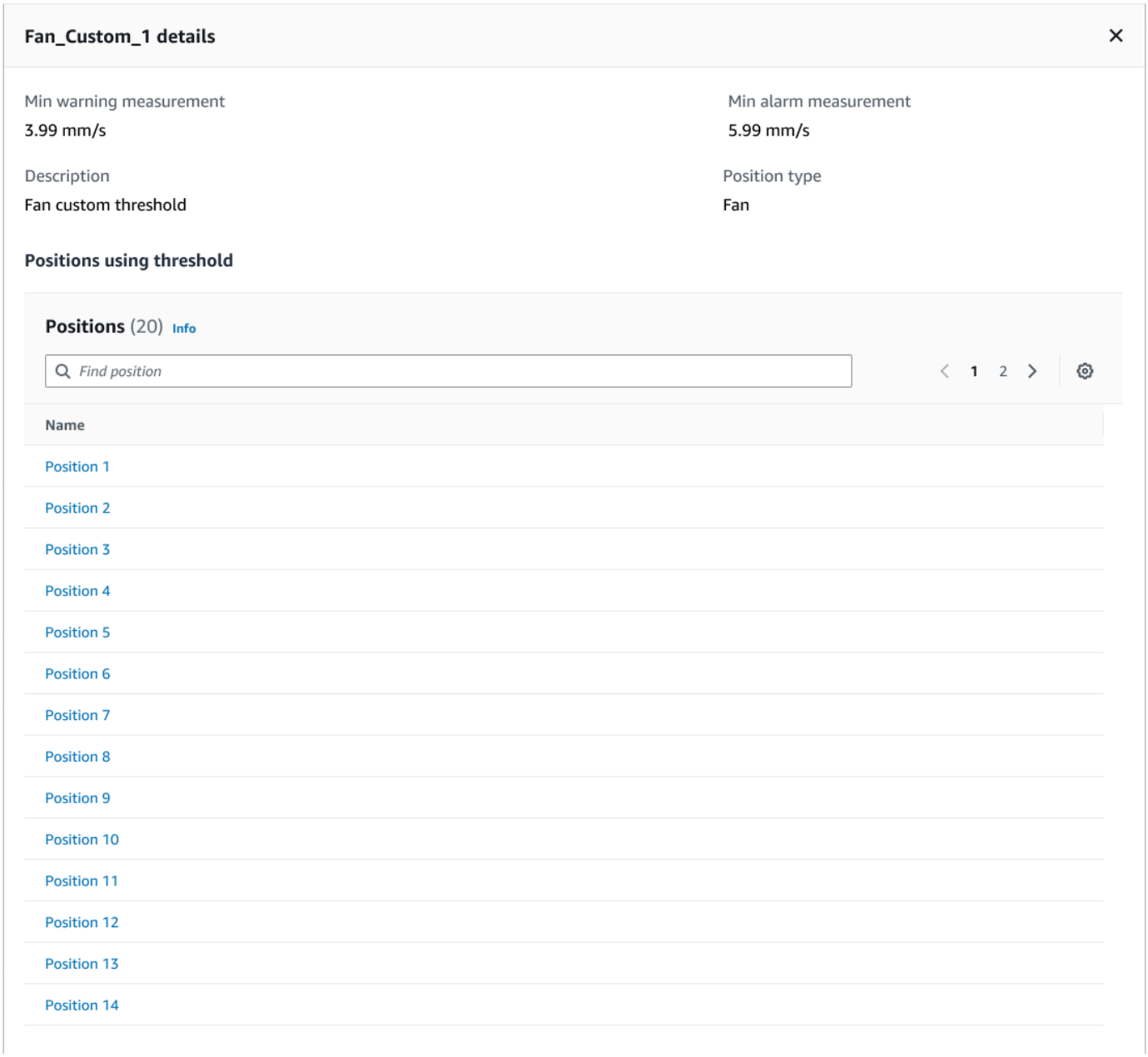
   If you're choosing an existing project, from the left navigation menu, select **Projects**, and then select the project you want to create custom classes for.
4. From the project details page, choose **Open in Amazon Monitron web app**.




5. In the Amazon Monitron web app page, from the left navigation pane, choose **Settings**.




6. Then, from **Classes**, select the machine class you would like to delete, and select **Delete**.




**Important**

You can't delete custom machine classes that are currently in use by one or more positions. You will be prompted with a list of positions currently using the machine class and you will need to update these positions to a different machine class before deleting the machine class attached to these positions.

7. To confirm deletion, type **`delete`**, and then select **Save**.

# Managing assets

Use the Amazon Monitron app to list all the assets in your site or project.




**Single axis vibration - Vrms**
(10-1000Hz) (mm/s)



# Viewing the list of assets

The **Assets** page displays the list of assets. The **Assets** page is the app's main page. The main page is the page you see when you open the app. To return to the **Assets** page from another page in the app, use this procedure.

**Topics**


- To open the Assets list


## To open the Assets list

1. Choose the menu icon (☰).




2. Choose **Assets**.

# Adding an asset

After you set up your site or project, add the assets that your sensors will monitor.

> **Note**
>
> After you create an asset, you can change only its name.

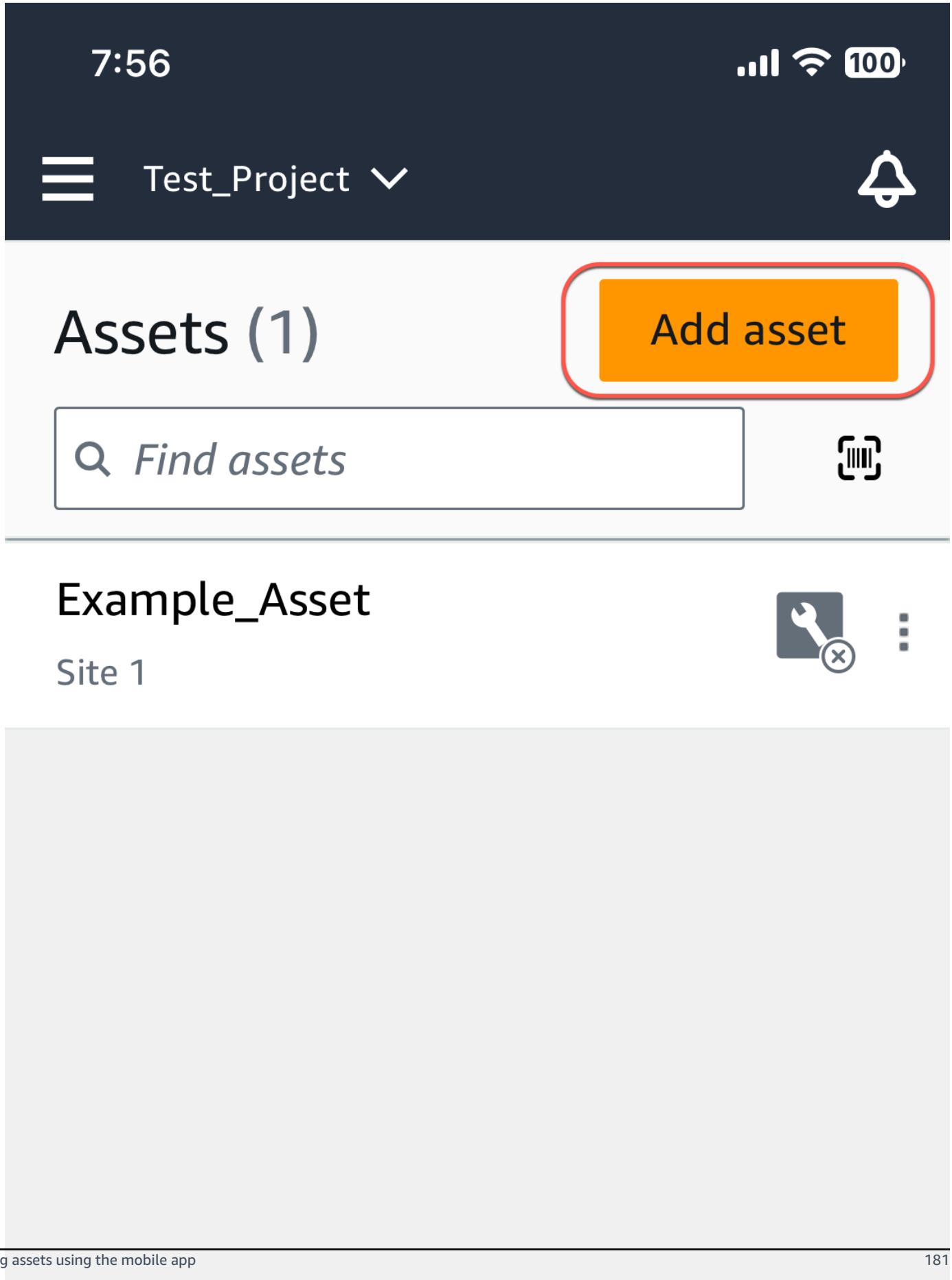
**Topics**


- Adding assets using the mobile app
- Adding assets using the web app


## Adding assets using the mobile app

### To add an asset using the mobile app

1. Sign in to your mobile app and select the project you want to add an asset to.

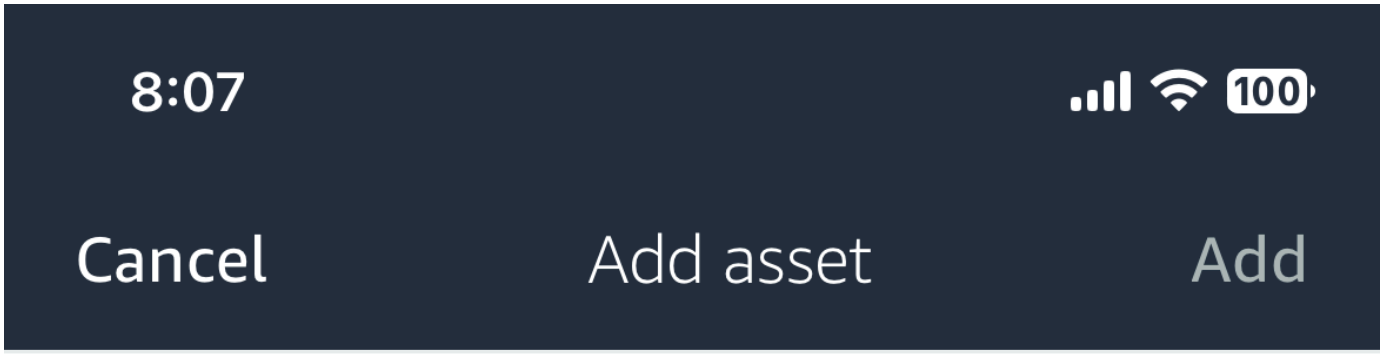

7:56
100
Test_Project
Assets (1)
Add asset
Find assets
Example_Asset
Site 1

2. Make sure you're on the correct site your project that you want to add the asset to. The project or site name indicates that you are at that level in the app.




   For more information about changing from site level to project level and vice versa, see Navigating between projects and sites in the mobile app.

3. From the **Assets** page, choose **Add asset**.
4. On the **Add asset** page, for **Asset name**, add a name for the asset you want to create and then select **Add**.




You are adding this asset to the project. We recommend you add it to a site. Once you add an asset you can't move it.
Learn more

## Asset name

Name for the asset to be monitored.

*Example: Pump*

Maximum 60 characters.

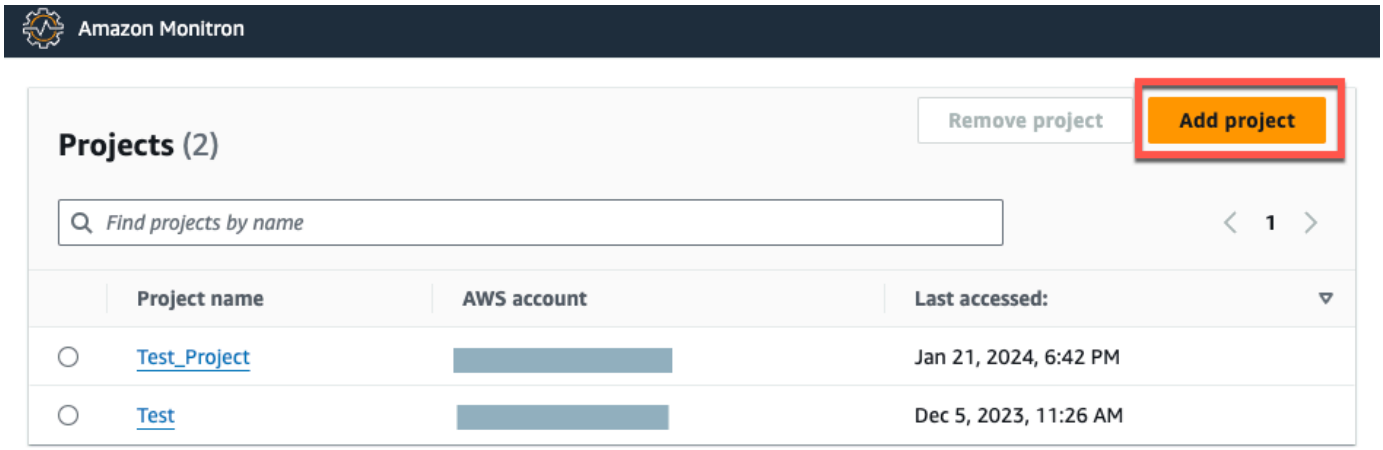
> **Note**
>
> If you have a QR code identifying the asset name, you can scan it by selecting the QR code.

When you've added your first asset, it's displayed on the **Assets list** page.

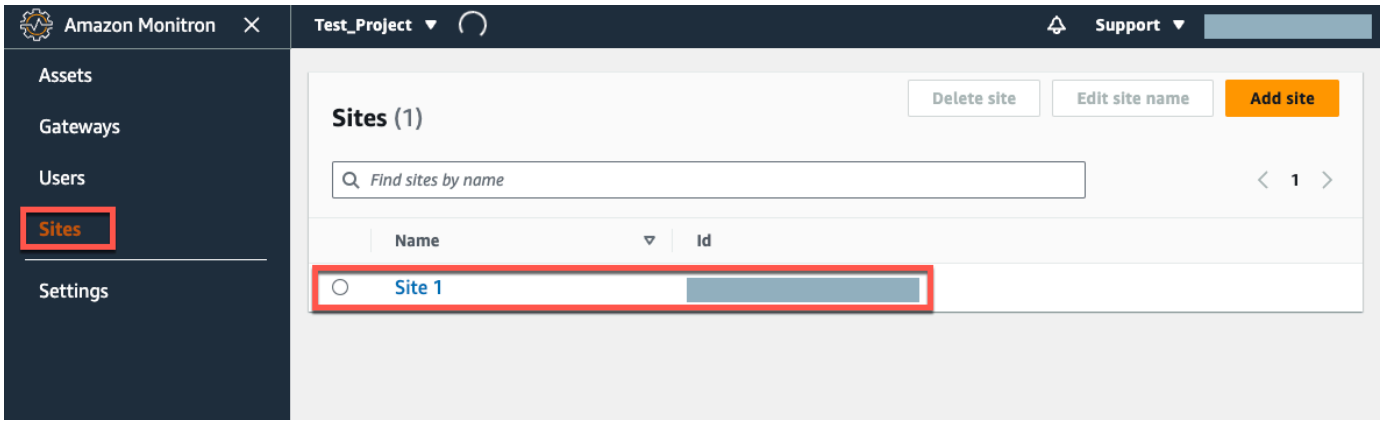
## Adding assets using the web app

### To add an asset using the web app

1. Sign in to your web app and select the project you want to add an asset to.

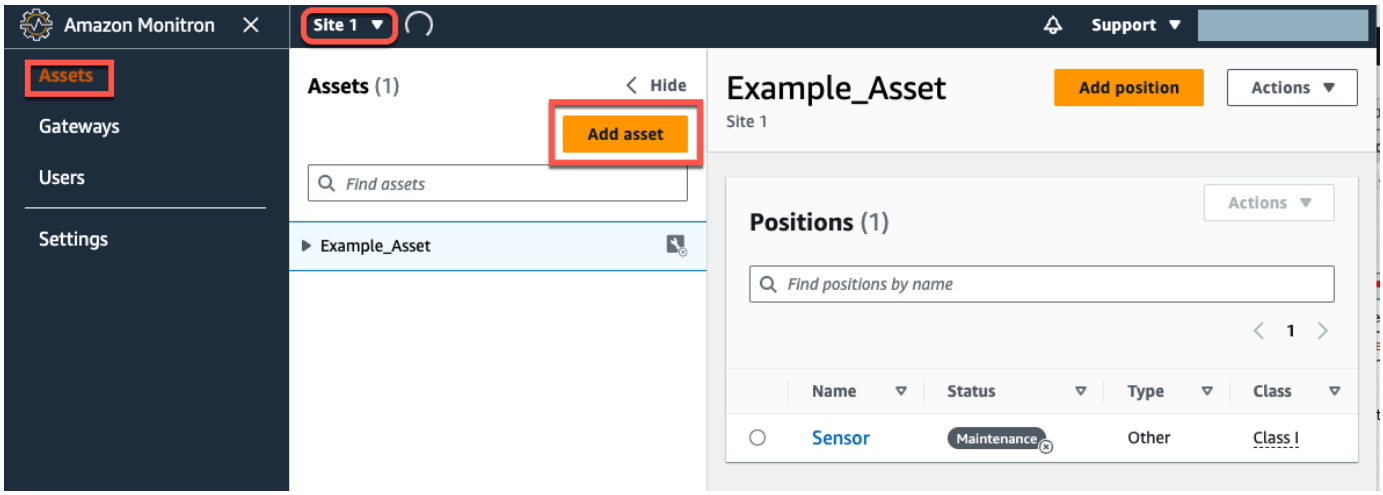



2. From the left navigation menu, choose **Sites**, and then select the site you want to the asset to.

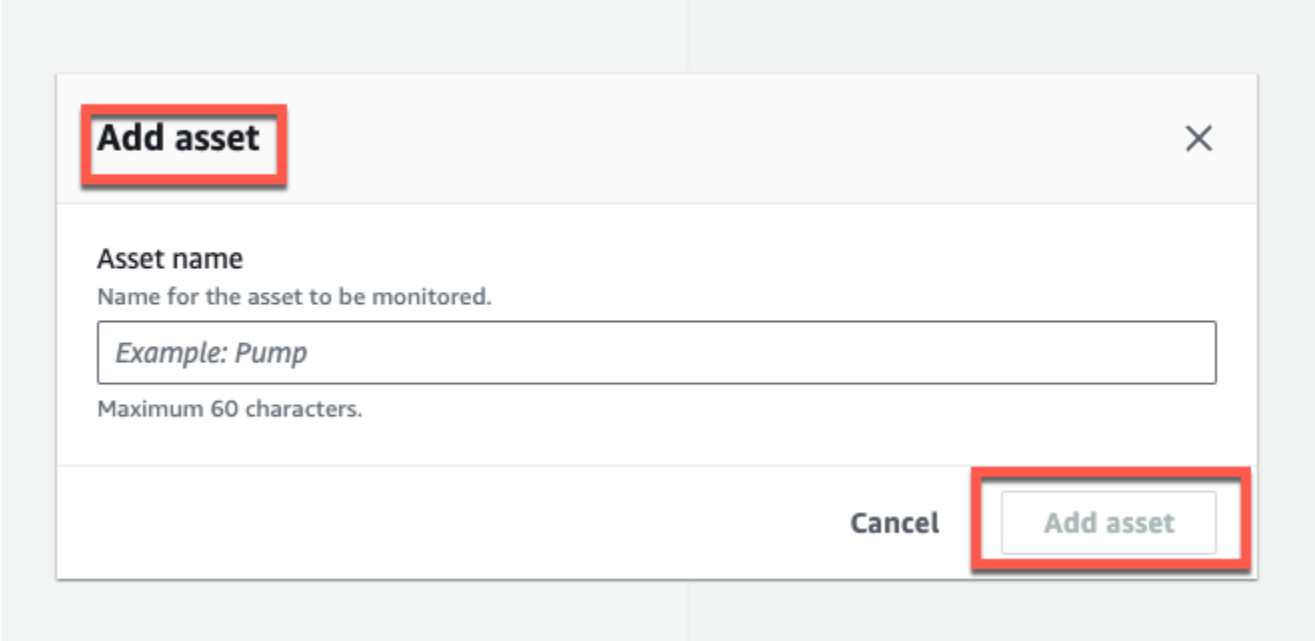


> **Note**
>
> You can also add the asset directly to a project.

3. From the **Assets** page, choose **Add asset**.




4. On the **Add asset** page, for **Asset name**, add a name for the asset you want to create and then select **Add asset**.




When you've added your first asset, it's displayed on the **Assets list** page.

# Changing an asset name

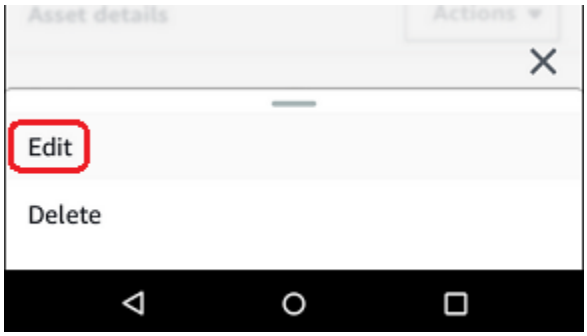
After you add an asset, you can change both its name and machine class.

**Topics**


- To change an asset's name in the mobile app
- To change an asset's name in the web app


## To change an asset's name in the mobile app

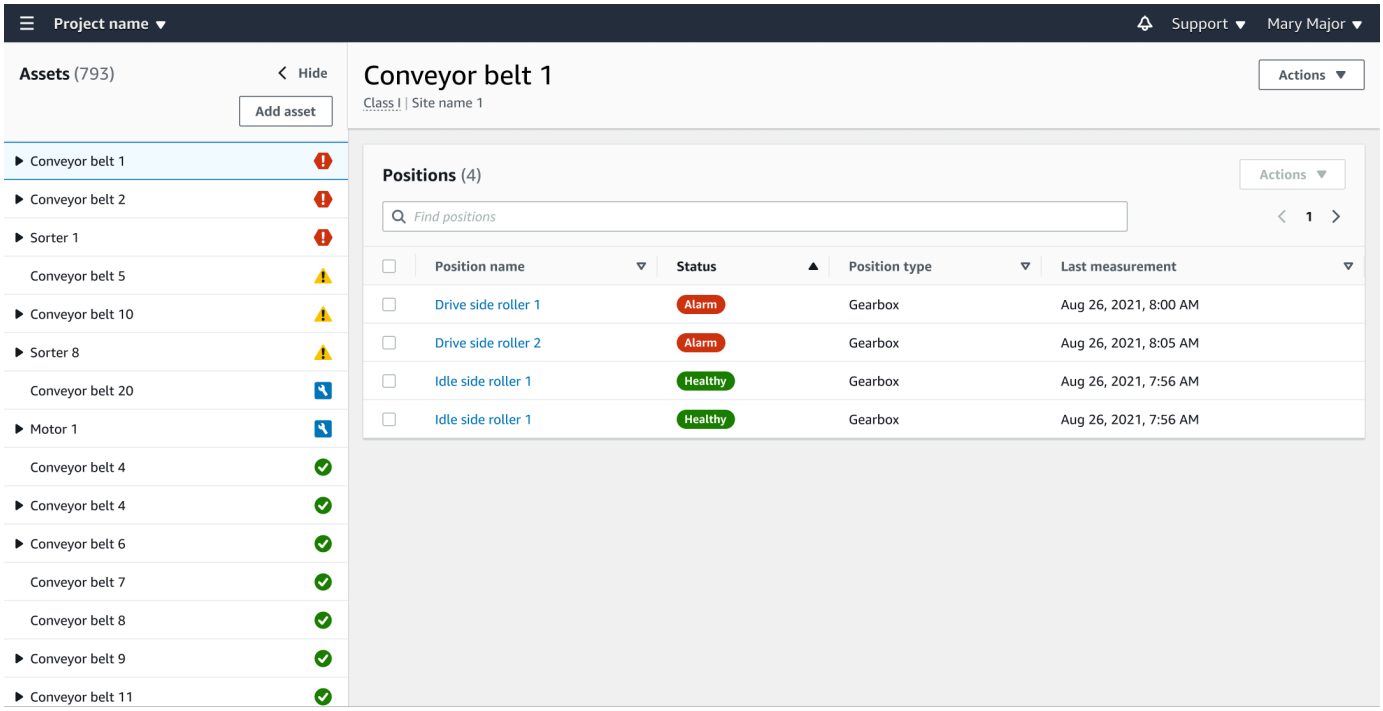
1. From the app's main menu, choose **Assets**.
2. For **Asset details**, choose **Actions**.
3. Choose **Edit asset**.




4. Enter a new name.
5. Choose **Save**.

## To change an asset's name in the web app

1. Select the asset.
2. In the large tab, choose the **Actions** button from the right end of the row containing the asset name.




3. Enter a new name.
4. Choose **Save**.

# Moving an asset

Assets in a project can be grouped under various sites. If you need to re-organize your assets and sites, you can choose to move an asset from one site to another without having to create each asset again.

> **Note**
>
> You can move assets from the project level to the site level. However, you can't move assets from the site level to the project level.

Once an asset is moved, it continues generating notifications in its new destination site. All positions associated with the asset move to the new site. However, it stops generating notifications and being visible to users in its older source site.

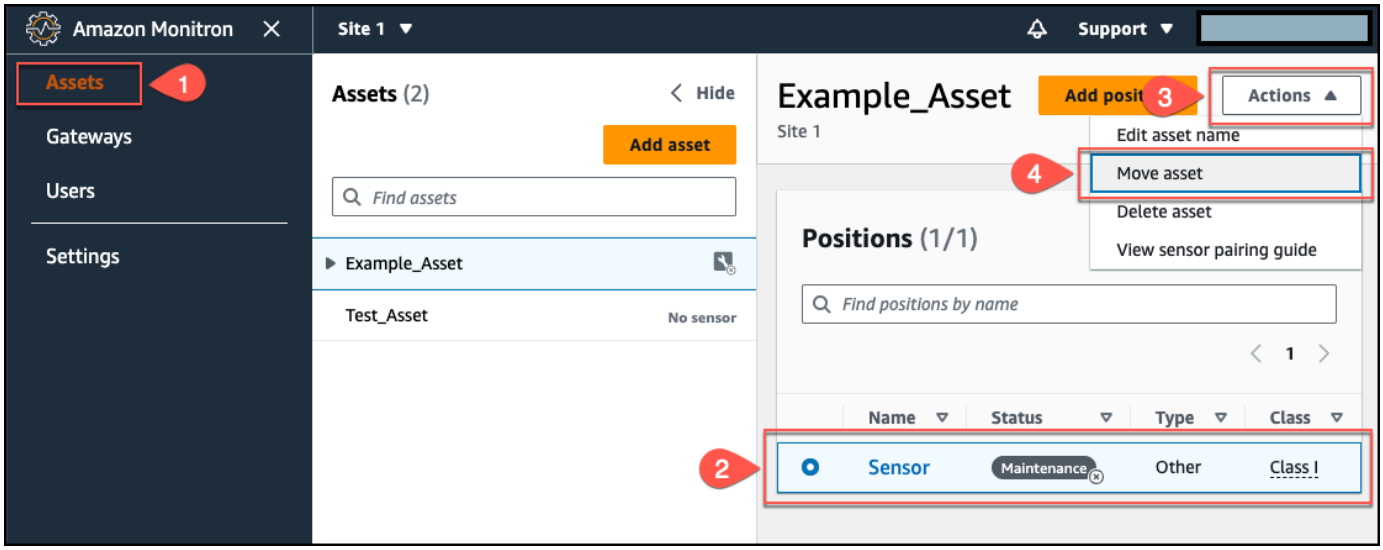
> **Important**
>
> Only an user with admin access to *both* source and destination sites can move an asset.

**Topics**

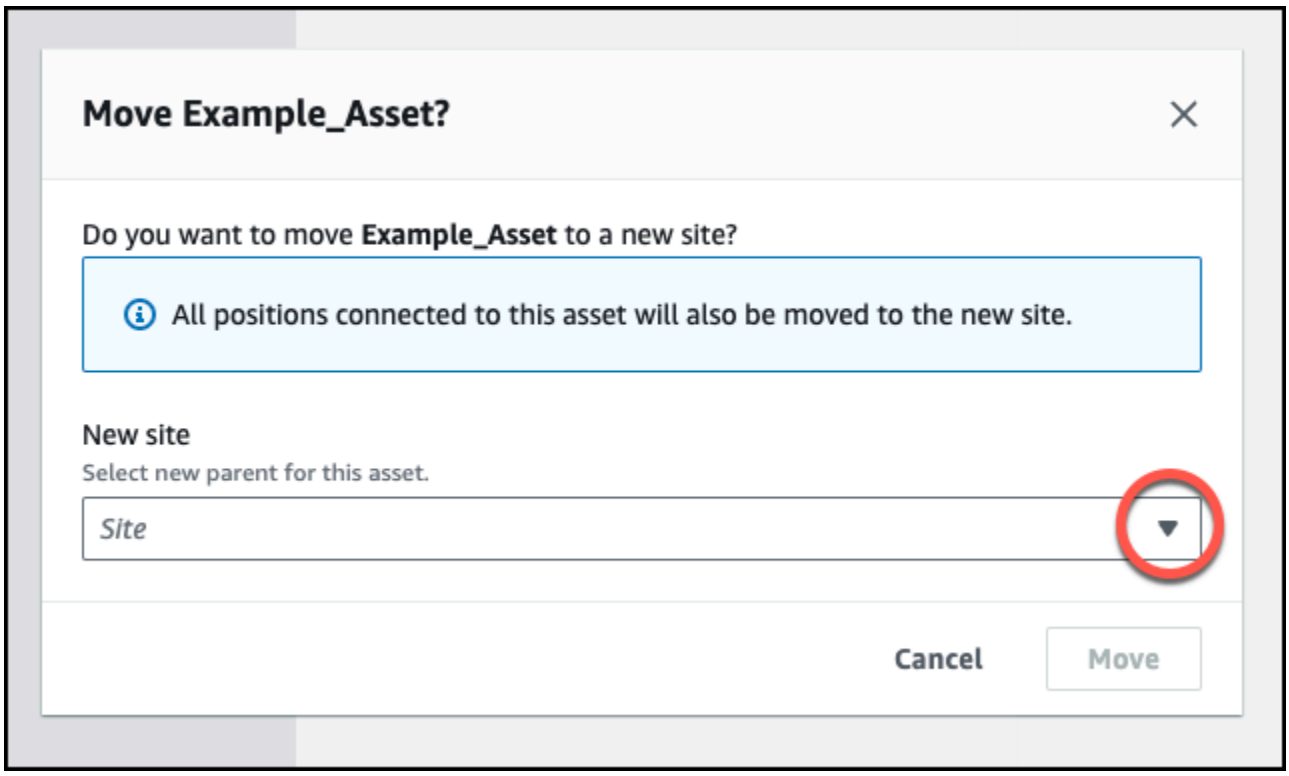

- To move an asset on the web app
- To move an asset on the mobile app

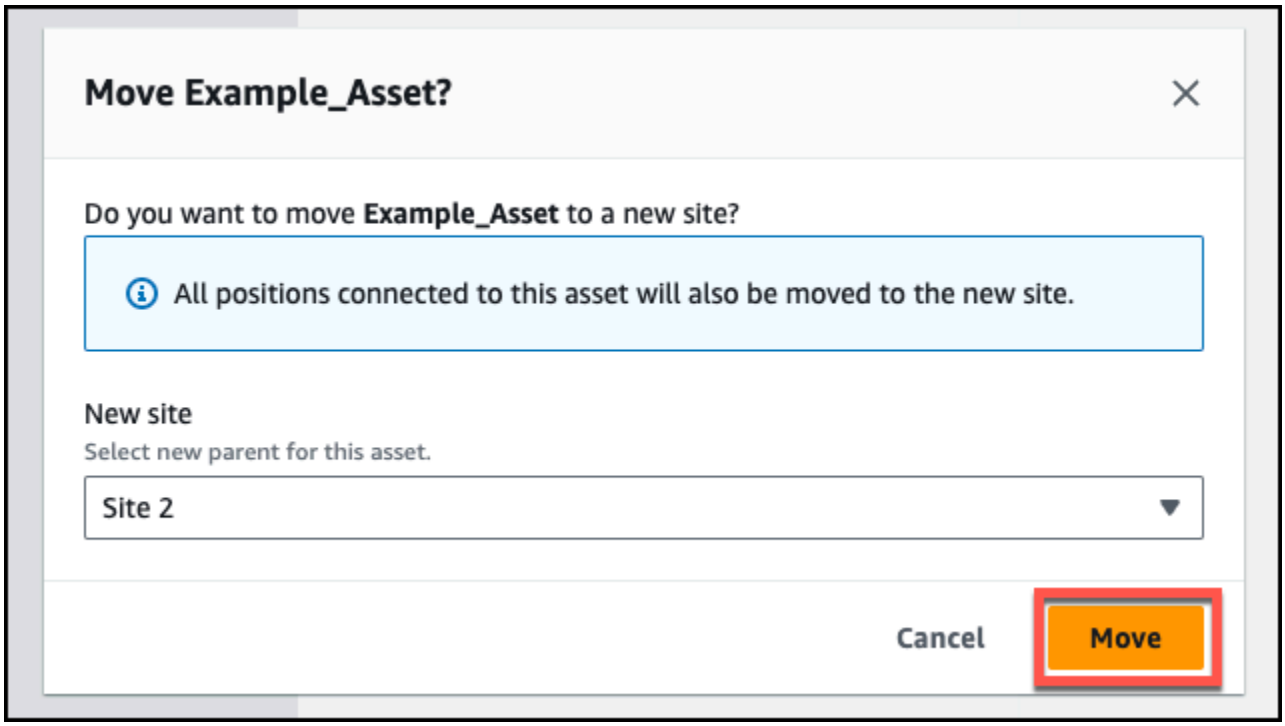

## To move an asset on the web app

1. From the web app's main menu, choose **Assets**.
2. Choose the asset that you want to move.
3. From the asset menu, choose **Actions**, and then choose **Move asset**.




4. From the dialog box that opens, select a site to move your asset to from the **New site** dropdown menu, and then select **Move**.

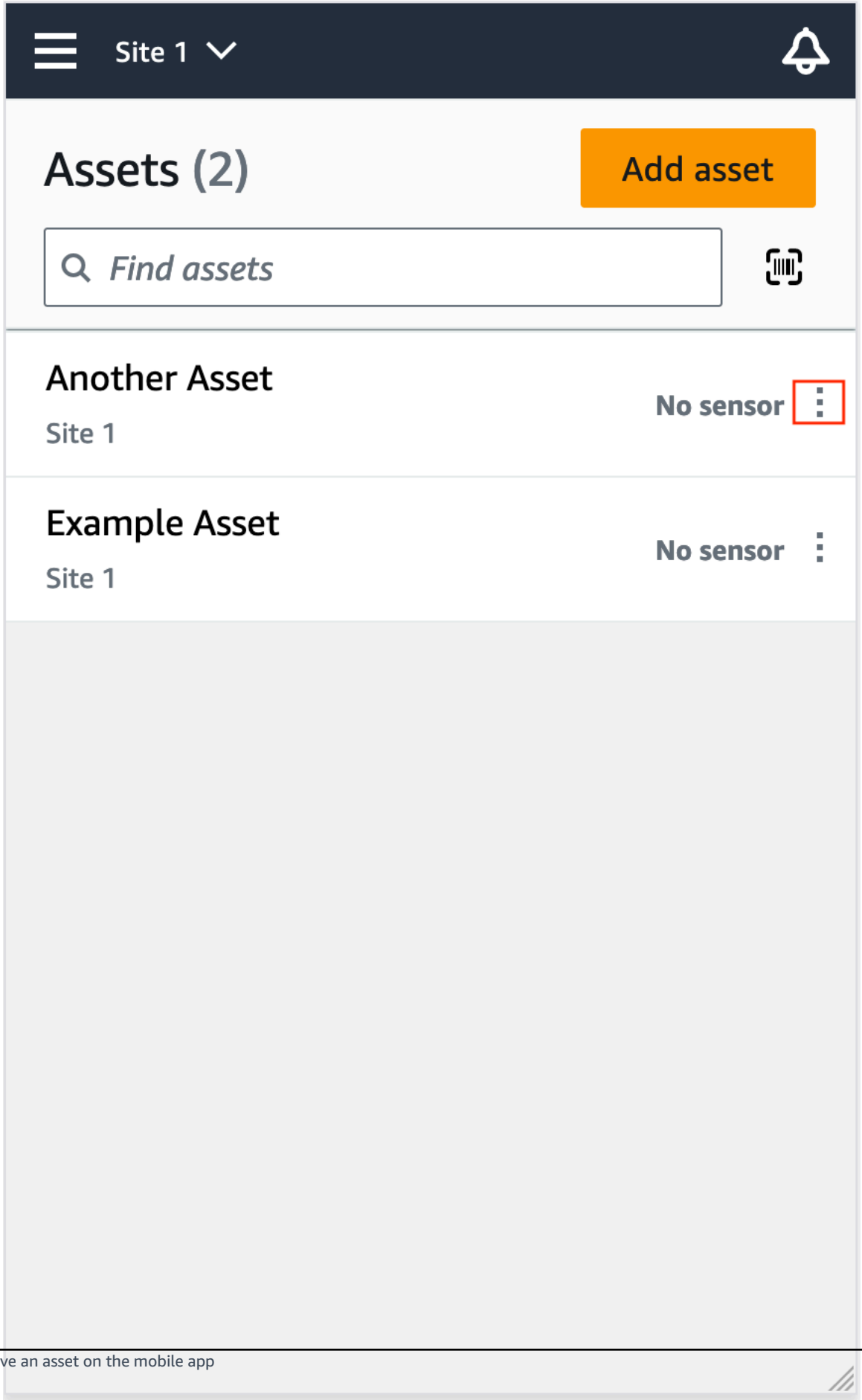


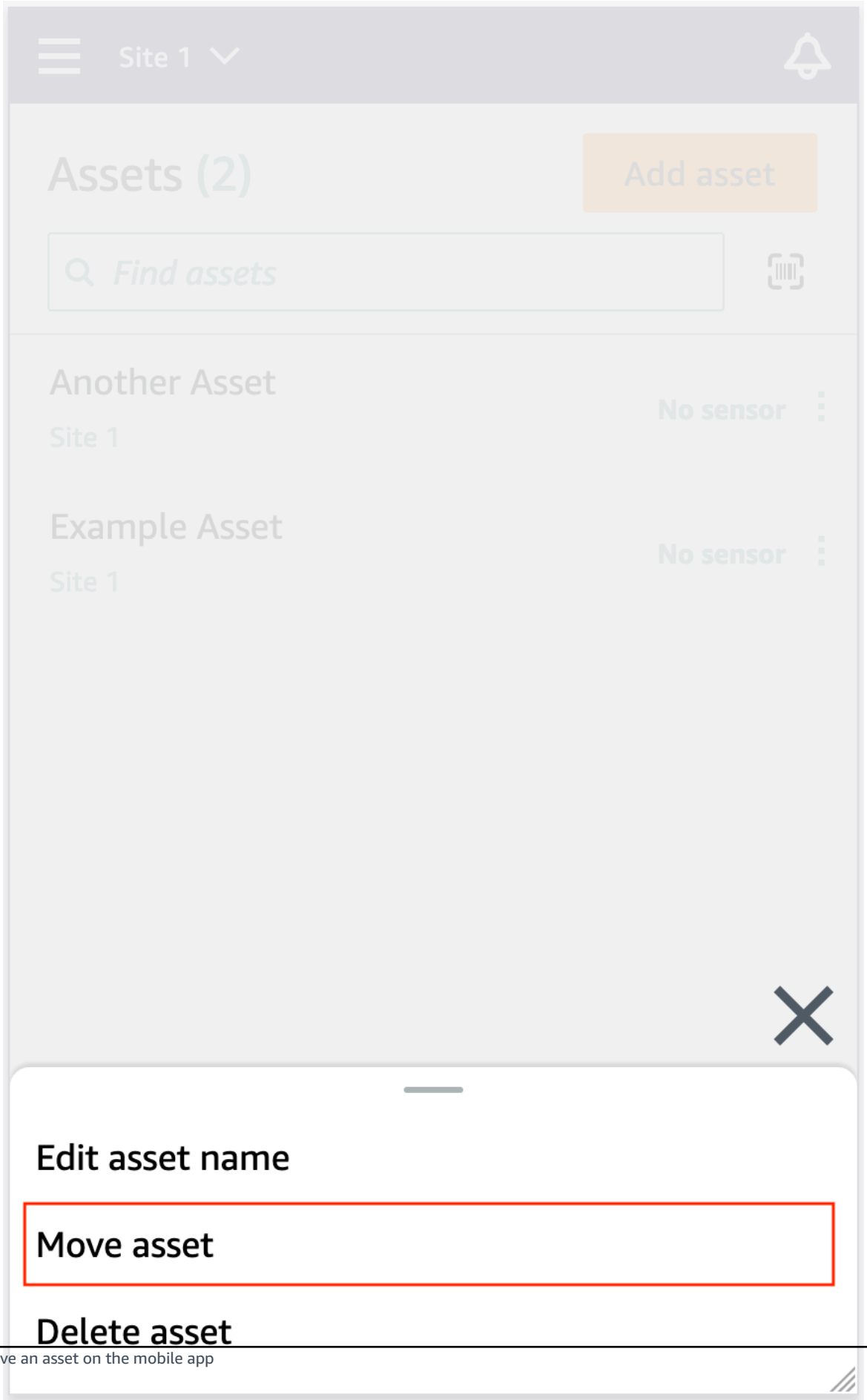

The app displays a success message if your asset is moved successfully.

# To move an asset on the mobile app

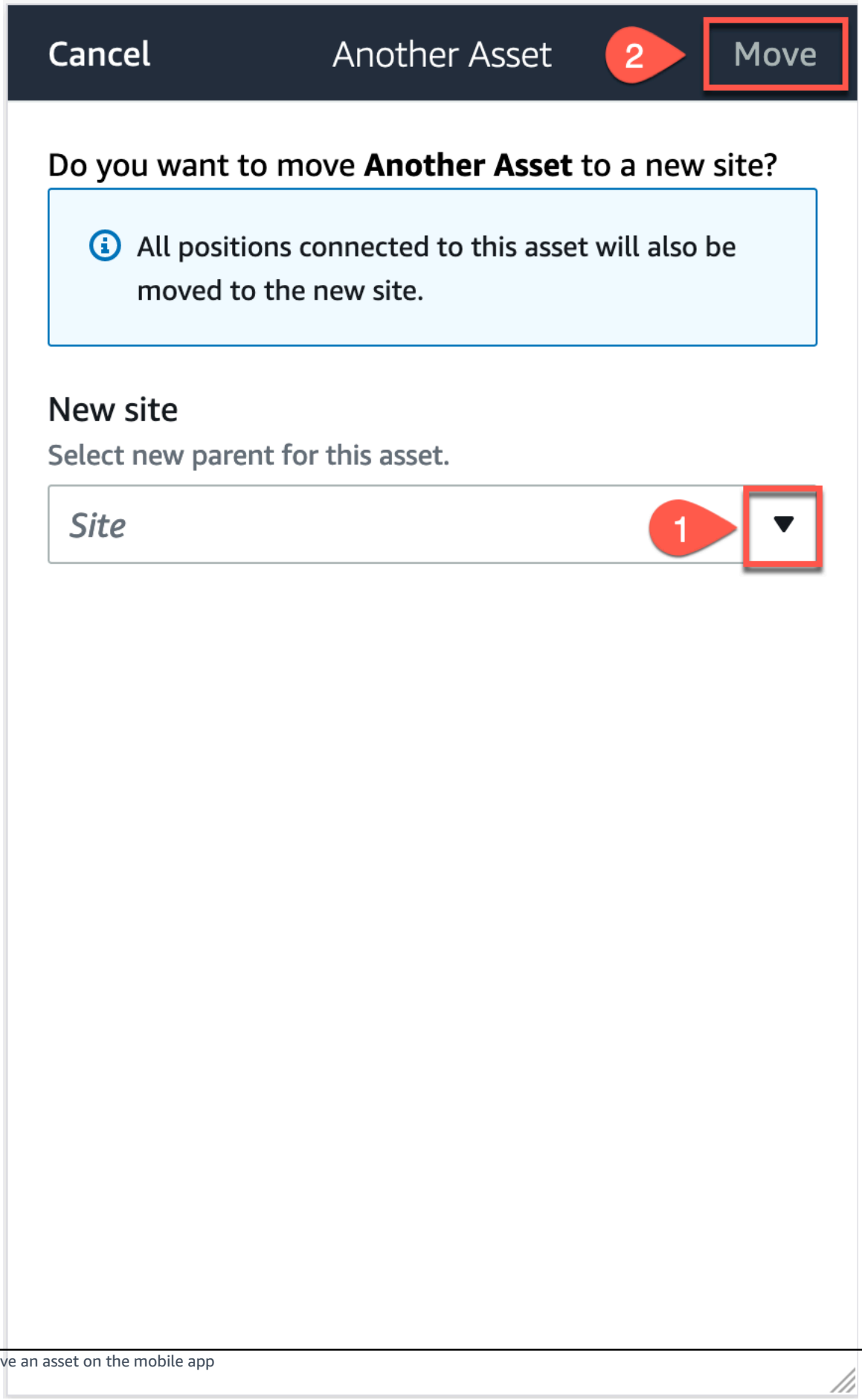
1. From the mobile app's main menu, choose **Assets**.
2. Choose asset that you want to move to a new site. Then, open the asset details menu.


Site 1
Assets (2)
Add asset
Find assets
Another Asset
Site 1
No sensor
Example Asset
Site 1
No sensor

3. From the asset details menu, choose **Move asset**.


Site 1
Assets (2)
Add asset
Find assets
Another Asset
Site 1
No sensor
Example Asset
Site 1
No sensor
Edit asset name
Move asset
Delete asset

4. From the asset page, from **New site**, choose the new site you want to move the asset to. Then, choose **Move**.


Cancel
Another Asset
2
Move
Do you want to move **Another Asset** to a new site?
All positions connected to this asset will also be moved to the new site.
New site
Select new parent for this asset.
Site
1

The app displays a success message if your asset is moved successfully.

# Deleting an asset

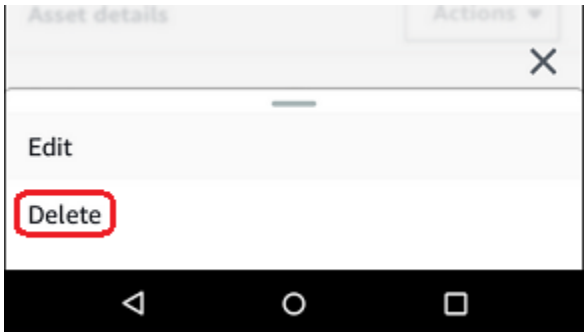
Deleting an asset removes all associated sensors and their positions, in addition to any historical data associated with them.

**Topics**

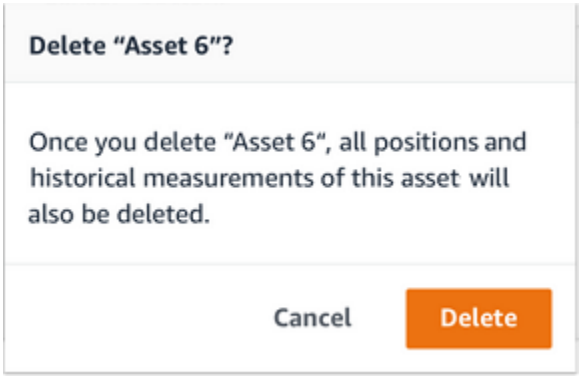

- To delete an asset


## To delete an asset

1. From the app's main menu, choose **Assets**.
2. Choose the asset that you want to delete.
3. For **Asset details**, choose **Actions**.
4. Choose **Delete asset**.

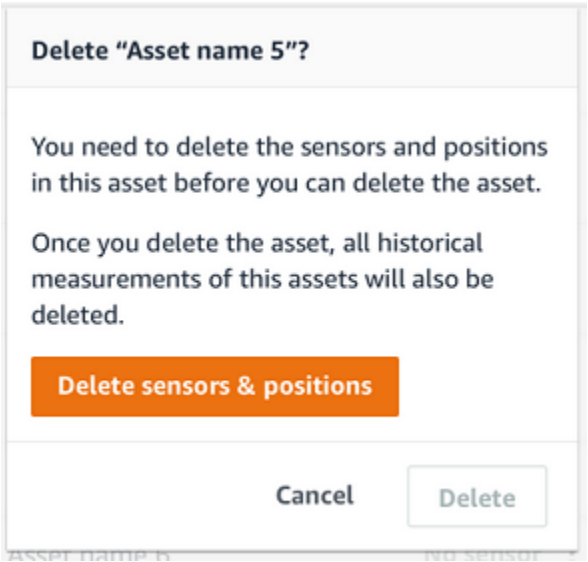



5. Choose one of the following options.
   - If there are no sensors paired with the asset, choose **Delete** and go to the next step.



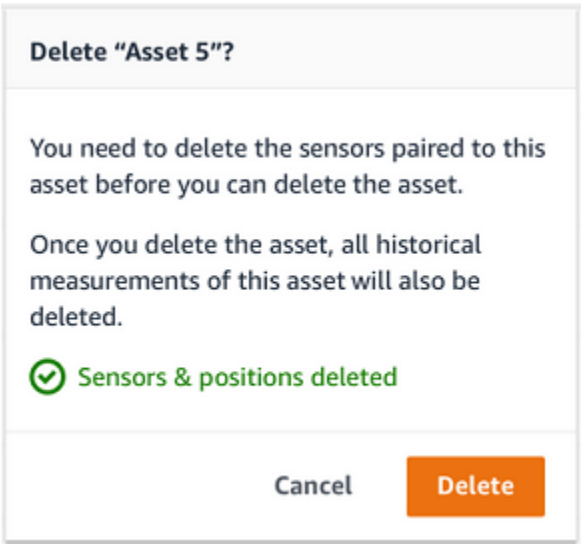
- If there are sensors paired with the asset, delete them.

  Choose **Delete sensors and positions**. When you delete a sensor or position, all historical measurements taken at this position will also be deleted.




  It can take some time for Amazon Monitron to delete all the paired sensors and positions.

6. Choose **Delete**.



# Sensors

Sensors collect the data from your equipment, then Amazon Monitron uses that data to detect developing abnormalities. Where you mount a sensor (the *position*) is extremely important for collecting and analyzing data.

To get a more detailed picture of your asset's health, you might need to collect data from multiple positions on your asset. You can place sensors on up to 20 positions on each asset. Each sensor position can be assigned a different machine class. If you have complex machinery with more than one potential point of failure, we recommend that you collect data from multiple positions.

**Topics**


- Positioning a sensor
- Mounting a sensor
- Adding a sensor position
- Pairing a sensor to an asset
- Renaming a sensor position
- Editing machine class
- Deleting a sensor
- Deleting a sensor position
- Understanding sensor details
- Identifying sensor position
- Ex-rated sensors


# Positioning a sensor

To detect abnormalities in machine components, mount sensors in all locations where temperature and vibrations can be measured effectively.

To achieve the greatest accuracy:

- Mount the sensor directly onto the housing of the target component.
- Minimize the length of the vibration transmission path (the distance between the source of vibration and sensor).

- Avoid mounting the sensor where its measurements may oscillate due to natural frequencies, such as on sheet metal covers.

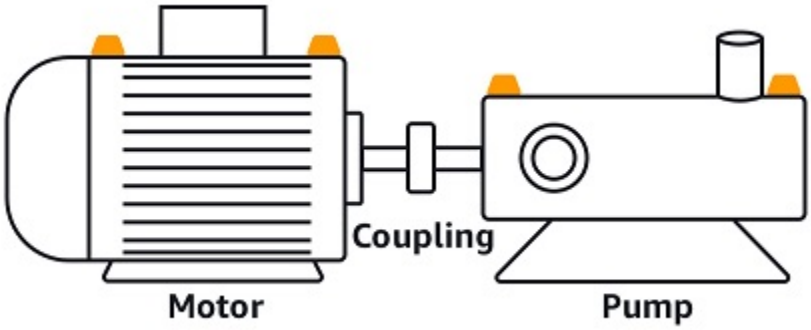
Vibration will attenuate up to 30-36" (75–90 cm) from the source.

Attributes of the vibration transmission path that can reduce the transmission path length include:

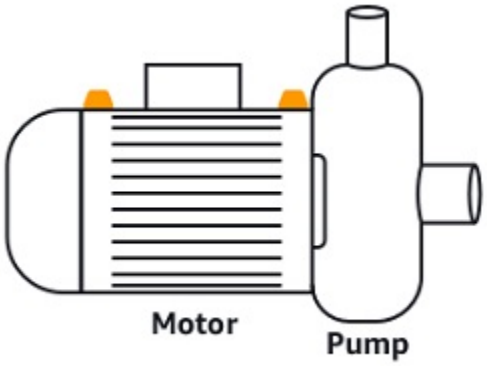
- the number of mounting surfaces, which can cause signal reflection
- materials such as rubber or plastic, which can absorb vibration

> **Note**
>
> Amazon Monitron sensors are 3-axis vibration sensors. The X, Y, and Z marks indicate the directions of the 3 three axes. These axes are marked on the sensor body. Therefore, it is not necessary to align any particular axis with the direction of the asset's vibration.

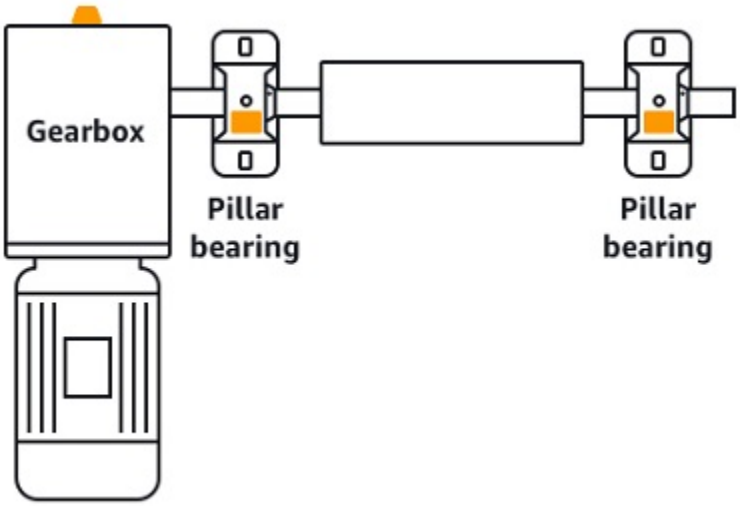
The following example of an electric motor pump set shows sensor locations, with four positions: two on the motor and two on the pump.




The following example shows where you might mount sensors if your primary concern is the motor rather than the pump.

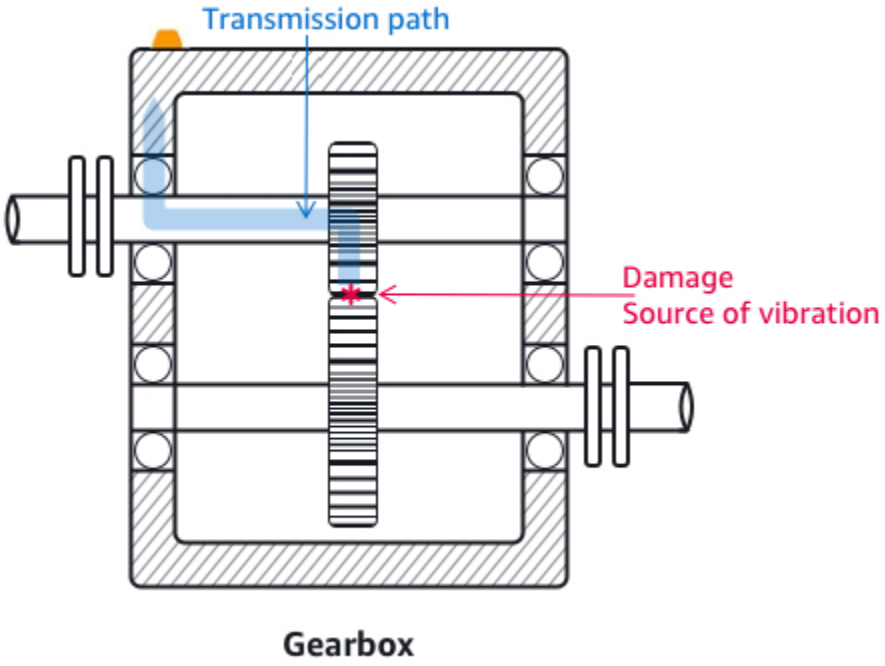



Gearboxes and bearings are also examples of common locations where you might want to place sensors.

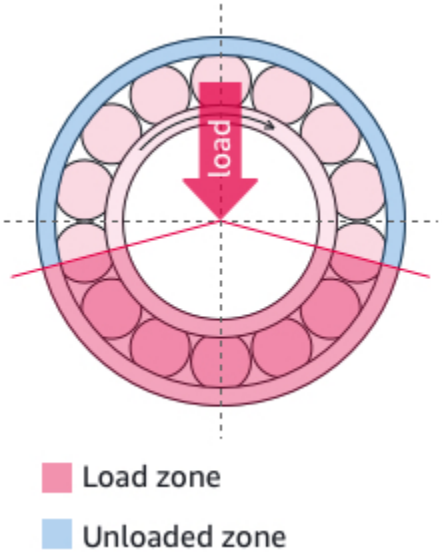



For complex equipment with multiple moving parts (such as gearboxes), position the sensor to minimize the length of the transmission path from the primary vibration source. Note that vibration is reduced when it is transmitted between adjacent parts of equipment, so the shortest distance between the sensor and the source of vibration is not always the best option.

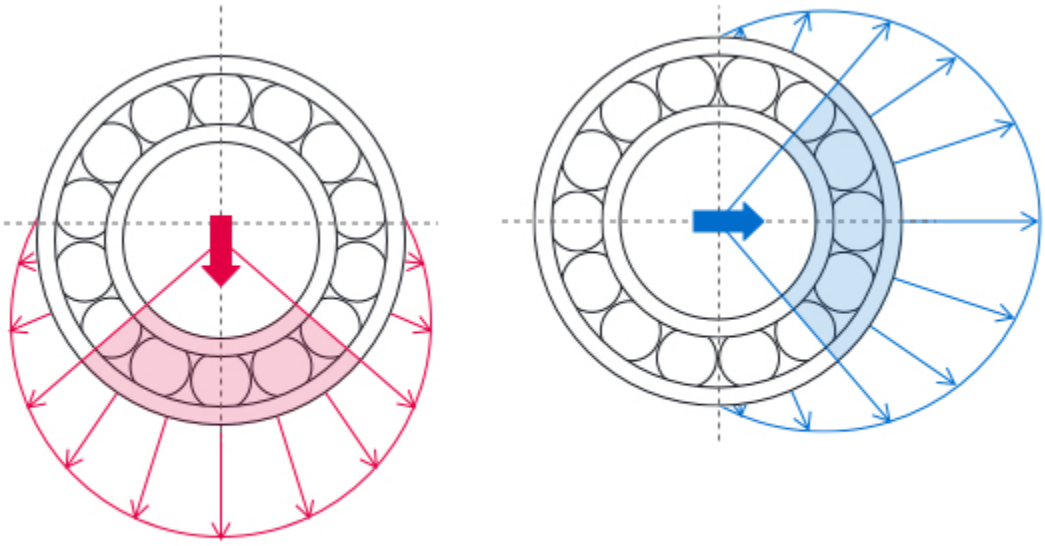
The following example of a gearbox shows how vibration can be transmitted through equipment in this way, along with a potential location for a sensor to detect this vibration.




For other types of equipment, the best position can be less obvious. For example, when placing a sensor to monitor bearings, position it close to the bearing's load zone, which is based on the direction of the load on the bearings as shown below.




Different types of loads on the bearings result in different load zones. Placing the sensor as close as possible to the center of the load zone is most likely to provide the best data.

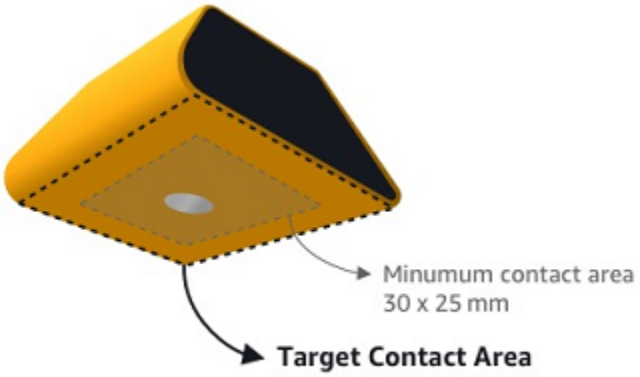



For information about how to mount sensors, see Mounting a sensor.

## Mounting a sensor

> **Warning**
>
> Before you install and use sensors, see the Amazon Monitron Sensor Device Safety and Compliance Guide. Before you install and use Ex-rated sensors, see the Ex Safety and Compliance Guide for all warnings and instructions.

The temperature and vibration detectors are located on the base of the Amazon Monitron sensors. Any area of the base is effective as a target contact area, but the contact area must be at least 30 x 25 mm for reliable detection. Center the target contact area over the mounting location for the most reliable results. The circular aluminum sensor (in the center of the target contact area) conducts heat directly from the asset's surface to the temperate sensing mechanism inside the Amazon Monitron sensor.




Determine the place and orientation where you can most effectively monitor the asset, and then mount sensor at that spot. To mount the sensor, you need to purchase an industrial adhesive. We recommend using cyanoacrylate epoxies like Loctite 454 and Loctite 3090 or Loctite 4070 or something similar. If the surface on which you mount the sensor is flat and relatively smooth, only a thin layer of adhesive such as Loctite 454 is needed. If the surface is rounded or somewhat uneven, apply a slightly thicker layer of adhesive such as Loctite 3090 or Loctite 4070.

If you are uncertain of where to mount your sensor, see Positioning a sensor.

**Warning**

When installing sensors, check and obey applicable safety regulations. You are solely responsible for safely installing the sensor on any equipment or machine part. To mount a sensor, you use industrial adhesive. Always consult and obey the adhesive manufacturer's safety and handling instructions.
For more information about the recommended adhesive, see Loctite 454 Technical Information, or Loctite 3090 Technical Information, or Loctite 4070 Technical Information, as appropriate.

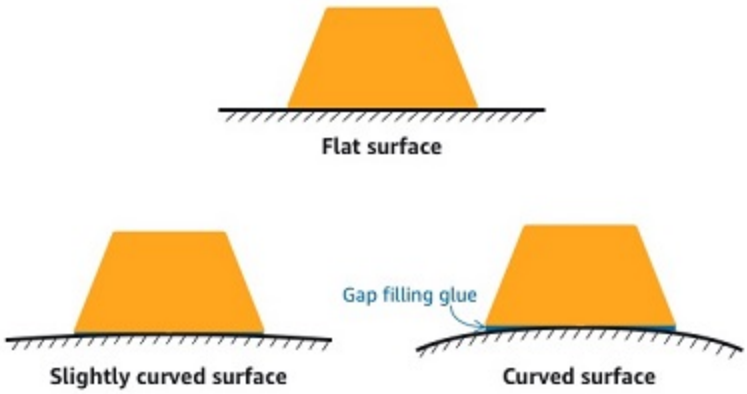
**To mount a sensor**

1. Remove all oil and grease from the position on the asset where you want to mount the sensor.
2. If the surface that you're mounting the sensor to is flat and relatively smooth, apply a thin layer of adhesive such as Loctite 454 to the bottom of the sensor, maximizing the area that will be in contact with the asset.

If the surface is rounded or somewhat uneven, apply a slightly more liberal layer of adhesive such as Loctite 3090 or Loctite 4070 to the bottom of the sensor. The layer of adhesive can bridge distances of up to 5 mm between the surface and the sensor if necessary.

3. Hold the sensor to the mounting location on the machine part for 30 seconds, pressing firmly.

   If you're mounting the sensor on a curved surface, put a small amount of additional adhesive on each side for better contact between the sensor and the surface. Based on the surface and the adhesive used, your results should look similar to the following.




# Adding a sensor position

When you pair a sensor to an asset, you record the type of position. The type of position tells Amazon Monitron how to assess the position when it analyzes the data from that sensor.

You can create and update asset positions from both the Amazon Monitron web app and the Amazon Monitron mobile app. Using the apps, you can:

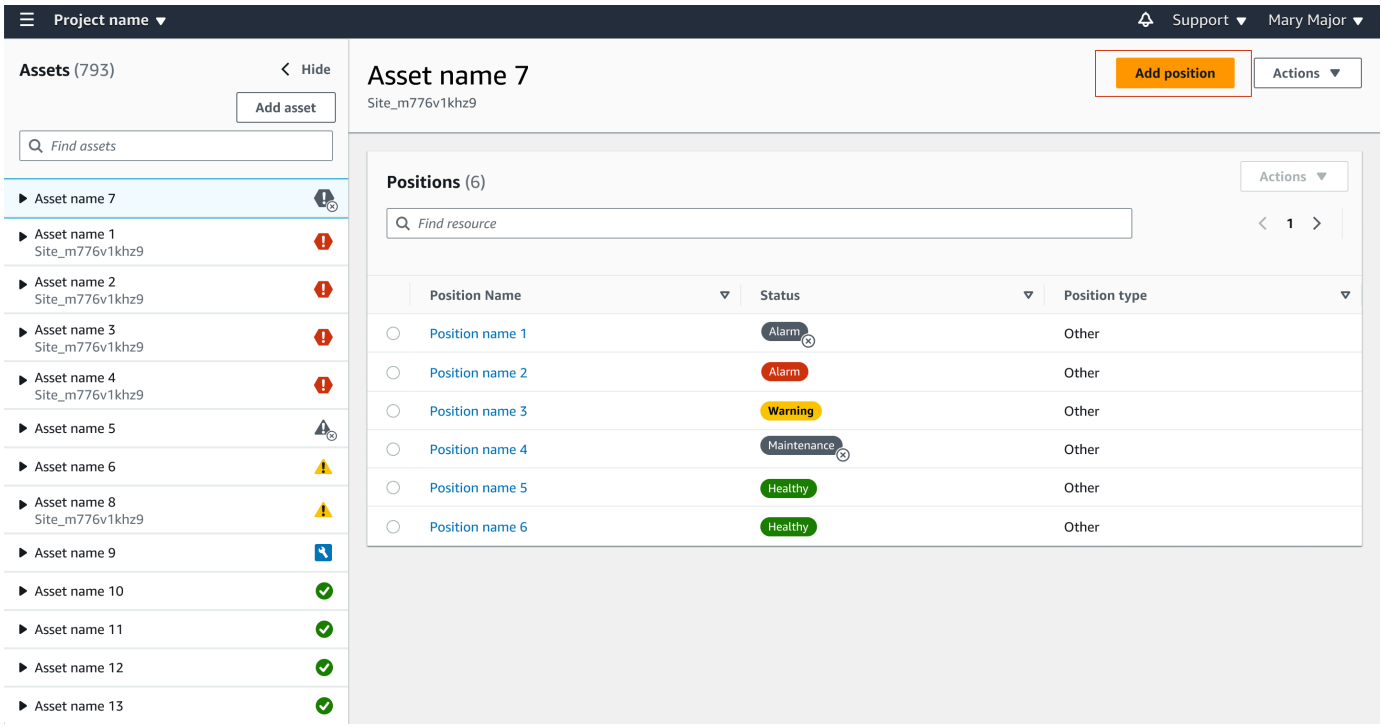
- Add a new position to an existing asset
- Add a new position to new asset
- Pair a new sensor with an existing position
- Add a new position to an existing asset without assigned position

**Topics**

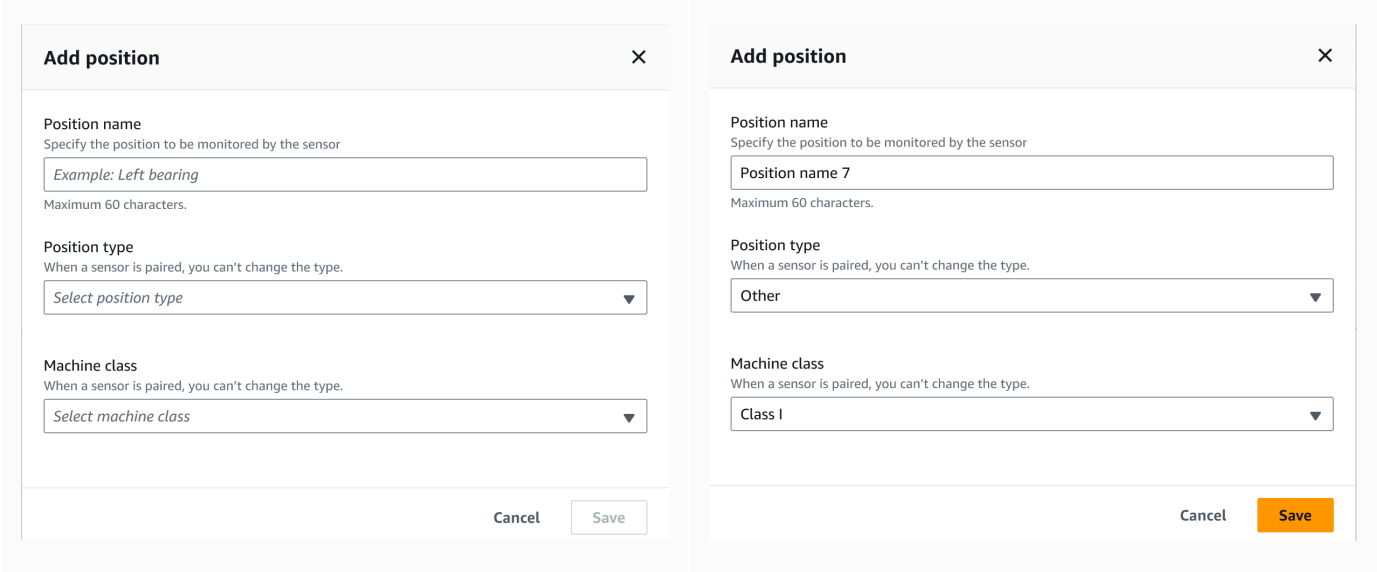
- To add a sensor position on the web app
- To add a sensor position on the mobile app


# To add a sensor position on the web app

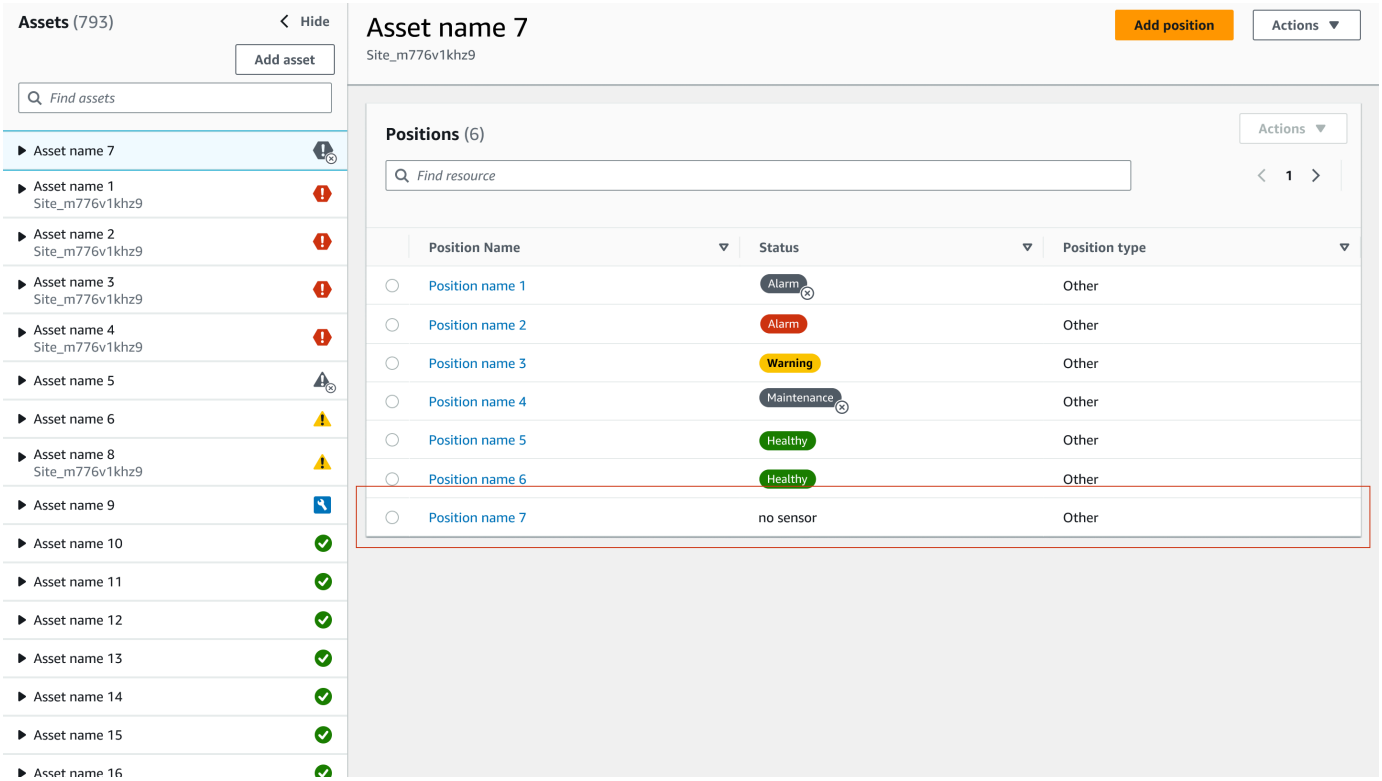
1. Choose the sensor whose position you want to create or edit from the **Assets** list.
2. Select the **Add position** button.




3. In the dialog box that opens, enter your **Position name**, **Position type** and **Machine class**.



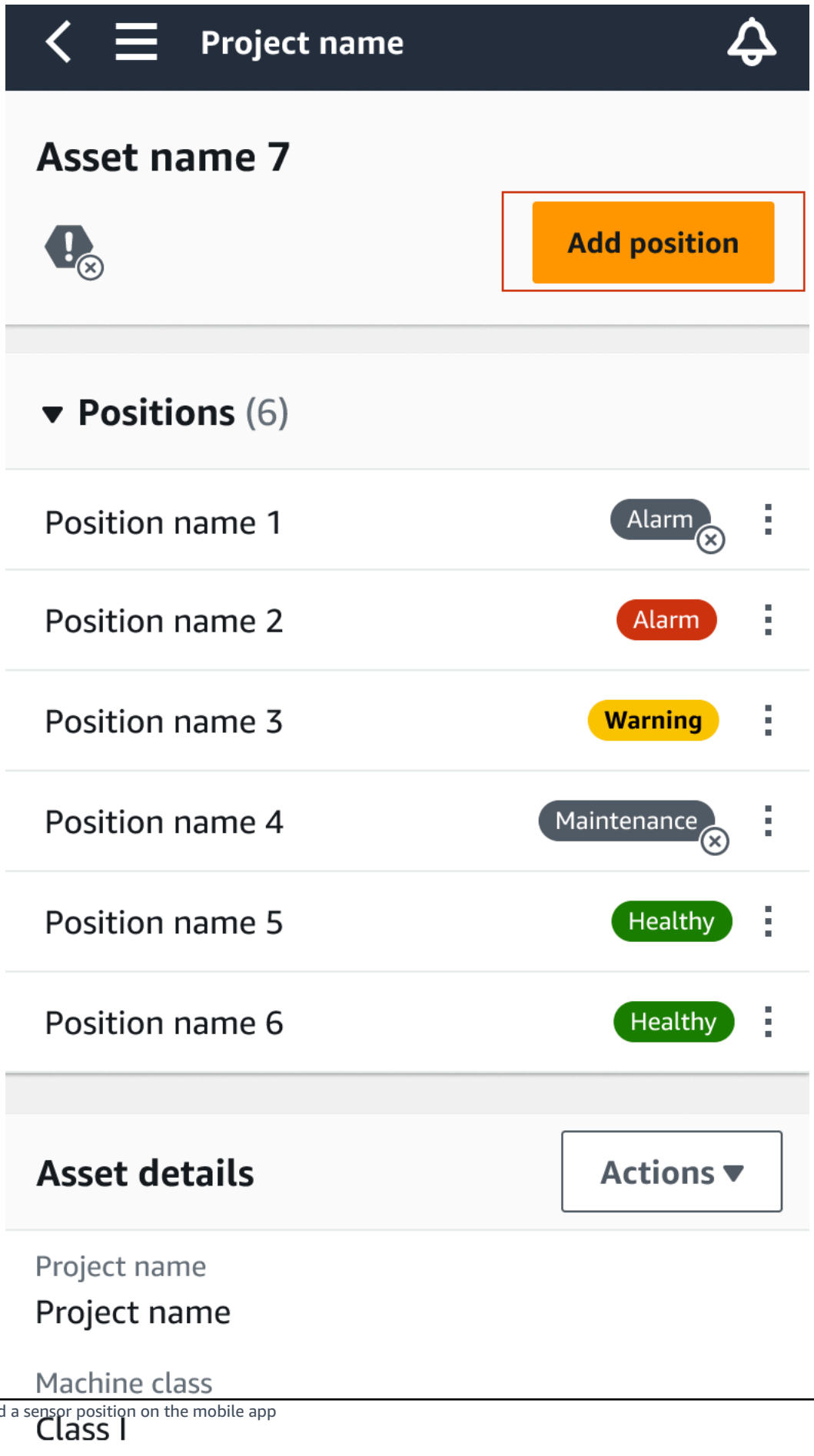

4. Choose **Save**.
5. Your position is added to the asset.



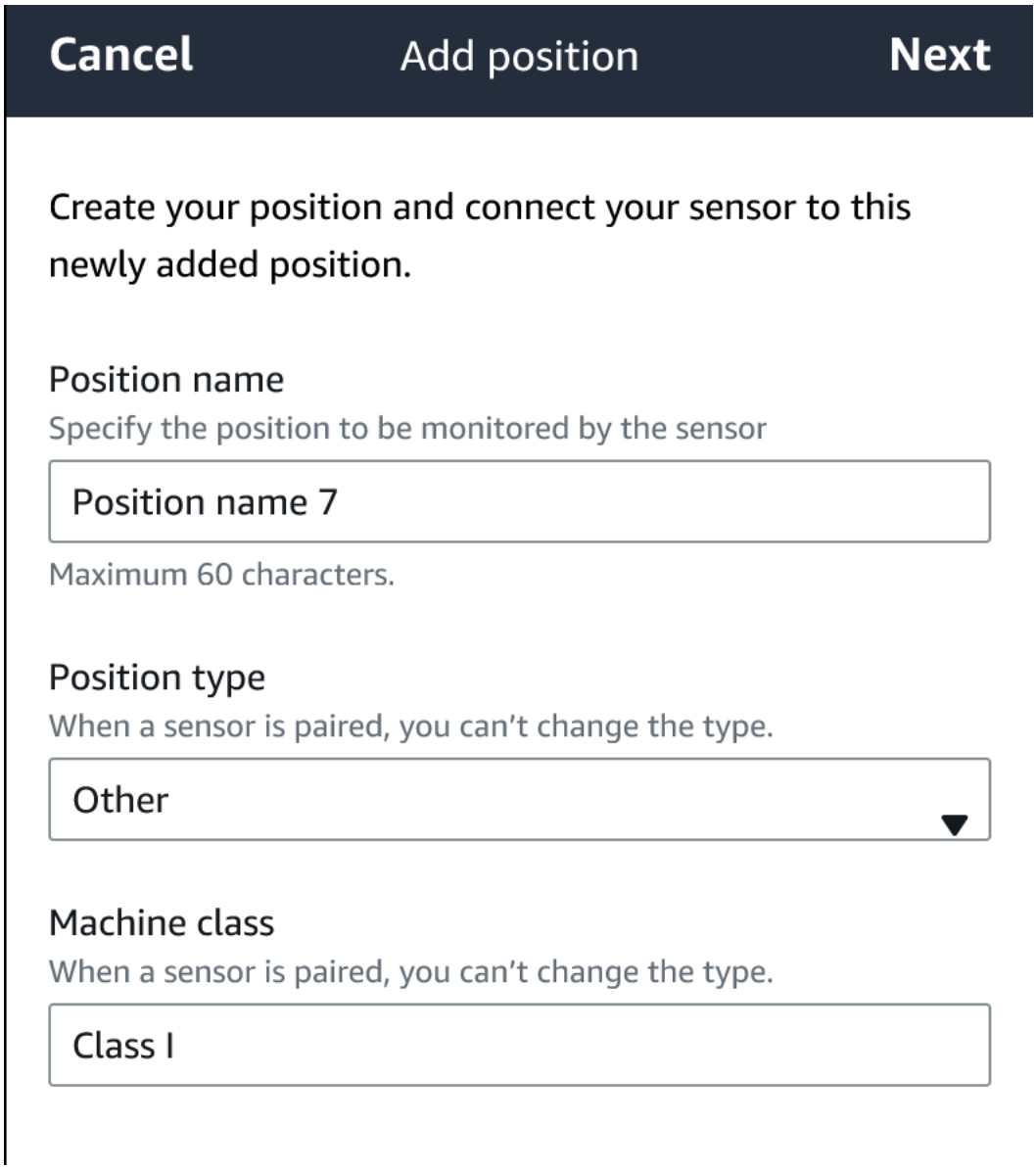

# To add a sensor position on the mobile app

1. Choose the sensor whose position you want to create or edit from the **Assets** list.

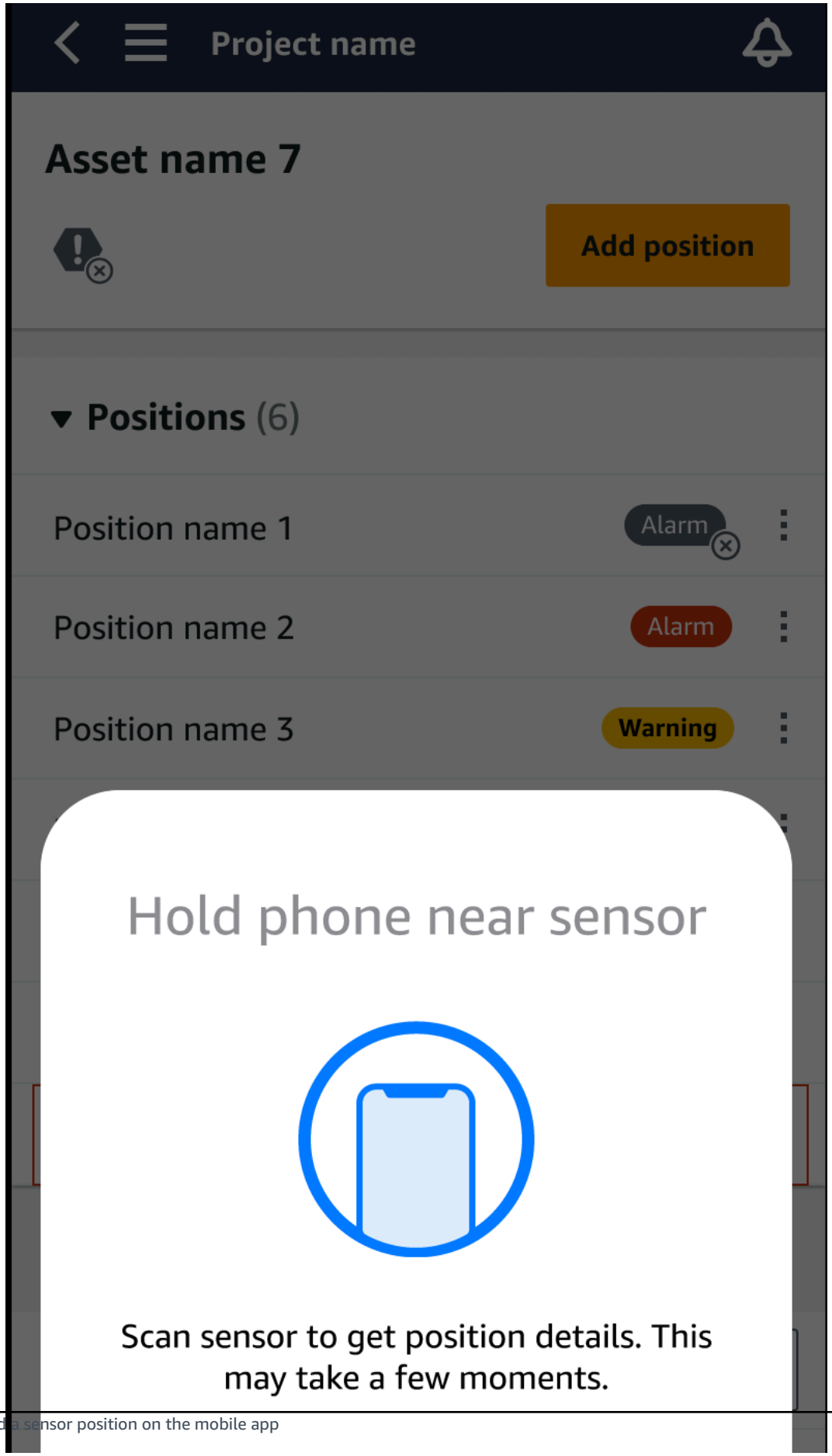
2. Select the **Add position** button.


Project name
Asset name 7
Add position
Positions (6)
Position name 1
Alarm
Position name 2
Alarm
Position name 3
Warning
Position name 4
Maintenance
Position name 5
Healthy
Position name 6
Healthy
Asset details
Actions
Project name
Project name
Machine class
Class I

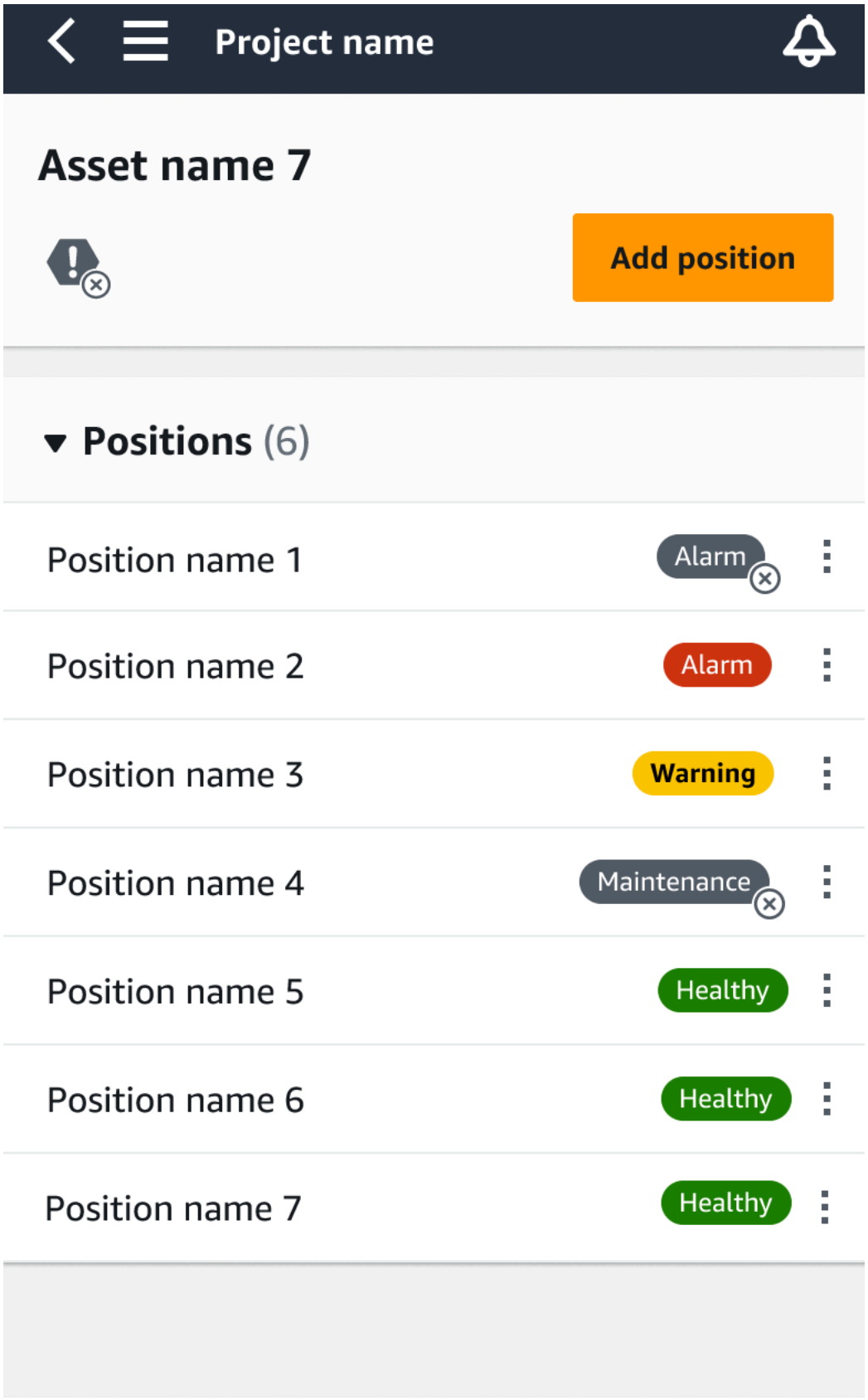
3. In the dialog box that opens, enter your **Posion name**, **Position type**, and **Machine class**.




4. Choose **Next**.
5. Re-scan your sensor with your mobile device to save the position.


Project name
Asset name 7
Add position
Positions (6)
Position name 1
Alarm
Position name 2
Alarm
Position name 3
Warning
Hold phone near sensor
Scan sensor to get position details. This may take a few moments.

6. Your position is added to the asset.



# Pairing a sensor to an asset

After you've added an asset, pair it to one or more of the sensors to monitor its health. Each sensor is mounted on the asset in its own position. Each sensor mounted on the asset can be assigned its own machine class.

When you pair a sensor to an asset, you record the type of position. The type of position tells Amazon Monitron how to assess the position when it analyzes the data from that sensor. Each position can give a very different view of the asset. You will often need to monitor multiple locations on a large asset to get a clear picture of its health. You can place up to 20 sensors at different positions on an asset. Less complex assets might require only one or two sensors.

Each sensor measures the temperature and vibration at its position. You can name a position anything you like, and you can change the name later if necessary. For example, a sensor set up to monitor the pump in the previous example might have a position of *Left Position*, with a position type of `Pump`. The position name identifies the location, whereas the position type tells Amazon Monitron which part of the asset it's monitoring. You can also edit the machine class assigned to each sensor.

For more information about where to place sensors, see Positioning a sensor.

**Important**

After you pair a sensor to an asset, Amazon Monitron establishes a baseline for that position. The baseline tells Amazon Monitron how the asset performs under normal conditions. Amazon Monitron uses this information to identify abnormal conditions. During this time, Amazon Monitron assumes that conditions are normal and won't produce any alarms.

**Topics**


- To pair a sensor to an asset


## To pair a sensor to an asset

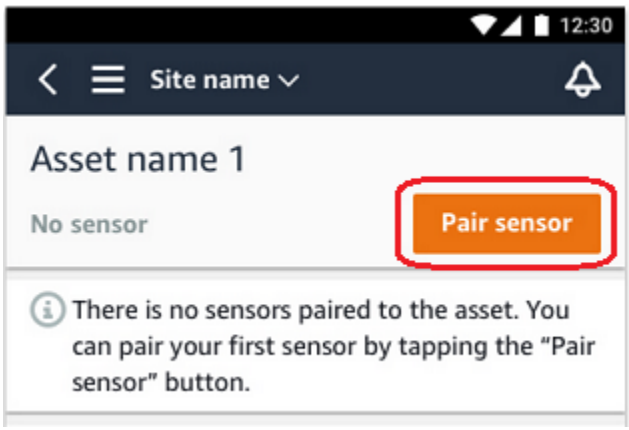
1. Ensure that near field communication (NFC) is turned on for your smartphone.

> **Tip**
>
> For many smartphone models, NFC is turned on by default. The following resources might help you determine whether you need to turn on NFC, and how to do so:
>
> - About NFC (Samsung)
> - Models that support NFC Tag Reader (iPhone)

2. From the **Assets** list, choose the asset.

   - If you just created the asset:

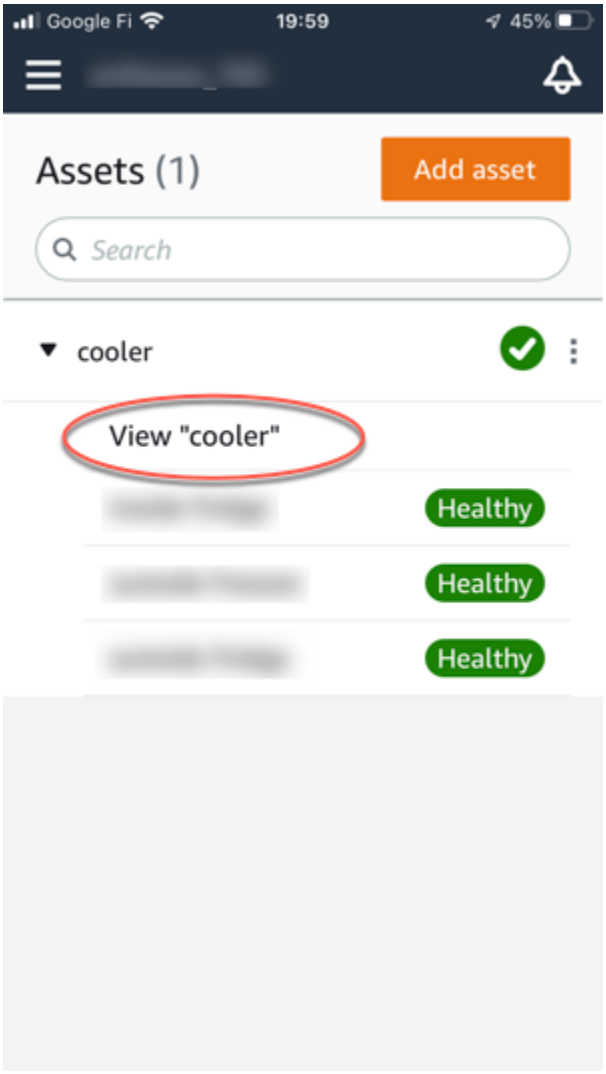
     Choose **Add position**.

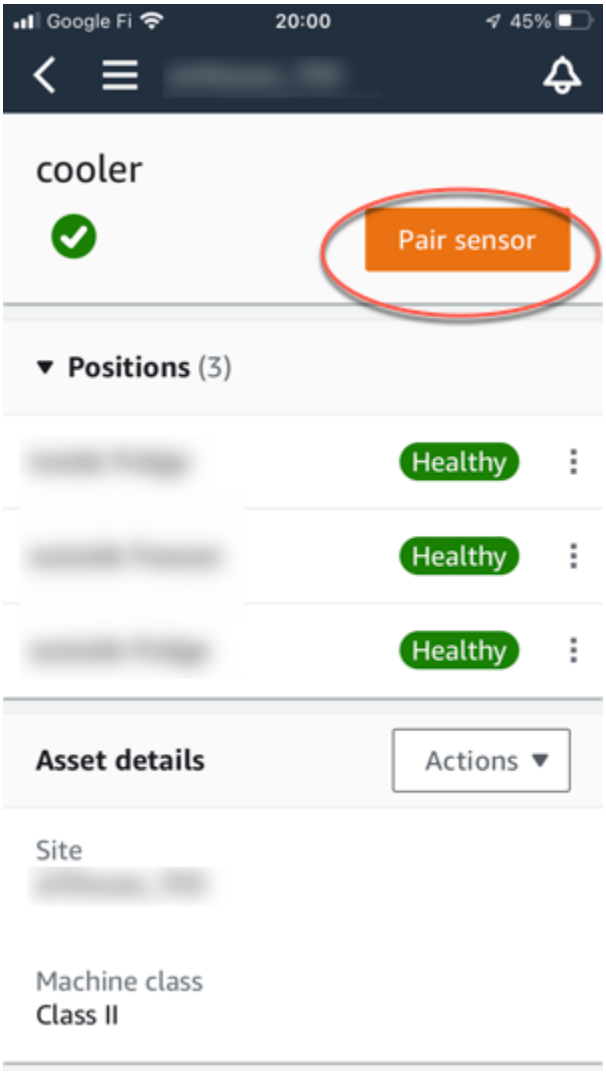
   - If you created the asset earlier, and have already paired more than one sensor to it:

     a. After you choose the asset, you will see a dropdown list of sensors associated with that asset.

        Choose the **View** option at the top of that list.




b. Choose **Pair sensor**.




3. Place your sensor on the machine in the correct location. For more information about placing sensors, see Positioning a sensor and Mounting a sensor.
4. Name the position that the sensor will monitor.

   We recommend that you use a name that is clear and easy for you to work with.
5. For **Position type**, choose the position type.

   Valid values:

   - Bearing
   - Compressor
   - Fan
   - Gearbox

- Motor
- Pump
- Other

> **Note**
>
> After you pair a sensor to an asset, you can't change the position type. If you need to change the type, you must delete the sensor and re-add it.

6. For **Machine class**, choose the machine class of the asset part you are positioning the sensor on. Valid options are based on the ISO 20816 standards.

   **Class I**

   Individual parts of engines and machines, integrally connected to the complete machine in its normal operating condition, for example, production electrical motors of up to 15 kilowatts (kW) or 20 horsepower (hp).

   **Class II**

   Medium-sized machines (typically electrical motors with 15 to 75 kW (20 to 101 hp) output) without special foundations, rigidly mounted engines or machines (up to 300 kW or 402 hp) on special foundations.

   **Class III**

   Large prime-movers and other large machines with rotating masses mounted on rigid and heavy foundations that are relatively stiff in the direction of vibration.

   **Class IV**

   Large prime-movers and other large machines with rotating masses mounted on rigid and heavy foundations that are relatively soft in the direction of vibration measurement, for example, turbo-generator sets and gas turbines with outputs greater than 10 megawatt (MW) or 13,404 hp.

7. Choose **Next**.
8. Hold your smartphone close to the sensor to commission it. Don't move your smartphone while you are commissioning the sensor.



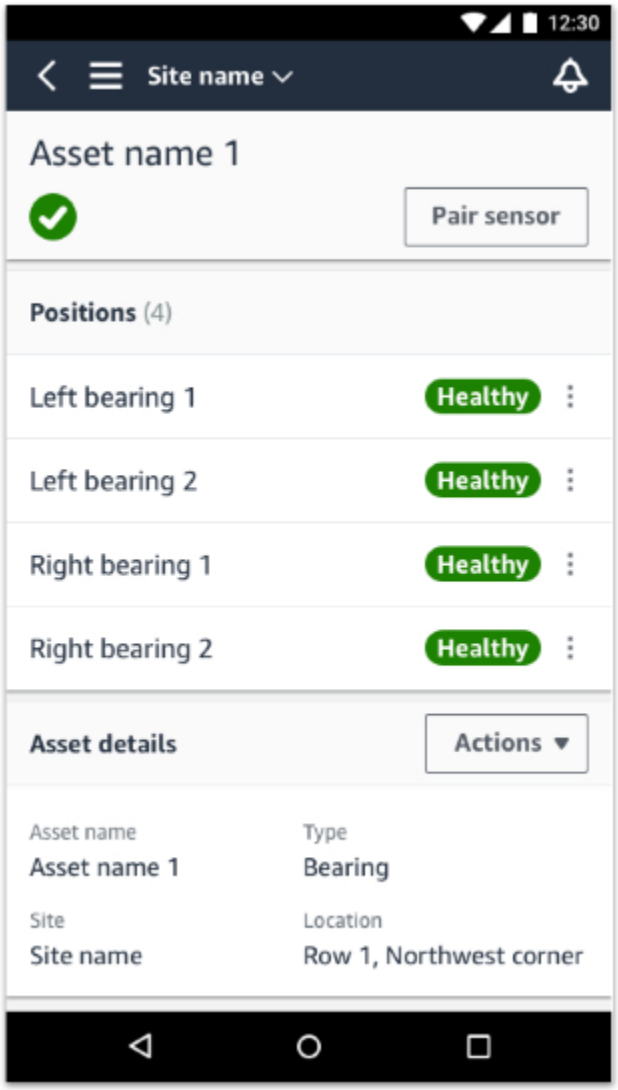
It can take a few moments for Amazon Monitron to commission the sensor and pair with it. While it's connecting, you will see the following message.




**Note**

The appropriate way to hold your mobile device while pairing depends on the type of mobile device you have. For more information, see Troubleshooting Amazon Monitron device issues.

When more than one sensor is paired with a given asset, the **Assets** page shows each sensor position and its health status, but not the specific details about each position. To display the details, choose the position from the list. For more information about the data you can monitor with each asset, see Understanding sensor measurements.




Positions are displayed in status order. For example, a position that's in an alarm state is displayed above a position that's in an acknowledged state. Positions that are in a healthy state follow those in an acknowledged state.

# Renaming a sensor position

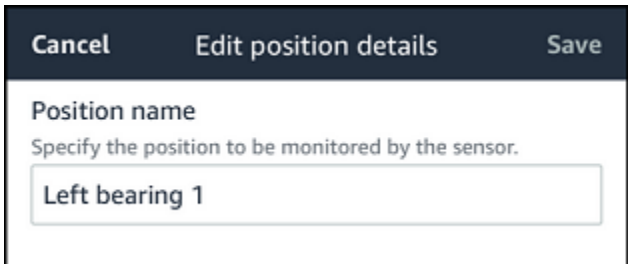
### Topics

- Renaming a sensor position on the mobile app

- Renaming a sensor position on the web app


## Renaming a sensor position on the mobile app

1. From the **Assets** list, choose the asset with the sensor position whose name you want to change.
2. Choose the sensor with the position whose name you want to change.
3. Choose the **Sensor details** tab.
4. Under **Position details**, choose **Actions**.
5. Choose **Edit position details**.
6. For **Position name**, enter a new name.

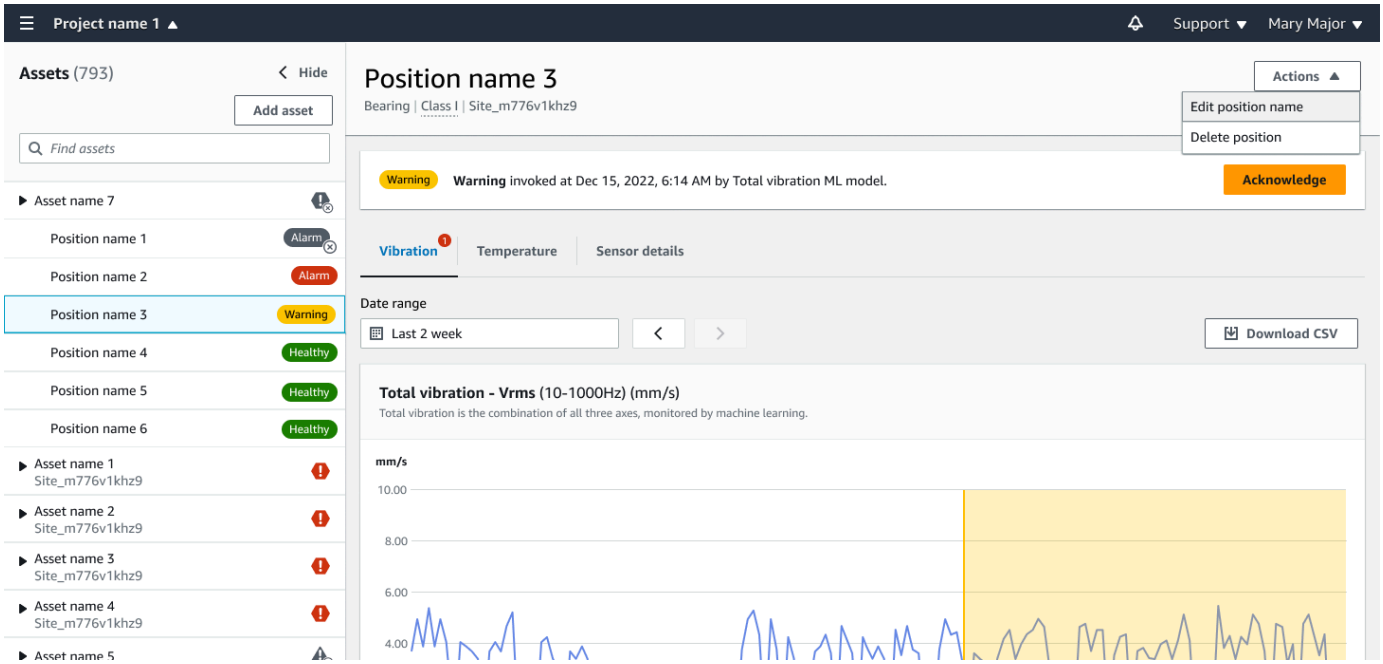



7. Choose **Save**.

## Renaming a sensor position on the web app

1. Select the position.

   Choose the **Actions** button in the **Positions** table.




2. Choose **Edit position name**.
3. For **Position name**, enter a new name.
4. Choose **Save**.

# Editing machine class

You can edit the machine class of a sensor from both the mobile and web apps, from either the **Asset detail** section or the **Position detail** section.

When you edit a sensor's machine class, asset condition alerts based on the updated machine class take effect from the next measurement after the update.

> **Important**
>
> You cannot edit a sensor's machine class if it has an unresolved alert. You must resolve any alerts before editing machine class.

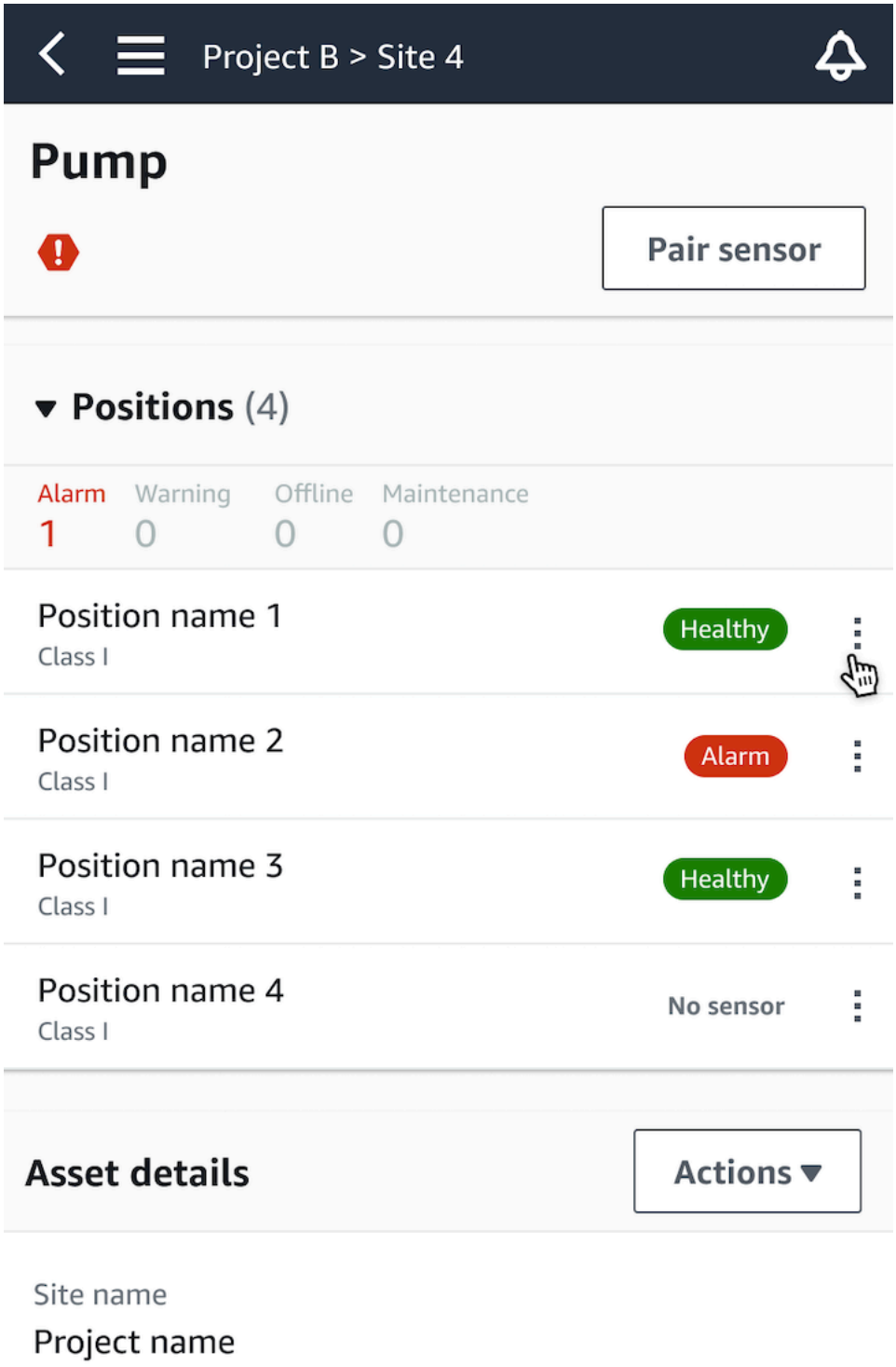
### Topics


- To edit machine class on the mobile app
- To edit machine class on the web app

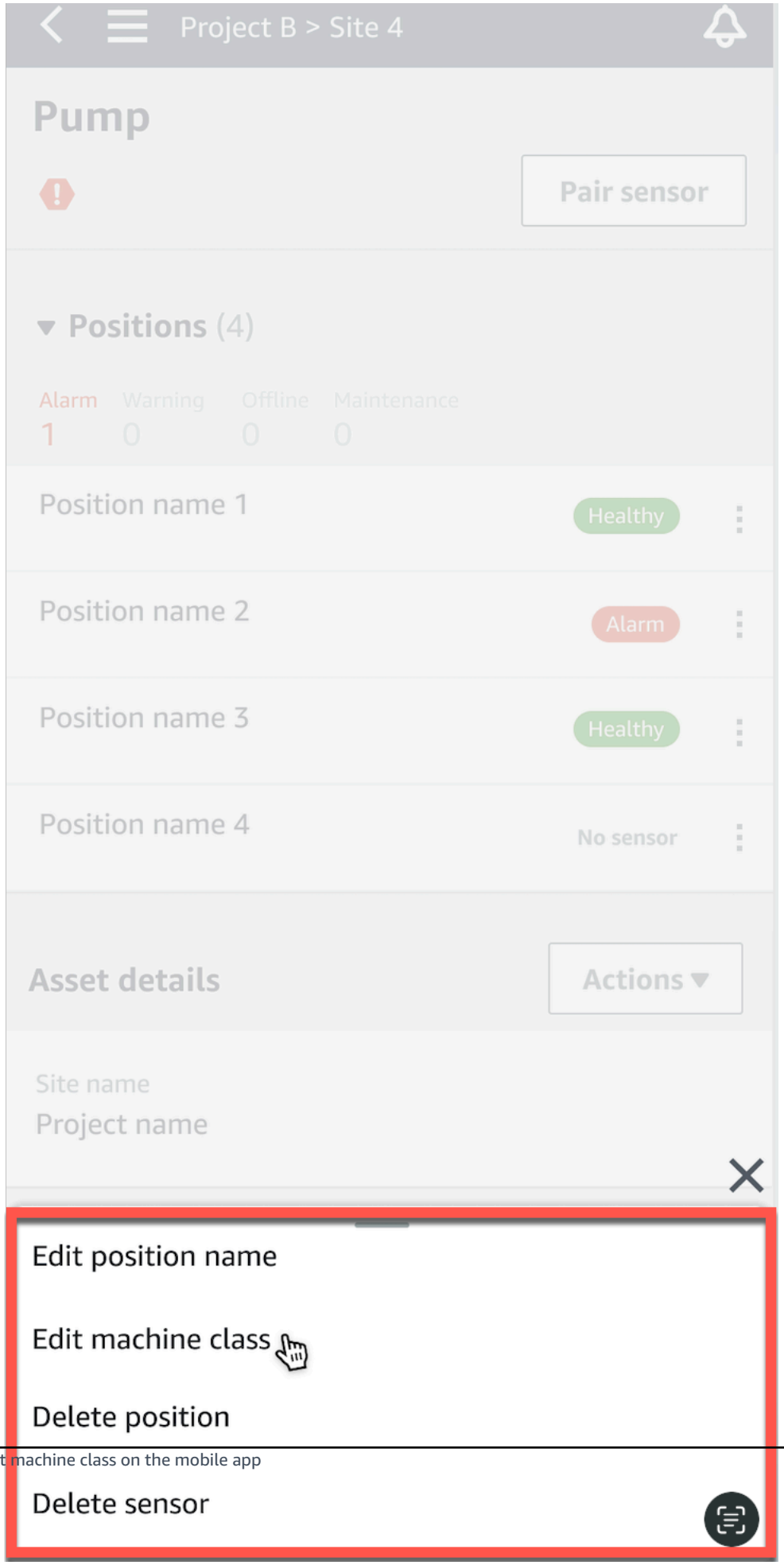
- To edit machine class from the position detail page


## To edit machine class on the mobile app

1. From the **Assets** list, choose the asset with the sensor position you want to edit.
2. From the **Positions** list, choose the sensor with the position whose machine class you want to change.
3. Choose to see more sensor details.




4. From the options that appear, choose **Edit machine class**.

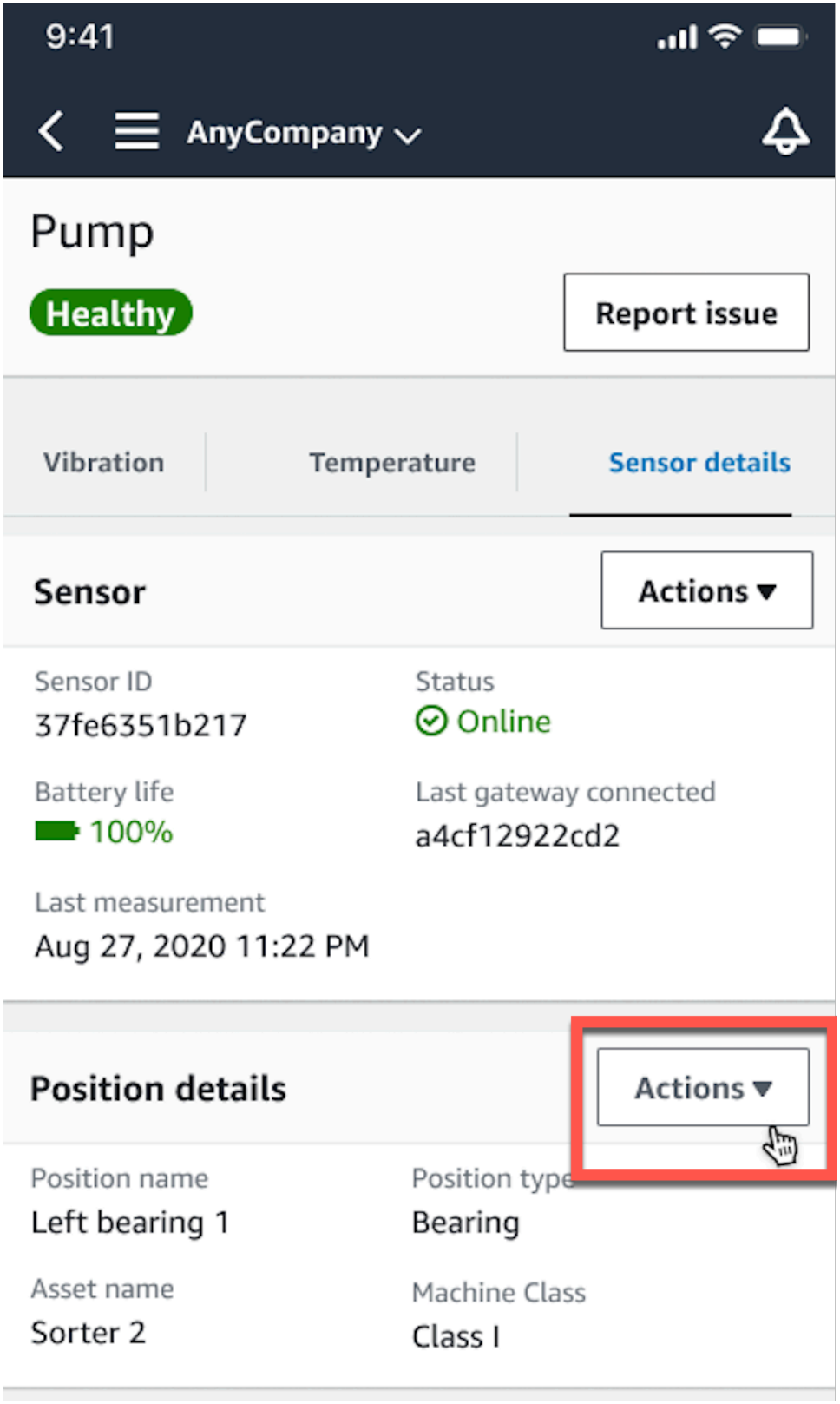

Project B > Site 4
Pump
Pair sensor
Positions (4)
Alarm
1
Warning
0
Offline
0
Maintenance
0
Position name 1
Healthy
Position name 2
Alarm
Position name 3
Healthy
Position name 4
No sensor
Asset details
Actions
Site name
Project name
Edit position name
Edit machine class
Delete position
Delete sensor

5. From **Edit machine class** choose the new machine class you want to assign to the sensor. Select **Save**.

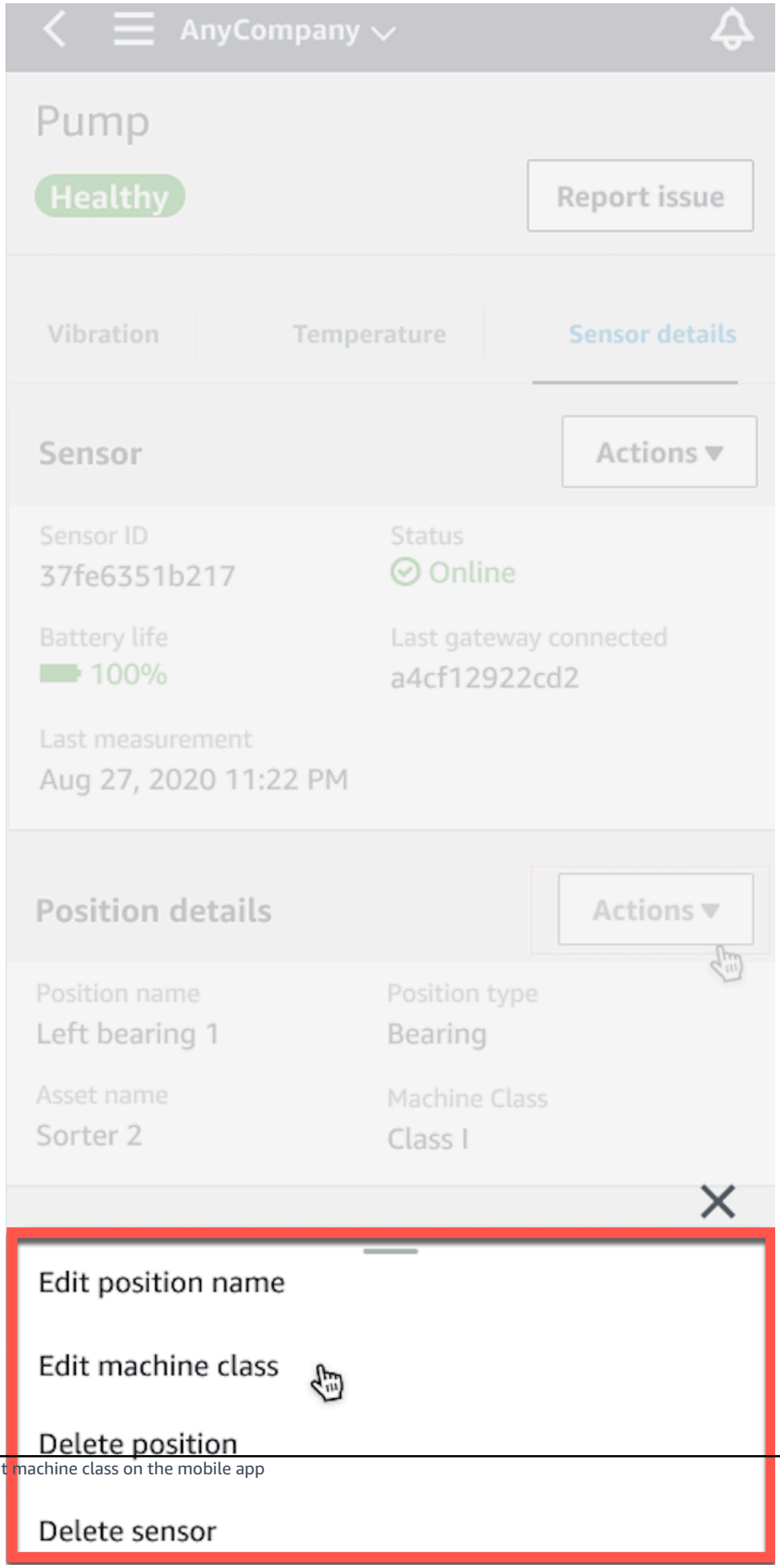
> **Note**
>
> The new machine class will take effect at the next measurement interval. The single-axis chart threshold will be updated.

**To edit a machine class from the position detail page**

1. From the **Position details** list, choose the **Actions** tab.




2. From the options that appear, choose **Edit machine class**.

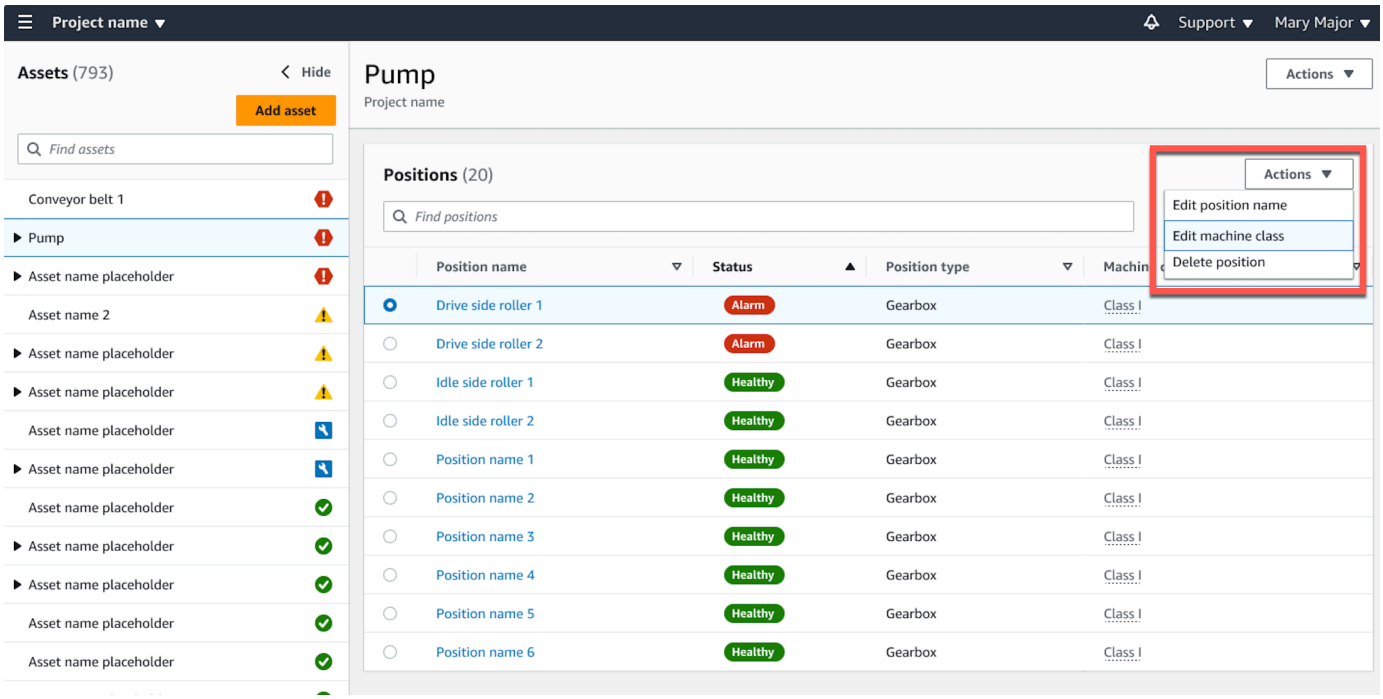

AnyCompany
Pump
Healthy
Report issue
Vibration
Temperature
Sensor details
Sensor
Actions
Sensor ID
37fe6351b217
Status
Online
Battery life
100%
Last gateway connected
a4cf12922cd2
Last measurement
Aug 27, 2020 11:22 PM
Position details
Actions
Position name
Left bearing 1
Position type
Bearing
Asset name
Sorter 2
Machine Class
Class I
Edit position name
Edit machine class
Delete position
Delete sensor

3. From the **Edit machine class** menu choose the new machine class you want to assign to the sensor. Choose **Next**.

> **Note**
>
> The new machine class will take effect at the next measurement interval. The single-axis chart threshold will be updated.

## To edit machine class on the web app

1. From the **Assets** table, choose the **Actions** button.
2. From the options, choose **Edit machine class**.

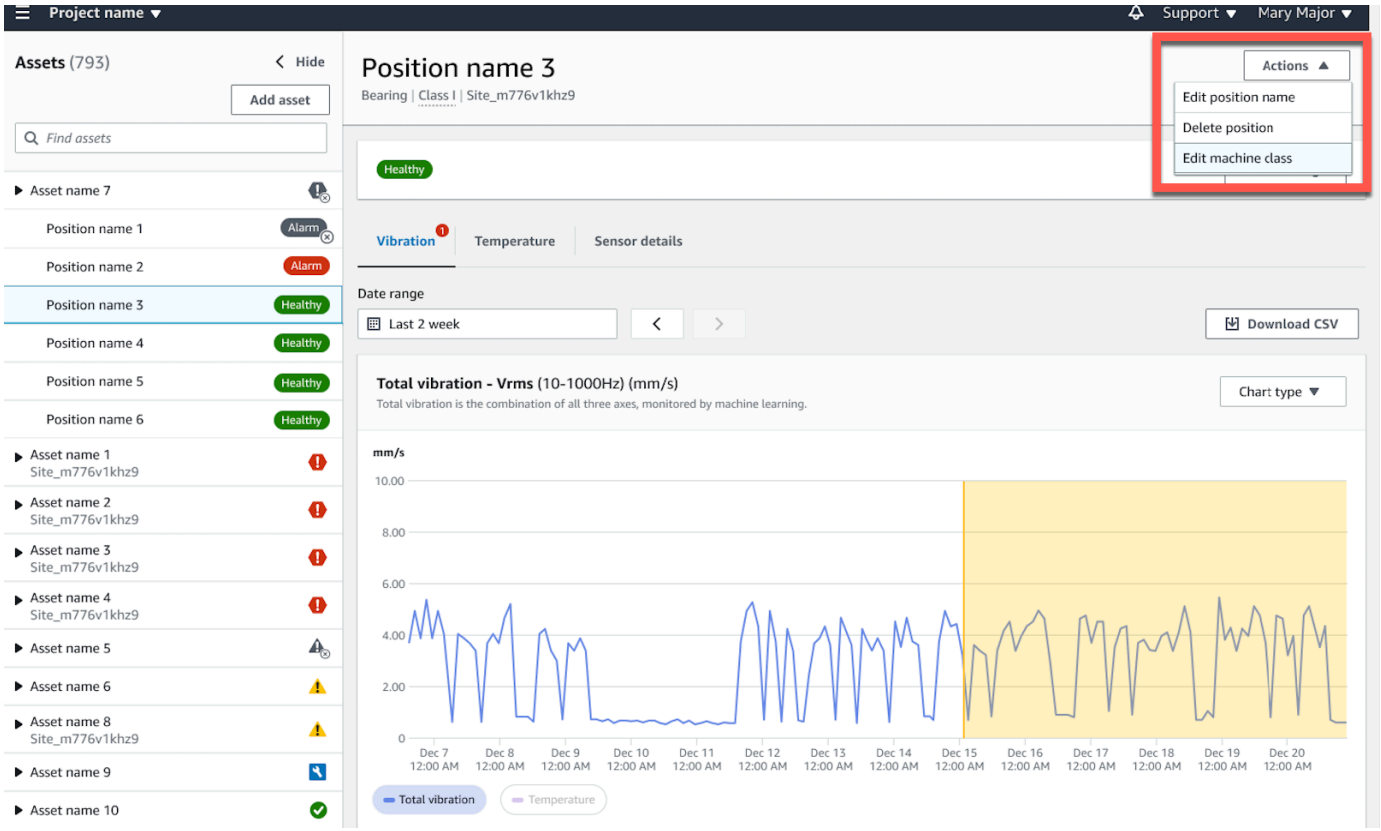



3. From the **Edit machine class** menu choose the new machine class you want to assign to the sensor and then select **Save changes**.

> **Note**
>
> The new machine class will take effect at the next measurement interval and impact position status. The single-axis chart threshold will be updated.

## To edit machine class from the position detail page

1. From the **Positions** table, choose the **Actions** button.
2. From the options, choose **Edit machine class**.




3. From the **Edit machine class** menu choose the new machine class you want to assign to the sensor and then select **Save changes**.

> **Note**
>
> The new machine class will take effect at the next measurement interval. The single-axis chart threshold will be updated.

# Deleting a sensor

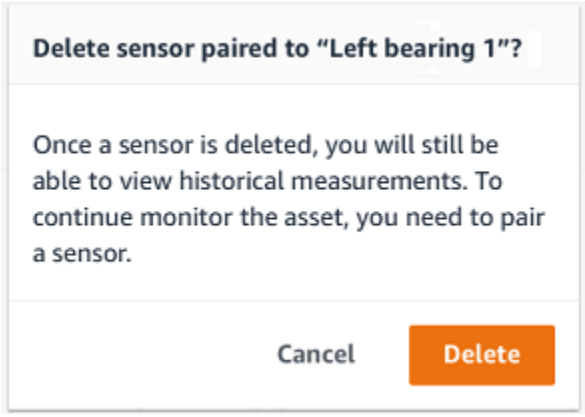
Deleting a sensor prevents Amazon Monitron from collecting more data with it. It doesn't delete the data that it has already collected.

### Topics

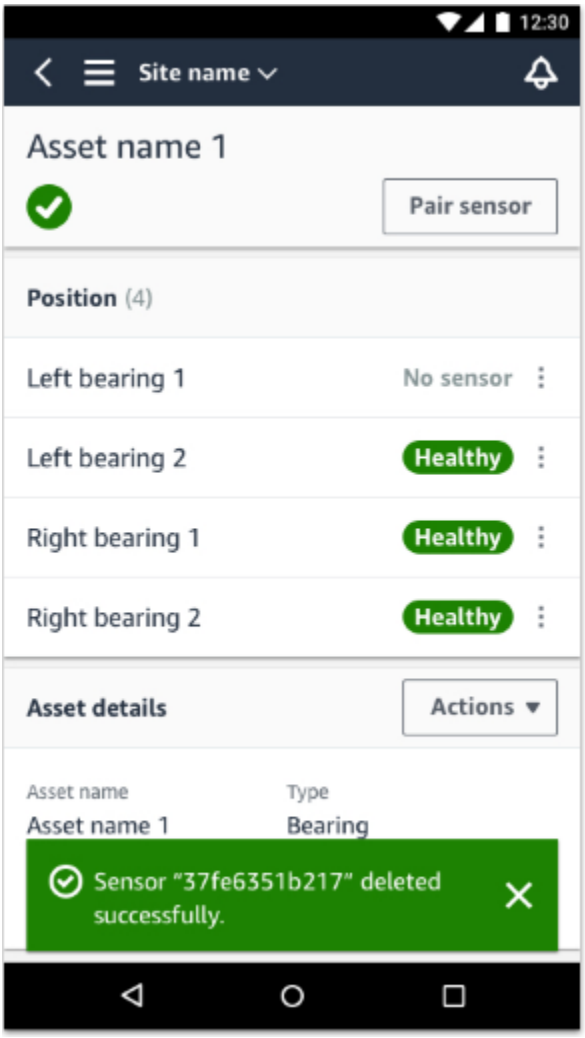
- To delete a sensor in the mobile app
- To delete a sensor in the web app


## To delete a sensor in the mobile app

1. From the **Assets** list, choose the asset that is paired to the sensor that you want to delete.
2. Choose the sensor.
3. Under **Sensor**, choose **Actions**.
4. Choose **Delete sensor**.
5. Choose **Delete**.

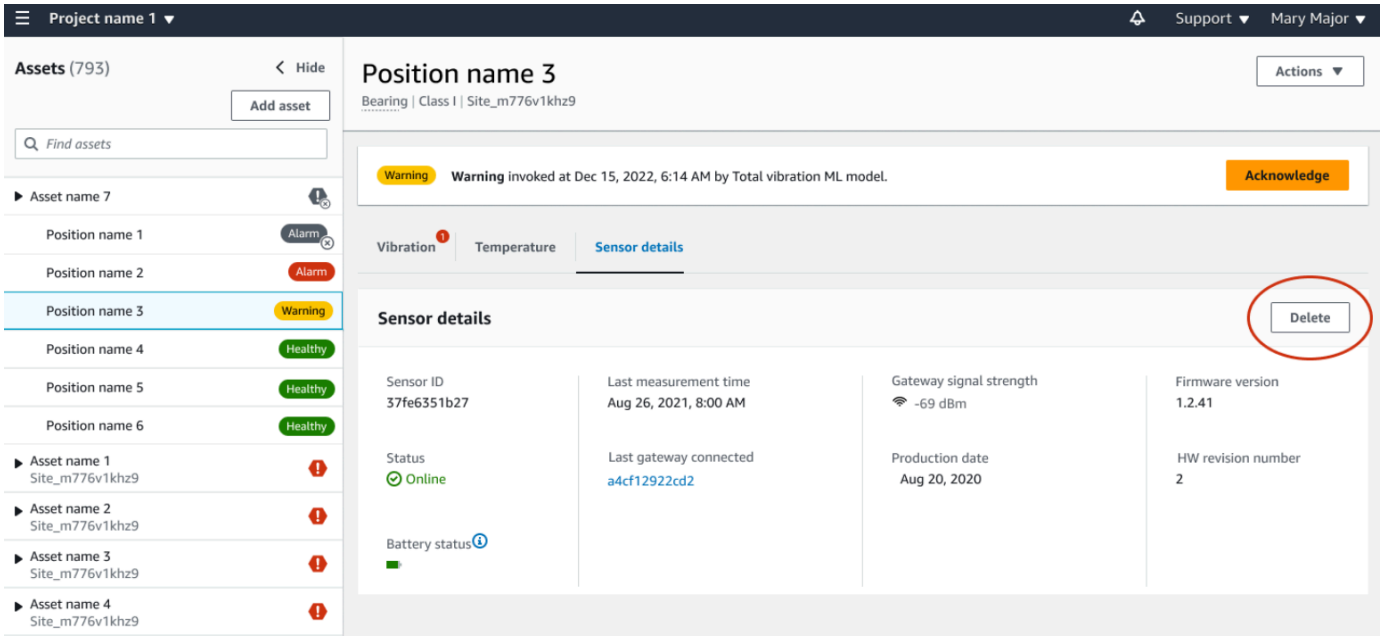



After a sensor has been deleted, the status for that position says **No sensor**.




## To delete a sensor in the web app

- Choose **Delete** from the **Sensor details** tab.




# Deleting a sensor position

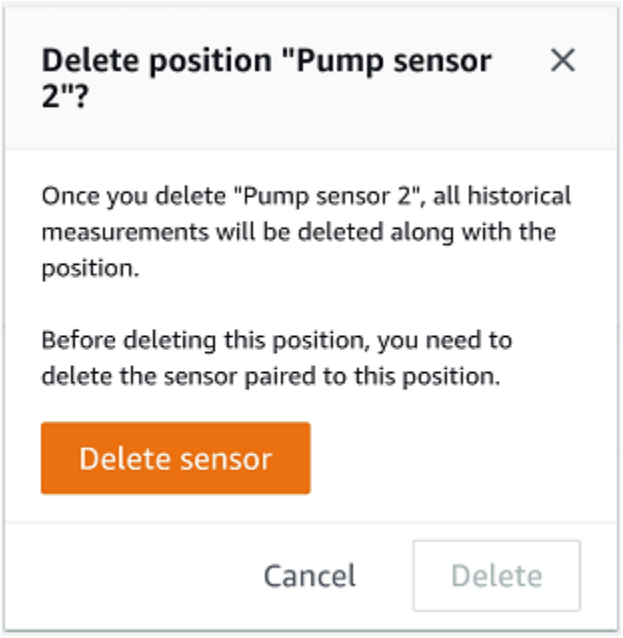
Deleting a sensor position removes that data collection point from the asset. If a sensor is still paired to this position, you need to remove it before you can delete the position.

**Topics**


- To delete a sensor position in the mobile app
- To delete a sensor position in the web app


## To delete a sensor position in the mobile app

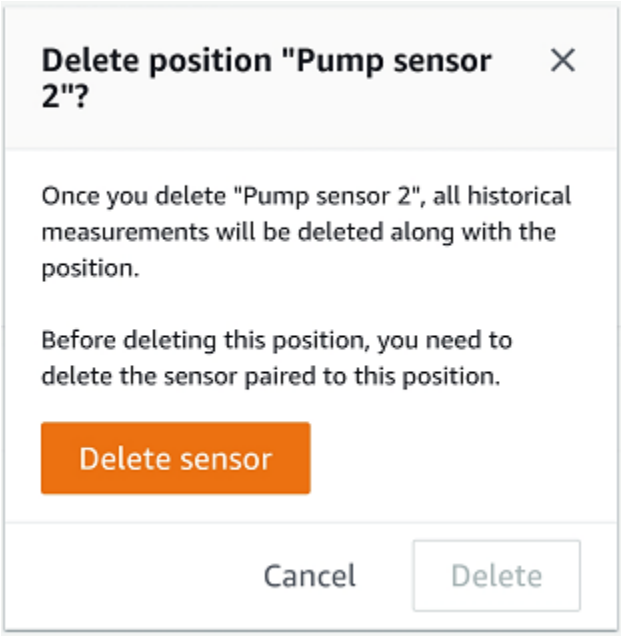
1. From the **Assets** list, choose the asset that has the sensor position that you want to delete.
2. Under **Sensors**, choose **Actions**.
3. Choose **Delete position**.
4. If the position has a sensor paired to it, delete the sensor by choosing **Delete sensor**. Otherwise, skip to the next step.




5. Choose **Delete**.

## To delete a sensor position in the web app

1. Select the position.
2. Choose the **Actions** button in the **Positions** table.
3. Choose **Delete position**.
4. If the position has a sensor paired to it, delete the sensor by choosing **Delete sensor**. Otherwise, skip to the next step.




5. Choose **Delete**.

# Understanding sensor details

To check that a sensor is performing as expected, check its details page. The **Sensor details** page shows the following information:

- Sensor ID
- Sensor status
- Date the sensor was last commissioned
- Date of the last measurement
- Last gateway it connected to
- Current signal strength of the last gateway
- Sensor type
- Firmware version
- Sensor battery status

### Topics


- Viewing sensor details
- Sensor connectivity status

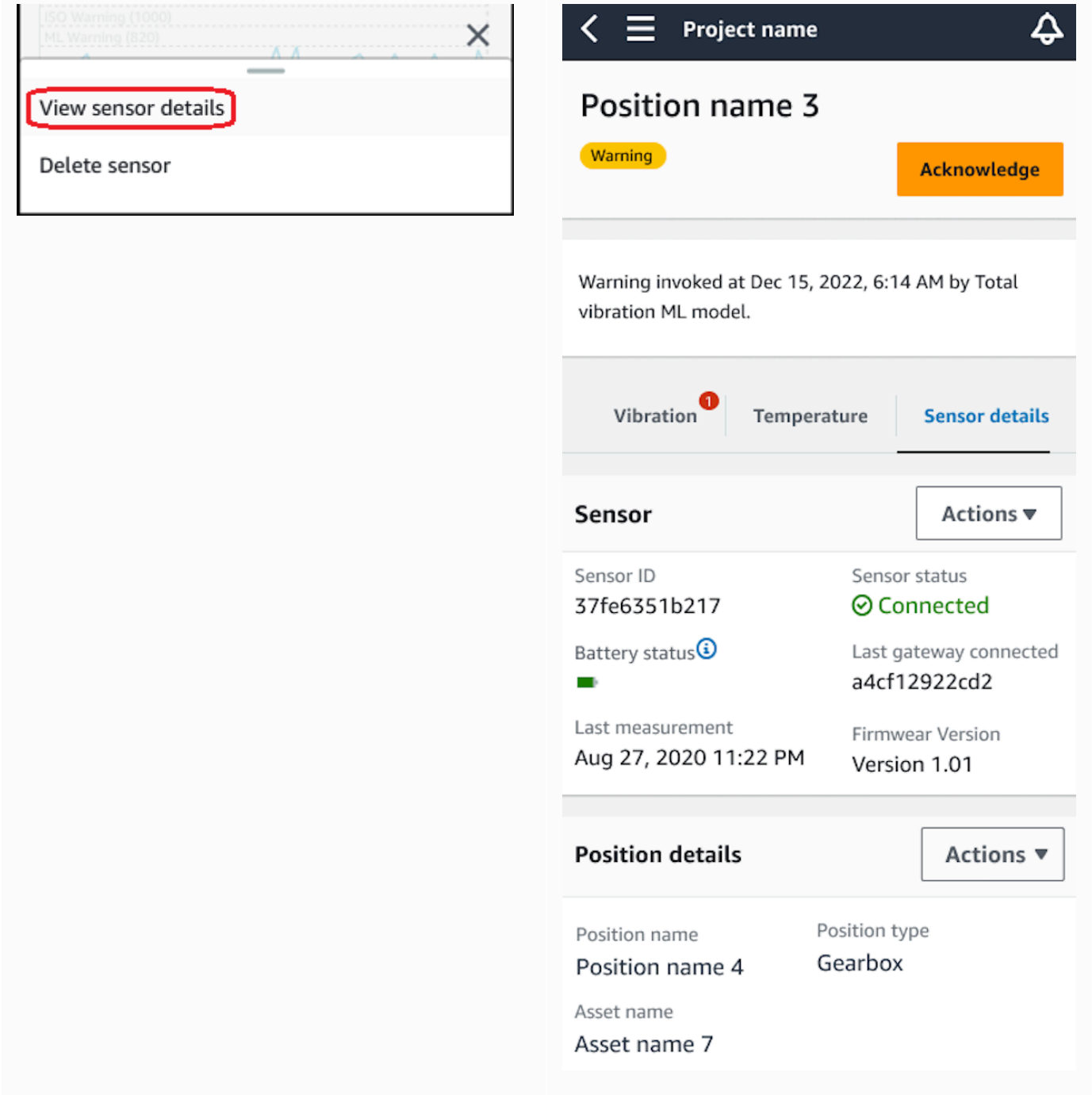
- Sensor battery status

# Viewing sensor details

You can view sensor details on both the mobile and web app. The following section shows you how.

## To view sensor details in the mobile app

1. From the **Assets** list, choose the asset that is paired with the sensor that you want to view.
2. Choose the sensor.
3. Select the Position that is connected to the sensor you want to view.
4. Choose the **Sensor details** tab.
5. Choose the **Sensor Actions** button.
6. Choose **View sensor details**.

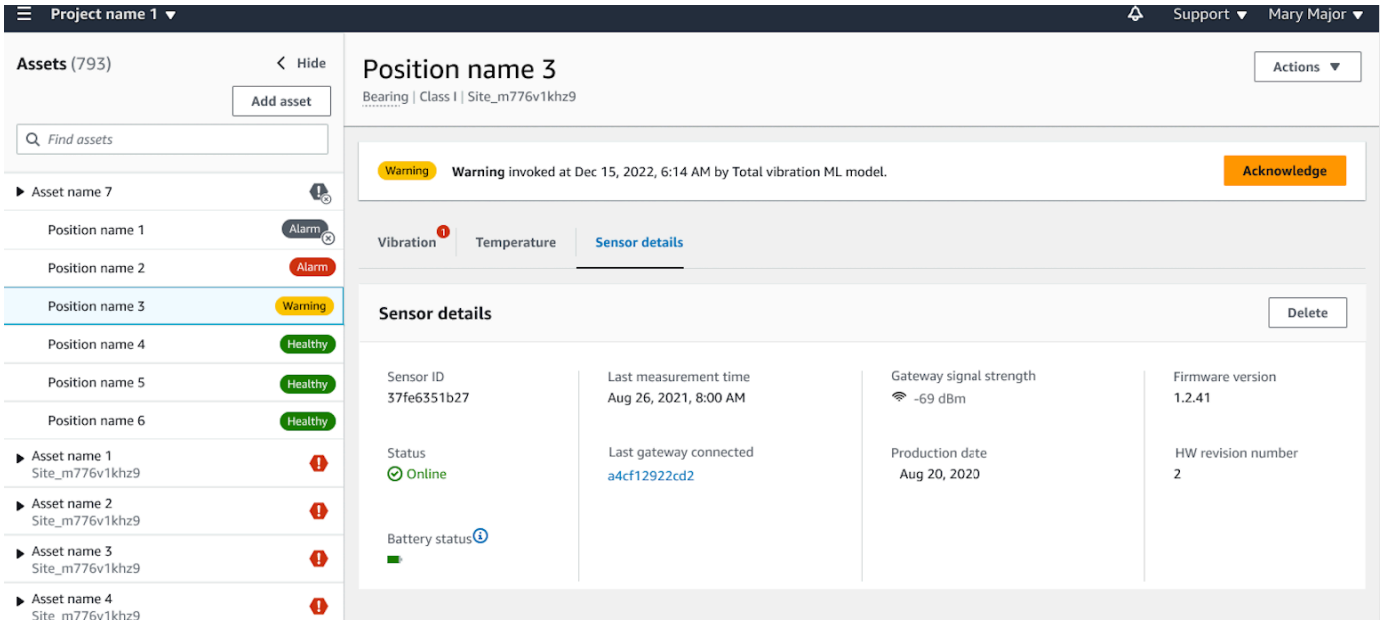



The **Sensor details** page is displayed.

## To view sensor details in the web app

1. From the **Assets** list, choose the asset that is paired with the sensor that you want to view.

2. Information about the sensor will be shown automatically in the **Sensor details** tab on the lower right side of the app window.



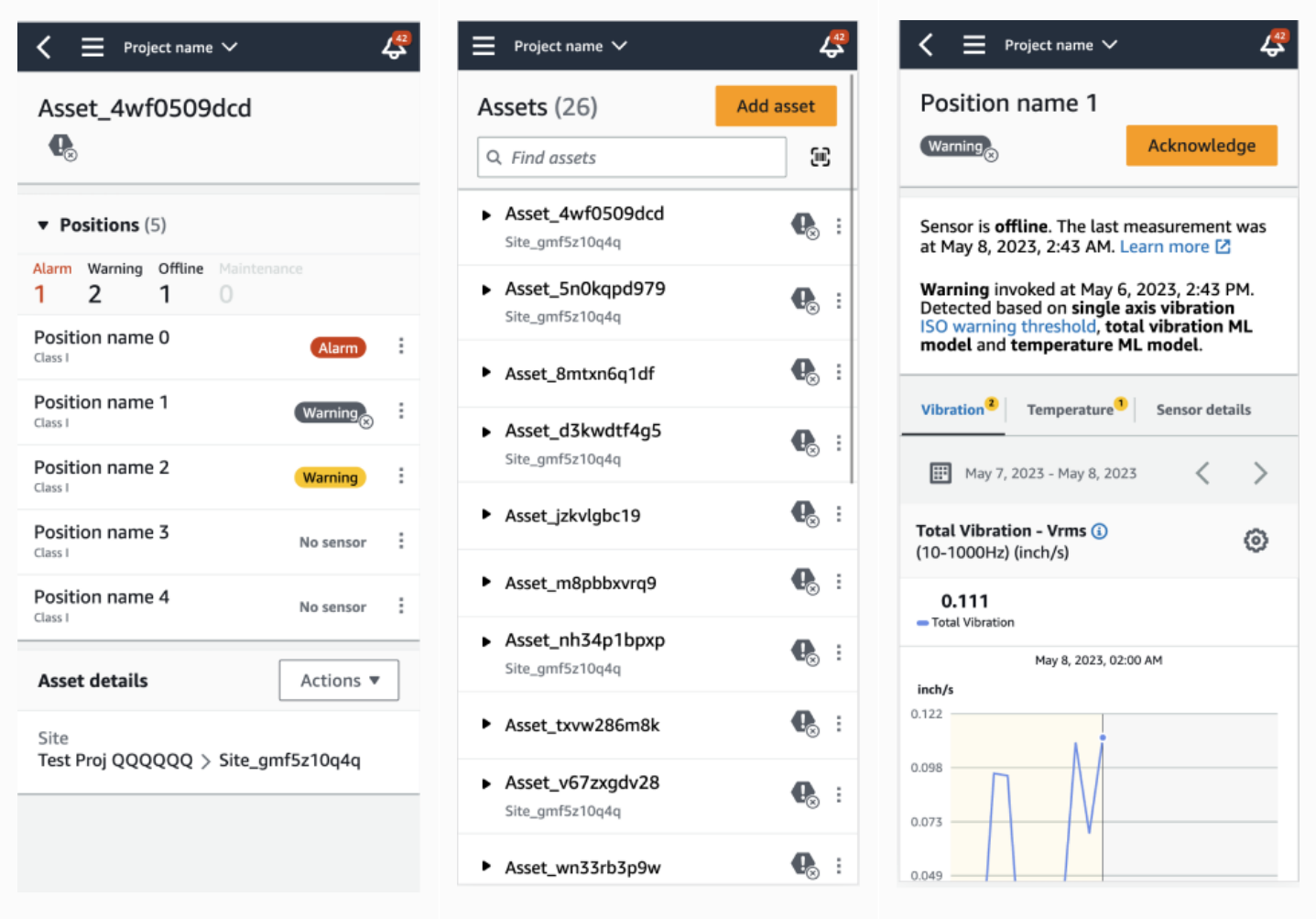

## Sensor connectivity status

When you create a sensor, you can monitor its position and connectivity status on the Amazon Monitron assets list. Sensor position states are **healthy/maintenance/warning/alarm** and sensor connectivity states are **online/offline**. A sensor's default state is **online**. If it times out due to connectivity issues, its state will change to **offline**. Once connectivity is restored, the sensor will return to an **online** state. A sensor will maintain its most recent states if it goes offline.

An asset's badge on the asset list shows its most severe position and connectivity states. If its position includes both **warning** and **healthy** states, it will have a **warning** state on the asset list. If at least one asset is **offline**, it will have an **offline** state in the asset list.

> **Note**
>
> If a sensor is **offline**, its status is prioritized in the Amazon Monitron application asset list. The app does not support notifications if a sensor goes offline, but the app will indicate if a device goes offline.

The following images show sensors that are offline.




## Sensor battery status

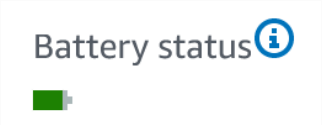
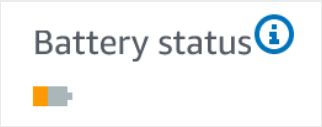
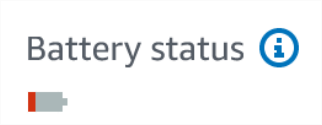
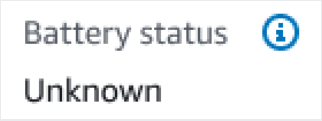
To help you keep track of your sensor health, each Amazon Monitron displays a sensor battery life status. You can check your sensor battery life from both the mobile app and the web app. You can use this battery status to decide when to buy new sensors.

> **Note**
>
> Estimated remaining battery life is calculated based on 5 years sensor battery life for a sensor taking measurements hourly.

**Important**

Battery life status is not available for sensors with a firmware version less than 1.6.0. You need to wait until the sensor is updated to view battery life status.

The following table shows the different sensor battery states:

| Battery status | Condition | Time remaining | Action |
|---|---|---|---|
|   | **Normal** | Sensor battery is in healthy state. | No sensor battery monitoring currently needed. |
|   | **Low** | Battery has less than 1 year of life left. | Begin monitoring your sensor battery. |
|   | **Urgent** | Battery has less than 3 months of life left. | Replace your sensor as soon as possible. |
|   | **Unknown** | Battery life status is unknown. | 1. If commissioning sensor for the first time, wait for a minute till the sensor sends its first measurement.<br>2. Then, make sure you have commision ed a gateway correctly and take |

| Battery status | Condition | Time remaining | Action |
|---|---|---|---|
| | | | a measurement using the mobile app.<br><br>See Gateways and Taking a one-time measurement for details. |

**Note**

If you do not replace your sensor after its battery status is urgent, the sensor's connectivity state will change to **Offline**.

# Identifying sensor position

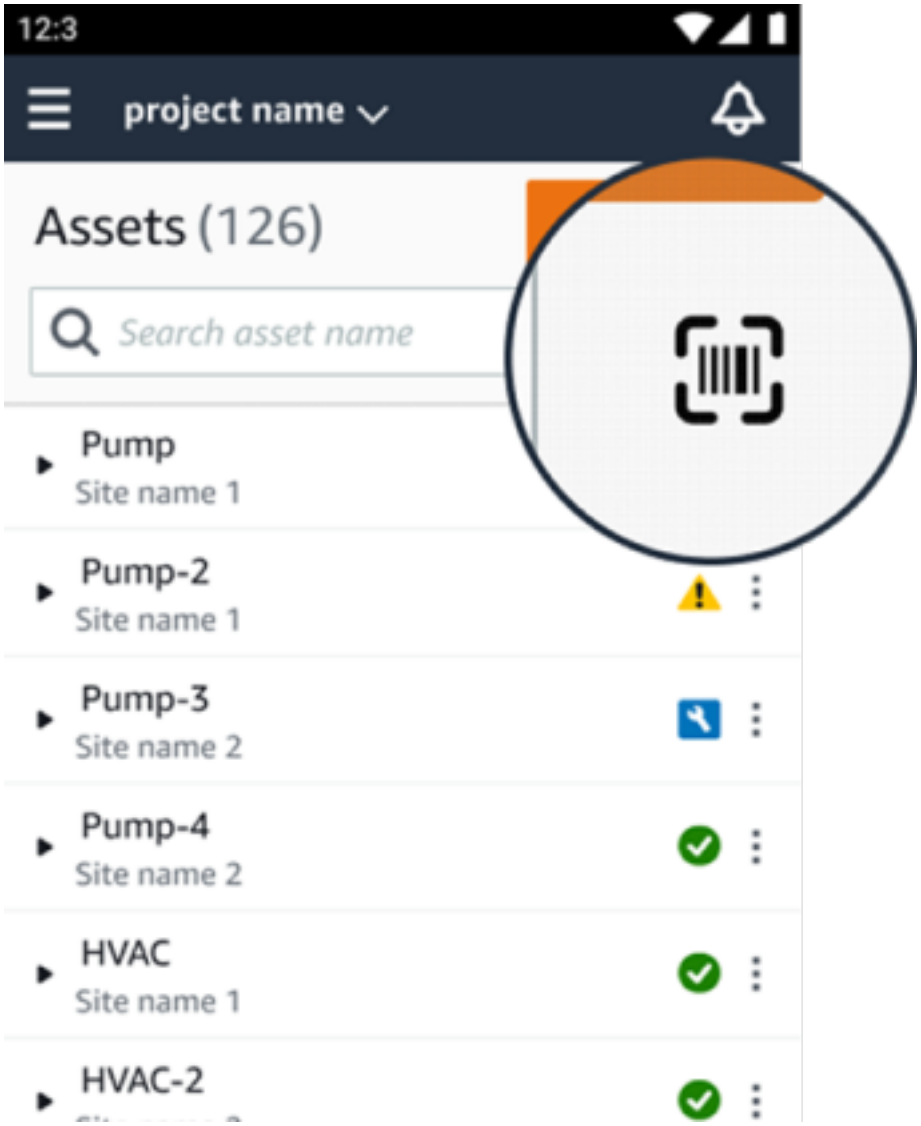
Use the mobile app to find sensors in the factory or shop floor without searching through your asset list.

**Topics**

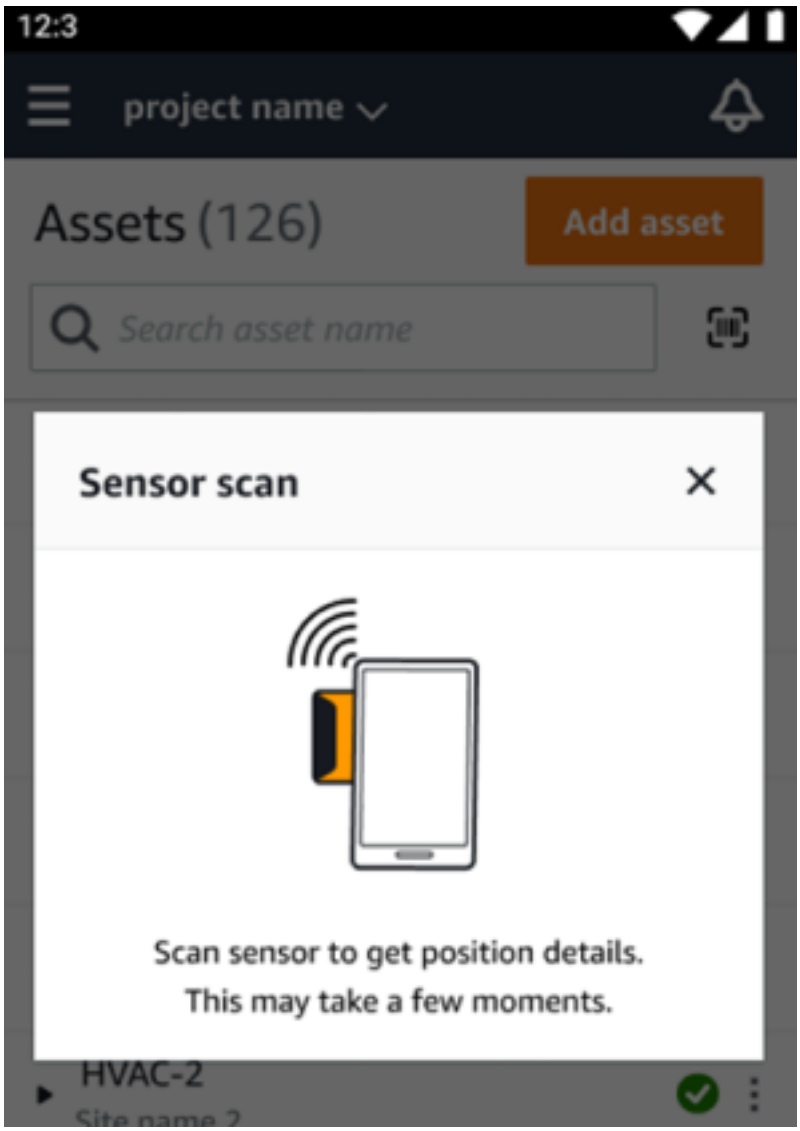
- Identifying paired sensor
- Missing or unread sensor
- Permissions and site commissioning issues
- Scanning sensor from another site

## Identifying paired sensor

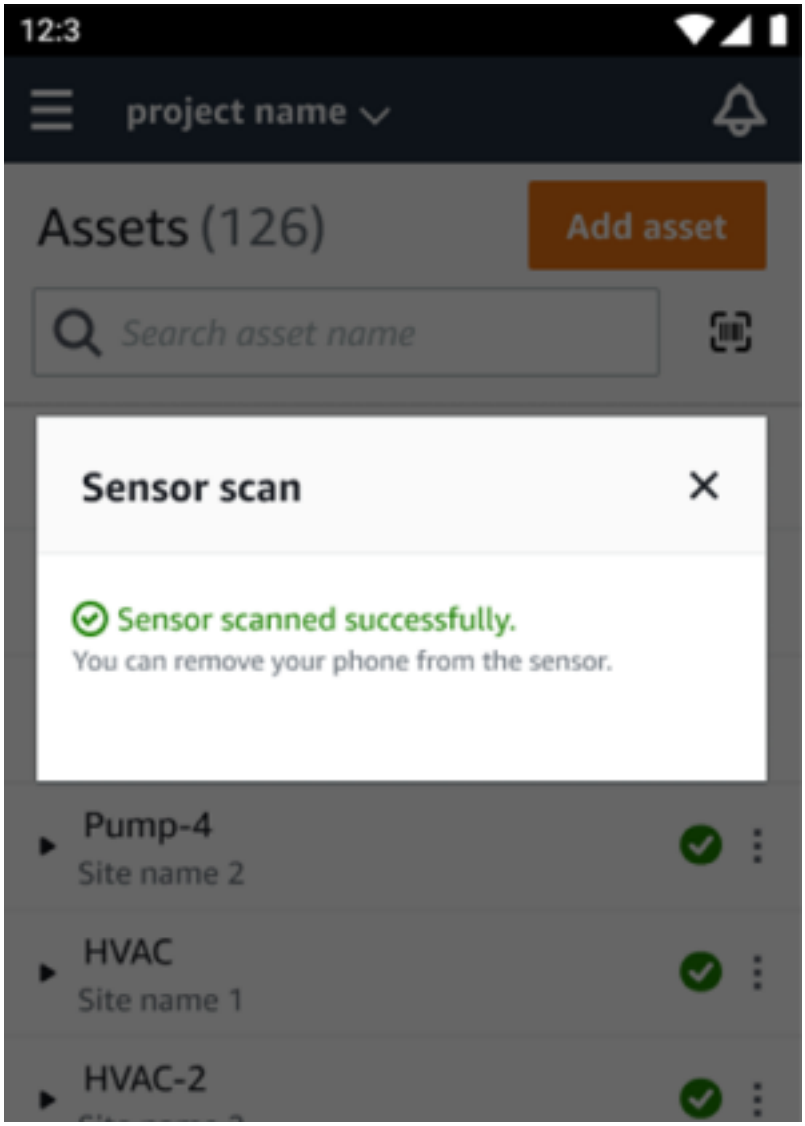
1. If the sensor has been paired, select the **scan sensor** icon from your asset page to scan any sensor affiliated with your project.




2. Select a desired asset to scan.
3. Hold your phone near the sensor and scan it to read its position details. It may take a few moments for the mobile app to generate results.



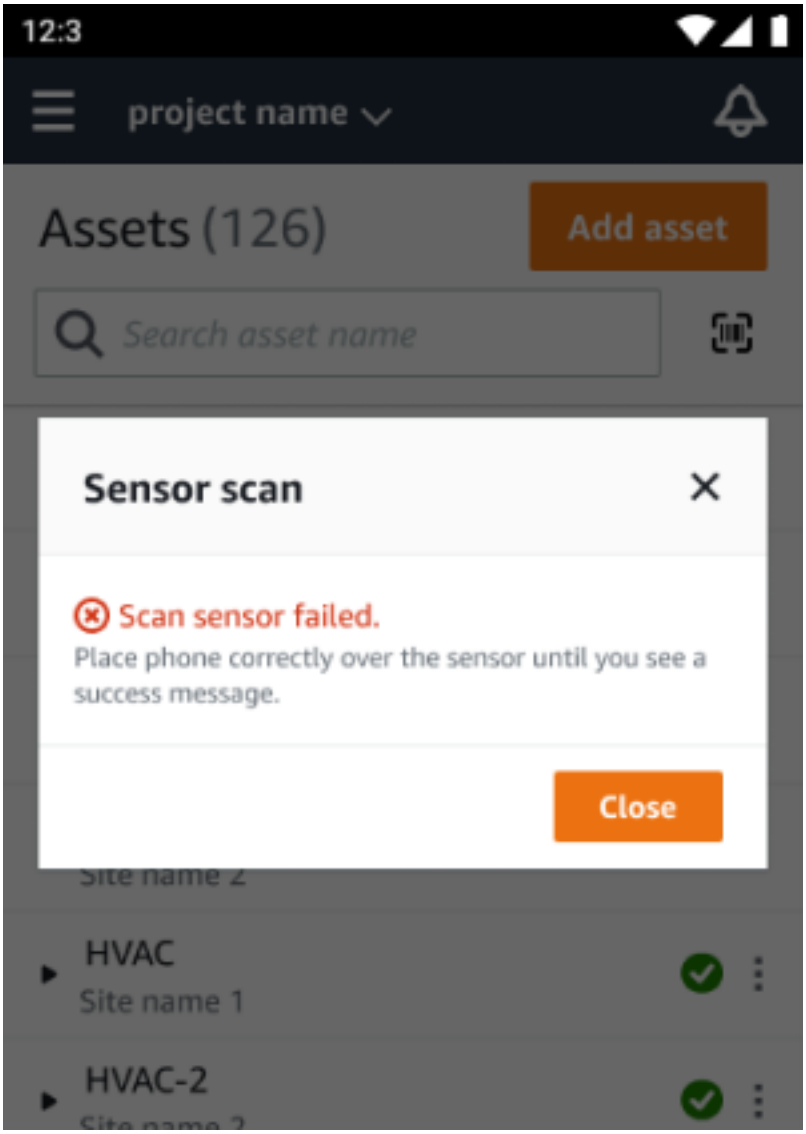

4. After you've scanned your sensor successfully, your mobile app will show the sensor's position and details.


12:3
project name
Assets (126)
Add asset
Search asset name
Sensor scan
Sensor scanned successfully.
You can remove your phone from the sensor.
Pump-4
Site name 2
HVAC
Site name 1
HVAC-2




## Missing or unread sensor

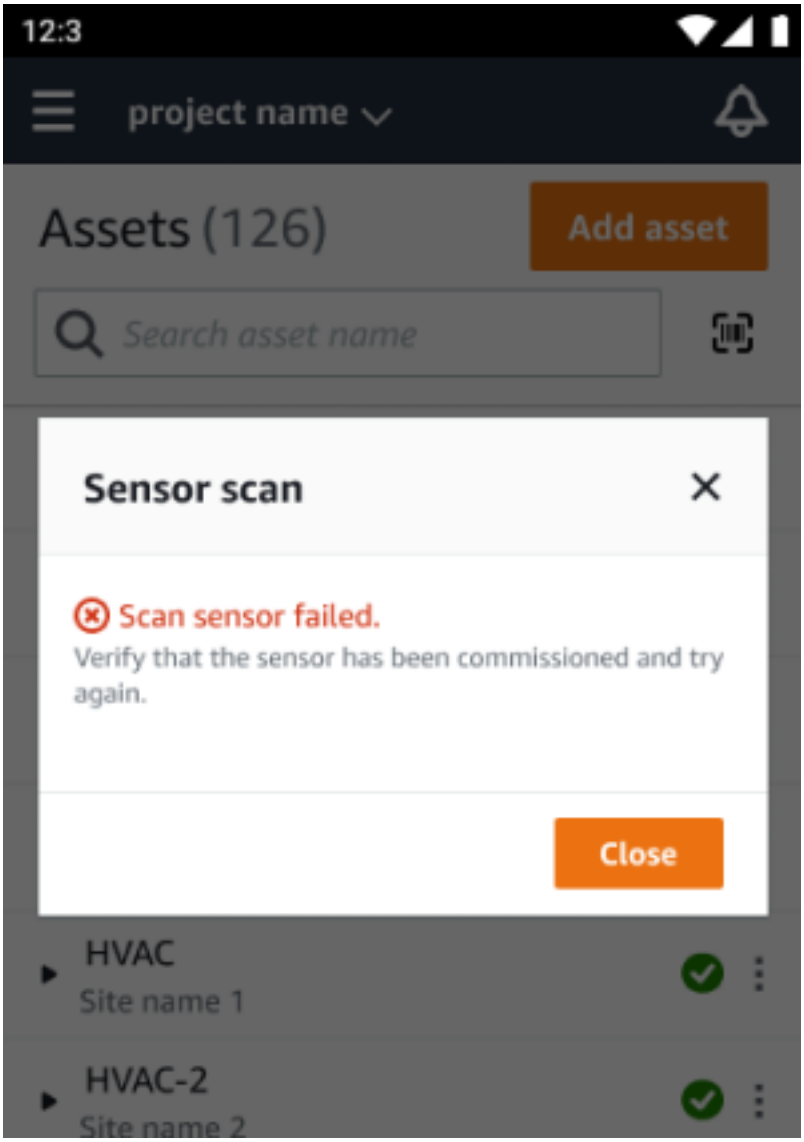
If the sensor is not read during the scan, place your phone correctly over the sensor until you see a success message.



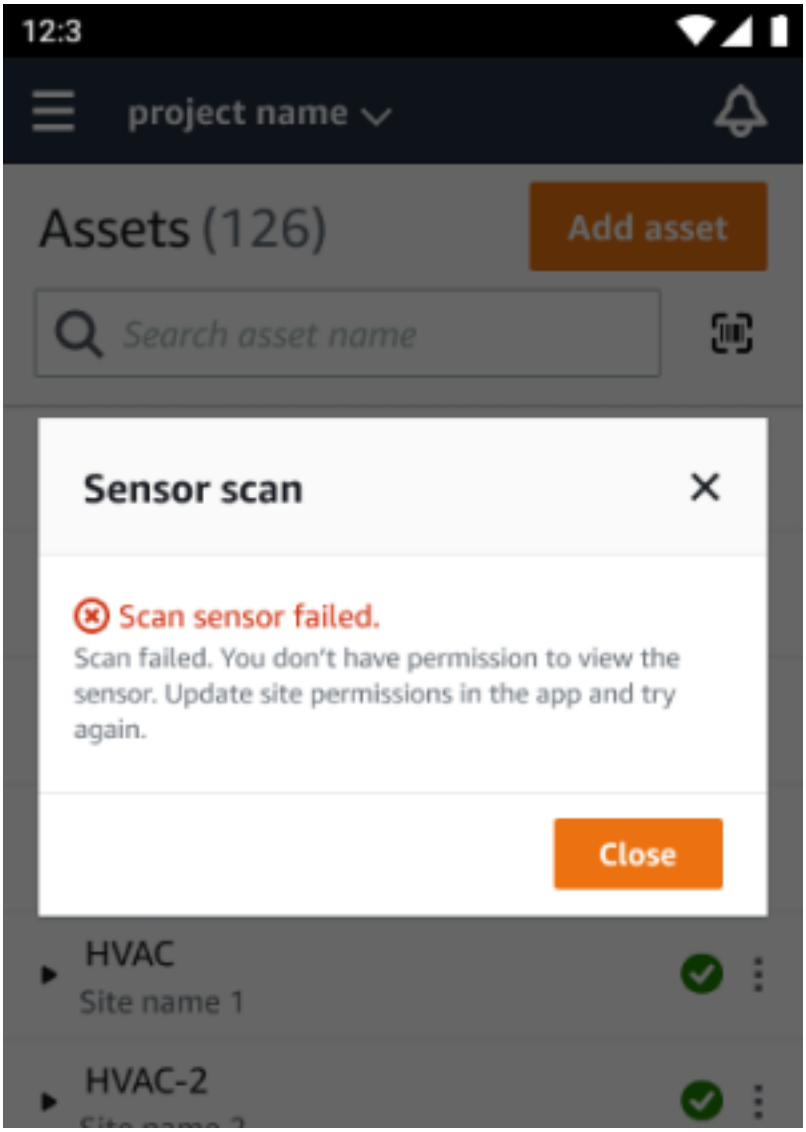

If no sensor was added, add an asset and try again.

## Permissions and site commissioning issues

If the sensor hasn't been commissioned for a site, commission the sensor and try again.

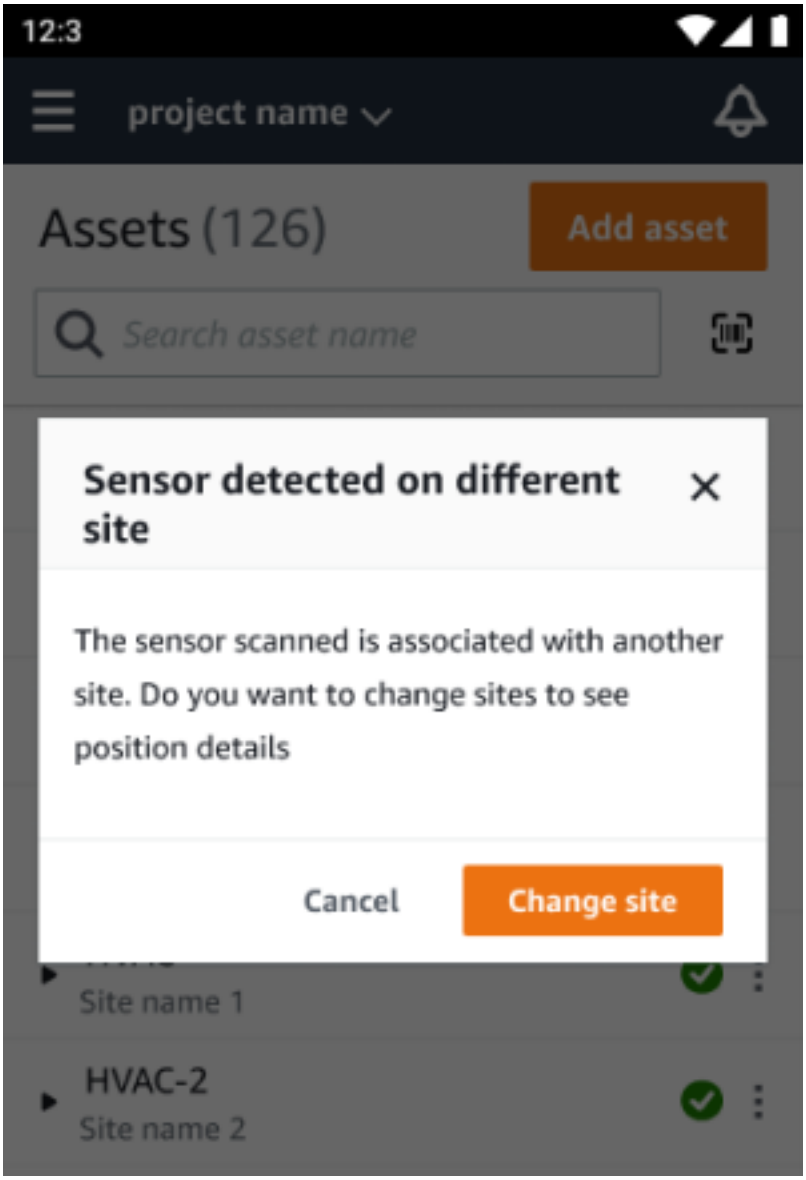



If the sensor was commissioned for a site that you can't access, update site permissions in the app and try again to read the sensor’s position details.




## Scanning sensor from another site

If you scan a sensor that is commissioned for another site, and you're redirected to that site, scan the sensor on that site.

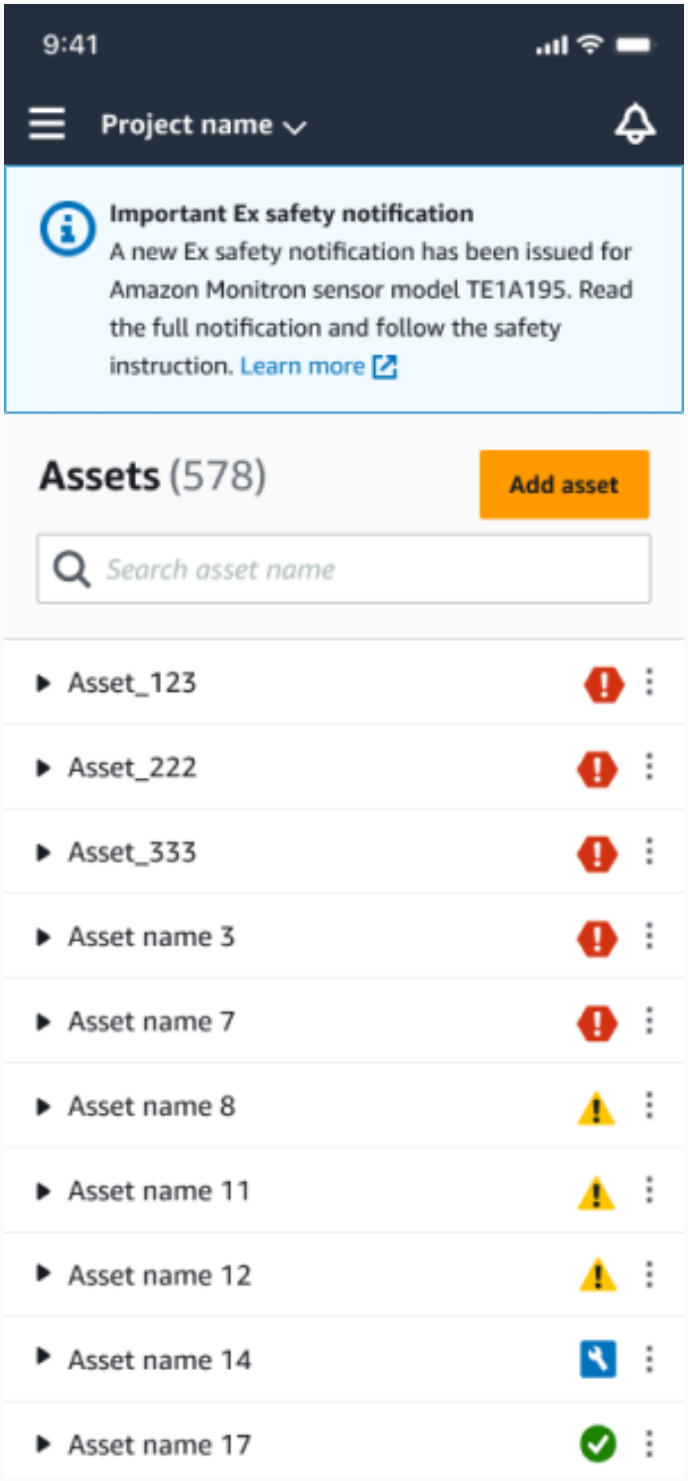


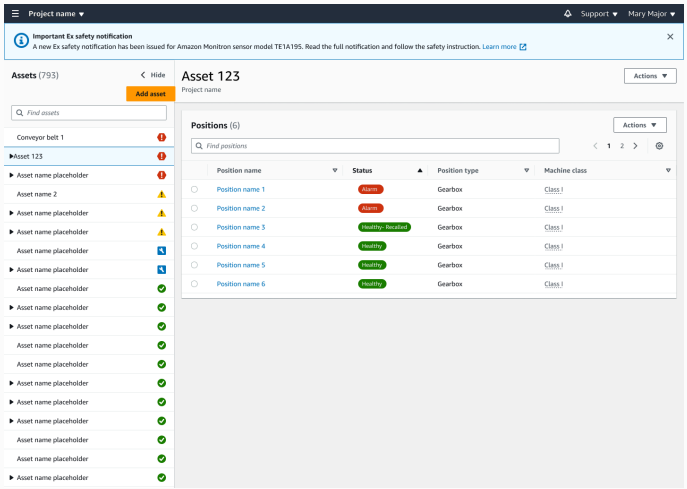

# Ex-rated sensors

> **Warning**
>
> Before installing and using a sensor, see Ex Safety and Compliance Guide for all warnings and instructions.

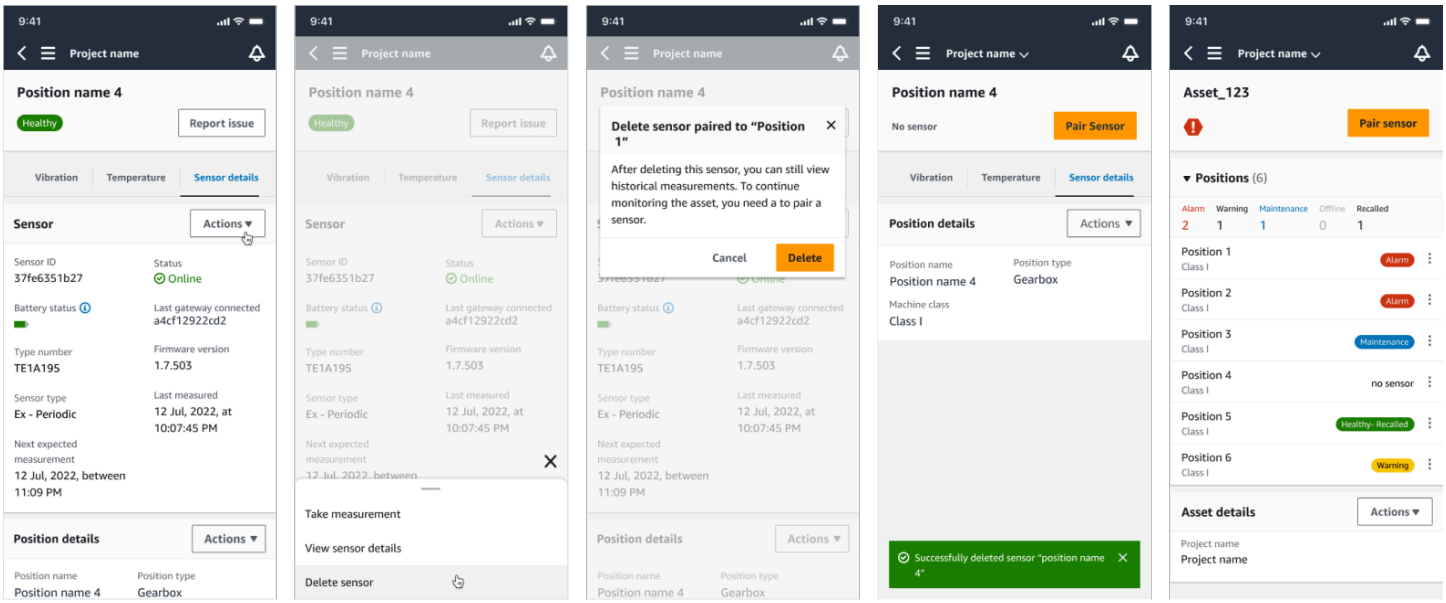
Amazon Monitron can notify you about product issues that could affect safety in explosive and hazardous areas. You'll receive these notifications in the web app if you're an existing customer with sensors installed.

If a sensor has an urgent safety advisory, you'll receive a notification and explanation when you log on to the web or mobile app. Before you can proceed, you'll be required to acknowledge the advisory and perform the recommended actions in the safety warning. For example, you may need to physically remove a sensor from a hazardous area, as it could be a potential ignition source.



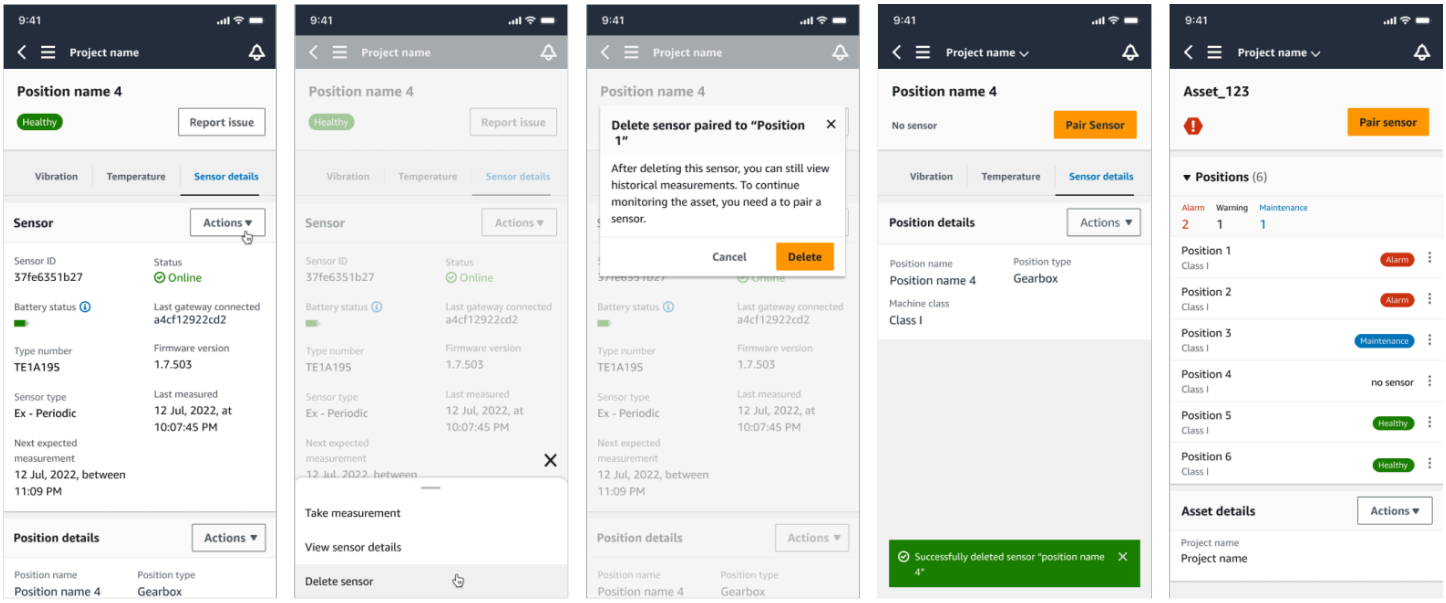
When a sensor has a healthy position status, you can use the sensor to take measurements, view sensor details, or delete the sensor.

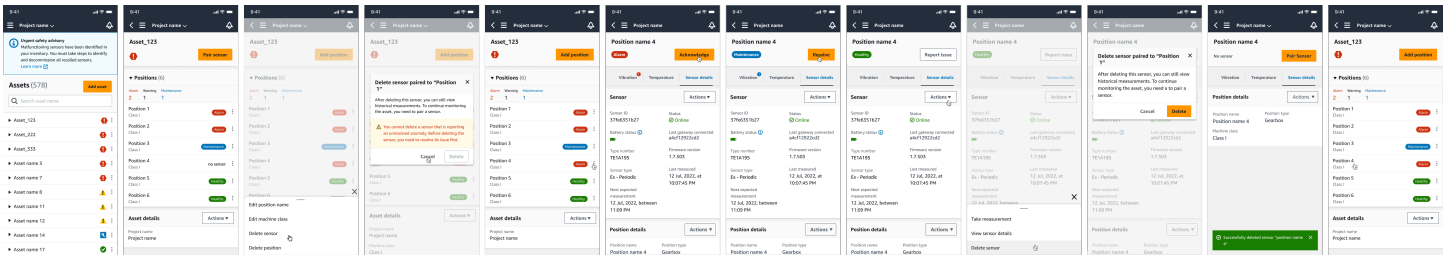



If you need to delete a sensor, make sure it's in a healthy state first. A sensor's position must be in a healthy state before you can delete it. If you do remove a sensor that is under safety notification or not in a healthy state, you'll receive a notification explaining that you must clear the alert first.

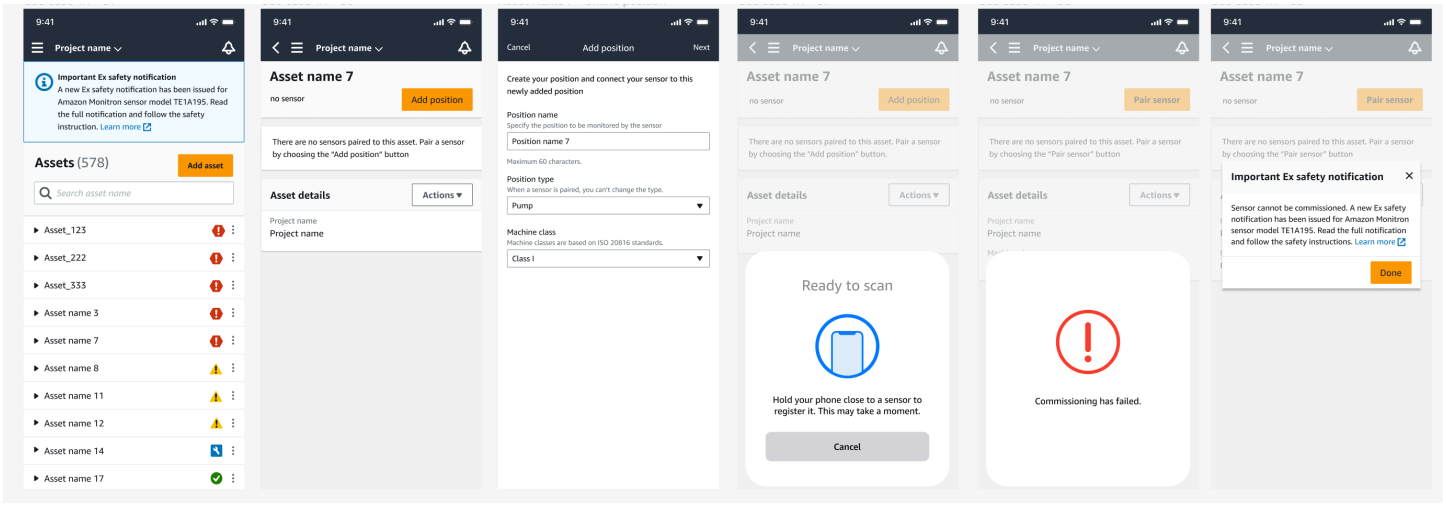
**To clear the alert:**

1. In the asset list, select the unhealthy sensor.
2. Review the errors.
3. Select **Acknowledge** to confirm that you understand the active alerts related to the sensor.
4. Select **Resolve** to fix the anomaly that the sensor is reporting. After resolving the issue, the sensor should return to a healthy state.
5. Delete the sensor from either the **Asset list** or the **Position details** page.



If you try to commission a sensor under a safety notification, the commissioning process will fail. You'll receive a notification describing the reason for the failure.



# Understanding sensor measurements and monitoring machine abnormalities

Amazon Monitron monitors temperature and vibration data from sensors and watches asset conditions for abnormalities that might indicate developing faults. You monitor your assets either with the Amazon Monitron web app, or with the Amazon Monitron mobile app, which you download and install on your smartphone. Amazon Monitron supports only smartphones using Android 8.0+ or iOS 14+ with Near Field Communication (NFC) and Bluetooth.

This topic describes how to read sensor measurements, respond to notifications about machine abnormalities, and take one-time measurements.

**Topics**


- Choosing your measurement viewing platform
- Viewing sensor measurements
- Understanding sensor measurements
- Understanding asset status
- Acknowledging a machine abnormality
- Resolving an abnormality
- Taking a one-time measurement


## Choosing your measurement viewing platform

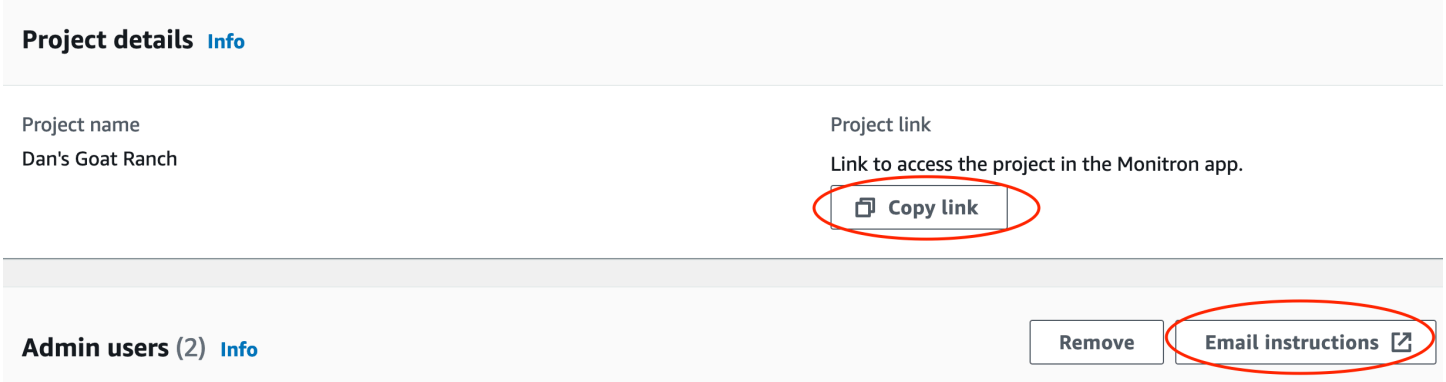
There are two ways to use Amazon Monitron to view your assets' measurements and abnormalities. You can view them in the mobile app, or you can view them in the web app. Each way has its advantages.

With the mobile app, you use your phone's Bluetooth and Near Field Communication (NFC) capabilities to install and configure gateways and sensors, as explained in Wi-Fi gateways.

With the web app, you download your data to a .csv file. Also, your monitor is probably bigger than your phone, so the web app may be a better place to see measurements using line graphs.

You can activate either the mobile app or the web app by clicking on a link to your project. This is the link that the administrator sends to the user, as explained in Sending an email invitation. But

you can re-generate this link from the **Projects** page by selecting a user and then choosing **Email instructions**, or by choosing **Copy link** under **Project details.**




**Topics**

- In-app updates

# In-app updates

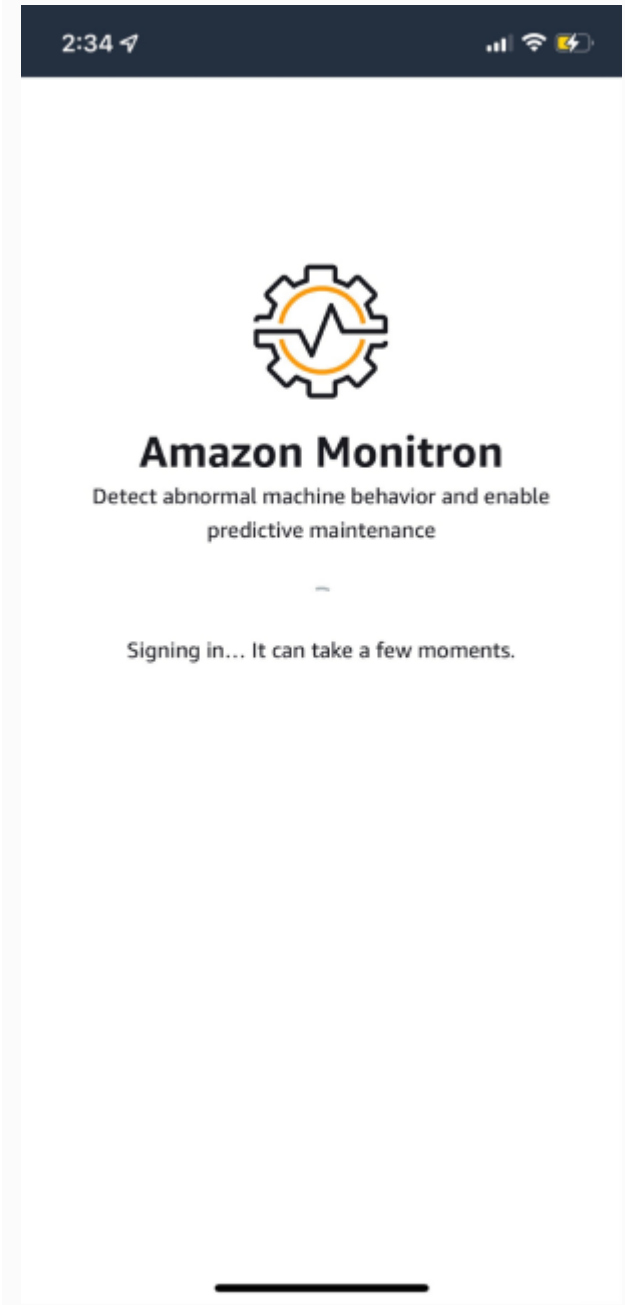
For access to the latest Amazon Monitron features, regularly check your mobile device for updates. Periodically, Amazon Monitron releases new application versions that you'll need to manually update if you don't enable automatic updates. These notifications will be provided on the web app as they become available.

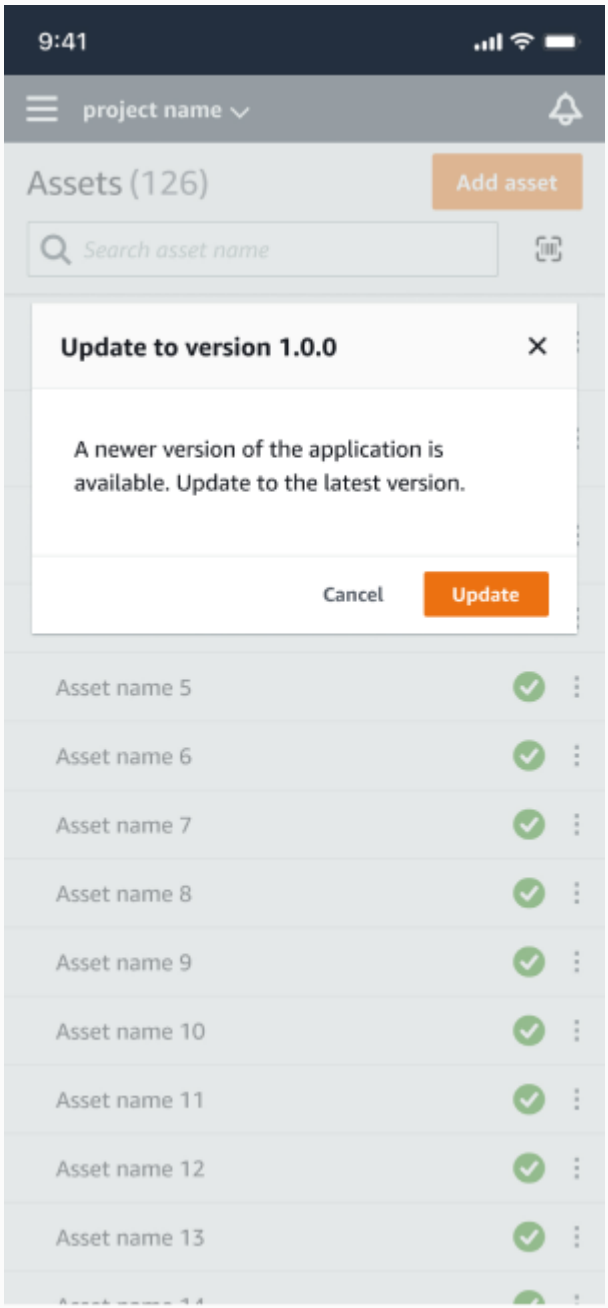
### Flexible and immediate updates

Amazon Monitron provides two kinds of in-app updates: flexible and immediate. **Flexible updates** allow you to elect whether or not to update the Amazon Monitron app once you've signed in. **Immediate updates** contain security updates, and must be installed in order to use the app. You can install updates from the Amazon Monitron app, or directly from Google Play or the App Store.

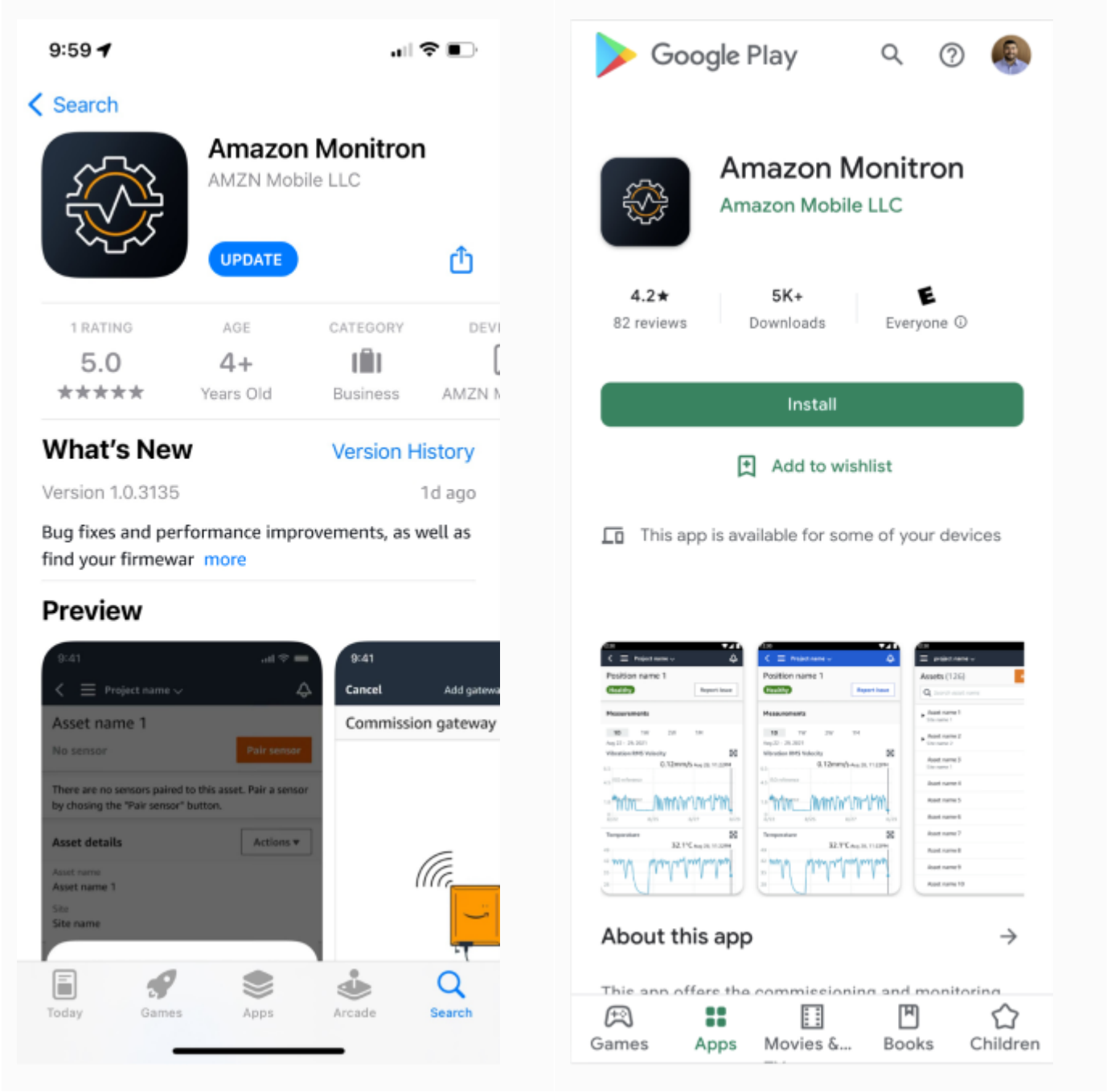
To manually install the latest updates:

1. Sign in to the Amazon Monitron app and choose **Update**.

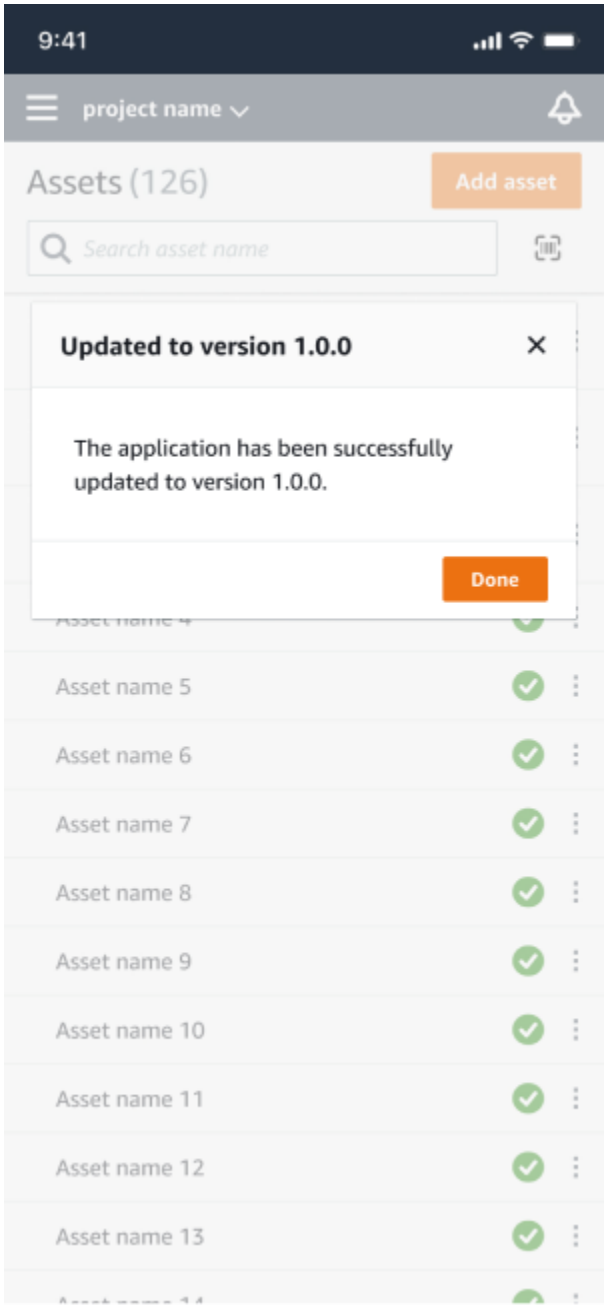



2. When you select **update**, you'll be directed to Google Play or the App Store. Select **Update** or **Install** to start the update.




3. If you start the update process within the Amazon Monitron app, you'll see a success message in the app once the update has been installed.



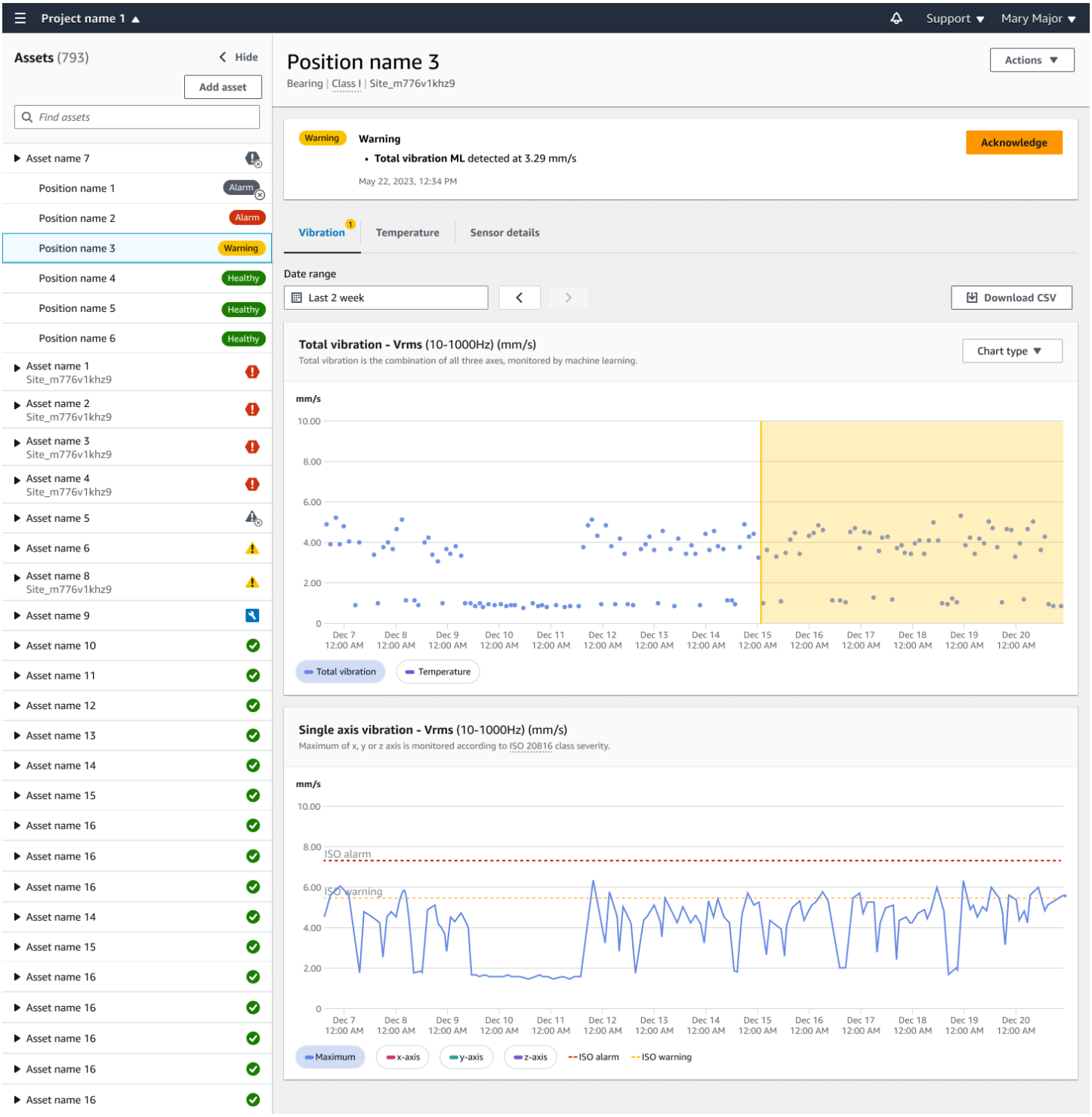

**Note**

You will not see the success message if the update happens automatically, or if you initiate the update process within the App Store or Google Play.

# Viewing sensor measurements

You can choose to view your sensor measurement data in two chart formats: scatter plot and line plot. The following image shows the scatter plot view on the top and the line plot view on the bottom.

> **Note**
>
> You can select your sensor measurement view from the **Chart type** menu in your mobile and web app.


Project name 1
Support
Mary Major
Assets (793)
Hide
Add asset
Find assets
Asset name 7
Position name 1
Alarm
Position name 2
Alarm
Position name 3
Warning
Position name 4
Healthy
Position name 5
Healthy
Position name 6
Healthy
Asset name 1
Site_m776v1khz9
Asset name 2
Site_m776v1khz9
Asset name 3
Site_m776v1khz9
Asset name 4
Site_m776v1khz9
Asset name 5
Asset name 6
Asset name 8
Site_m776v1khz9
Asset name 9
Asset name 10
Asset name 11
Asset name 12
Asset name 13
Asset name 14
Asset name 15
Asset name 16
Asset name 16
Asset name 16
Asset name 14
Asset name 15
Asset name 16
Asset name 16
Asset name 16
Asset name 16
Position name 3
Bearing | Class I | Site_m776v1khz9
Actions
Warning
Warning
• Total vibration ML detected at 3.29 mm/s
May 22, 2023, 12:34 PM
Acknowledge
Vibration
Temperature
Sensor details
Date range
Last 2 week
Download CSV
Total vibration - Vrms (10-1000Hz) (mm/s)
Total vibration is the combination of all three axes, monitored by machine learning.
Chart type
mm/s
10.00
8.00
6.00
4.00
2.00
0
Dec 7 12:00 AM
Dec 8 12:00 AM
Dec 9 12:00 AM
Dec 10 12:00 AM
Dec 11 12:00 AM
Dec 12 12:00 AM
Dec 13 12:00 AM
Dec 14 12:00 AM
Dec 15 12:00 AM
Dec 16 12:00 AM
Dec 17 12:00 AM
Dec 18 12:00 AM
Dec 19 12:00 AM
Dec 20 12:00 AM
Total vibration
Temperature
Single axis vibration - Vrms (10-1000Hz) (mm/s)
Maximum of x, y or z axis is monitored according to ISO 20816 class severity.
mm/s
10.00
8.00
ISO alarm
6.00
ISO warning
4.00
2.00
0
Dec 7 12:00 AM
Dec 8 12:00 AM
Dec 9 12:00 AM
Dec 10 12:00 AM
Dec 11 12:00 AM
Dec 12 12:00 AM
Dec 13 12:00 AM
Dec 14 12:00 AM
Dec 15 12:00 AM
Dec 16 12:00 AM
Dec 17 12:00 AM
Dec 18 12:00 AM
Dec 19 12:00 AM
Dec 20 12:00 AM
Maximum
x-axis
y-axis
z-axis
ISO alarm
ISO warning

# Understanding sensor measurements

When a sensor is initially paired to an asset, Amazon Monitron will learn from the vibration and temperature data collected from the equipment, establishing a baseline to determine what is "normal" for that asset. It will use this learning to detect potential failures in the future.

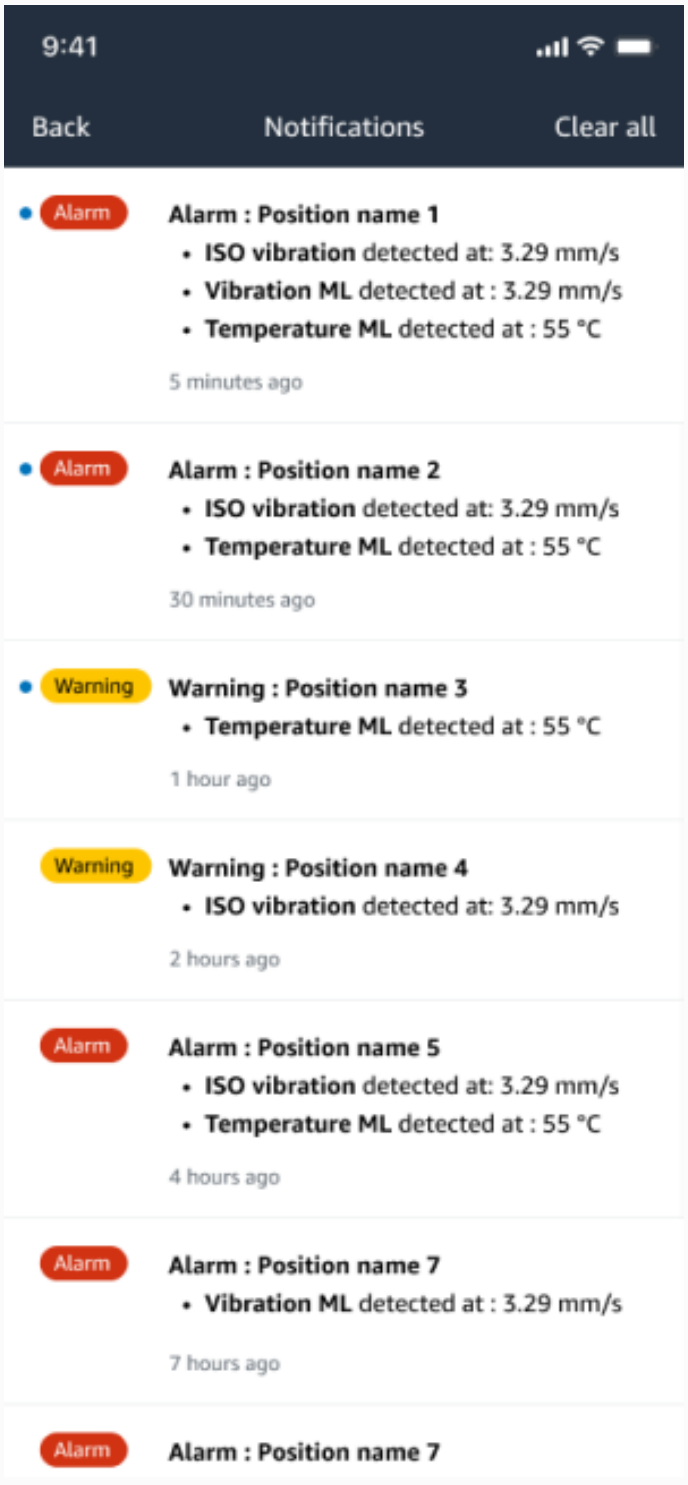
Depending on the situation, operational scenario, use case, and various parameters like the asset's duty cycle, Amazon Monitron will take between 14 and 21 days to establish this baseline. During this initial learning and training phase, the asset is assumed to be healthy.

After establishing a baseline for the asset, Amazon Monitron monitors the data it collects, looking for an event or trend that indicates a potential failure. It specifically watches for increases in temperature, or vibration levels, or both. Increases in temperature and vibrations are two of the main indicators of a malfunctioning machine. Machine abnormalities often indicate that an asset is starting to fail.

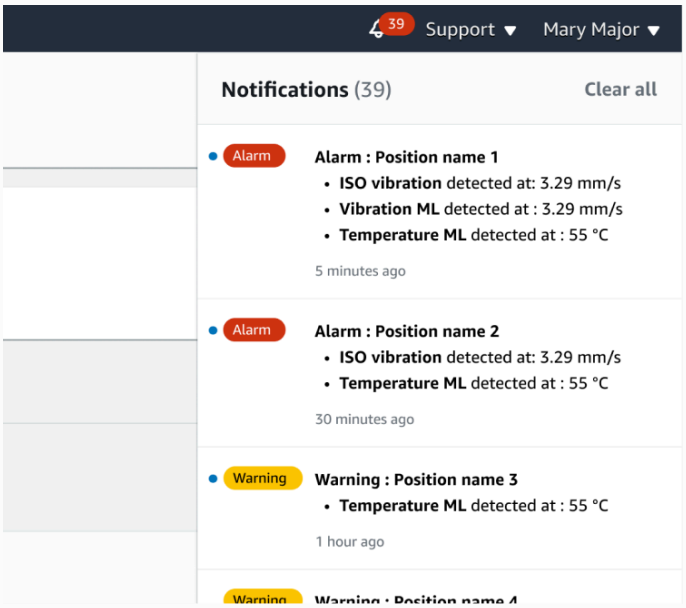
Amazon Monitron uses vibration thresholds established by the International Organization of Standardization (ISO) for your class of machinery. It applies the ISO thresholds in combination with its self-training model to assess actual thresholds to fit your equipment. For example, if your machine runs a little hot or a little cold, or if it vibrates a little bit more than standard, Amazon Monitron adjusts the thresholds slightly so that it can more accurately identify when the machine is acting abnormally.

The only alarms you will recieve during the initial learning and training period will be from the ISO model (which does not require any learning period). You should treat ISO alarms during the training period as you would any alarm—acknowledge the alarm, perform any necessary review of the machine, and then close out the alarm with the suitable action taken code. After that time, Amazon Monitron continues to fine-tune the baseline, building a better picture of "normal" as the sensor collects more data.

If temperature or vibration levels inconsistently rise above the modified threshold, a failure might be possible, but is probably not imminent. In that case, Amazon Monitron sends a `Warning` notification. If the increase is consistently above the threshold, the conditions are clearly abnormal and a failure is much more likely. Under those circumstances, Amazon Monitron sends an `Alarm` notification to the mobile or web app.




a mobile app notification




a web app notification

In this example, the Position 3 sensor has detected a persistent increase in temperature and vibration, indicating that a potential failure needs to be investigated.




**Single axis vibration - Vrms**
(10-1000Hz) (mm/s)



# Understanding asset status

When a sensor detects a machine abnormality, the status of the asset changes. When a problem occurs, you can see it in the **Assets** list in the Amazon Monitron app.

**Topics**


- The Assets list
- Asset and position status
- Notifications


## The Assets list

The **Assets** list displays every asset in your site or project, showing the assets for the site or project that you are currently viewing. For more information about sites and projects, see Navigating between projects and sites in the mobile app.

When you open the Amazon Monitron mobile app, it displays the list of assets associated with the site or project that you last worked with. To navigate to the **Assets** list from elsewhere in the app, use the following procedure.

**To open the assets list in either the mobile app or the web app**

1. Choose the menu icon (☰).
2. Choose **Assets**.

   The assets list is displayed.

| | |
|---|---|
| the assets list in the mobile app | |

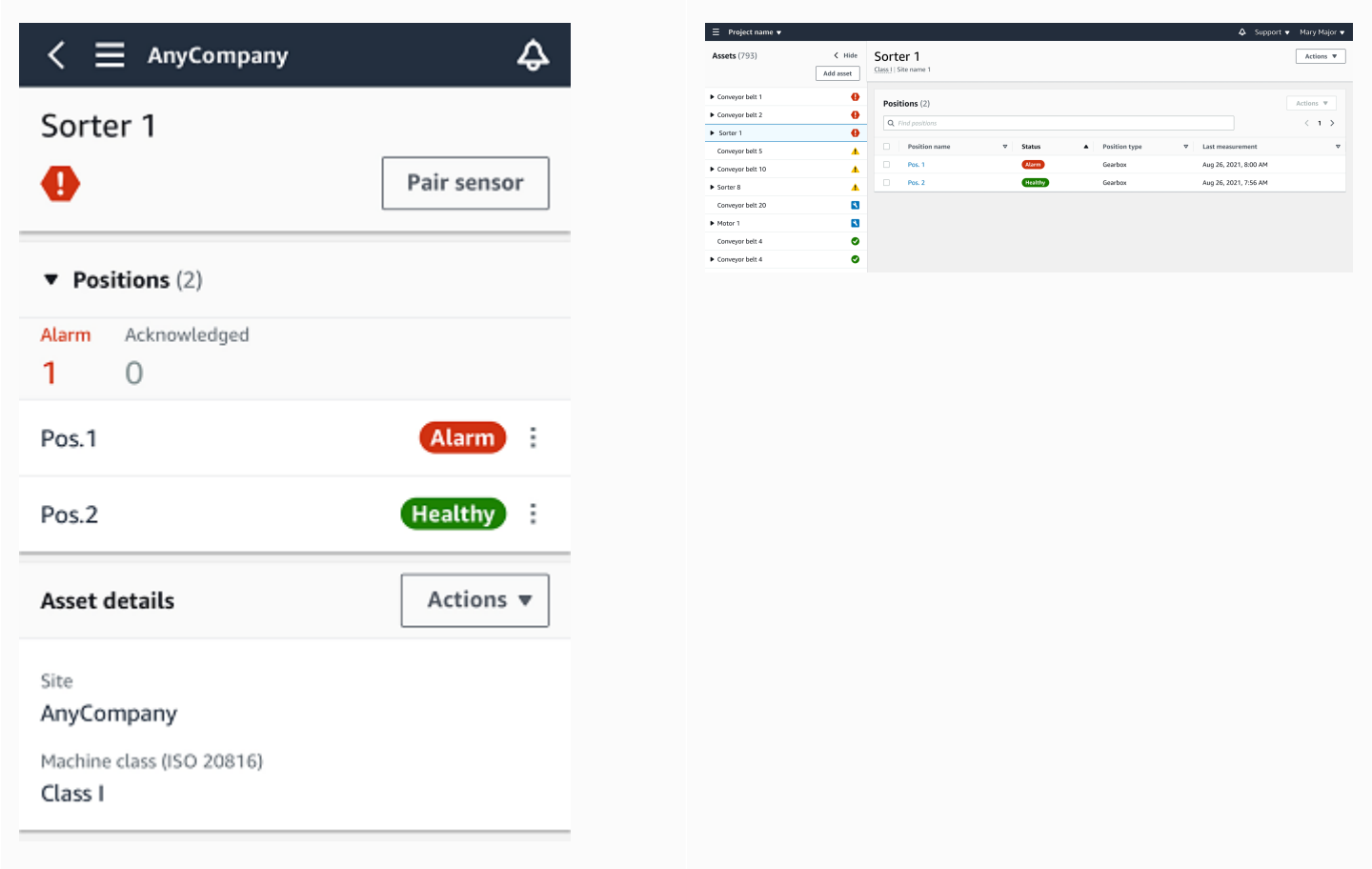
## Asset and position status

The **Assets** list shows the status of each listed asset with an icon, as shown in the following table.

| Status | Meaning |
|---|---|
|  | **Healthy state**: The status of all sensor positions on the asset is healthy. |
|  | **Warning state**: A warning has been triggered for one of the positions of this asset, indicating that Amazon Monitron has detected early signs of potential failure. Amazon Monitron identifies warning condition s by analyzing equipment vibration and temperatu re, using a combination of machine learning and ISO vibration standards. |
|  | **Alarm state**: An alarm has been triggered for one of the positions of this asset, indicating that the machine vibration and temperature is out of the normal range at this position. We recommend that you investigate the issue at the earliest opportuni ty. An equipment failure |

| Status | Meaning |
| --- | --- |
| | might occur if the issue isn't addressed. |
|  | **Acknowledged state**: The warning or alarm state of the position has been acknowled ged by a technician, but the asset has not yet been fixed. |
| No sensor | **No sensor**: At least one position for the asset doesn't currently have a sensor paired to it. |

To learn more about a problem, choose the asset and look at the status of underlying sensor positions.




Amazon Monitron uses icons similar to the asset status icons to show the status of sensor positions.

| Status | Meaning |
| --- | --- |
| Healthy | The position is healthy. All measured values are within the normal range. |
| | **Warning state**: A warning has been triggered for one of the positions of this asset, indicatin g that Amazon Monitron has detected early signs of potential failure. Amazon Monitron identifies warning conditions by analyzing equipment vibration and temperature, using a combination of machine learning and ISO vibration standards. |

| Status | Meaning |
| --- | --- |
| Alarm | An alarm has been triggered for this position, indicating that the machine vibration and temperature is out of the normal range at this position. We recommend that you investiga te the issue at the earliest opportunity. An equipment failure might occur if the issue isn't addressed. |
| Acknowledged | The warning or alarm state of the position has been acknowledged by a technician, but not yet fixed. |
| No sensor | No sensors are currently paired with the position. |

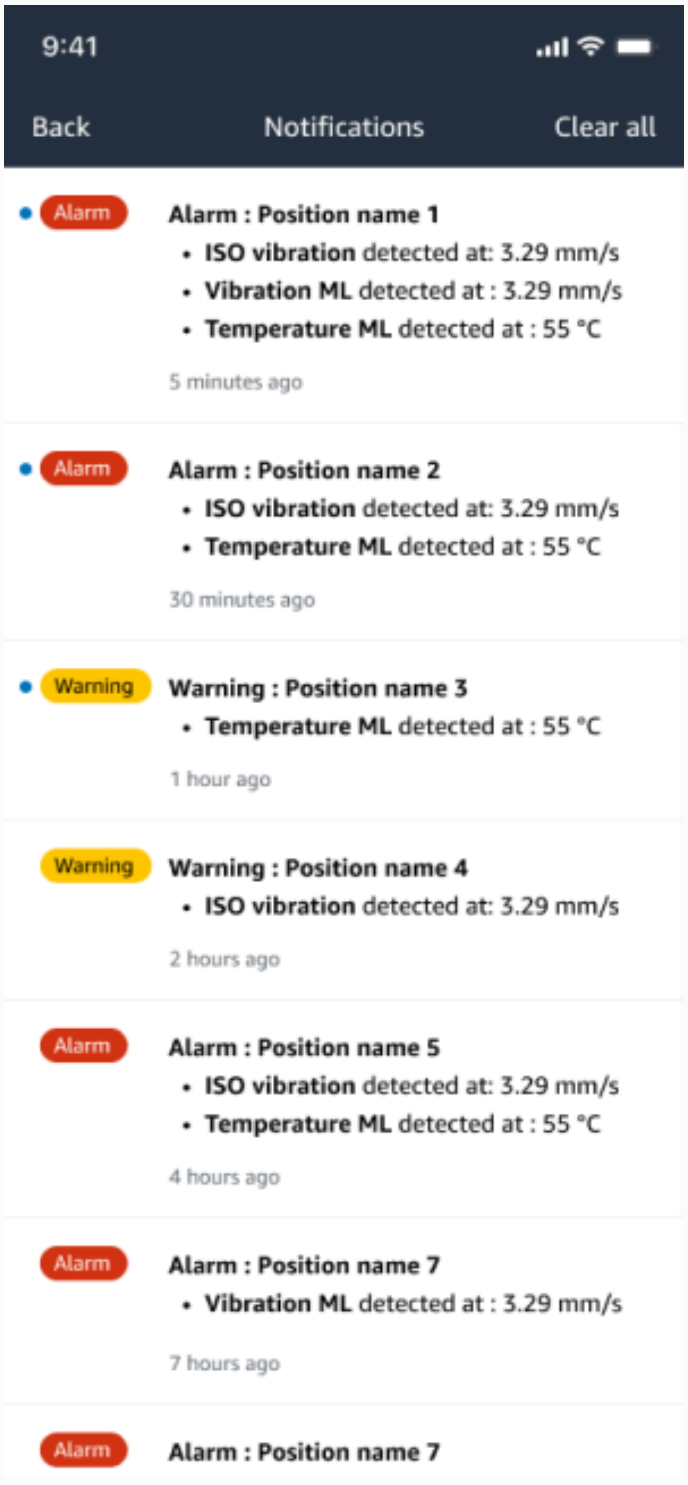
## Notifications

When a warning or an alarm alert is generated, Amazon Monitron sends a notification to the admin user and technician in the app. Authorized personnel can also see notifications by choosing the notification icon in the mobile app when it displays an alert symbol (

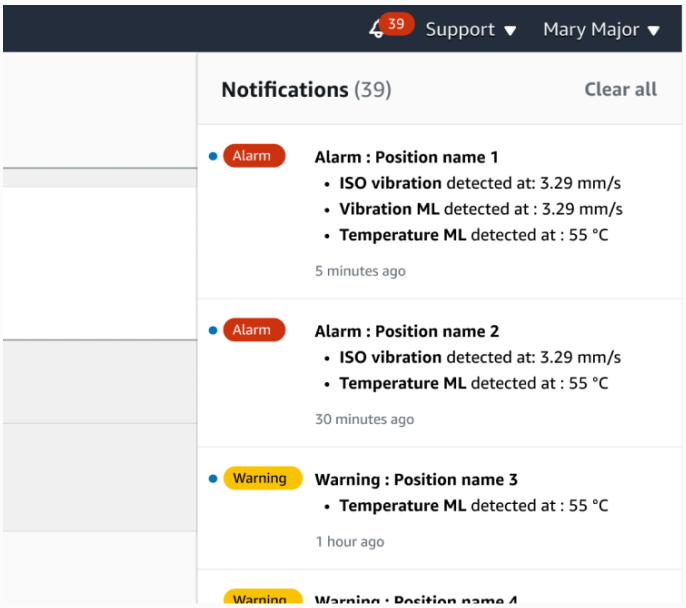


).

Choosing the notification icon opens the **Notifications** page, which lists all pending notifications.




a notification in the mobile app




a notification in the web app

# Acknowledging a machine abnormality

After receiving a notification, the admin user or technician must acknowledge it. Acknowledging the notification lets other users know that the issue has been noted and that action will be taken.

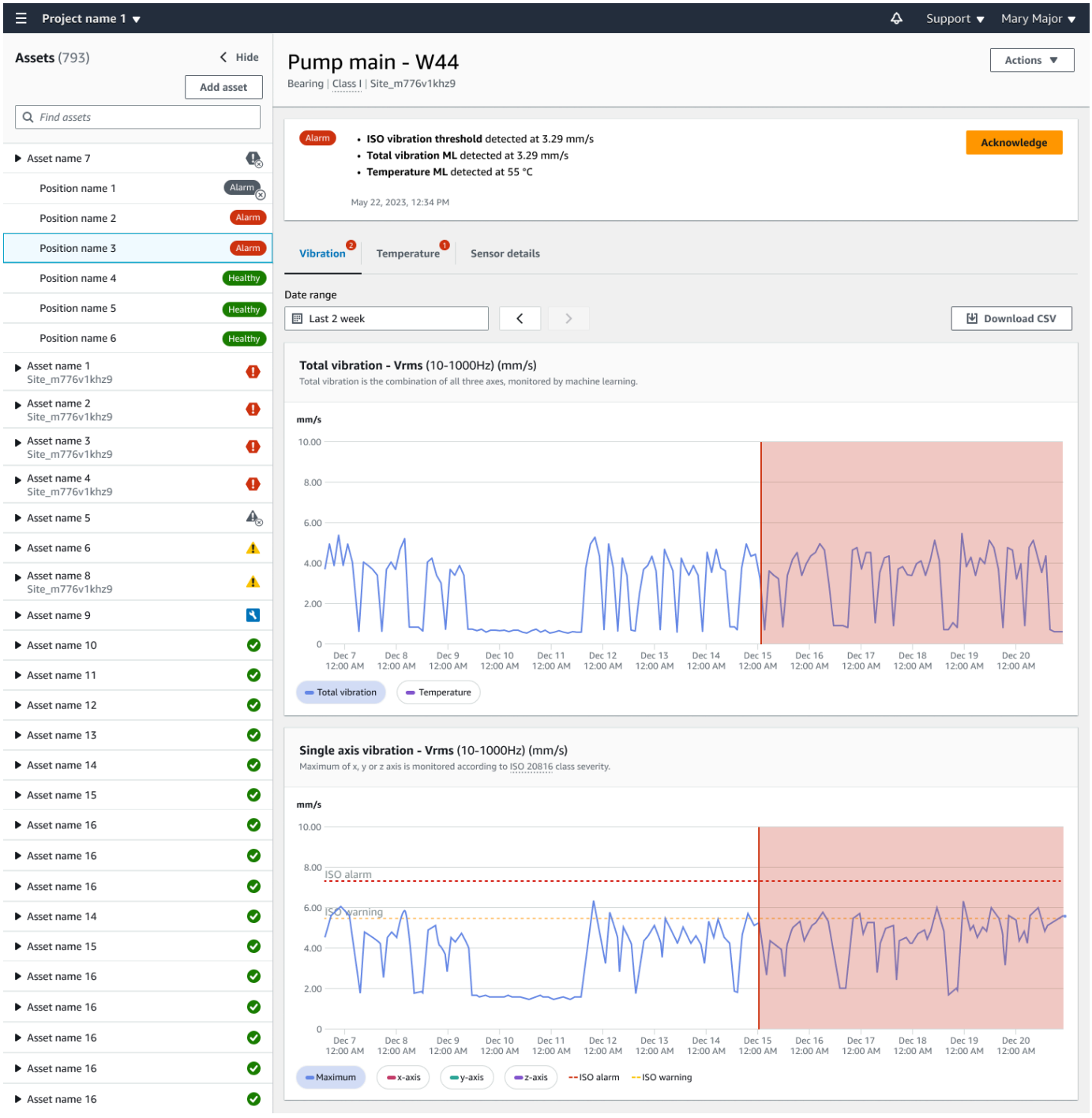
**Topics**


- To view and acknowledge a machine abnormality


## To view and acknowledge a machine abnormality

1. From the **Assets** list, choose the asset that is reporting an abnormality.
2. To view the issue, choose the position with the abnormality.

   Sensor measurements that show the anomaly are displayed.




3. Choose **Acknowledge**.

   The status of the asset changes to **Maintenance**.

# Resolving an abnormality

After an abnormality has occurred and been acknowledged, it must be addressed. You might fix it yourself, or call in a specialist. After the machine that reported the abnormality has been fixed, resolve the abnormality in the Amazon Monitron app.

Resolving an abnormality returns the sensor to a healthy state. It also sends Amazon Monitron information about the problem so it can better predict similar abnormalities.

You can choose from among many common types of failure (called failure modes) and causes of failures. If none of the modes or causes apply to your situation, choose **Other**.

**Topics**


- Failure modes
- Failure causes
- To resolve a machine abnormality using the mobile app


## Failure modes

The following are the Amazon Monitron failure modes or types:

- **No failure detected (mute alert)**: Alert won't trigger if same abnormal condition is detected
- **Blockage**: Obstruction that causes restrictive operation
- **Cavitation**: Loss of pump suction pressure
- **Corrosion**: Moist corrosion, fretting corrosion, false brinelling
- **Deposit**: Build up of particles
- **Imbalance**: Rotating component out of balance
- **Lubrication**: Insufficient lubrication or improper lubrication
- **Misalignment**: Rotating assembly is not aligned
- **Other**
- **Resonance**: External vibration sources
- **Rotating looseness**: Rotating components like fan blade or pulley loose
- **Structural looseness**: Mounting of component is loose

- **Transmitted fault**: Caused by external forces
- **Undetermined (keep monitoring)**: Alert will trigger if same abnormal condition is detected.

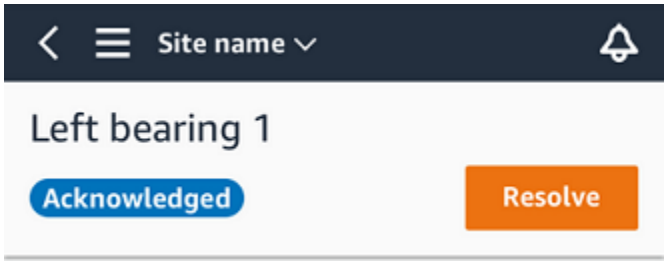
## Failure causes

The following are the Amazon Monitron failure causes:

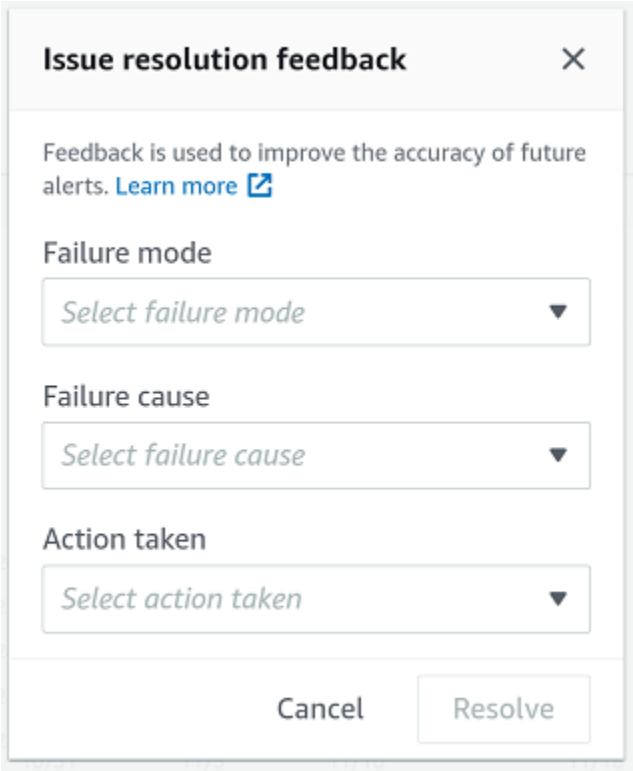
- **Administrtion**: Operator error
- **Design**: Manufacturer design insufficient
- **Fabrication**: Asset was modified from original state
- **Maintenance**: Lack of maintenance performed on asset
- **Operation**: Operation state change
- **Other**: Storage, transportation (vibration/shock), bearing selection. manufacturing concerns, material concerns
- **Quality**: Manufacturer quality insufficient
- **Undetermined**: No root cause determined
- **Wear**: Breakdown/Degradation over time

## To resolve a machine abnormality using the mobile app

1. From the **Assets** list, choose the asset that had an abnormality that you resolved.
2. Choose the position with the abnormality.
3. Choose **Resolve**.




4. For **Failure mode**, choose the type of failure that occurred.




5. For **Failure cause**, choose the cause of the failure.
6. For **Action taken**, choose which action you took.
7. Choose **Submit**.

# Taking a one-time measurement

In addition to viewing the measurements that a sensor normally makes, you can take a one-time measurement with a sensor at any time.

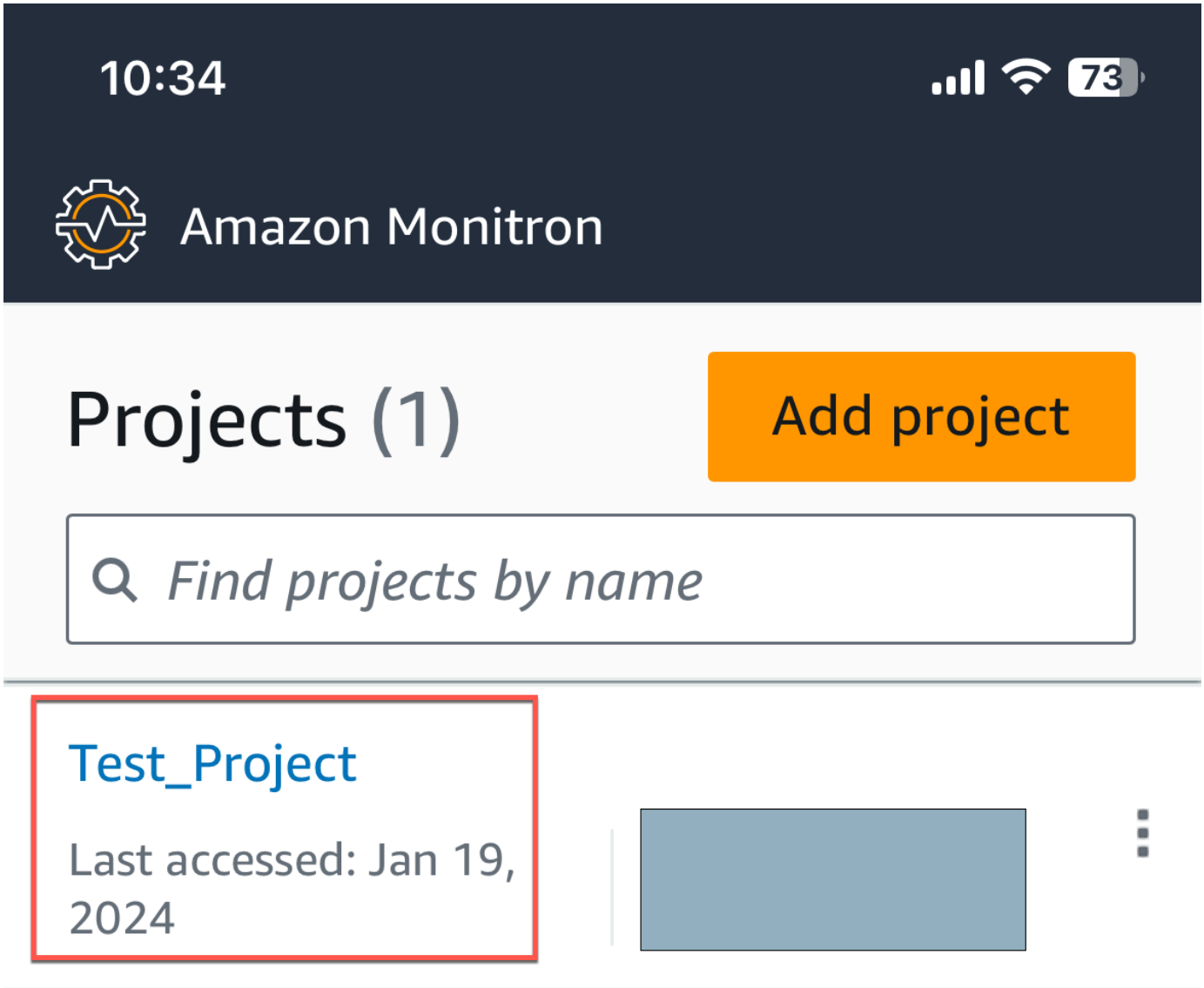
> **Important**
>
> You can only take a sensor meaurement using the Amazon Monitron mobile app. Both admins and technicians can take this action.

### Topics

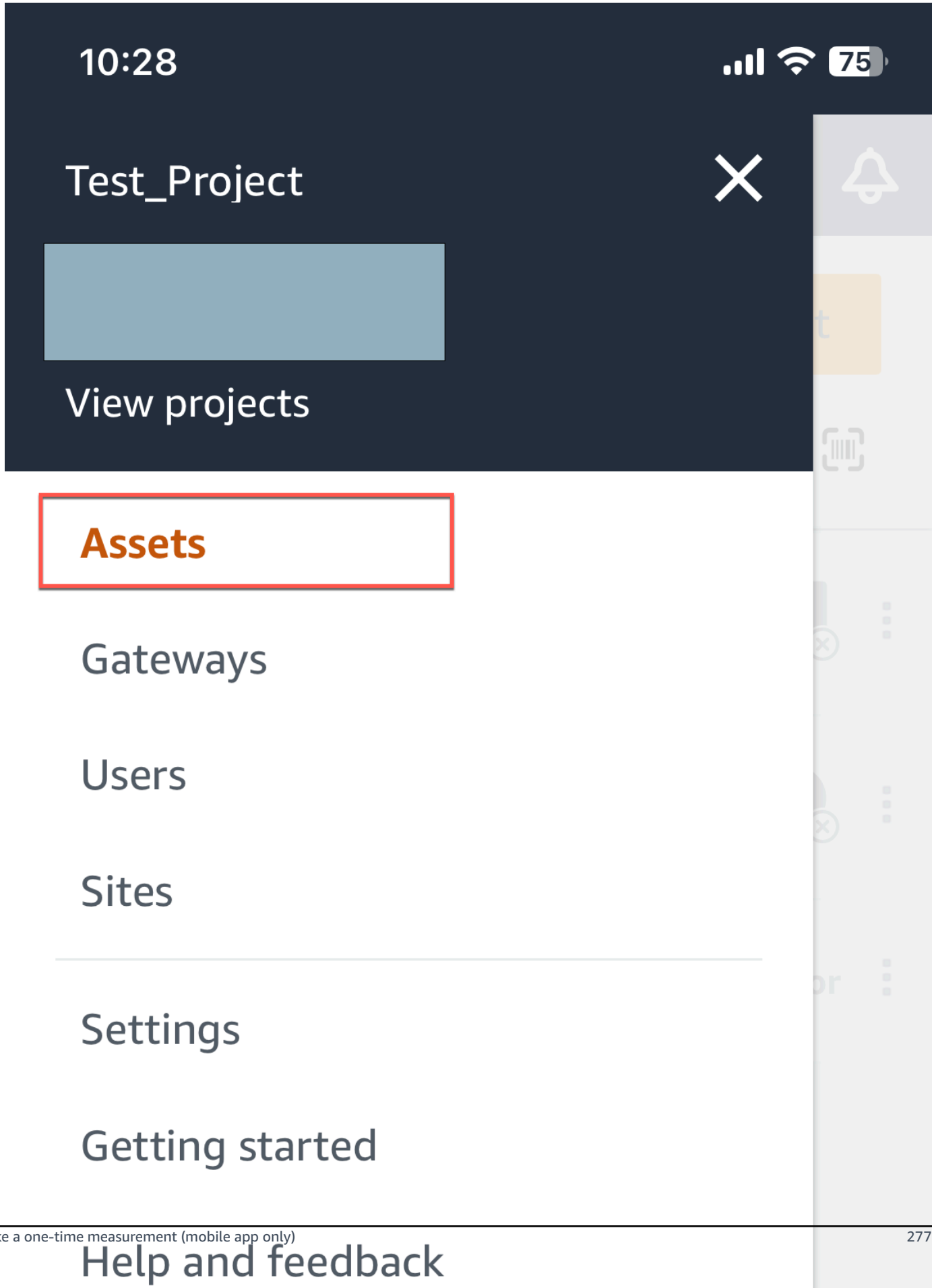
- To take a one-time measurement (mobile app only)

# To take a one-time measurement (mobile app only)

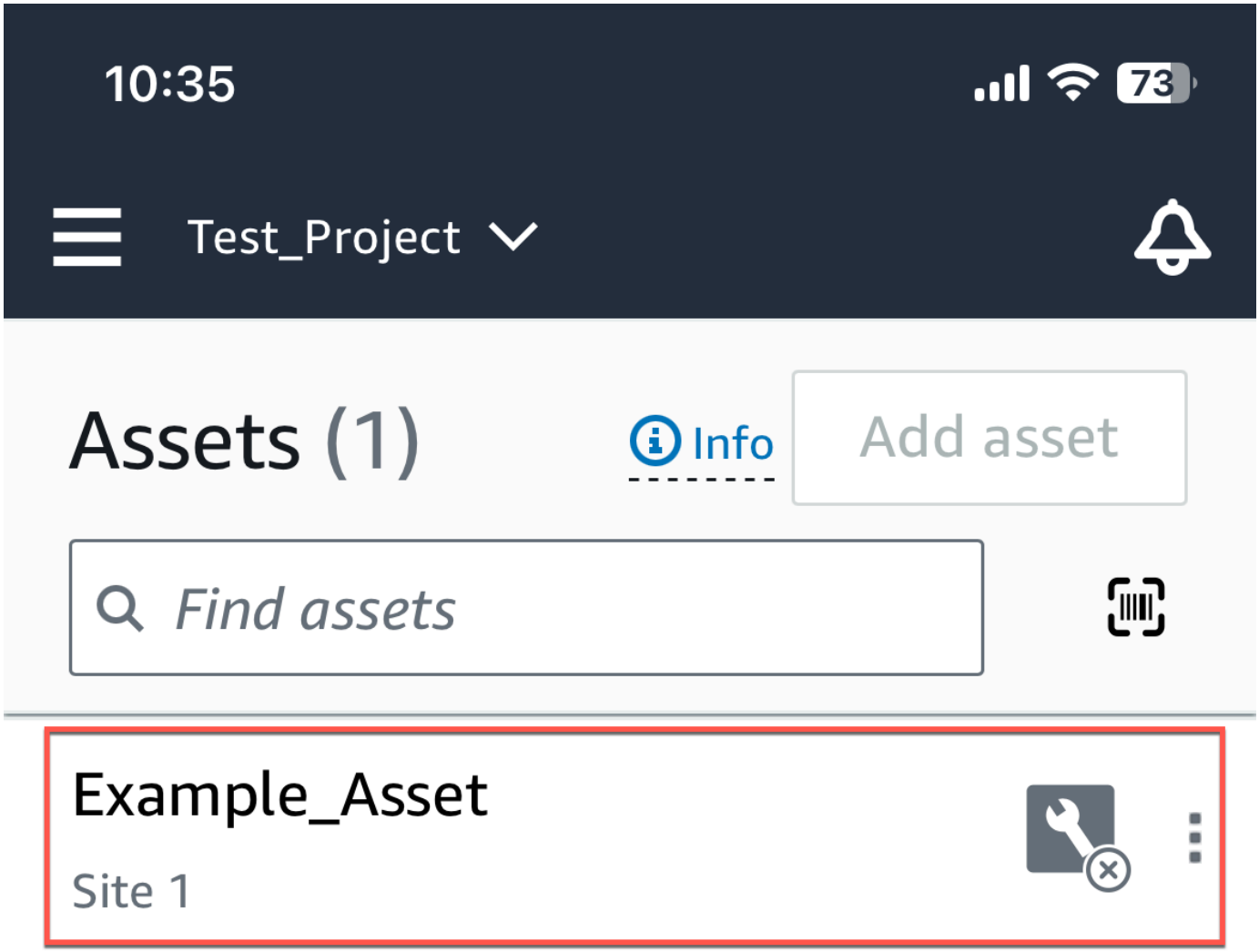
1. From the Amazon Monitron mobile app, select your project.


10:34
73
Amazon Monitron
Projects (1)
Add project
Find projects by name
Test_Project
Last accessed: Jan 19, 2024

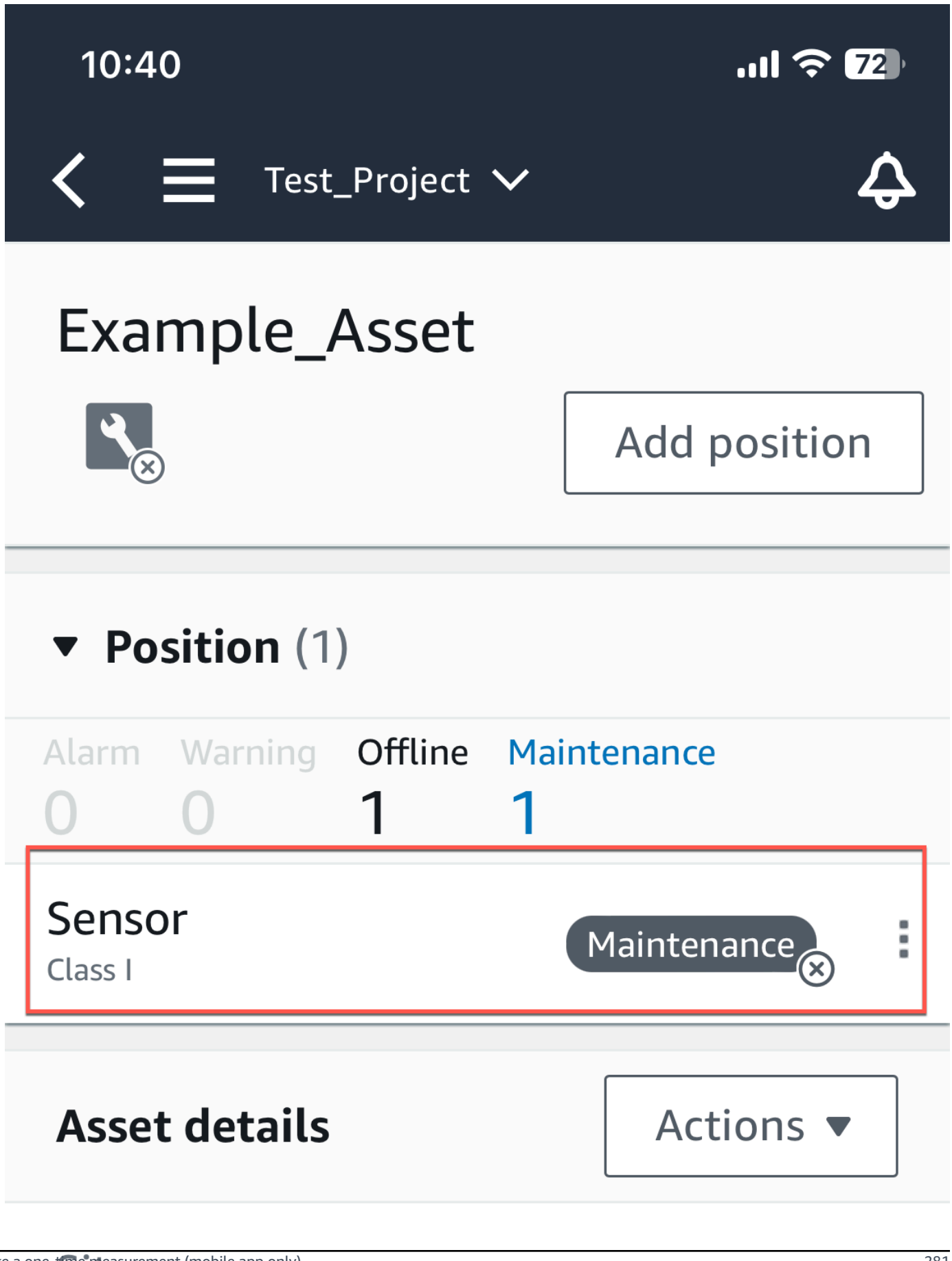
2. From the Amazon Monitron projects menu, select **Assets** .


10:28
75
Test_Project
View projects
Assets
Gateways
Users
Sites
Settings
Getting started
Help and feedback

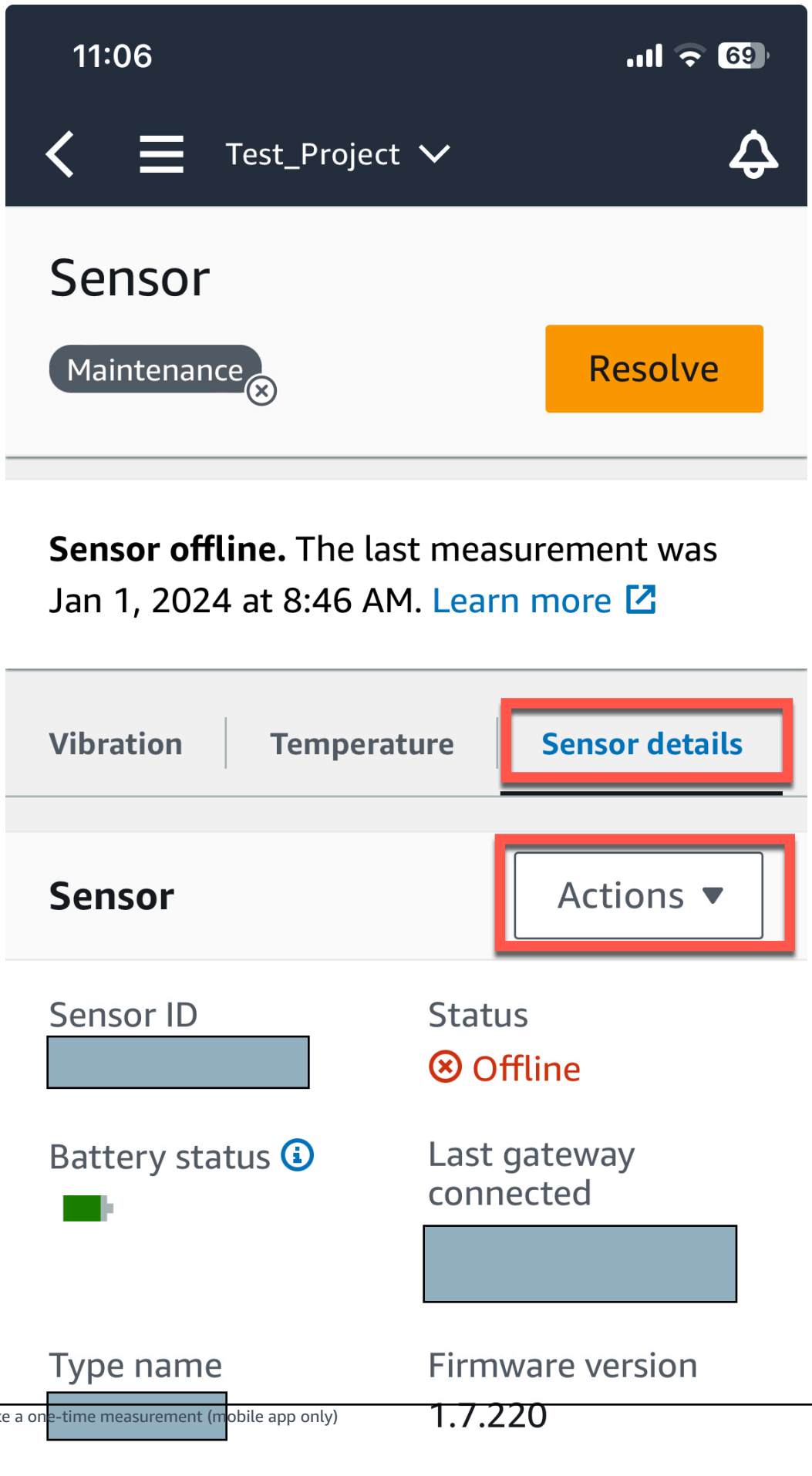
3. From the list of assets, choose the asset that is paired to the sensor whose measurement you want to take.


10:35
73
Test_Project
Assets (1)
Info
Add asset
Find assets
Example_Asset
Site 1

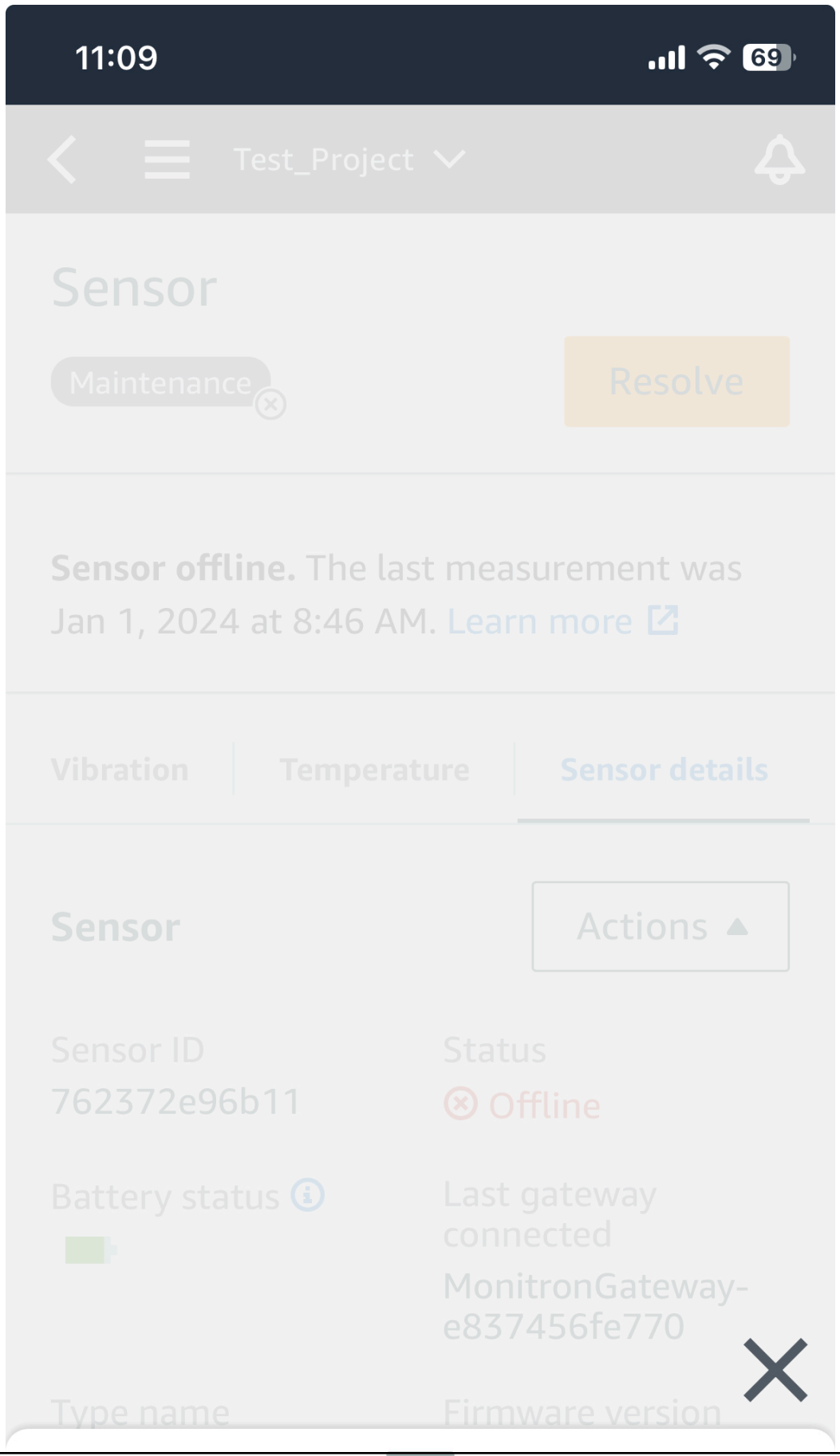
4. Then, select the sensor you want to take the measurement with.


10:40
72
Test_Project
Example_Asset
Add position
Position (1)
Alarm
Warning
Offline
Maintenance
0
0
1
1
Sensor
Class I
Maintenance
Asset details
Actions
Site
Test_Project > Site 1

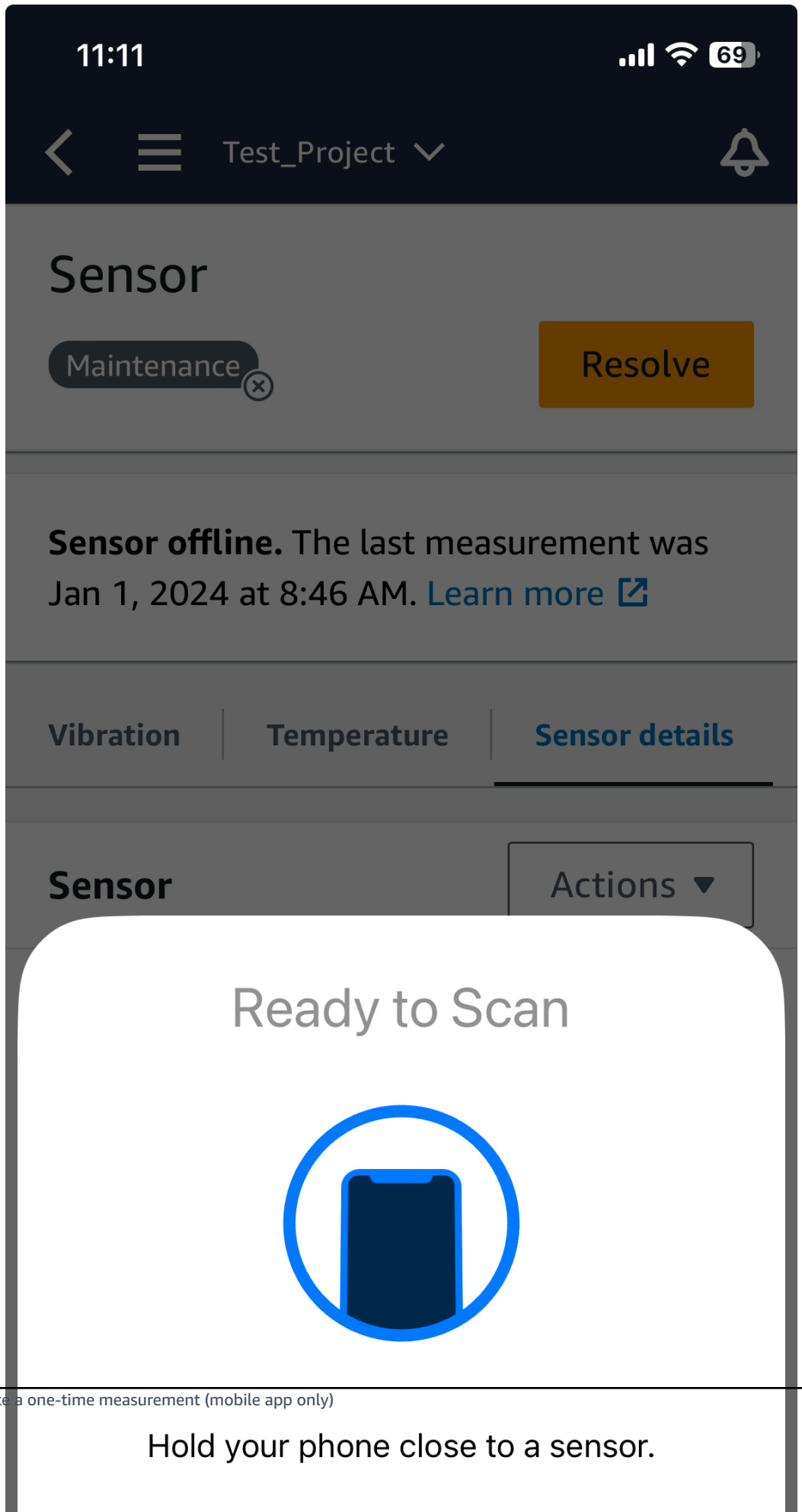
5. On the sensor page, from **Sensor details**, choose **Actions**.


11:06
69
Test_Project
Sensor
Maintenance
Resolve
Sensor offline. The last measurement was Jan 1, 2024 at 8:46 AM. Learn more
Vibration
Temperature
Sensor details
Sensor
Actions
Sensor ID
Status
Offline
Battery status
Last gateway connected
Type name
Firmware version
1.7.220
Sensor type
Last measured

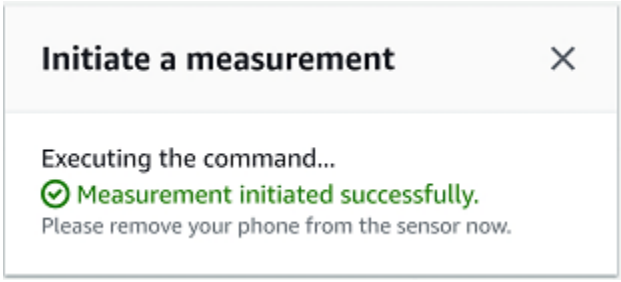
6. From **Actions**, choose **Take measurement**.


11:09
69
Test_Project
Sensor
Maintenance
Resolve
Sensor offline. The last measurement was Jan 1, 2024 at 8:46 AM. Learn more
Vibration
Temperature
Sensor details
Sensor
Actions
Sensor ID
762372e96b11
Status
Offline
Battery status
Last gateway connected
MonitronGateway-e837456fe770
Type name
Firmware version
Take measurement

7. Hold your smartphone close to the sensor.


11:11
69
Test_Project
Sensor
Maintenance
Resolve
Sensor offline. The last measurement was Jan 1, 2024 at 8:46 AM. Learn more
Vibration
Temperature
Sensor details
Sensor
Actions
Ready to Scan
Hold your phone close to a sensor.

8. When the measurement has been taken, move your smartphone away from the sensor.




The new measurement is added to the data that the sensor has already collected.

# Managing 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.

> **Important**
>
> Amazon Monitron requires an email address for each app user. If you use directories like Microsoft Active Directory or an external ID provider, you need to make sure that email addresses for your users are added and synced.

After creating a project or site, you need to add users to them. As an admin user, you can add users to three different roles: `Admin`, `Technician`, or `Viewer`. A user's role determines what they can do with Amazon Monitron. The extent of their role permissions is determined by whether they are added at the project level or at the site level. Setting a user's role at the project level gives the user permissions across all sites in that project. Setting a user's role at the site level gives the user permissions only to that site.

**Topics**


- Managing admin users
- Managing non-admin users


# 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.

> **Important**
>
> Amazon Monitron requires an email address for each app user. If you use directories like Microsoft Active Directory or an external ID provider, you need to make sure that email addresses for your users are added and synced.

**Topics**


- User directory setup
- Adding users as an admin
- Managing users as an admin user
- Removing an admin user
- Sending an email invitation


## User directory setup

Amazon Monitron uses AWS IAM Identity Center to manage user access. Users are added from this IAM Identity Center user directory.

How you add an admin user depends on how IAM Identity Center has been set up for your organization.

> **Important**
>
> Amazon Monitron requires an email address for each app user. If you use directories like Microsoft Active Directory or an external ID provider, you need to make sure that email addresses for your users are added and synced.

**Topics**


- Understanding SSO requirements
- Adding admin users using the native IAM Identity Center directory
- Adding admin users using Microsoft Active Directory
- Adding admin users using an external ID provider
- Returning to Amazon Monitron with IAM Identity Center


### Understanding SSO requirements

When you create a project, Amazon Monitron automatically detects whether IAM Identity Center has been enabled and configured on your account and whether all prerequisites for using IAM Identity Center 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 IAM Identity Center for your organization, see AWS Single Sign-On.

**Important**

Amazon Monitron supports all IAM Identity Center regions except opt-in and government regions. The list of regions supported are:

- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Mumbai)
- Asia Pacific (Tokyo)
- Asia Pacific (Seoul)
- Asia Pacific (Osaka)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- Europe (Stockholm)
- South America (São Paulo)

### IAM Identity Center prerequisites

Before you can set up IAM Identity Center, you must:

- Have first set up the AWS Organizations service and have **All features** set to enabled. For more information about this setting, see Enabling All Features in Your Organization in the *AWS Organizations User Guide*.

- Sign in with the AWS Organizations management account credentials before you begin setting up IAM Identity Center. These credentials are required to enable IAM Identity Center. For more information, see Creating and Managing an AWS Organization in the *AWS Organizations User Guide*. You cannot set up IAM Identity Center while signed in with credentials from an Organization's member account.
- Have chosen an identity source to determine which pool of users has SSO access to the user portal. If you choose to use the default IAM Identity Center identity source for your user store, no prerequisite tasks are required. The IAM Identity Center store is created by default once you enable IAM Identity Center and is immediately ready for use. There is no cost for using this store. Alternatively, you can choose to Connect to your external identity provider using Azure Active Directory. If you choose to connect to an existing Active Directory for your user store, you must have the following:
  - An existing AD Connector or AWS Managed Microsoft AD directory set up in AWS Directory Service, and it must reside within your organization's management account. You can connect only one AWS Managed Microsoft AD directory at a time. However, you can change it to a different AWS Managed Microsoft AD directory or change it back to an IAM Identity Center store at any time. For more information, see Create a AWS Managed Microsoft AD Directory in the *AWS Directory Service Administration Guide*.
  - Set up IAM Identity Center in the Region where your AWS Managed Microsoft AD directory is set up. IAM Identity Center stores the assignment data in the same Region as the directory. To administer IAM Identity Center, you should switch to the Region where you have setup IAM Identity Center. Also, note that IAM Identity Center's user portal uses the same access URL as your connected directory.
- If you currently filter access to specific Amazon Web Service (AWS) domains or URL endpoints using a web content filtering solution such as next-generation firewalls (NGFW) or secure web gateways (SWG), you must add the following domains and/or URL endpoints to your web-content filtering solution allow-lists in order for IAM Identity Center to work properly:

  **Specific DNS domains**

  - *.awsapps.com (http://awsapps.com/)
  - *.signin.aws

  **Specific URL End-points**

  - https://[yourdirectory].awsapps.com/start
  - https://[yourdirectory].awsapps.com/login

- https://[yourregion].signin.aws/platform/login

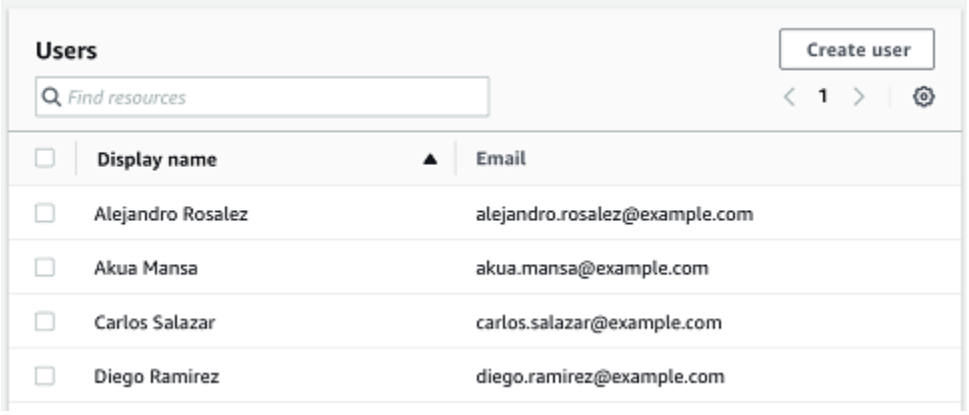
We highly recommend that before you enable IAM Identity Center you first check to see if your AWS account is approaching the quota limit for IAM roles. For more information, see IAM object quotas. If you are nearing the quota limit, consider increasing the quota. Otherwise, you may have issues with IAM Identity Center as you provision permission sets to accounts that have exceeded the IAM role limit.

## Adding admin users using the native IAM Identity Center directory

The simplest way to add admin users to your project is by using the IAM Identity Center native directory. You can use it by starting to use Amazon Monitron and letting it configure IAM Identity Center at a basic level for you. You can also set up IAM Identity Center before 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.

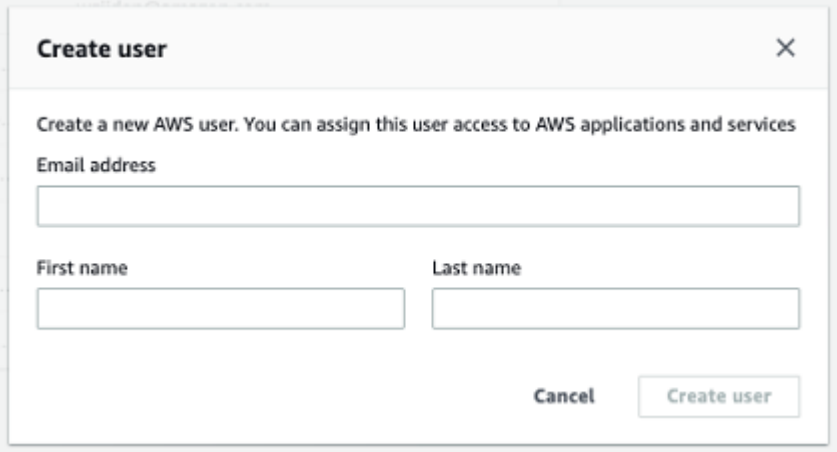
**To add an admin user when using the native IAM Identity Center directory**

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.

   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 IAM Identity Center to use it. IAM Identity Center 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.

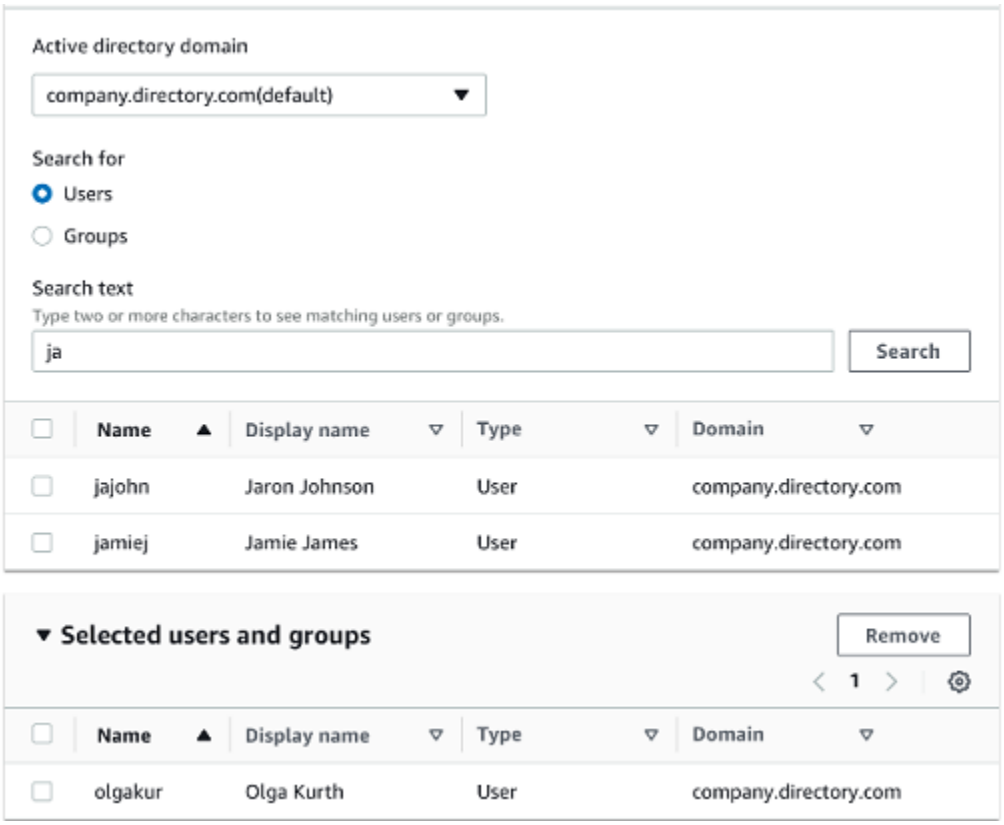
**Important**

Amazon Monitron requires an email address for each app user. Make sure that email addresses for your users are added and synced.

All Amazon Monitron admin users have access to identity information in the user directory that is configured in IAM Identity Center 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 IAM Identity Center 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

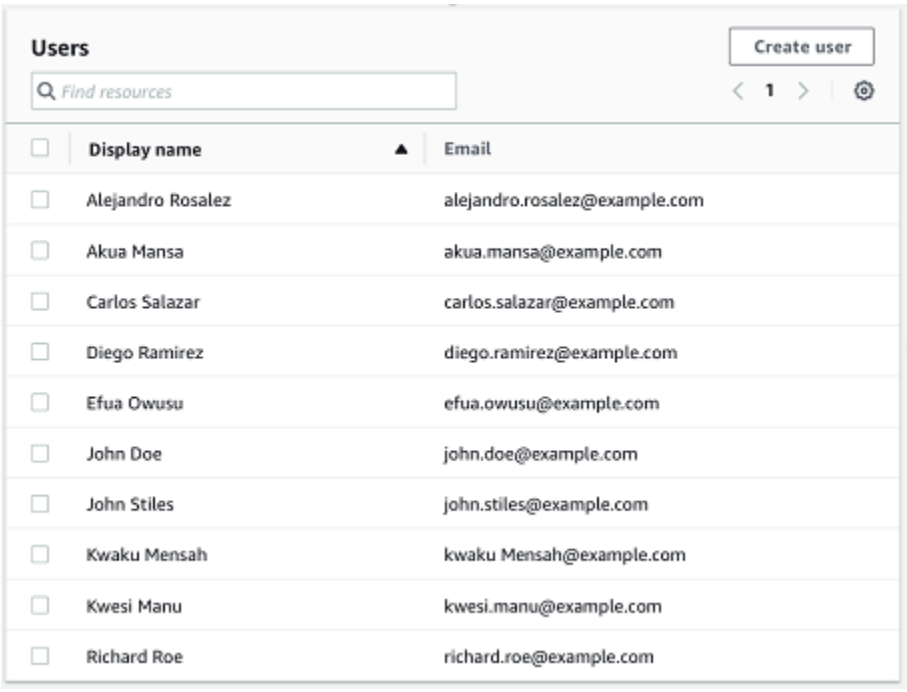
If you're using an external Identity provider (IdP), you can configure IAM Identity Center to use that provider through the Security Assertion Markup Language (SAML) 2.0 standard. This provides you with the pool of identities in your IdP directory. You can pull this pool when using the Amazon Monitron 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.

> **Important**
>
> Amazon Monitron requires an email address for each app user. Make sure that email addresses for your users are added and synced.

All Amazon Monitron admin users have access to identity information in the user directory that is configured in IAM Identity Center 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 IAM Identity Center 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.



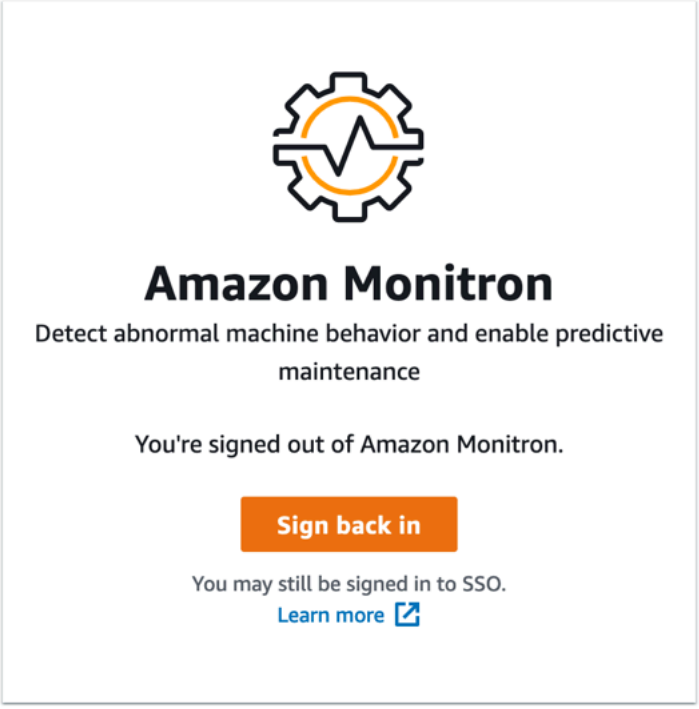

6. Choose **Add** to add the admin users.

## Returning to Amazon Monitron with IAM Identity Center

When you log out of the Amazon Monitron web app, you may still be signed in to AWS IAM Identity Center. Any other applications that you have opened from the user portal remain open and running.

There are two ways to log out of IAM Identity Center:

- Log out directly through the IAM Identity Center portal.
- Once an hour, AWS IAM Identity Center checks to see if you are actively using any AWS services. If you are not, then you are logged out of IAM Identity Center automatically.




To learn about admin users using IAM Identity Center, see User directory setup.

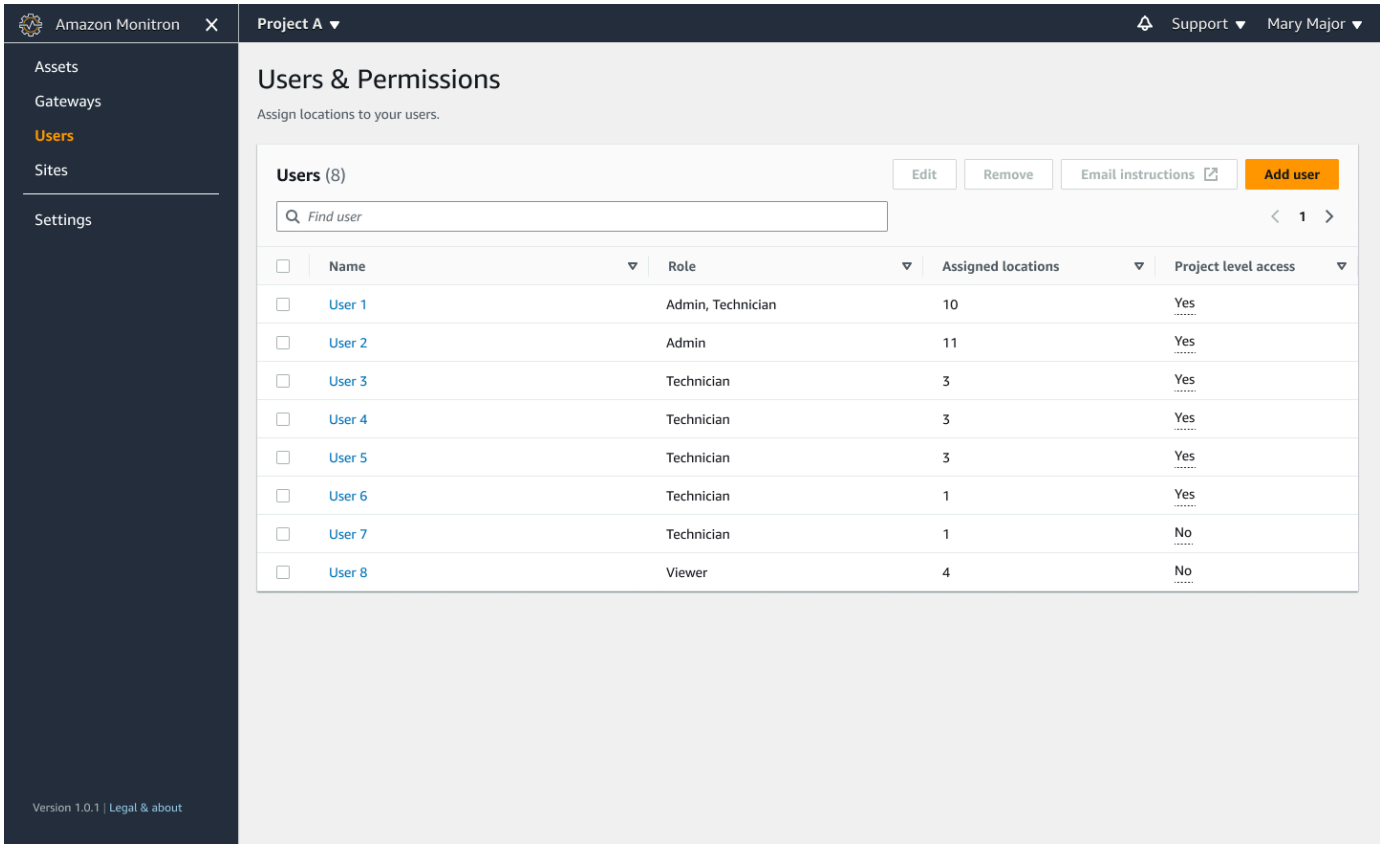
To learn about security best practices with Amazon Monitron and IAM Identity Center, see Security best practices for Amazon Monitron.

To learn about using the SSO user portal, see Using the user portal.

# Adding users as an admin

As an admin, you can add other users (including other admin users) in the Amazon Monitron web app.

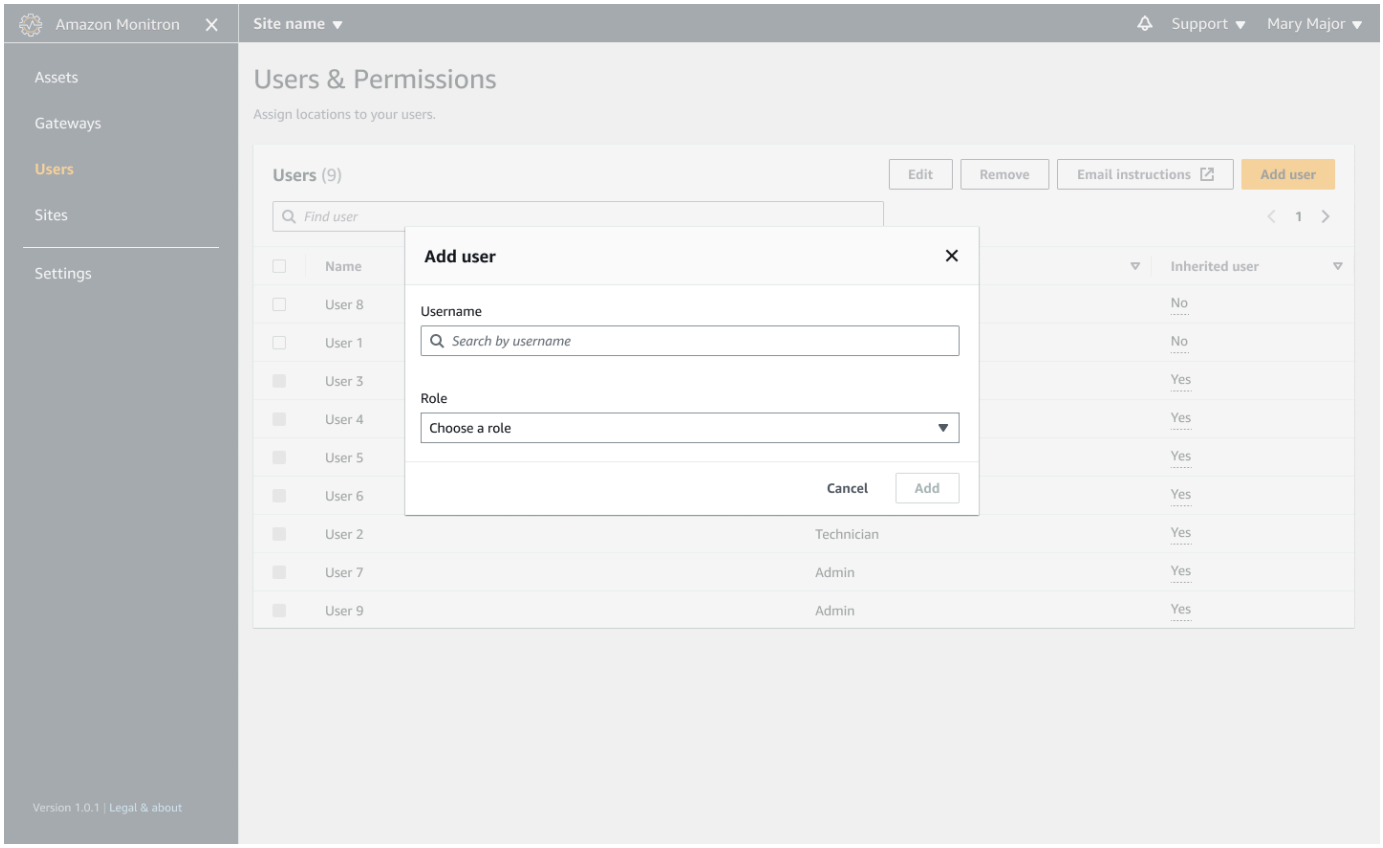
1. Navigate to the project or site that you want to add a user to, and then to the **Users** list.



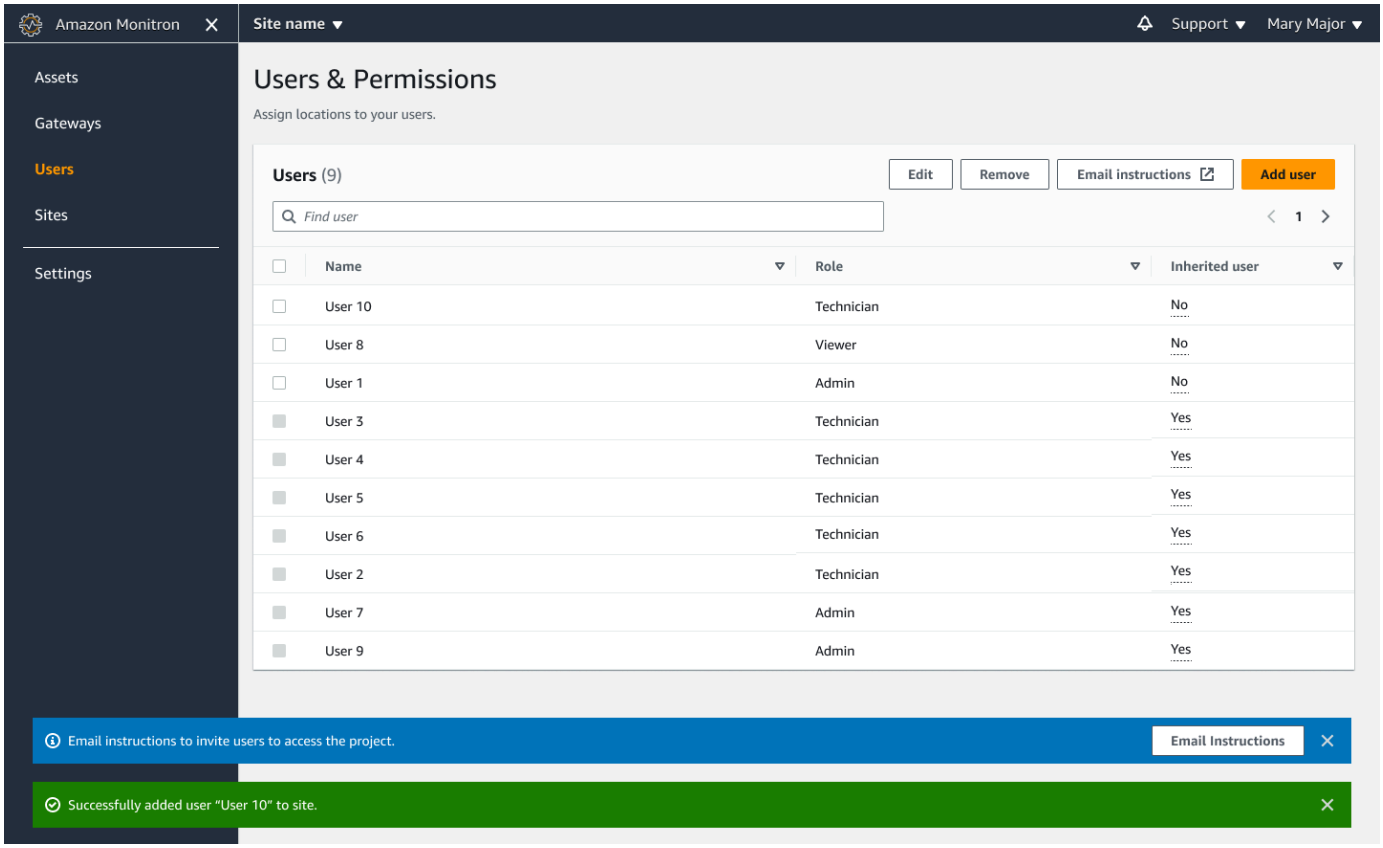

2. Enter a user name. Amazon Monitron searches the user directory for the user.

   Choose the user from the list and the role you want to assign to the user: **Admin**, **Technician**, or **Viewer**.

   Then, choose **Add user**.




3. The new user appears on the **Users** list.




Send the new user an email invitation with a link for accessing the project and downloading the Amazon Monitron mobile app. For more information, see Sending an email invitation.

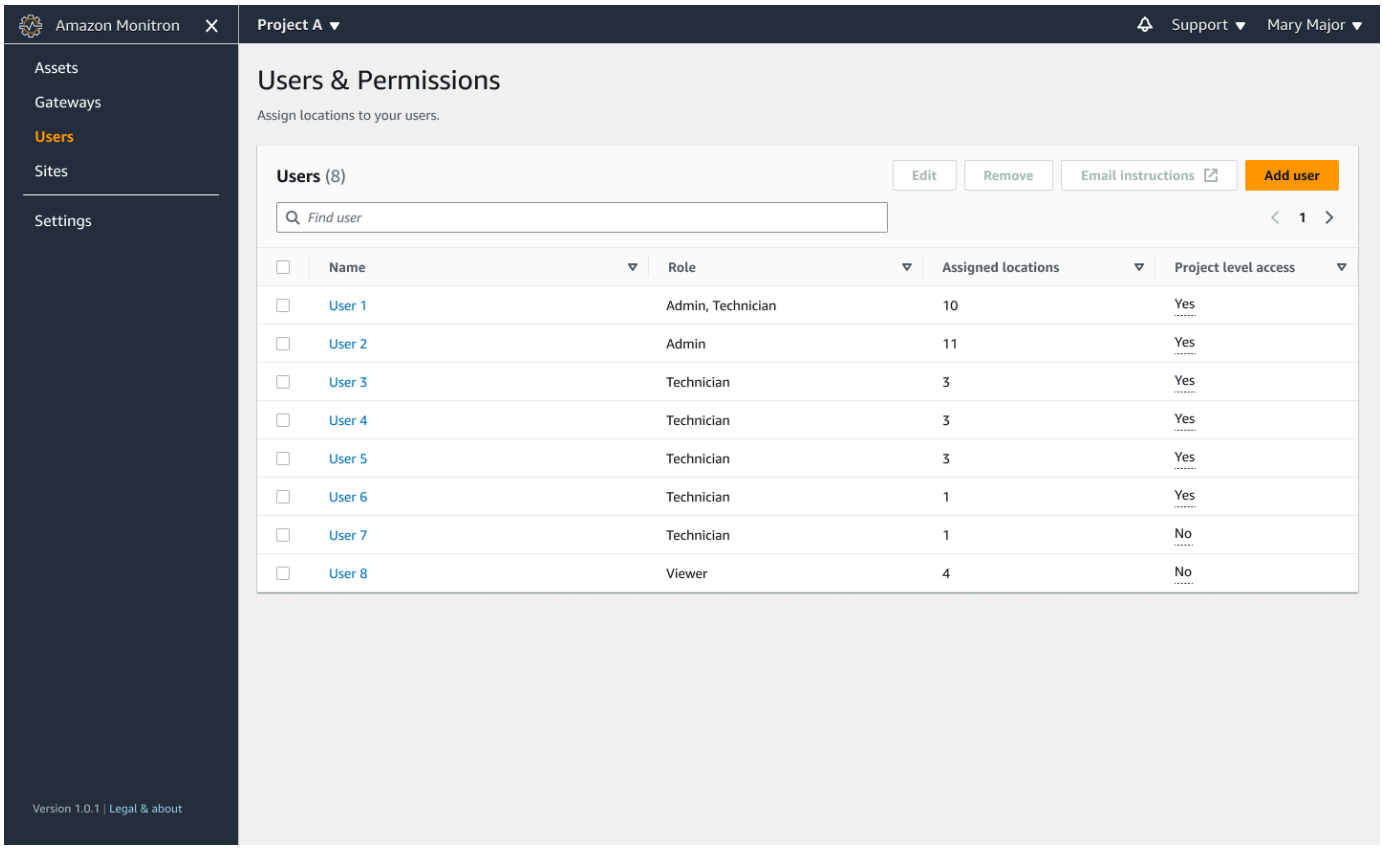
## Managing users as an admin user

As an admin, you can use the list of users to manage users in the Amazon Monitron web app. As project level admin, you can view all users at the project level and all users at a particular site level.

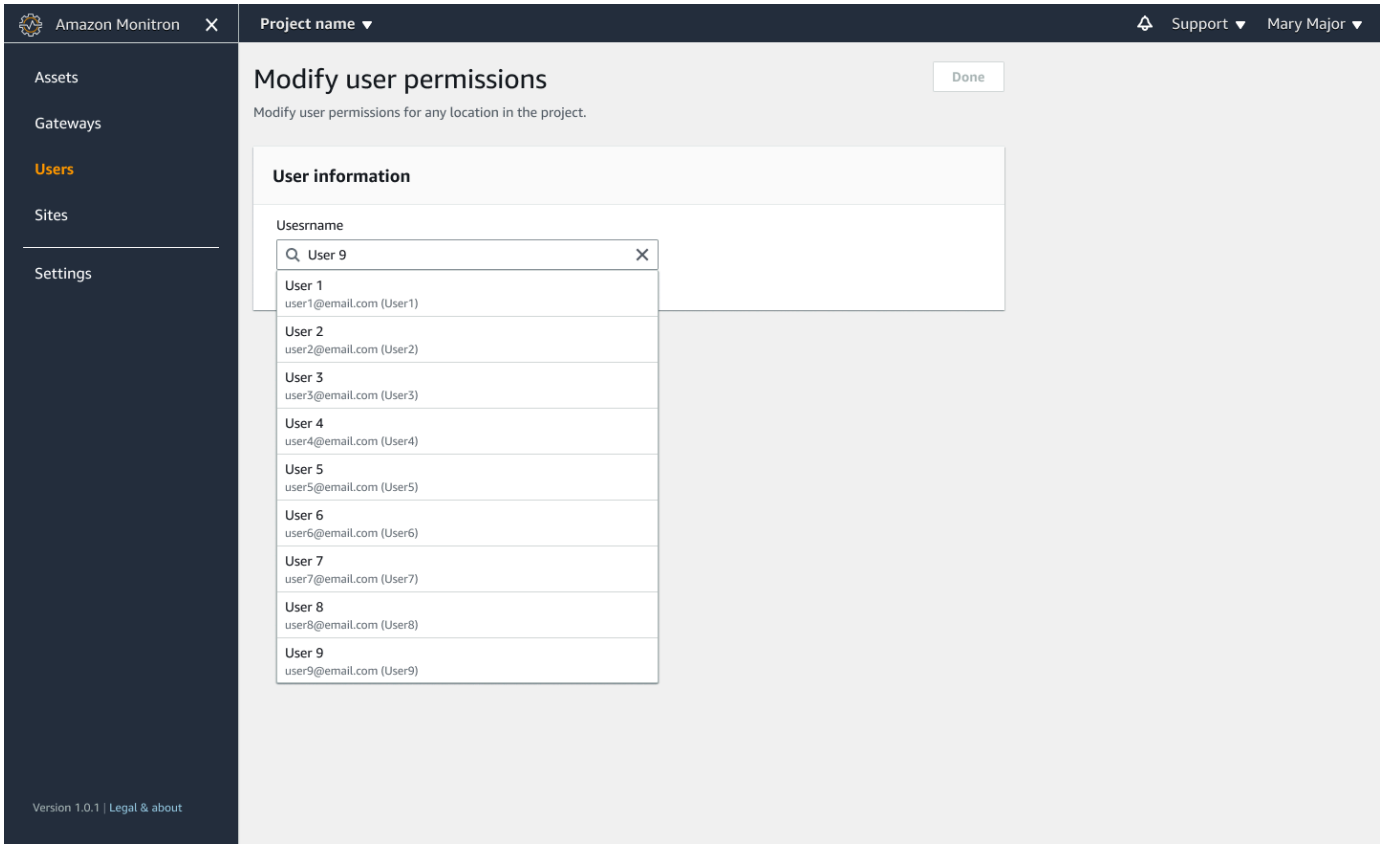
The **Users & Permissions** page displays the following information to make user management easier:

- **Name** – The name of the user.
- **Role** – The role assigned to the user, whether Admin, Technician, Viewer, or any combination of these.
- **Assigned locations** – The number of locations the user is assigned to.
- **Project level access** – Whether the user has project level access or only specific site level access.

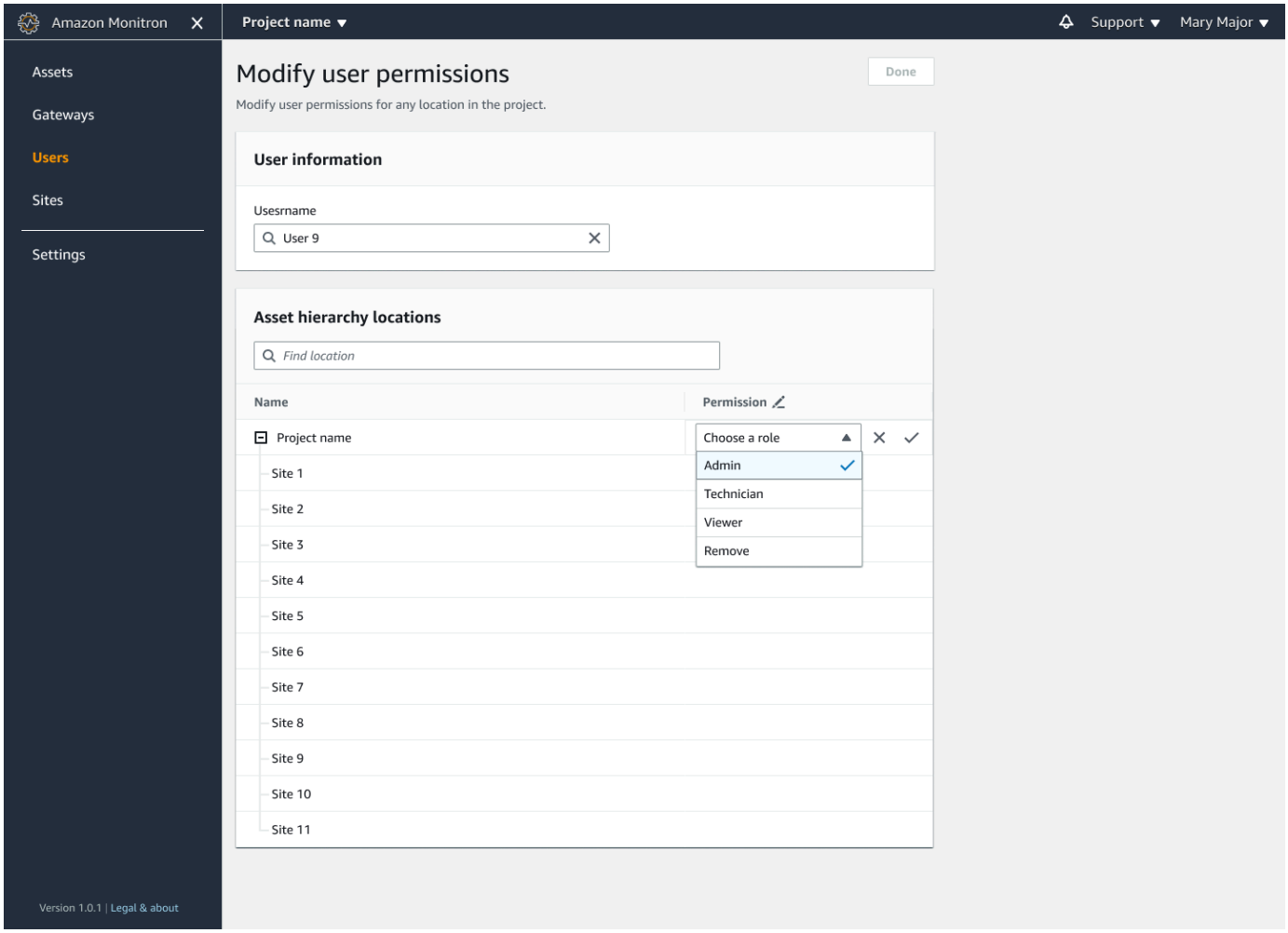
1. Navigate to the project or site that you want to add a user to or update user permissions from, and then to the **Users & Permissions** list.



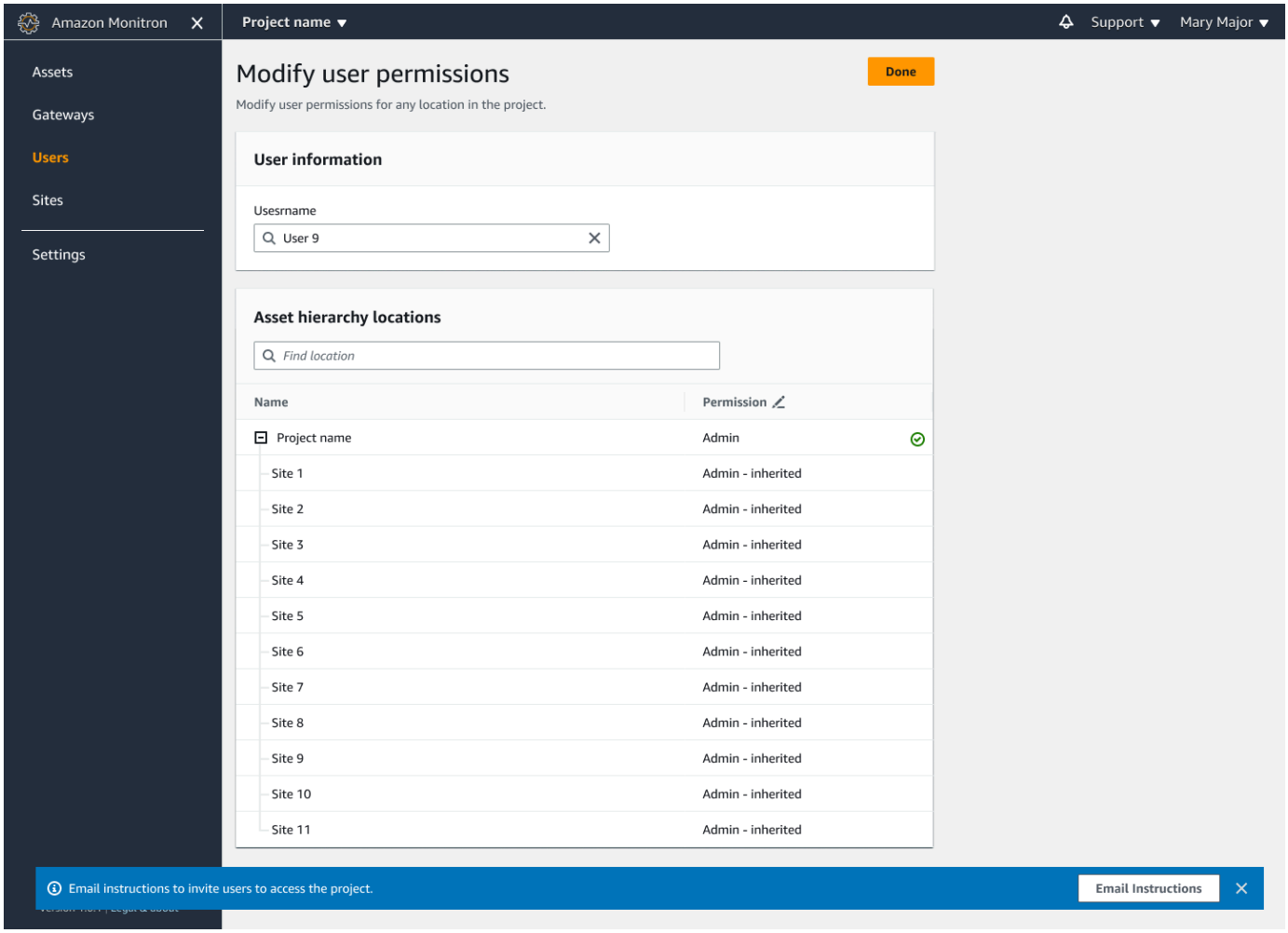

2. Select **Edit**. Then, from the **Modify user permissions** page, in **Username**, select the user whose details you want to view or edit. Amazon Monitron displays the list of locations the user is assigned to.




3. To change the role assigned to the user, select between **Admin**, **Technician**, and **Viewer**. Or, you can choose to **Remove** the user. Then, select **Done**.




Amazon Monitron diplays how the user was assigned permissions to all locations. If a user is assigned an **Admin** role at the project level, they inherit access to all locations within that project. In this case, Amazon Monitron indicates their access level as **Admin – inherited**.




# 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.

### Topics

- To remove an admin user

## 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 send them an email and invite them to download and log in to the Amazon Monitron mobile or web app. This invitation also contains instructions for connecting to your project.

**Topics**


- To generate an email invitation to a site or project using the mobile app
- To generate an email invitation to a site or project using the web app

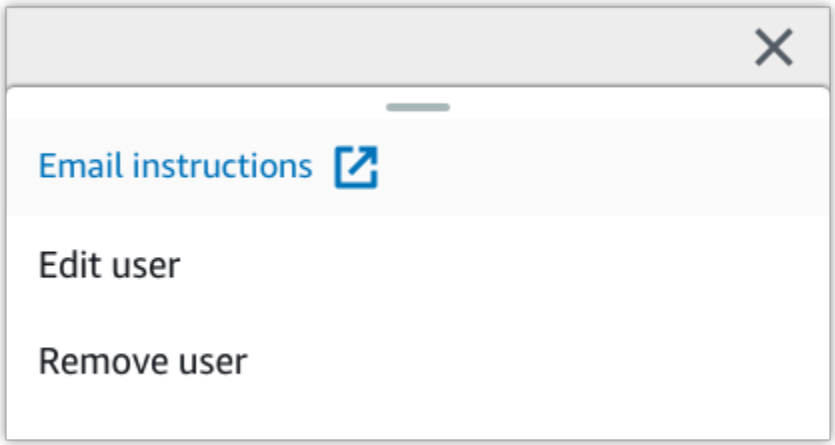

### To generate an email invitation to a site or project using the mobile app

1. Add the user to the site or project.
2. Choose the vertical ellipse icon (

   )

   next to the user that you added.
3. Choose **Email instructions**.



Your email application opens with a draft of the email invitation addressed to that user. It contains two links. One link is to download the Amazon Monitron mobile app from the Google Play Store. The other is to open the project to which the user has been added.

4. Verify that the email is correct, and then send it to the user.

### To generate an email invitation to a site or project using the web app

1. Add the user to the site or project.
2. Choose **Users** from the left nav.
3. Choose **Email instructions**.
4. Your email application opens with a draft of the email invitation addressed to that user. It contains two links. One is to download the Amazon Monitron mobile app from the Google Play Store. The other link opens the project to which the user has been added.
5. Verify that the email is correct, and then send it to the user.

> **Warning**
>
> Beware of phishing attacks. An attacker may send an email impersonating a Amazon Monitron project invitation email to your users. Warn them to make sure that the directory name is visible on the login screen before entering their sign-in credentials.

## Managing non-admin users

After creating a project or site, you need to add users to them. As an admin user, you can add users to three different roles: `Admin`, `Technician`, or `Viewer`.

A user's role determines what they can do with Amazon Monitron. The extent of their role permissions is determined by whether they are added at the project level or at the site level. Setting a user's role set at the project level gives the user permissions across all sites in that project. Setting a user's role at the site level gives the use permissions only to that site.

**Topics**


- Displaying a list of users
- Adding a user

- Changing a user role
- Removing a user

## Displaying a list of users

As an admin, you can use the list of users to manage users in the Amazon Monitron app. There are three levels you can choose from (depending on your admin role) to view a list of users:

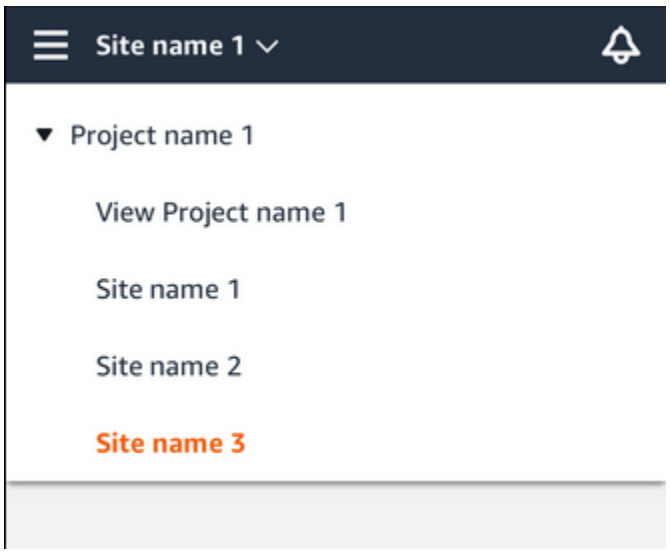
- As project level admin, you can view all users at the project level.
- As project level admin, you can view all users at a particular site level.
- As site level admin, you can view all users at a particular site level.

### Topics

- To display the list of users in the mobile app
- To display the list of users in the web app

### To display the list of users in the mobile app

1. Log into the Amazon Monitron mobile app on your smartphone.
2. Choose the project or site whose users you want to view.




3. Choose the menu icon (☰).



4. Choose **Users**.

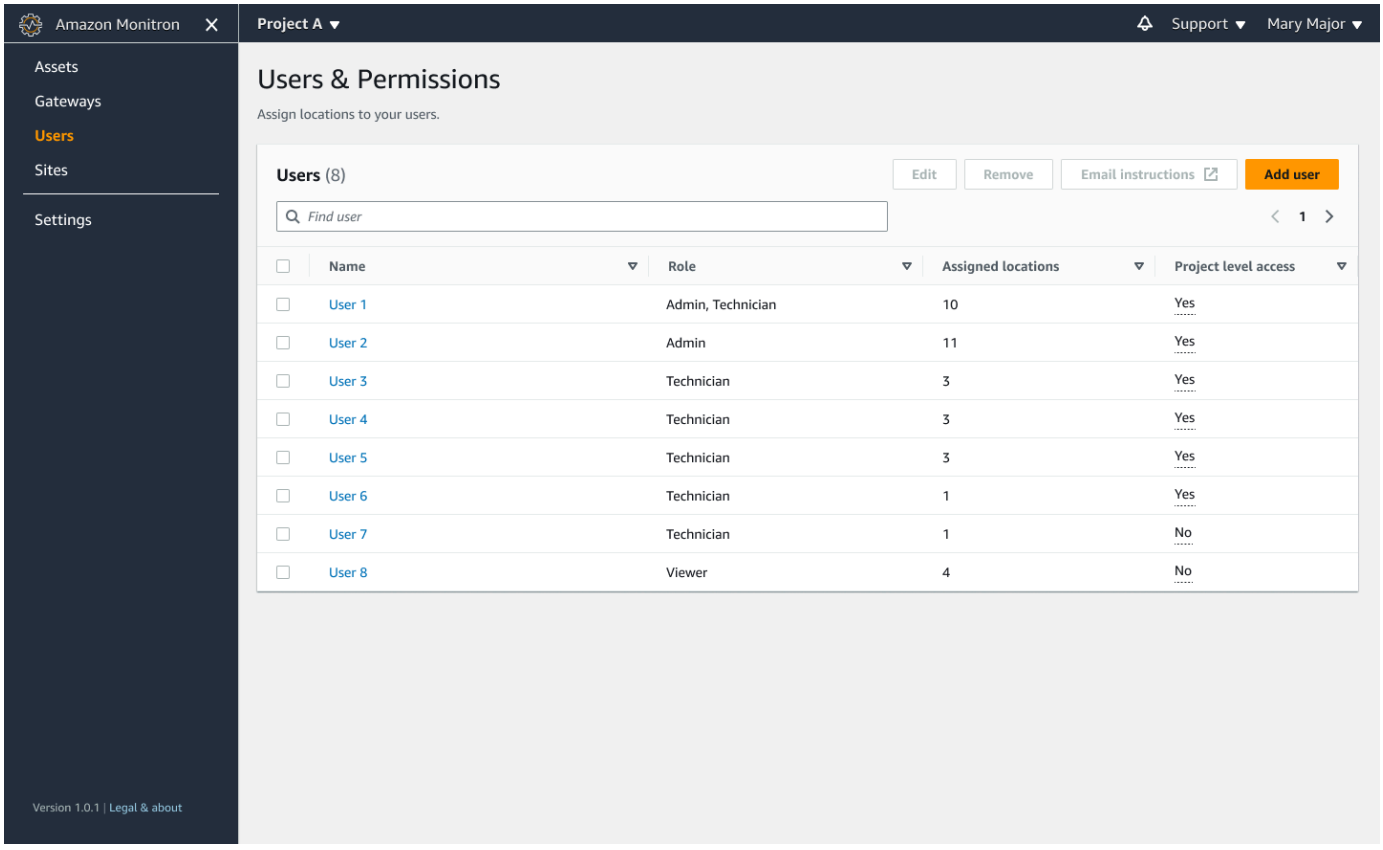
   A list of all users associated with the project or site is displayed.

## To display the list of users in the web app

The **Users & Permissions** page displays the following information to make user management easier:

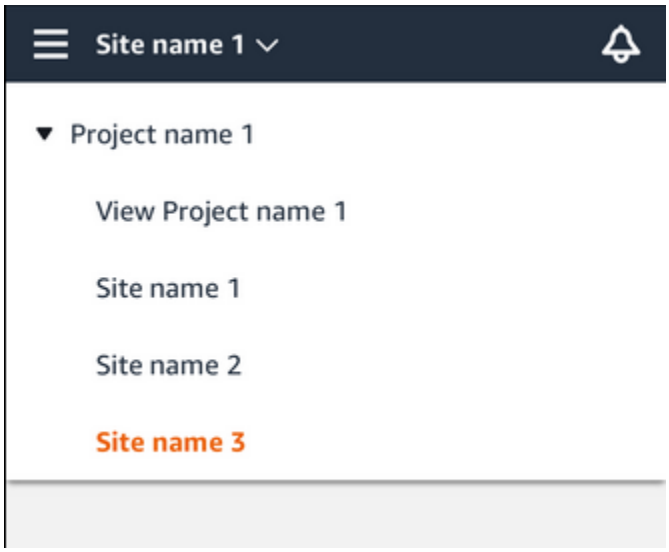
- **Name** – The name of the user.
- **Role** – The role assigned to the user, whether Admin, Technician, Viewer, or any combination of these.
- **Assigned locations** – The number of locations the user is assigned to.
- **Project level access** – Whether the user has project level access or only specific site level access.

1. Log into the Amazon Monitron web app.
2. Select **Users** from the left nav. The list of users will appear.




3. Choose the project or site whose users you want to view.

A list of all users associated with the project or site is displayed.




## Adding a user

When you add a new user, the role you choose determines the permissions that user has.

Users can have the following roles:

- **Admin**. An admin user has full access to all resources within the project or site to which they've been added. They can add other users, create assets, pair sensors to assets, and so on. They can also monitor assets and acknowledge and resolve abnormalities. If they are added at the project level, these permissions extend through the entire project. If they are added at the site level, these permissions are limited to only that site.
- **Technician**. A technician user has read-only permissions to the project or site to which they've been added and permissions for monitoring assets and acknowledging and resolving abnormalities. If they are added at the project level, these permissions extend through the entire project. If they are added at the site level, these permissions are for only that site.
- **Read only**. A user with read-only permissions has permission to read (but not add, change, or delete) details of all resources within the project or site to which they've been added.

You use the same procedure to add a new user to a project or to a site.

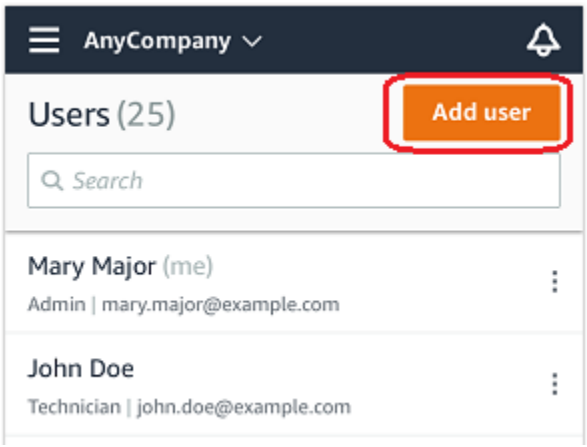
**Topics**

- To add a user using the mobile app

- To add a user using the web app

## To add a user using the mobile app

1. Log into the Amazon Monitron mobile app on your smartphone.
2. Navigate to the project or site that you want to add a user to, and then to the **Users** list.
3. Choose **Add user**.



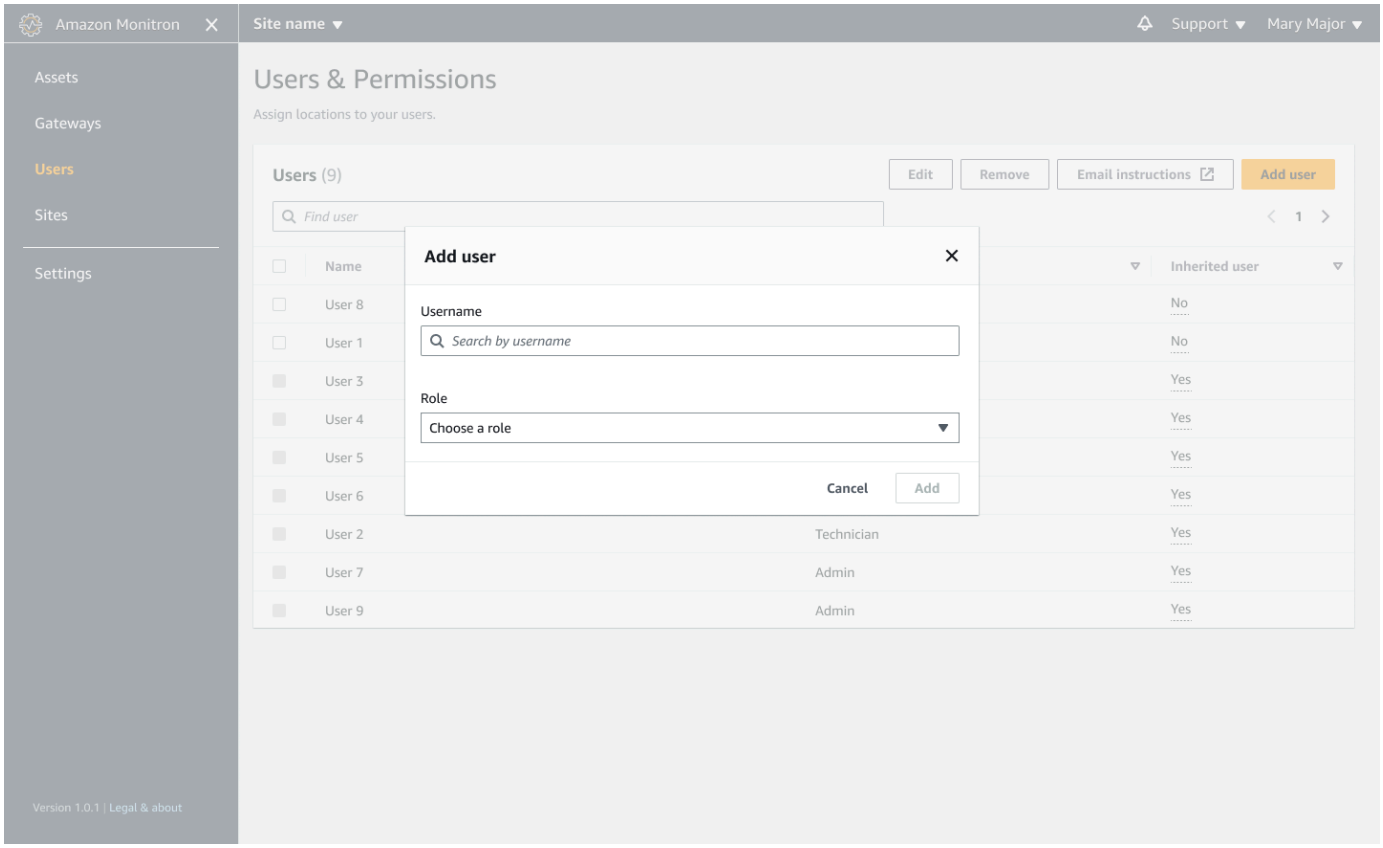

4. Enter a user name.

   Amazon Monitron searches the user directory for the user.
5. Choose the user from the list.
6. Choose the role that you want to assign the user: **Admin**, **Technician**, or **Viewer**.
7. Choose **Add**.

   The new user appears on the **Users** list.
8. Send the new user an email invitation with a link for accessing the project and downloading the Amazon Monitron mobile app. For more information, see Sending an email invitation.

## To add a user using the web app

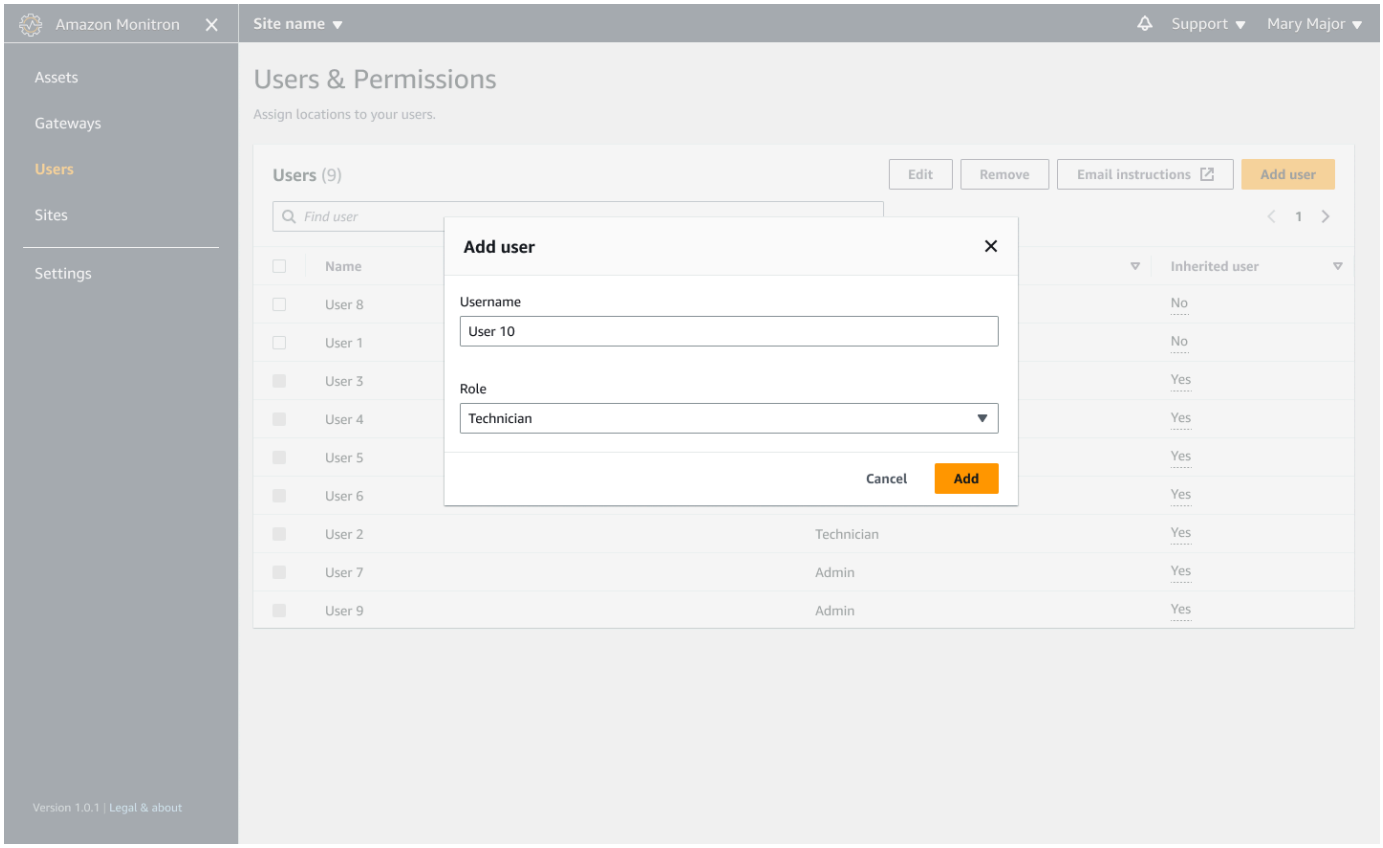
1. Navigate to the project or site that you want to add a user to, and then to the **Users** list.



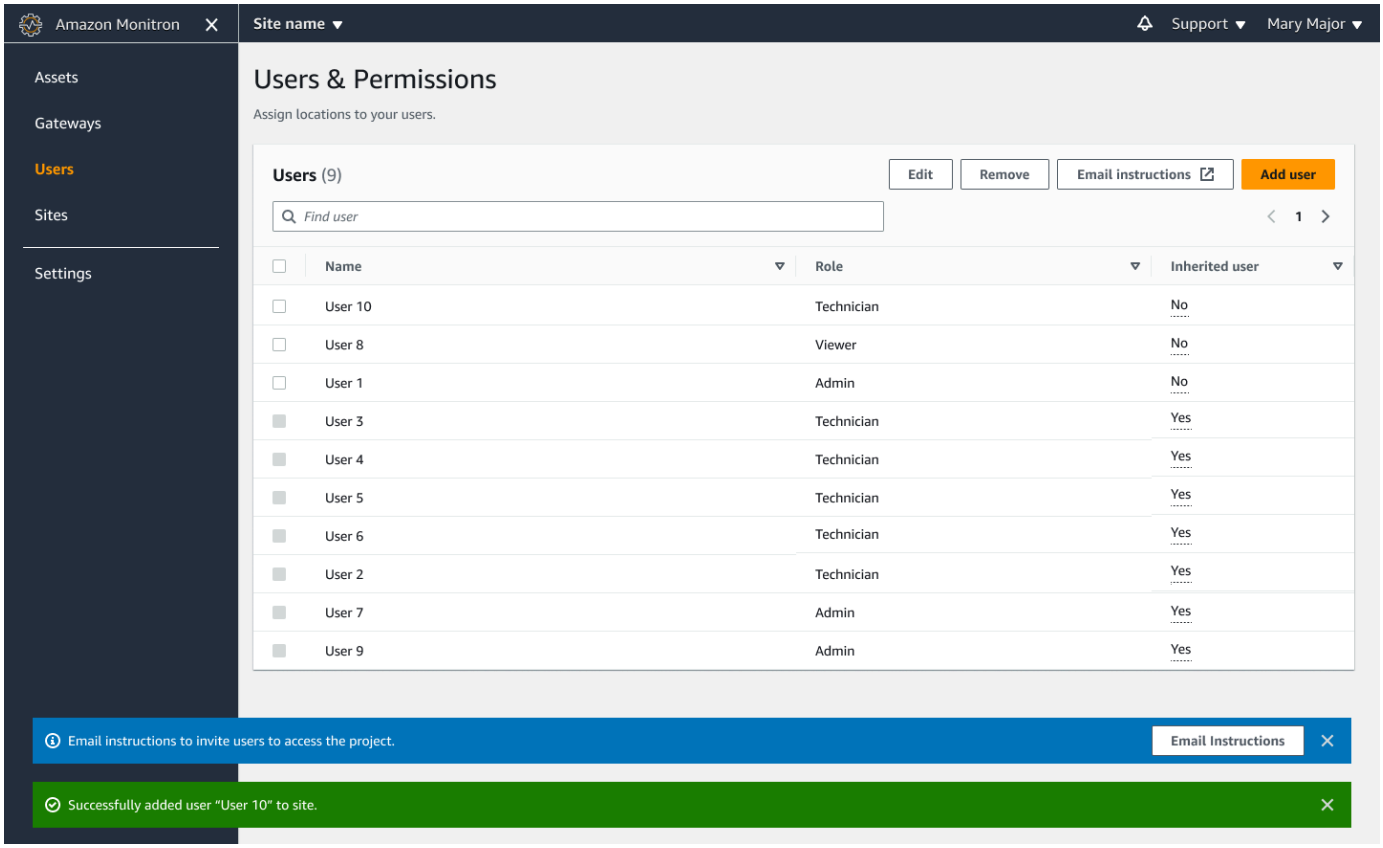

2. Enter a user name. Amazon Monitron searches the user directory for the user.

   Choose the user from the list and the role you want to assign to the user: **Admin**, **Technician**, or **Viewer**.

   Then, choose **Add user**.




3. The new user appears on the **Users** list.




Send the new user an email invitation with a link for accessing the project and downloading the Amazon Monitron mobile app. For more information, see Sending an email invitation.

## Changing a user role

You can change a user's role, but not a user's name. That's because the name is linked to the user directory that is linked to by Amazon Monitron.

To change a project or site's users, you must remove the previous users and add the new ones. For information on removing users from a project or site, see To remove a user using the mobile app. For information on adding new users, see Adding a user.

### Topics

- To change a user role using the mobile app
- To change a user role using the web app

## To change a user role using the mobile app

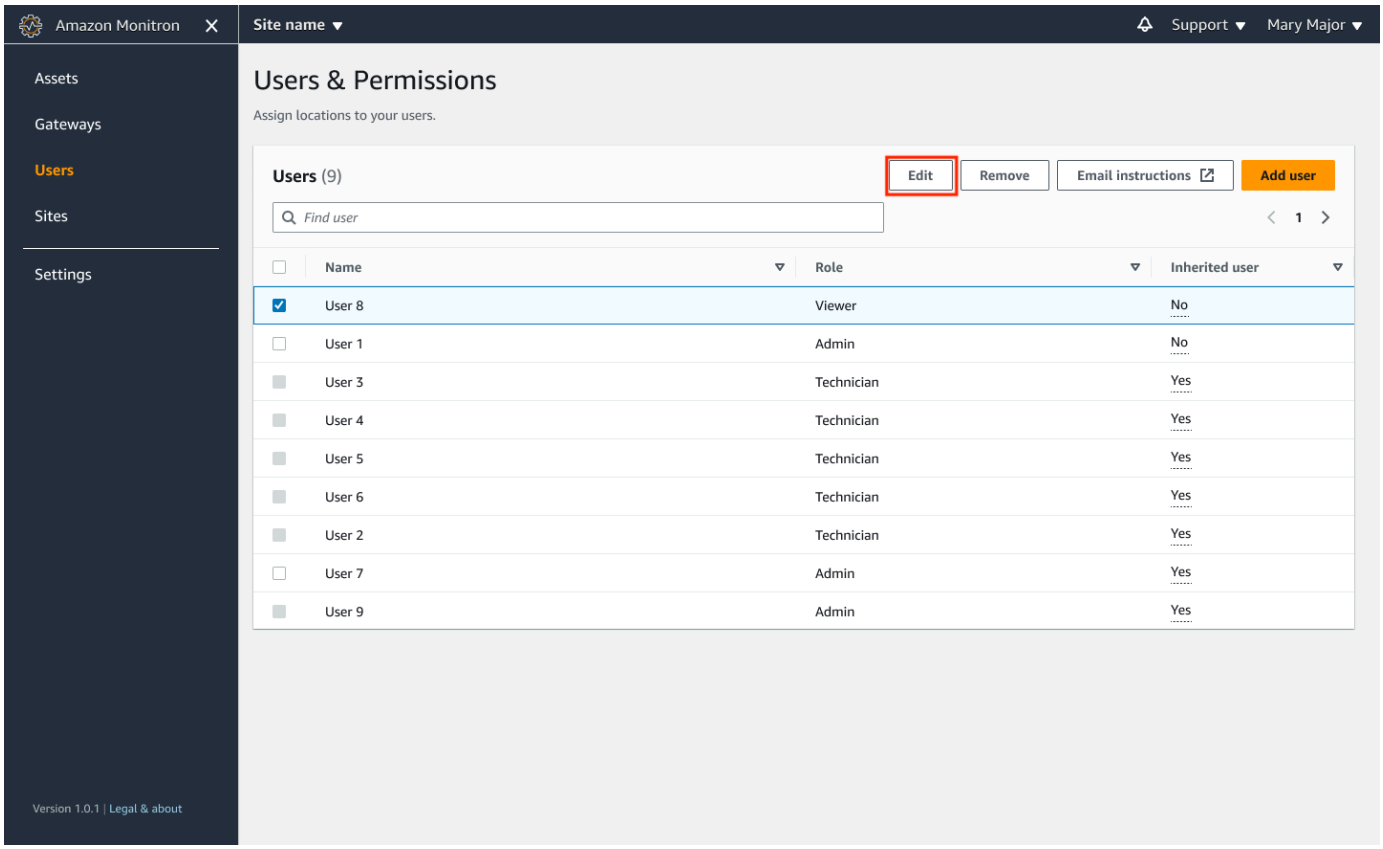
1. Log into the Amazon Monitron mobile app on your smartphone.
2. Navigate to the project or site for the user whose role you want to change, and then to the **Users** list.
3. Choose the vertical ellipsis (

   )

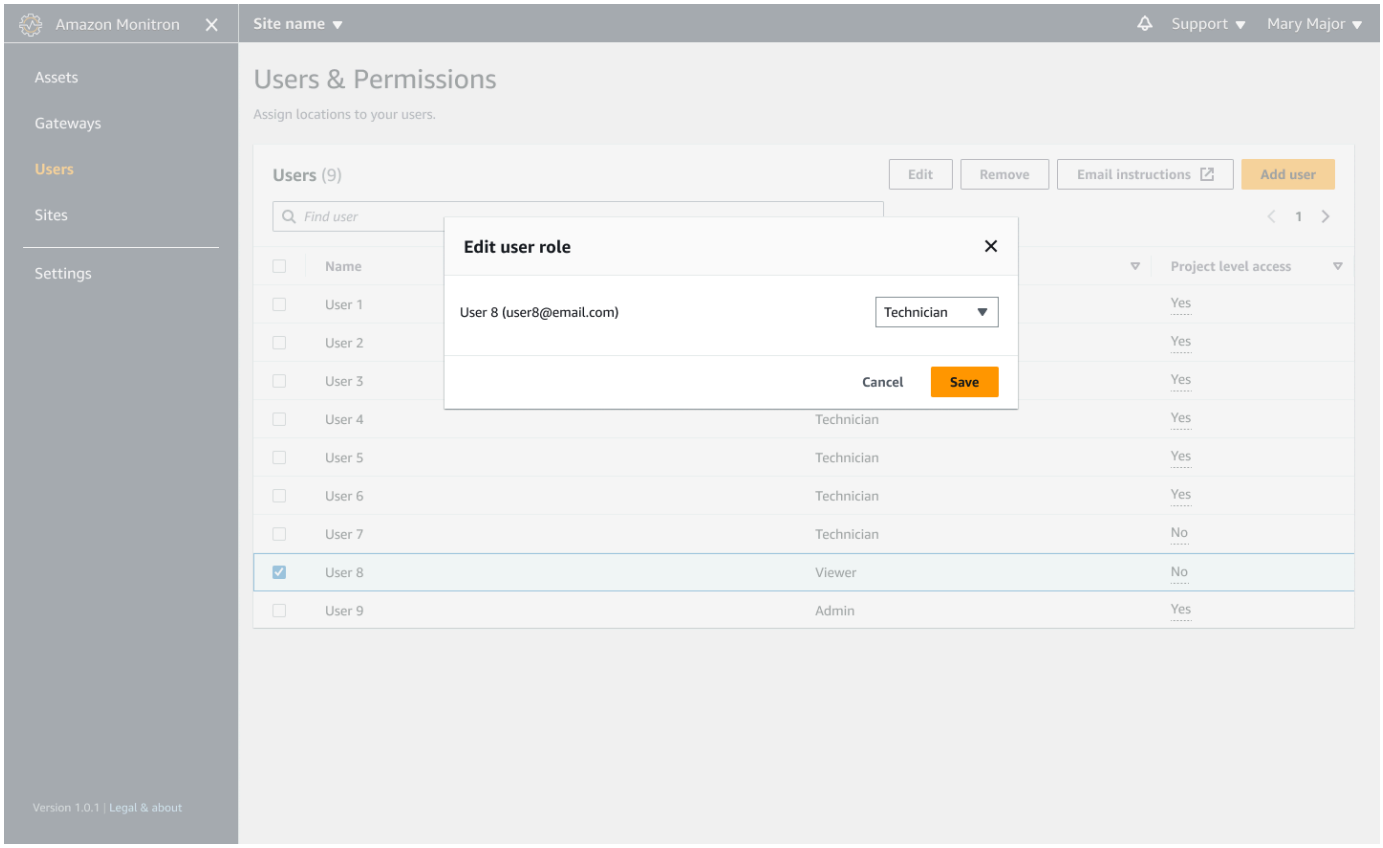
   next to the name of the user whose role you want to change.
4. Choose **Edit user**.
5. Choose a new role for the user: **Admin**, **Technician**, or **Read only**.
6. Choose **Save**.

## To change a user role using the web app

1. Choose **Users** from the navigation pane.



2. Choose **Edit user role**.
3. Choose a new role for the user: **Admin**, **Technician**, or **Viewer**.




4. Choose **Save**.

## Removing a user

Removing a user removes their permissions to access the site or project. It doesn't affect the user directory. Additionally, if the user has permissions to other sites or projects, this won't remove those permissions.

### Topics

- To remove a user using the mobile app
- To remove a user using the web app

### To remove a user using the mobile app

1. Log into the Amazon Monitron mobile app on your smartphone.

2. Navigate to the project or site, and then to the **Users** list page.
3. Choose the vertical ellipses (

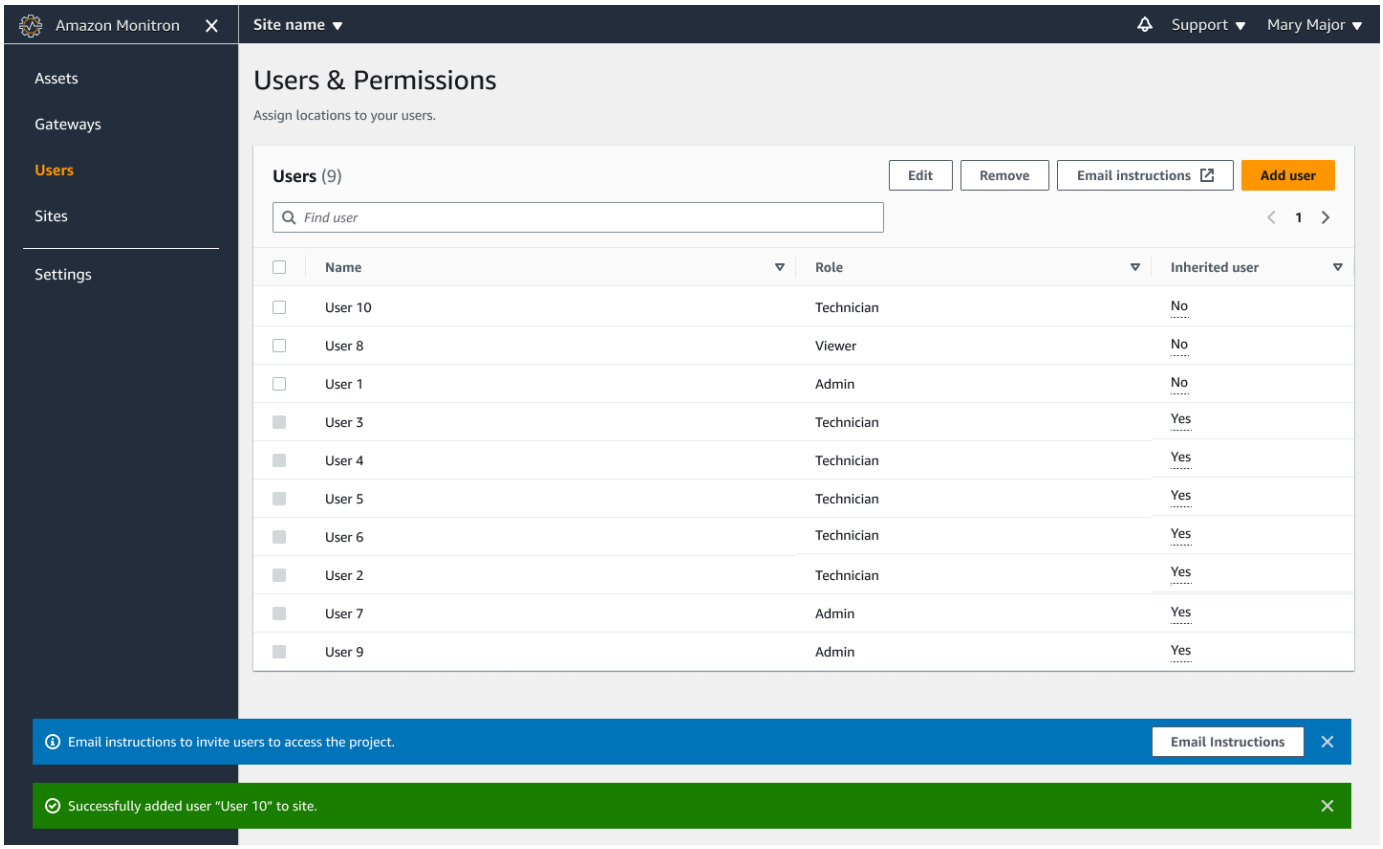


)

   next to the user name.
4. Choose **Remove user**.
5. On the **Confirmation** page, choose **Remove**.

## To remove a user using the web app

1. Select **Users** from the nav pane.




2. Select the user that you want to remove.
3. Choose **Remove**.

# Understanding networking with Amazon Monitron

As you plan your local network, and make decisions about how that network includes Amazon Monitron, it may be helpful to understand how each component relates to the others.

**Topics**


- Networking with your mobile device
- Securing your network


# Networking with your mobile device

From a networking perspective, the process of provisioning sensors or gateways goes like this.

**Topics**


- Setting up your Monitron network foundation with your mobile app
- Setting up your gateways
- Setting up your sensors


## Setting up your Monitron network foundation with your mobile app

1. Your mobile device uses Wi-Fi or a signal from outside the facility (such as a satellite or a tower) to connect to the internet.
2. Over the internet, you install the Amazon Monitron mobile app on your mobile device. (This only has to be done once per device.)
3. Over the internet, the Monitron app on your mobile device connects to the AWS infrastructure, authenticating with AWS IAM Identity Center.
4. Having been authenticated inside the AWS infrastructure, the app connects to the Amazon Monitron back end.
5. Using your authenticated app, you identify the framework of your local Amazon Monitron setup. This involves naming your local network and identifying how many gateways will be part of it.

## Setting up your gateways

1. In your mobile app, (running authenticated and securely over the internet), choose the option for adding a gateway.
2. You give your mobile app permission to access Bluetooth functionality on your mobile device.
3. The mobile app on your device, using Bluetooth, connects to your local gateway.
4. You give the app the name of your local network (Wi-Fi only).
5. You give the app the password to your local network.
6. The app, securely over the internet, communicates with the Monitron back end about your gateway.
7. On the front end, through Bluetooth on your mobile device, the app gives the gateway the token it needs to communicate with the Monitron back end.
8. The gateway uses your local network (Ethernet or Wi-Fi) to connect to the internet through your local internet access point.
9. Securely, over the internet, your gateway registers itself with the Monitron back end.
10. A representation of your gateway now appears in your app as a part of your network.

## Setting up your sensors

1. In the mobile app, you indicate the name and class of your asset (once per asset).
2. In the mobile app, you give a name to a sensor.
3. In your facility, you physically attach an un-paired sensor to your asset.
4. From the mobile app, using your device's NFC, you connect to the sensor.
5. The mobile app, using your device's NFC, tells the sensor about your local Monitron gateway, already set up.
6. The mobile app, securely over the internet, tells the Monitron back end about the sensor.
7. The sensor, using Bluetooth, begins to send data about the asset to the gateway.
8. The gateway, securely over the internet, sends the sensor's data to the Monitron back end.
9. In the mobile app (or the web app), securely over the internet, you can now view the analytical data about your asset.

# Securing your network

In order to allow your Amazon Monitron gateways to send data back to AWS, you should allow the following with regard to your local network traffic:

- Protocol UDP, port 53 - standard DNS port
- Protocol UDP, ports 67 and 68 - standard DHCP ports
- TCP ports 443 and 8883
- For Amazon Monitron gateways commissioned before 19th January, 2024:
  - Domains ending in `*.amazonaws.com`
- For Amazon Monitron gateways commissioned after 19th January, 2024:
  - Asia Pacific (Sydney) (ap-southeast-2) – 54.79.215.104 and 54.79.23.89
  - Europe (Ireland) (eu-west-1) – 54.72.131.46, 34.251.27.192, and 52.213.71.97
  - US East (N. Virginia) (us-east-1) – 3.215.69.205, 52.86.131.66, and 18.210.44.199

> **Note**
>
> There's no regression with new static IPs being enabled by default for previously commissioned devices as they have already been allow listed for IP domains ending in `*.amazonaws.com` (which already includes the new static IP domain of `amazonaws.com`). Decommissioning and recomissioning a gateway will switch it to static IP. You can't revert a gateway network configuration from a static IP to a dynamic IP.

If you are using an **Android mobile device** to provision your gateways and sensors, then you should allow the following with regard to your local network traffic:

- TCP ports 443, 5228, 5229, and 5230
- Domains ending in `*.google.com`, `*.googleapis.com`
- Any ports required by your telecom provider
- TCP port 5094 for SSL communications used on

  ***Vodafone devices***

If you are using an **Apple mobile device** to provision your gateways and sensors, then you should allow the following with regard to your local network traffic:

- TCP ports 443, 2197, and 5223
- Subnets 17.249.0.0/16, 17.252.0.0/16, 17.57.144.0/22, 17.188.128.0/18, and 17.188.20.0/23
- See also: Apple's list of required ports and hosts

Note: Amazon Monitron, Android, and Apple do not (per their respective documentation) require the following ports to be open:

- UDP port 443
- TCP port 80

# Accessing your Amazon Monitron data

There are two ways to access your raw Amazon Monitron data outside of Amazon Monitron.

You may want access your data on an ongoing basis, so that you can use it elsewhere. In that case, you can configure Amazon Monitron to automatically add your data to a Kinesis stream. From there, you can port it to various destinations, including Amazon S3 and Lambda. This process requires configuration, and that configuration requires an understanding of Kinesis Data Streams. However, once you have all the elements arranged to your satisfaction, you can keep your data streaming automatically.

Or you may want to access your data once in a while, just to gain a clear understanding of what kind of data you are storing and analyzing on AWS. In that case, you can ask AWS support to manually copy your data to Amazon S3. This process requires less configuration, but it cannot be automated. It only gives you the data that Amazon Monitron has accumulated up until now, in one chunk.

**Topics**


- Exporting your Amazon Monitron data to Amazon S3
- Amazon Monitron Kinesis data export v1
- Amazon Monitron Kinesis data export v2


# Exporting your Amazon Monitron data to Amazon S3

You may sometimes want to access the raw data that Amazon Monitron is storing for you, in order to stay informed about exactly what kind of data you're securely storing with AWS.

You can get your raw data by filing a support ticket with AWS, and by giving Amazon Monitron permission to deliver your data to you.

To get real time operational data for Amazon Monitron resources that can be consumed programmatically, consider exporting your data using Kinesis streams. For more information, see Amazon Monitron Kinesis data export v2.

**Topics**


- Prerequisites

- Exporting your data with AWS CloudFormation (recommended option)
- Exporting your data with the console
- Exporting your data with CloudShell

## Prerequisites

To successfully export your Amazon Monitron data, the following prerequisites must be met.

- You must not already have another export (of Amazon Monitron data) running in the same region.
- You cannot have run another export in same region in past 24 hours.

## Exporting your data with AWS CloudFormation (recommended option)

**Topics**

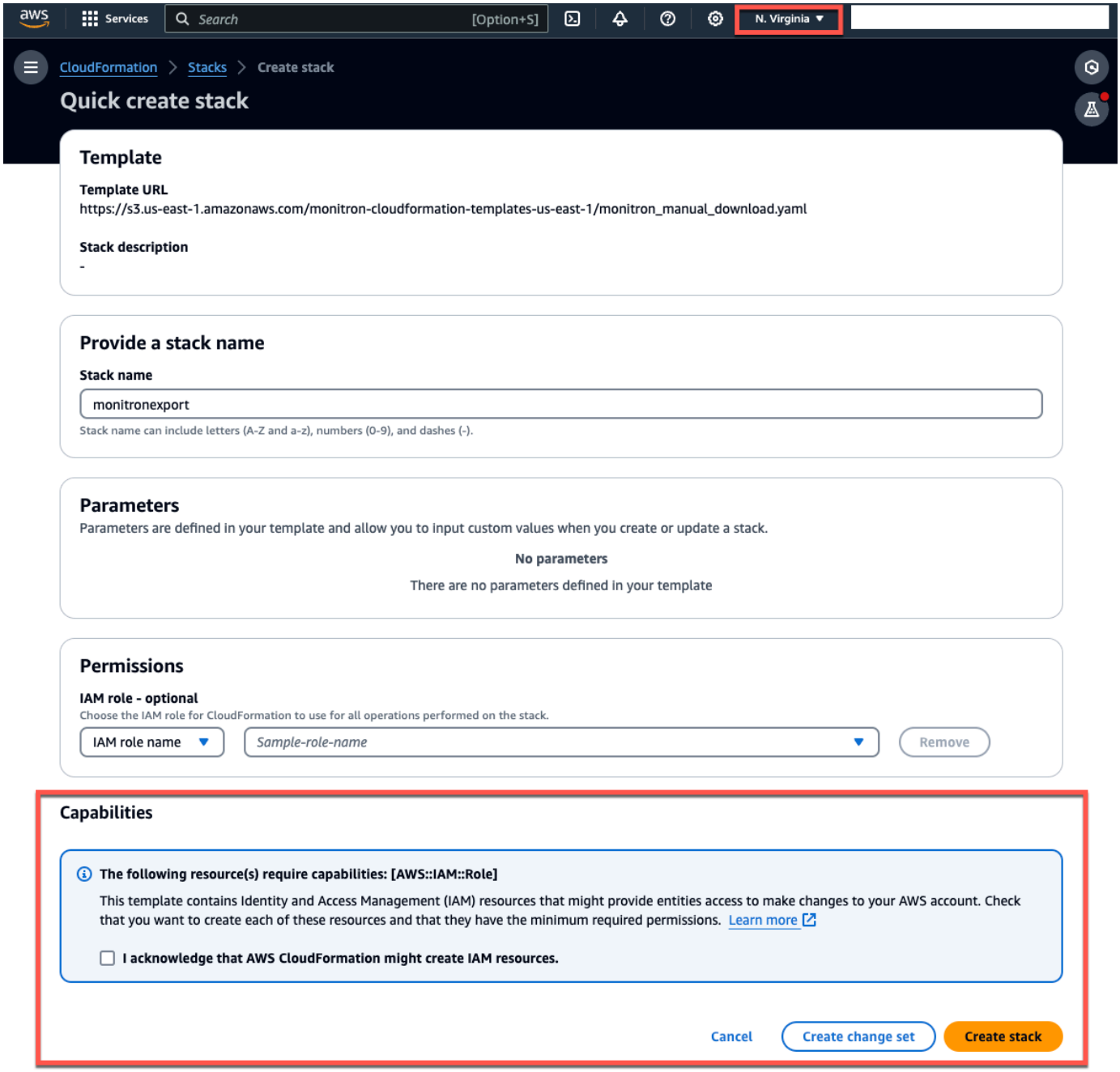
- Step 1: Create your Amazon S3 bucket, IAM role, and IAM policies.
- Step 2: Note your resources
- Step 3: Create the support case

### Step 1: Create your Amazon S3 bucket, IAM role, and IAM policies.

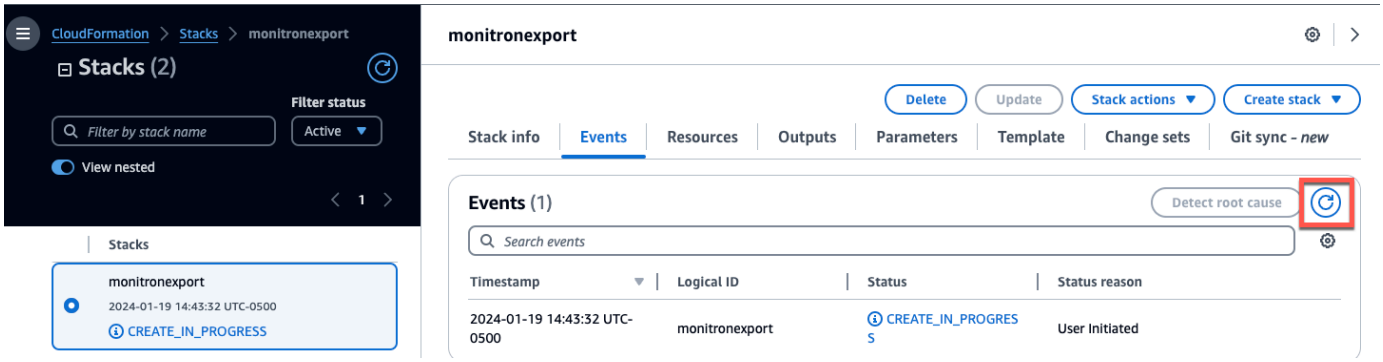
1. Sign in to your AWS account.
2. Open a new browser tab with the following URL.

```
https://console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/create/review?templateURL=https://s3.us-east-1.amazonaws.com/monitron-cloudformation-templates-us-east-1/monitron_manual_download.yaml&stackName=monitronexport
```

3. On the AWS CloudFormation page that opens, in the upper right corner, select the region in which you are using Amazon Monitron.
4. Choose **Create stack**.

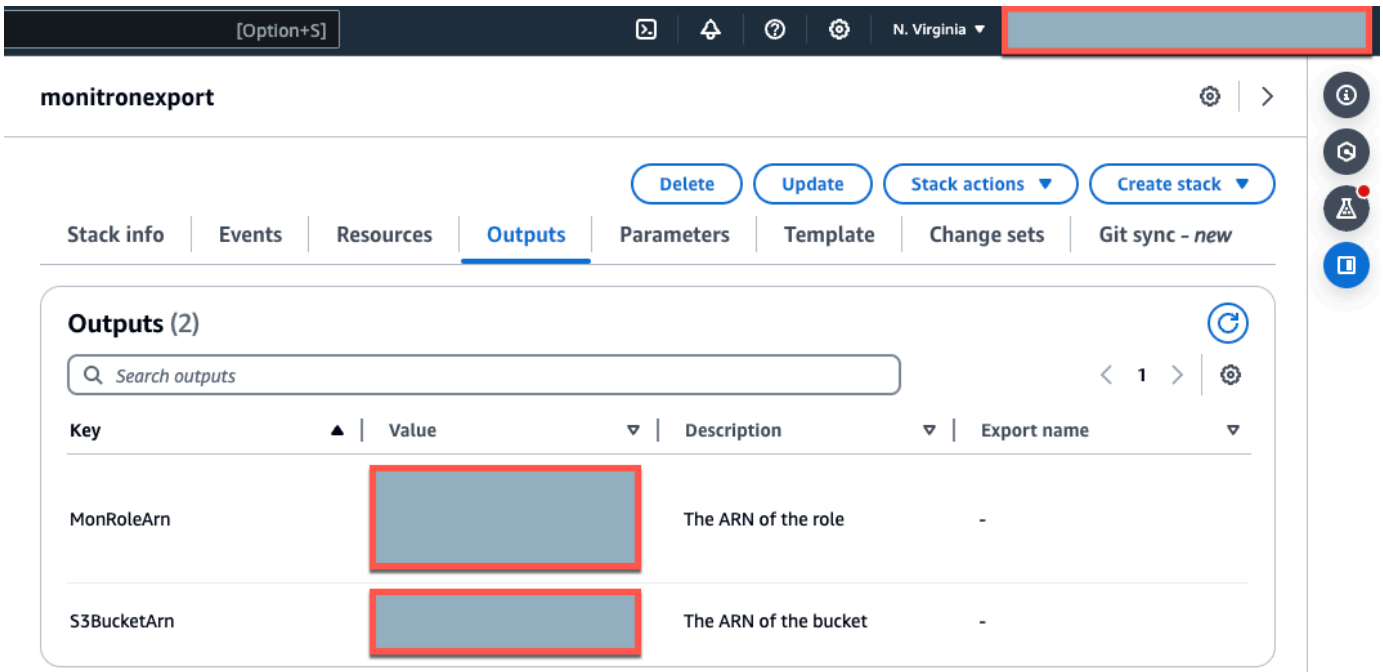



5. On the next page, choose the refresh icon as often as you like until the status of the stack (monitronexport) is CREATE_COMPLETE.



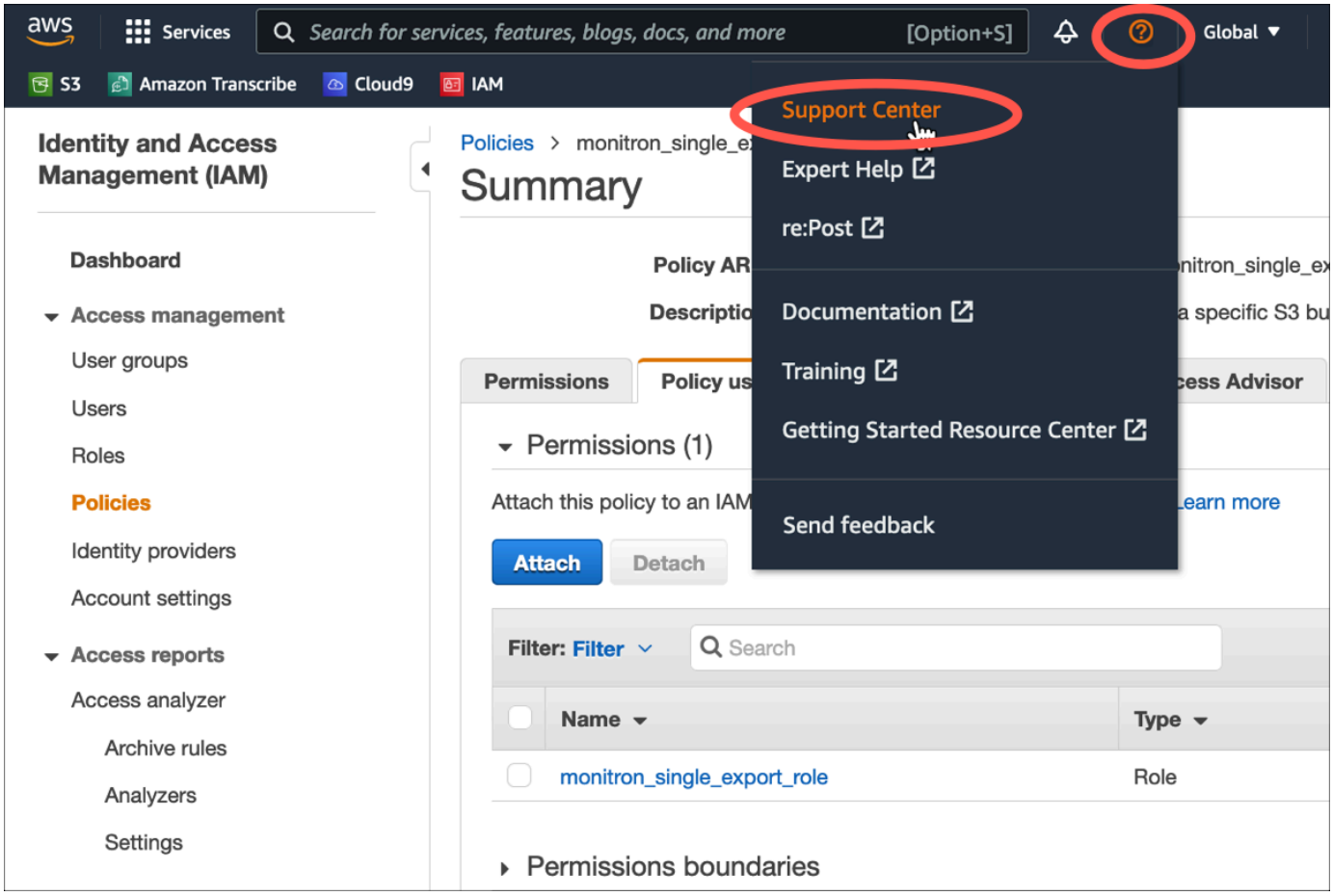

## Step 2: Note your resources

1. Choose the **Outputs** tab.
2. Note the value of the key `MonRoleArn`.
3. Note the value of the key `S3BucketArn`.
4. Note your account ID from the upper right corner of the page).
5. Note the region you chose in Step 1. It also now appears at the top of the page, to the left of your account ID.

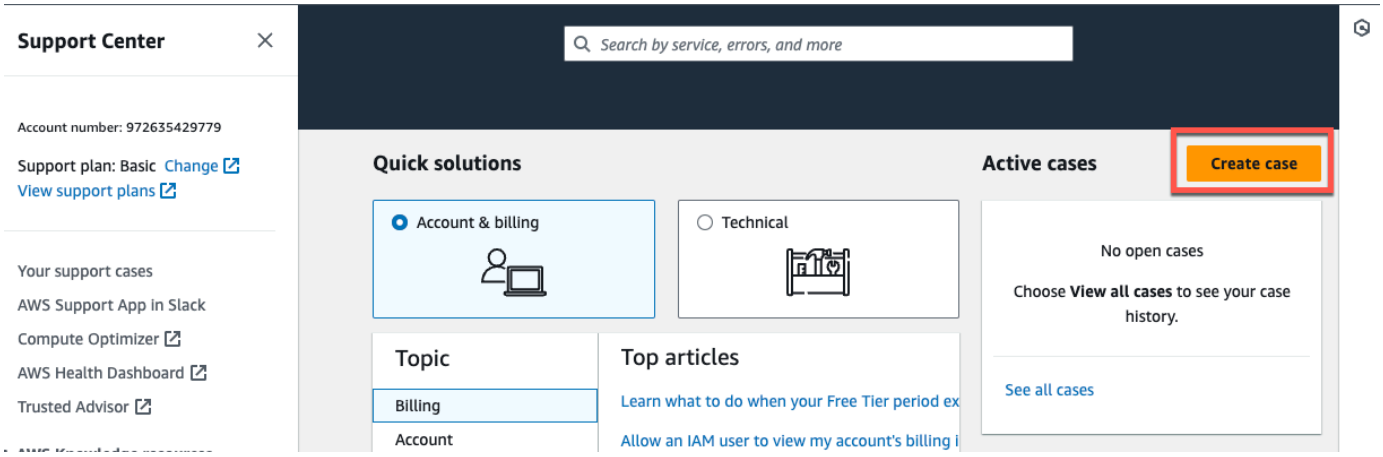


## Step 3: Create the support case

1. From your AWS console, choose the question mark icon near the upper right corner of any page, then choose **Support Center**.




2. On the next page, choose **Create case**.




3. On the **How can we help?** page, do the following:

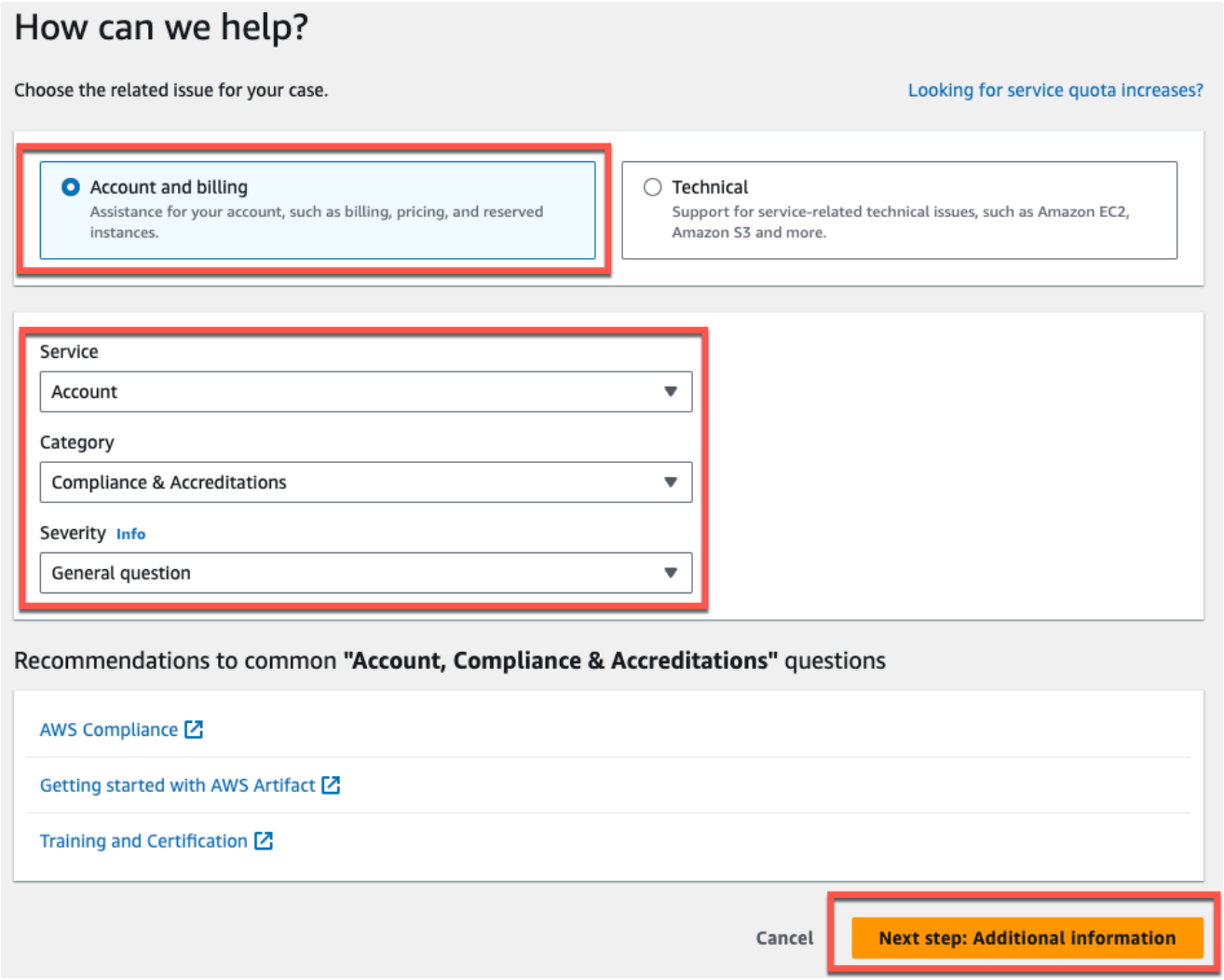
a. Choose **Account and billing support**.

b. Under **Service**, choose **Account**.

c. Under **Category**, choose **Compliance & Accreditations**.

d. Choose **Severity**, if that option is available to you based on your support subscription.

e. Choose **Next step: Additional information**.



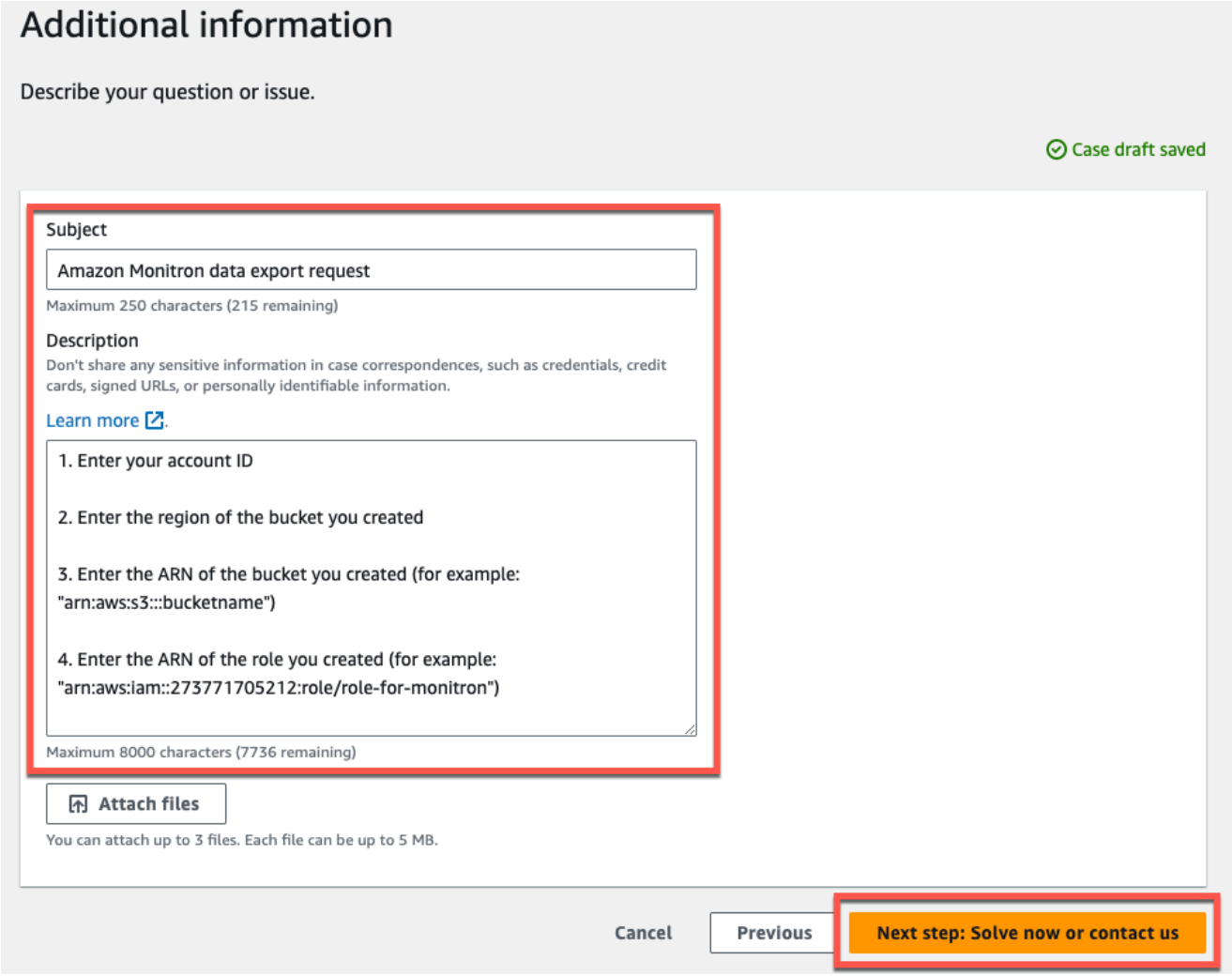

4. In **Additional information** do the following:

a. Under **Subject**, enter **Amazon Monitron data export request**.

b. In the **Description** field, enter:

1. your account ID
2. the region of the bucket you created
3. the ARN of the bucket you created (for example: "arn:aws:s3:::bucketname")

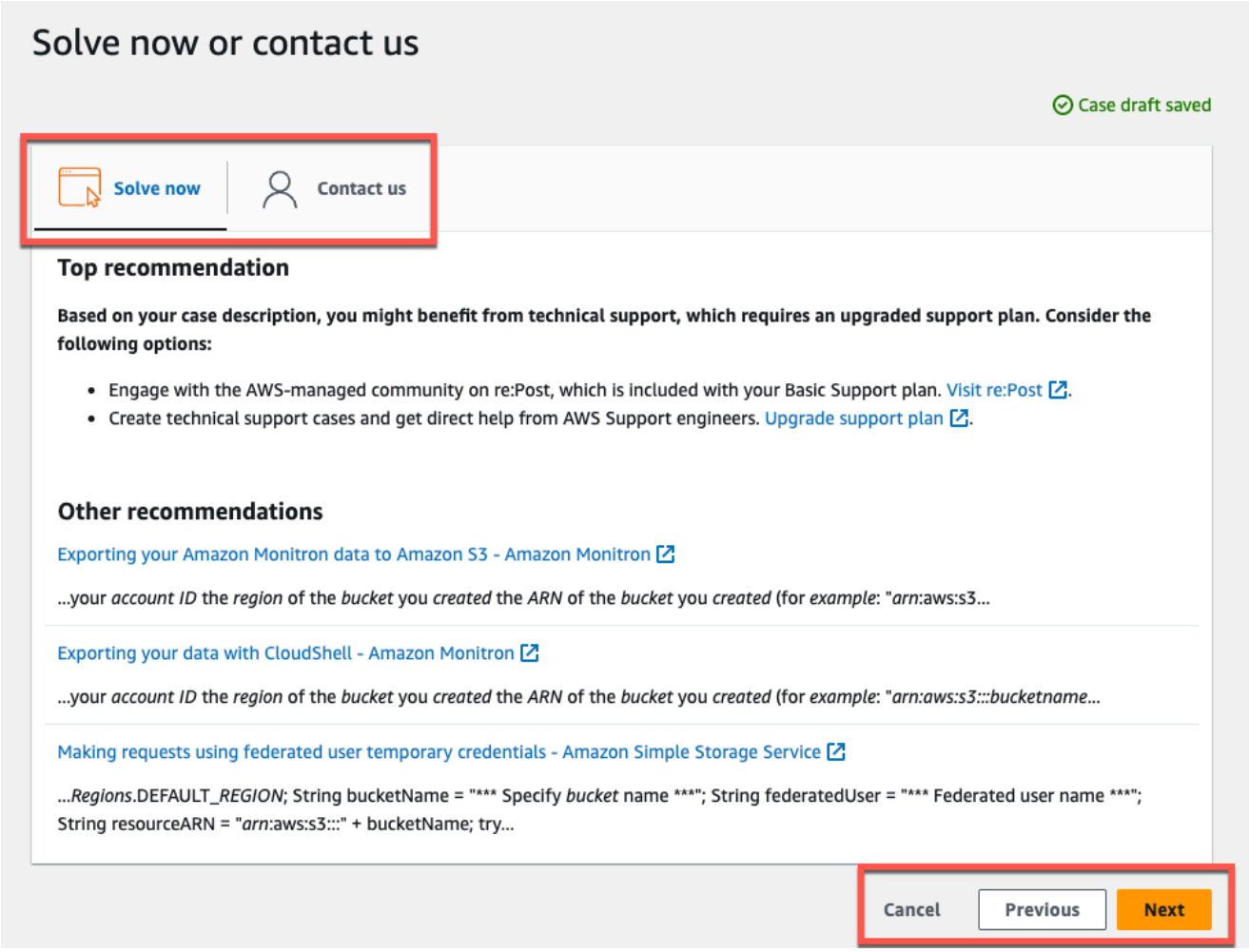
4. the ARN of the role you created (for example: "arn:aws:iam::273771705212:role/role-for-monitron")




c. Choose **Next step: Solve now or contact us**.

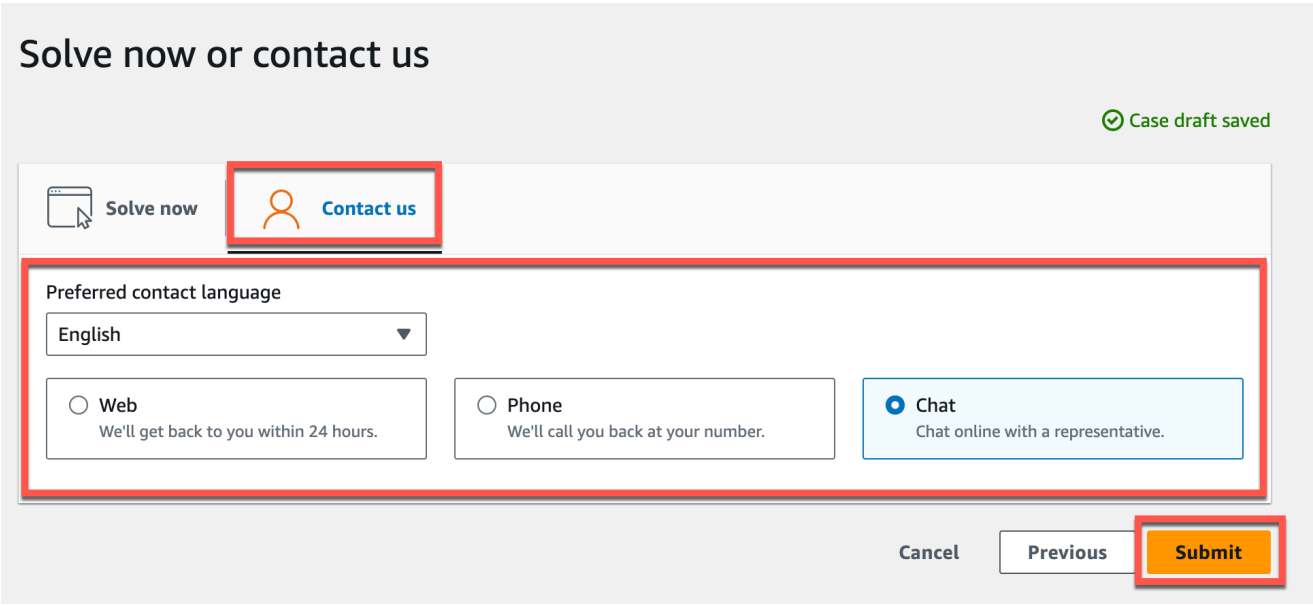
5. In **Solve now or contact us** do the following:

a. In **Solve now**, select **Next**.




b. In **Contact us**, choose your **Preferred contact language** and preferred method of contact.

c. Choose **Submit**. A confirmation screen with your case ID and details will be displayed.



An AWS customer support specialist will get back to you as soon as possible. If there are any issues with the steps listed, the specialist may ask you for more information. If all the necessary information has been provided, the specialist will let you know as soon as your data has been copied to the Amazon S3 bucket that you created above.

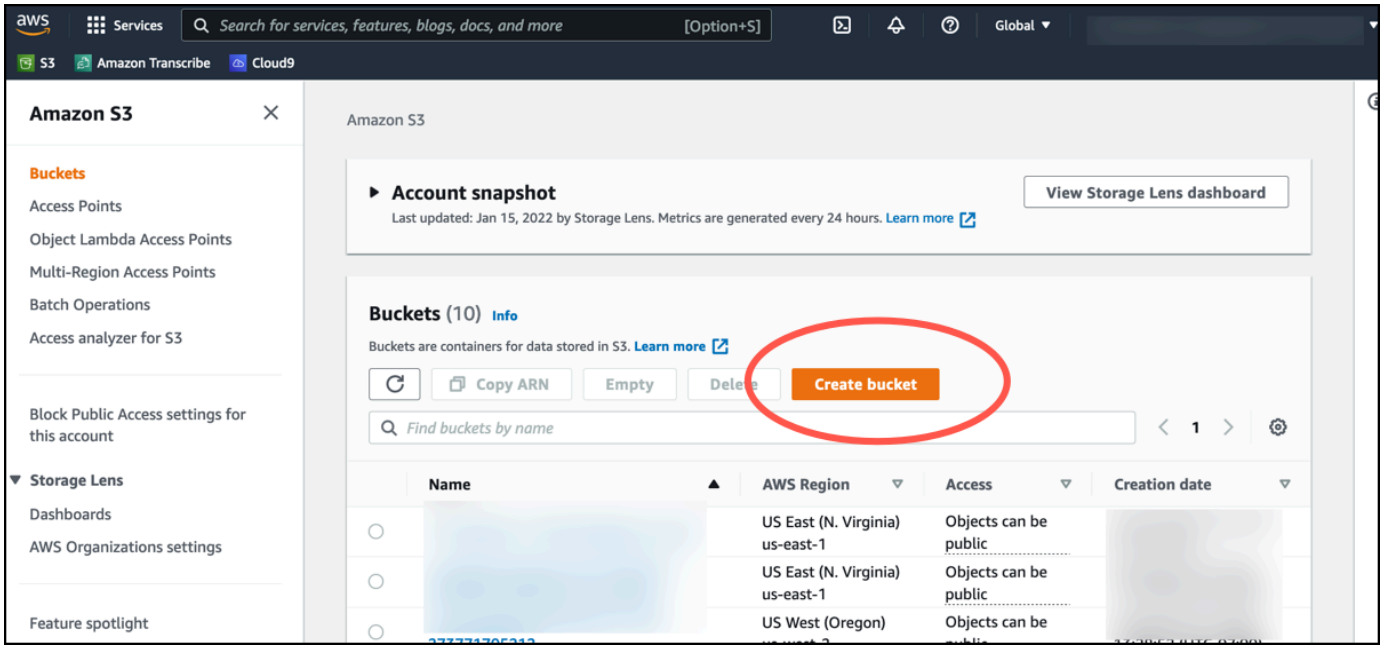
## Exporting your data with the console

### Topics


- Step 1: Setting up your Amazon S3 bucket
- Step 2: Give Amazon Monitron permission to access Amazon S3
- Step 3: Create the role
- Step 4: Create the trust policy
- Step 5: Create the support case


### Step 1: Setting up your Amazon S3 bucket

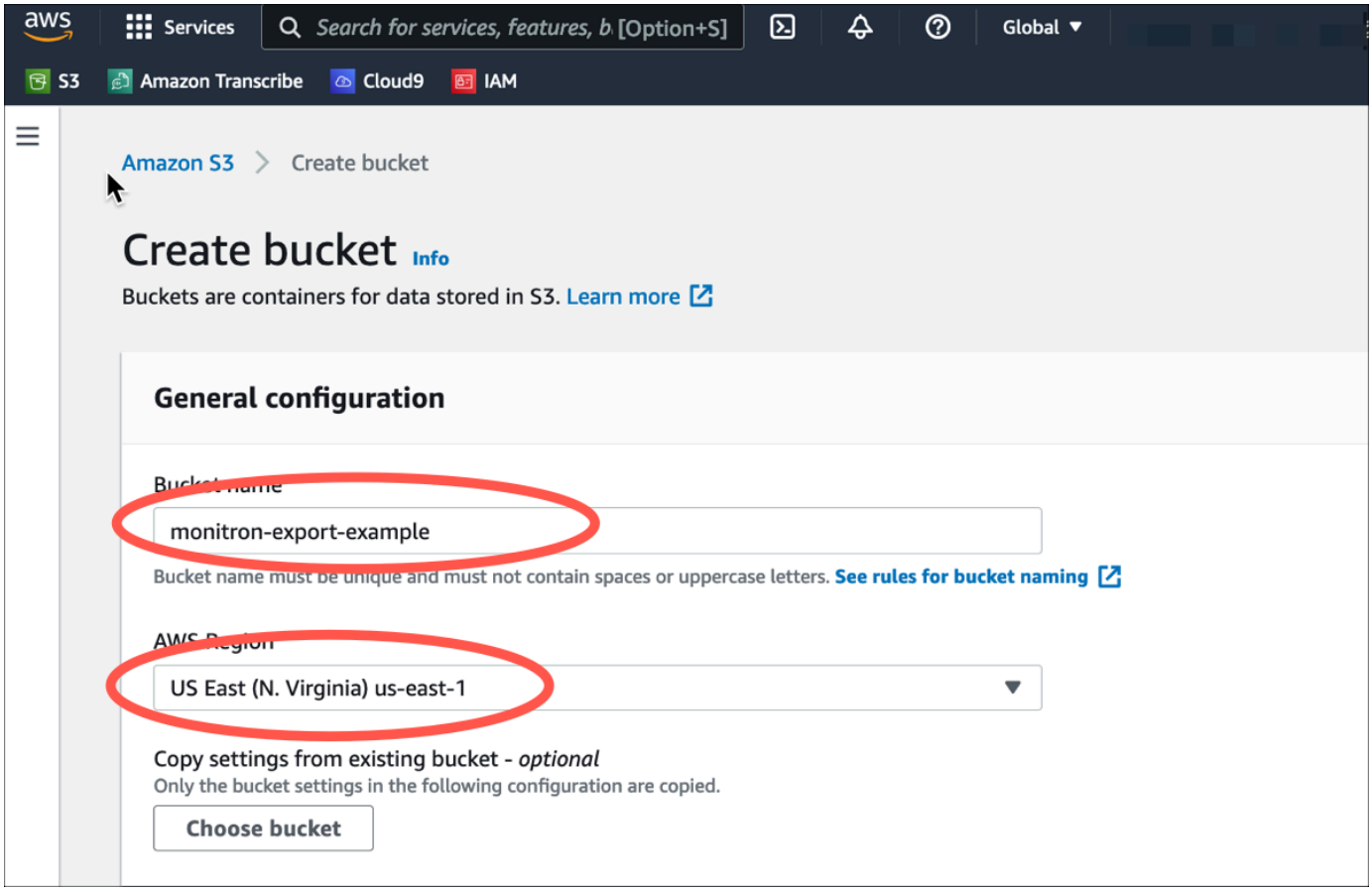
1. Open the Amazon S3 console.
2. Choose **Create bucket**.




3. Name your bucket and select an appropriate region. Then, at the bottom of the page, choose **Create bucket**.

> **Important**
>
> At this time, Amazon Monitron is only supported in three regions:
>
> - US East (N. Virginia) us-east-1
> - EU (Ireland) eu-west-1
> - Asia Pacific (Sydney) ap-south-east-2
>
> Therefore, your Amazon S3 bucket must be in one of those regions.

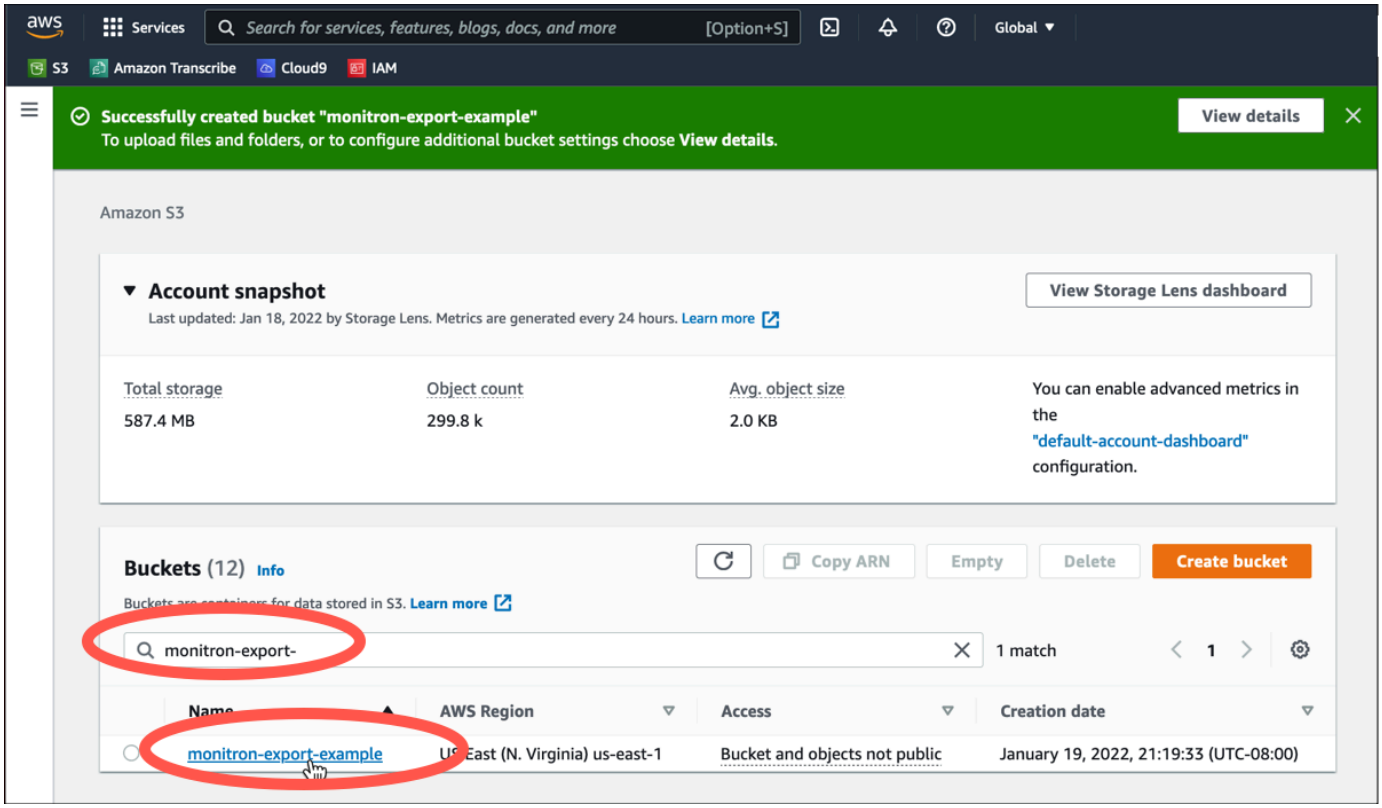
It must also be the same region in which you are using the Amazon Monitron service.



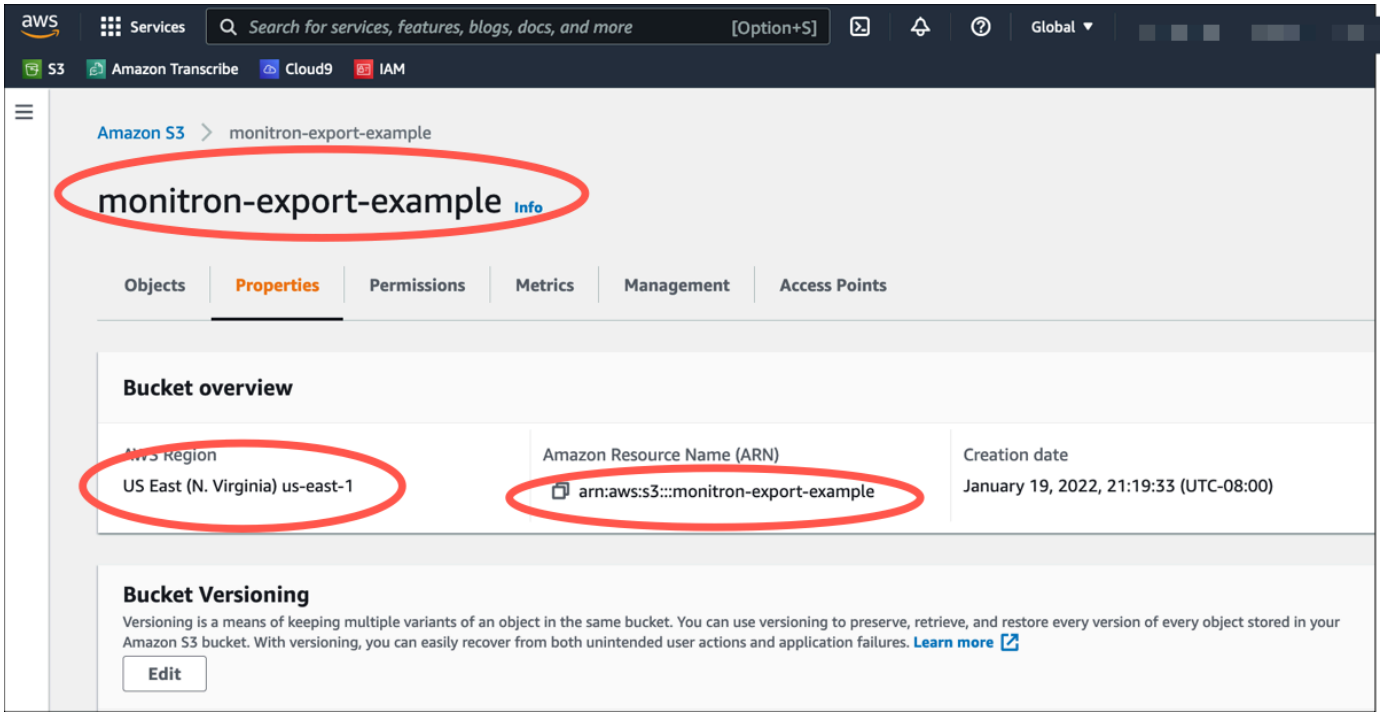

4. Review the rest of the options on the page, and make the appropriate choices, depending on your security needs and policies.

> **Important**
>
> You are responsible for taking the appropriate steps to secure your data. We strongly recommend using server-side encryption and blocking public access to your bucket.

5. Using the search box, find the bucket you just created, and then choose it.

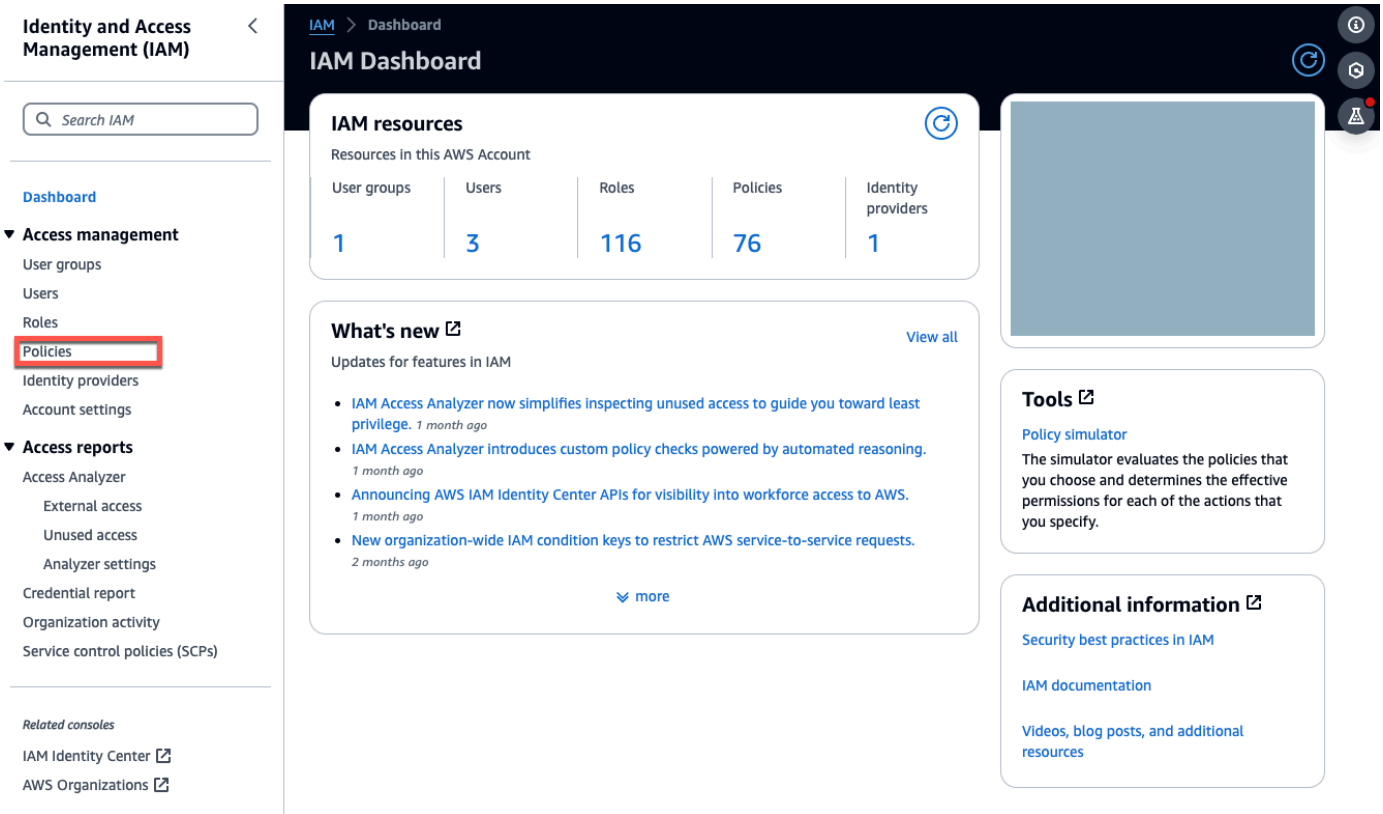



6. From the **Properties** tab, make a note of the name, ARN, and region of the bucket.

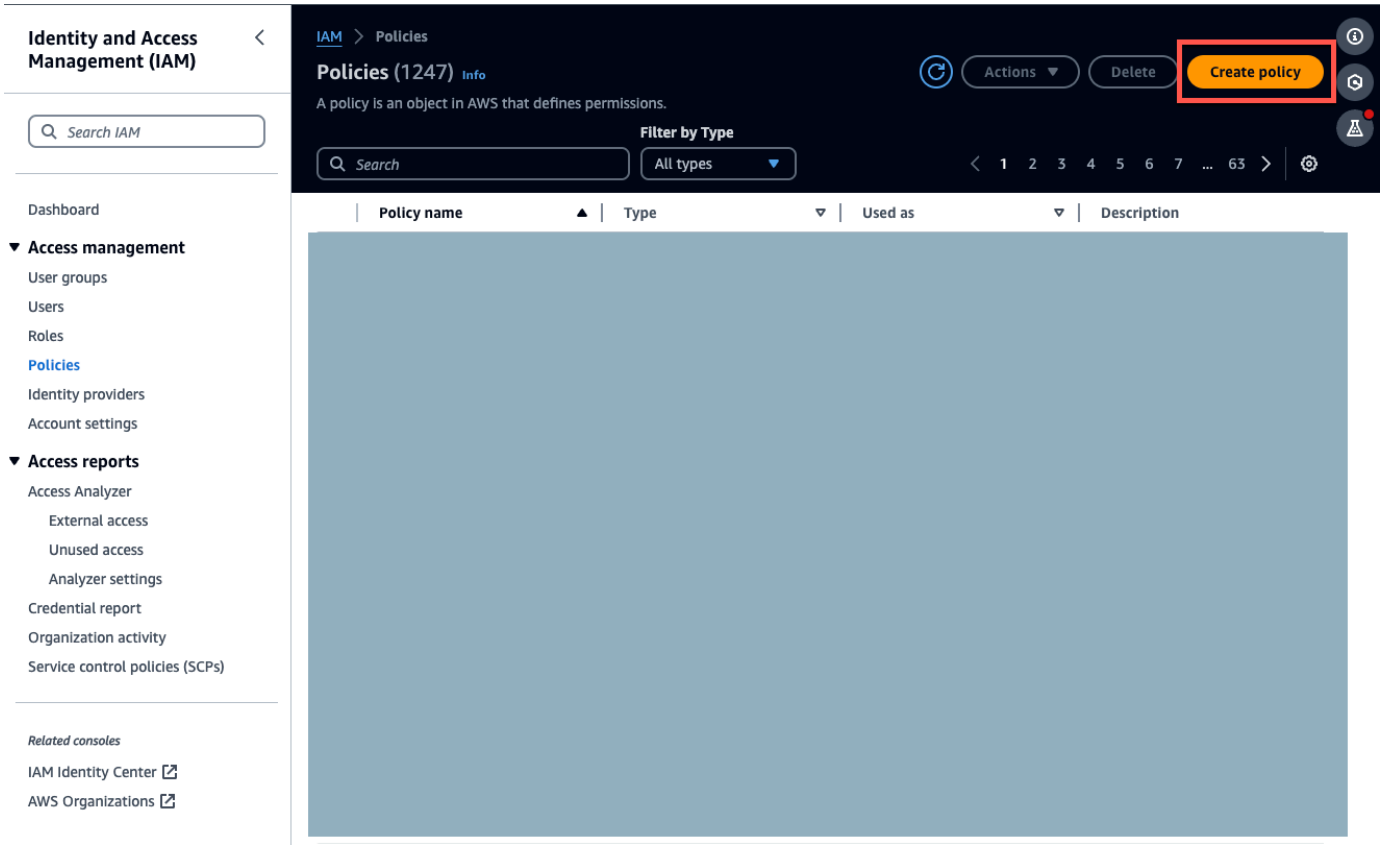



## Step 2: Give Amazon Monitron permission to access Amazon S3

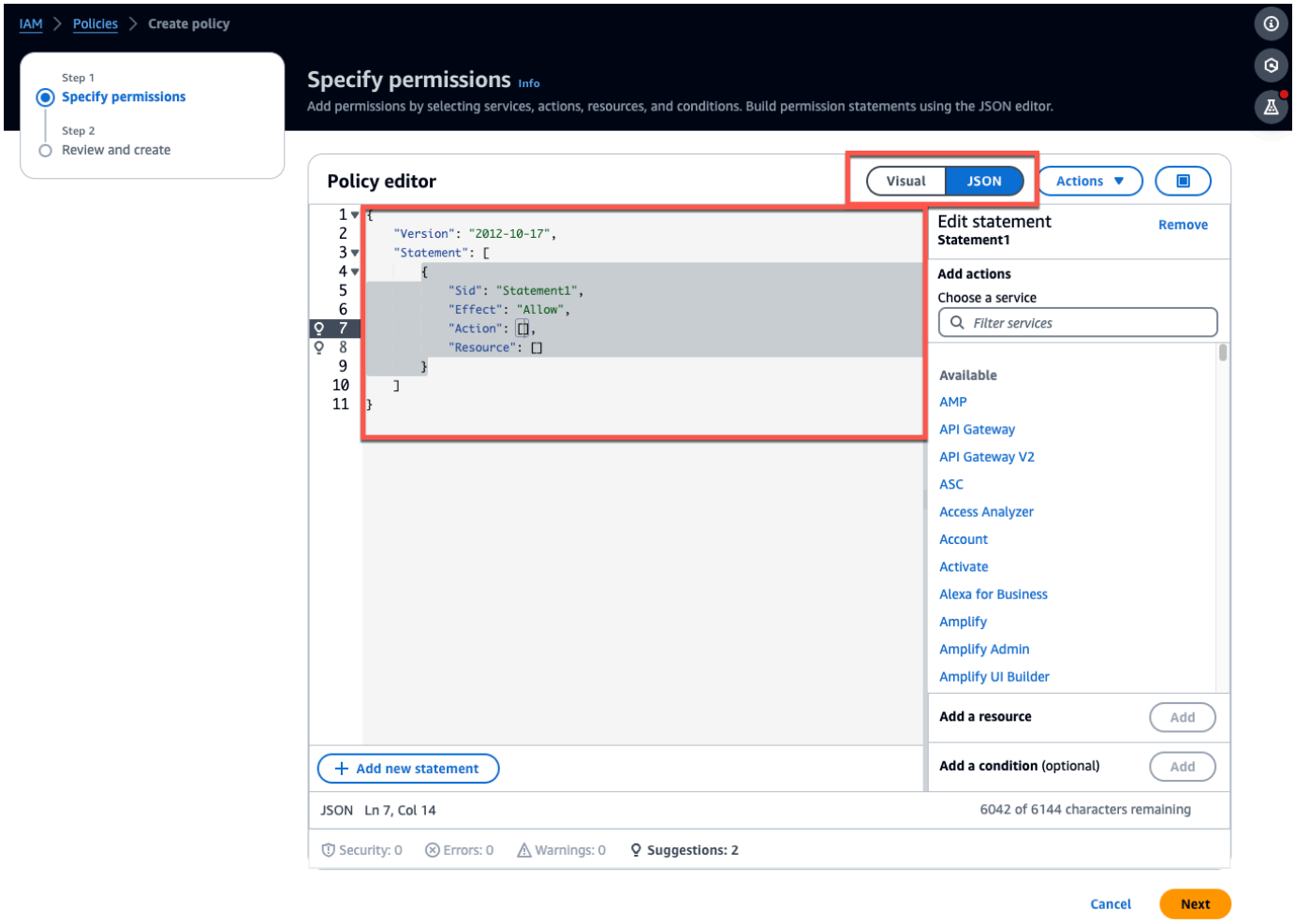
1. Open the IAM console and choose **Policies**.



2. Choose **Create policy**.



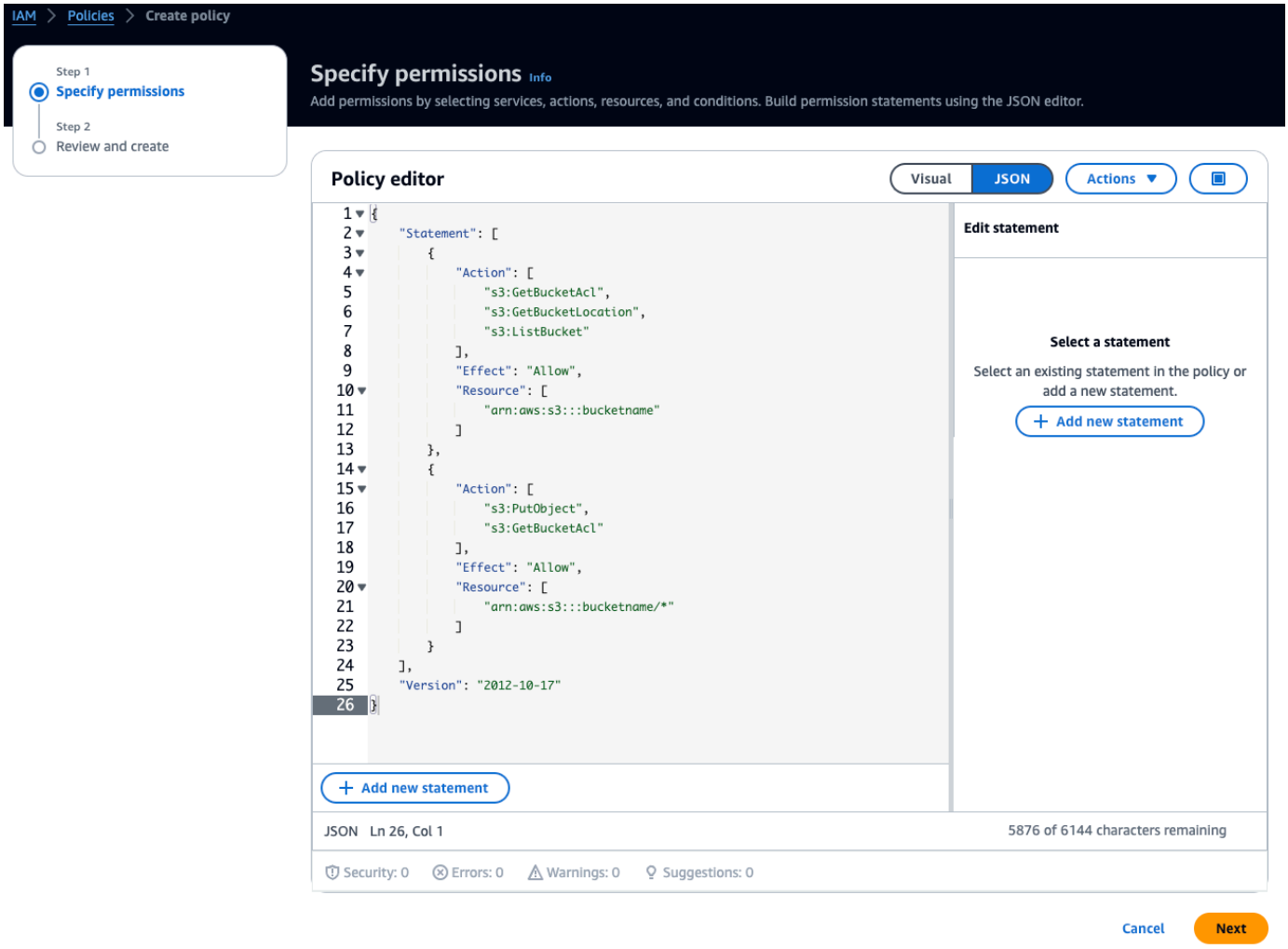

3. Select the **JSON** tab.




4. Delete the default JSON text so that the form is empty.
5. Paste in the bucket access policy.

```
{
    "Statement": [
        {
            "Action": [
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::bucketname"
            ]
        },
        {
```

```
            "Action": [
                "s3:PutObject",
                "s3:GetBucketAcl"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::bucketname/*"
            ]
        }
    ],
    "Version": "2012-10-17"
}
```



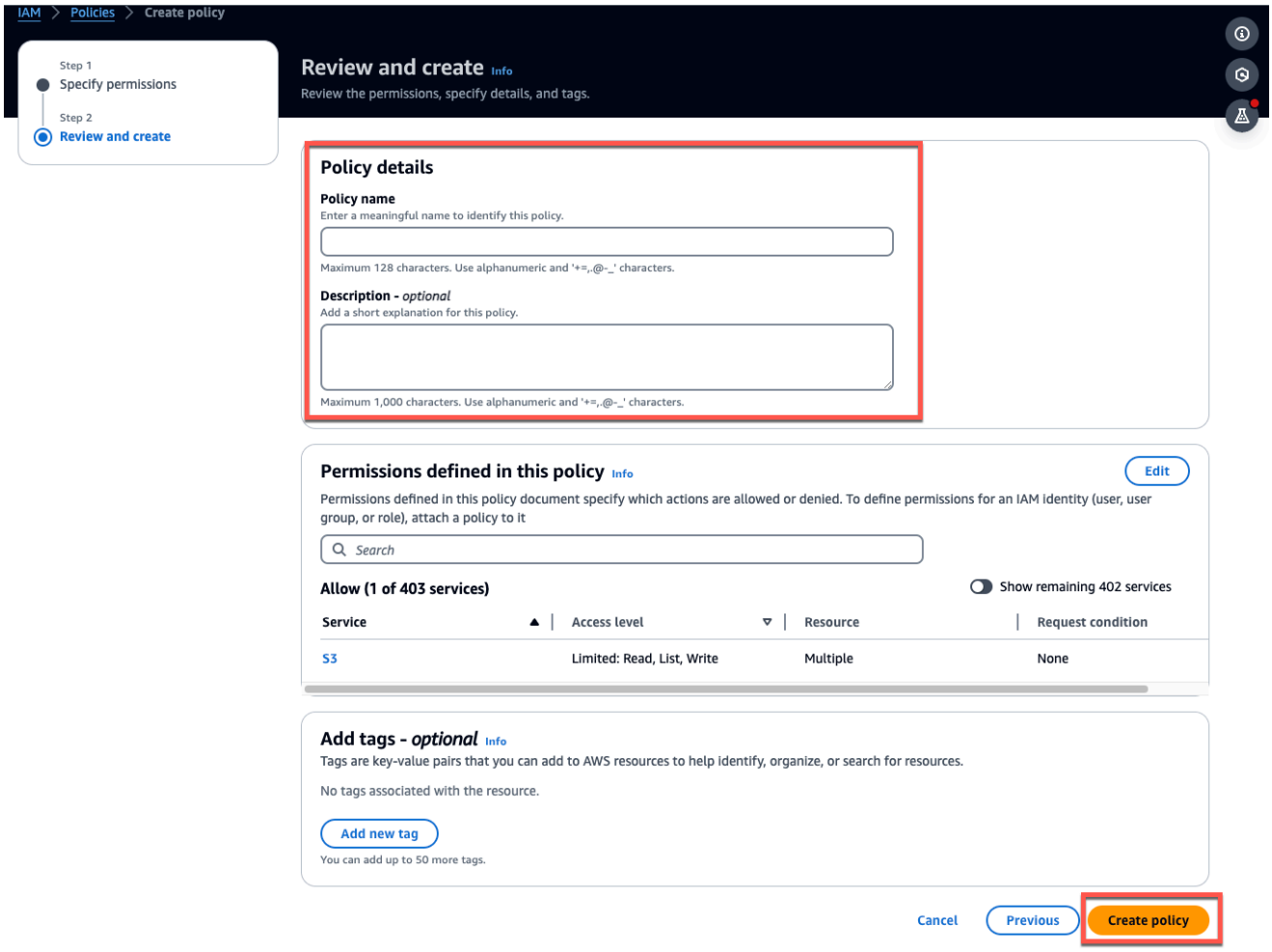

6. Select **Next**.
7. On the **Review and create** page, do the following:

a. In **Policy details**, enter a **Policy name** and optional **Description**.

b. Leave the **Permissions defined in this policy** section as is.

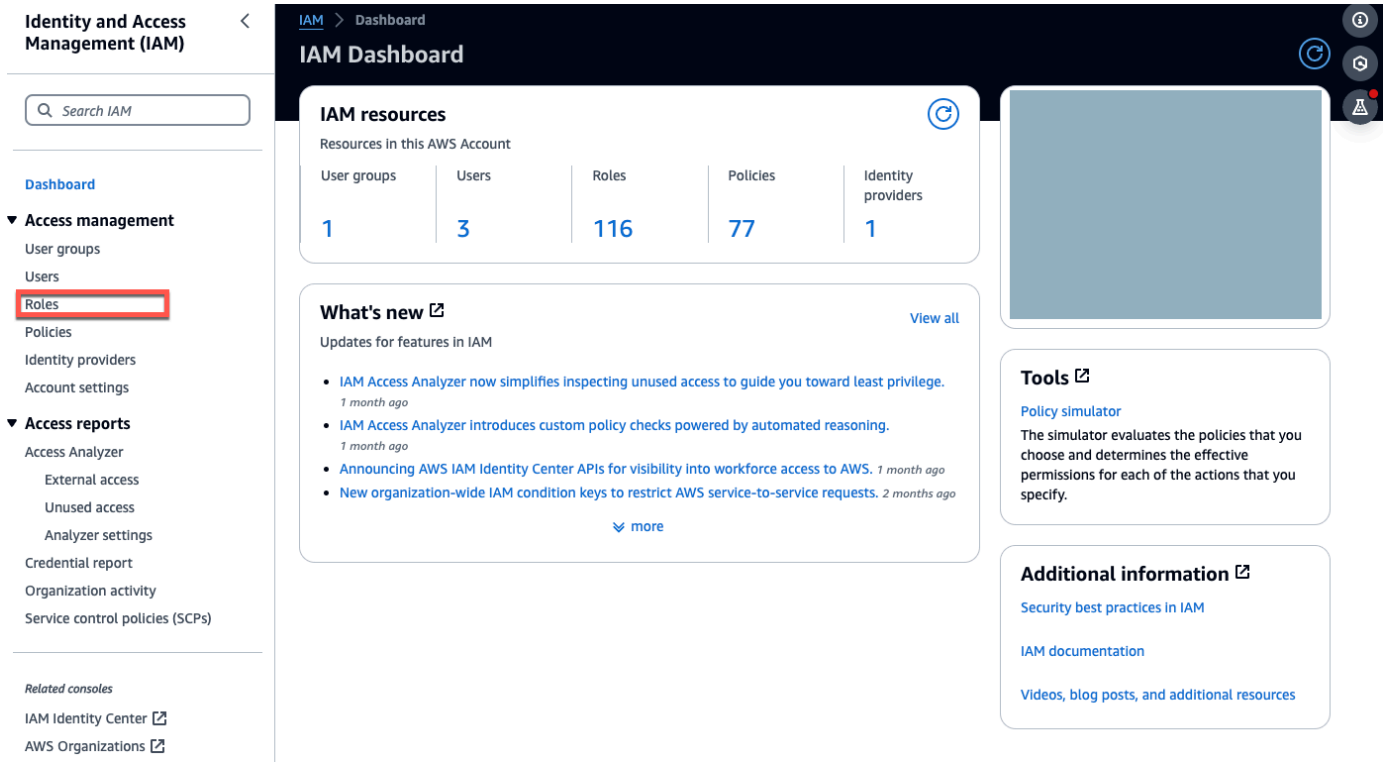
c. In **Add tags — *optional*, you can choose to add tags to keep track of your resources.**.

d. Choose **Create policy**.

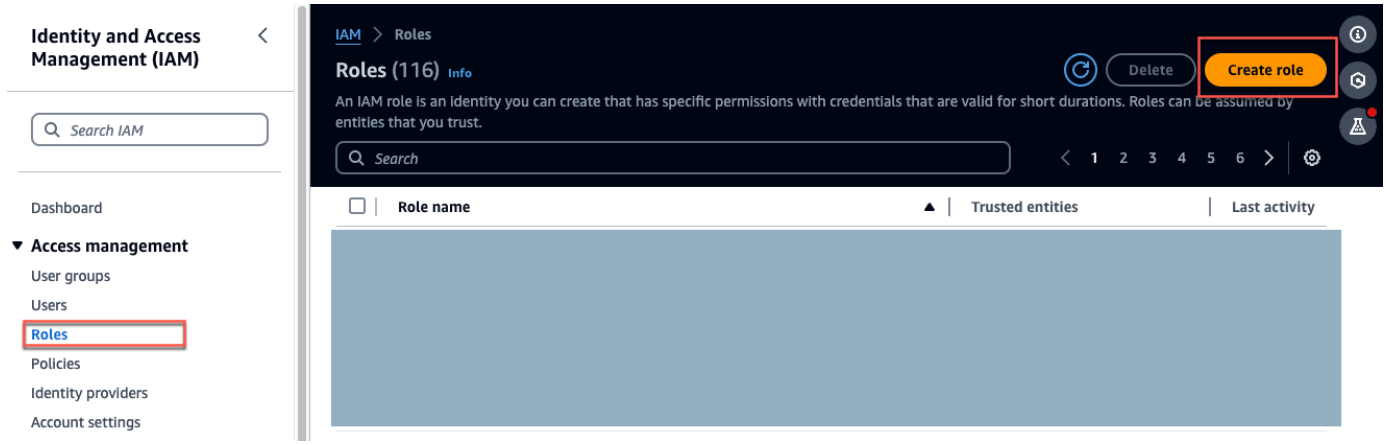



## Step 3: Create the role

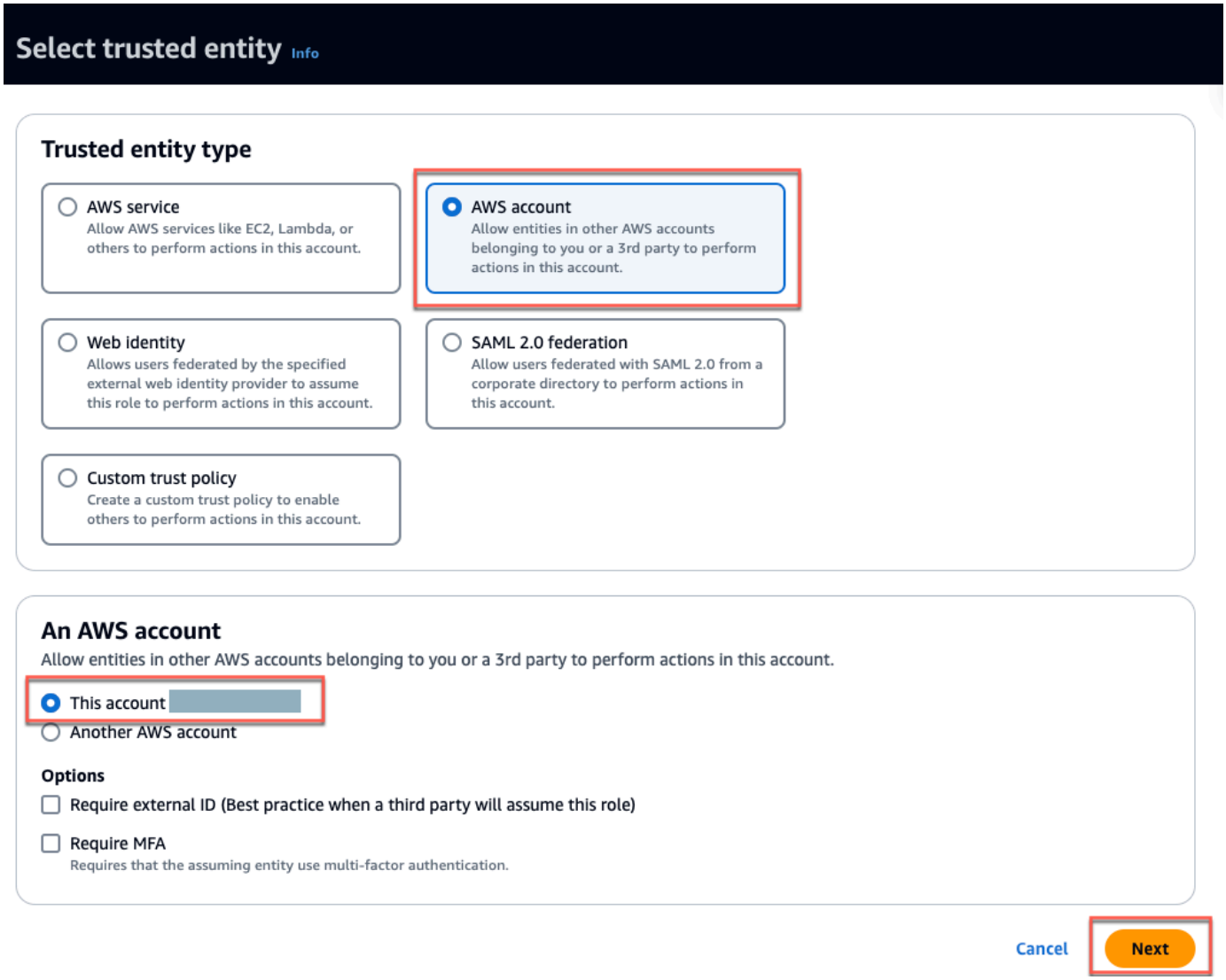
1. Open the IAM console and choose **Roles**.



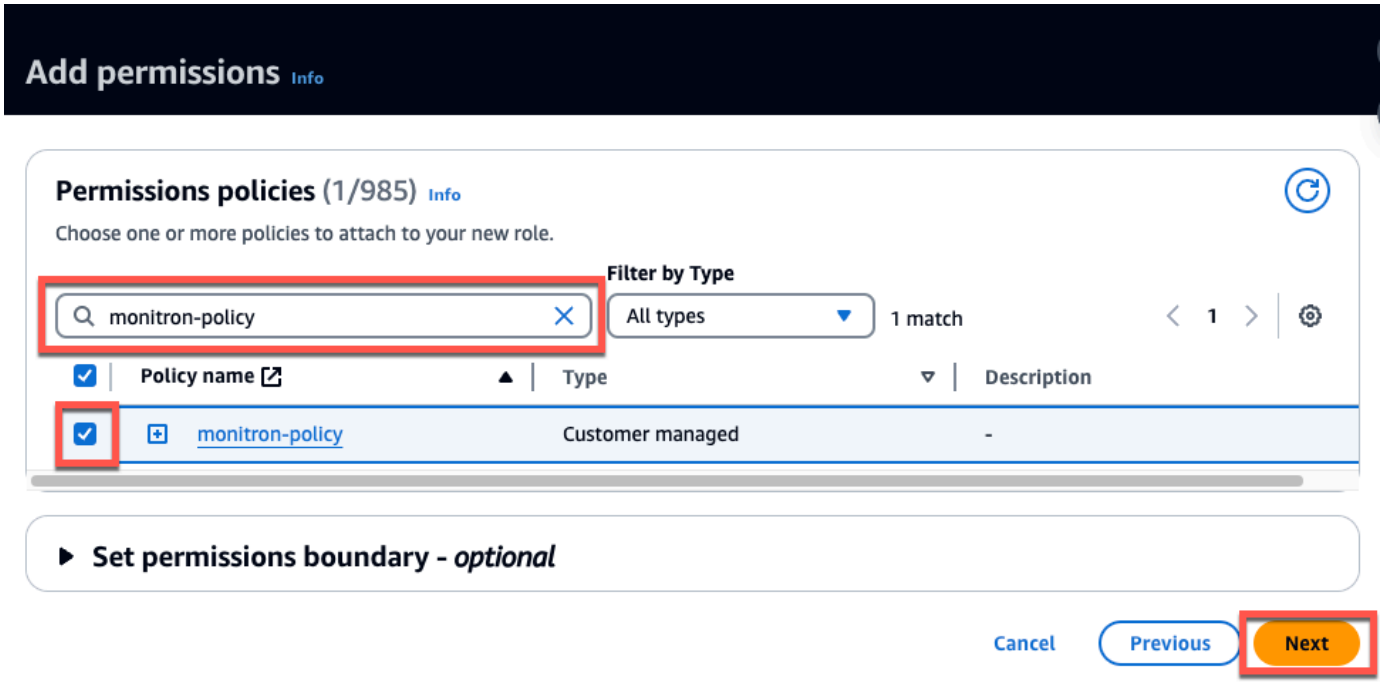

2. Choose **Create role**.




3. On the **Select trusted entity**, in **Trusted entity type**, choose **AWS account**.
4. In **An AWS account**, choose **This account**. You can customize additional setting using **Options**.
5. Choose **Next**.




6. In **Add permissions**, for **Permissions policies**, search for the policy you just created in the search box, and select your policy.



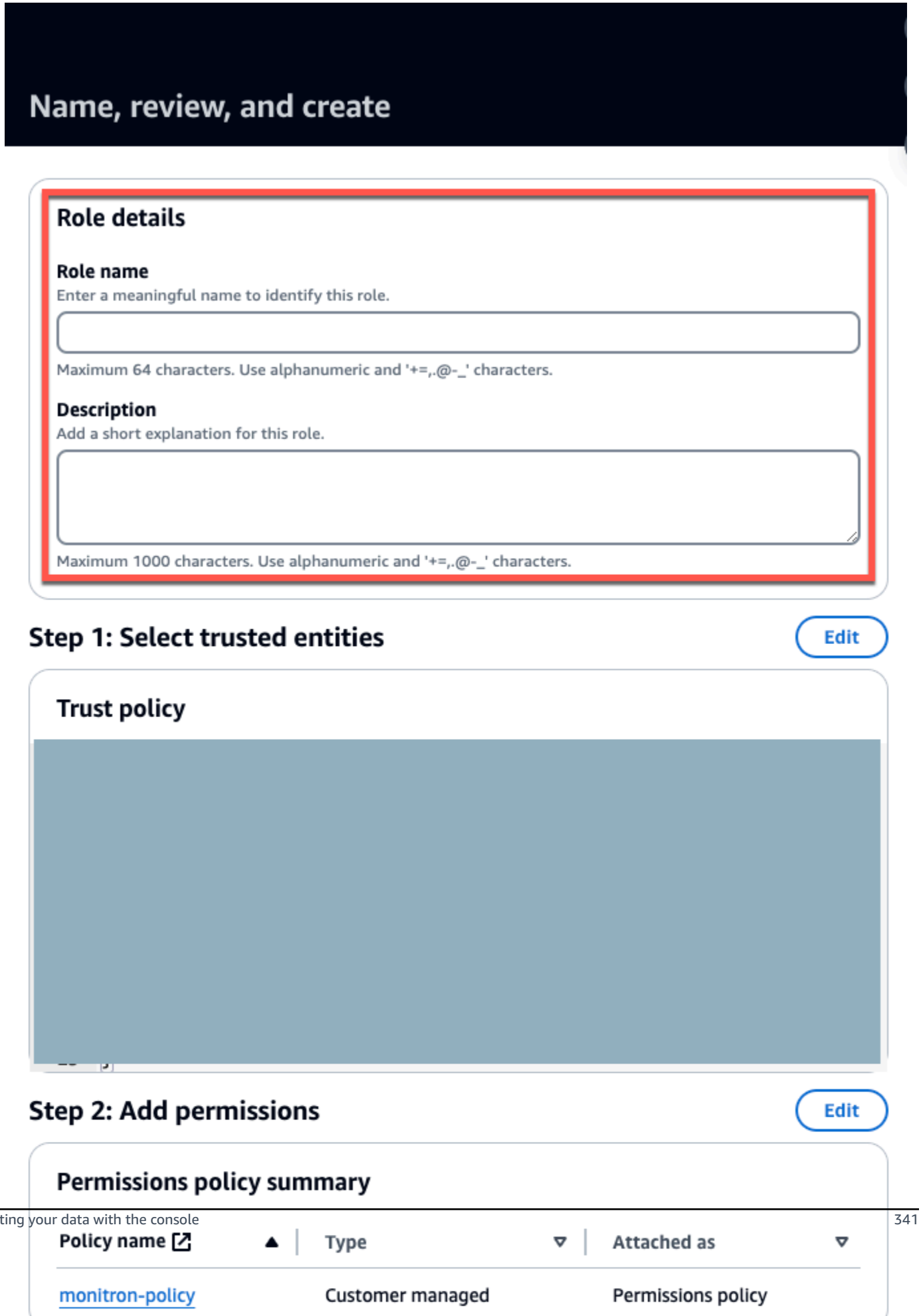

7. On the **Name, review, and create** page do the following:

   a. In **Role details** enter a **Role name** and optional **Description**.

   b. You can choose to ignore **Step 1: Select trusted entities** and **Step 2: Add permisions**.

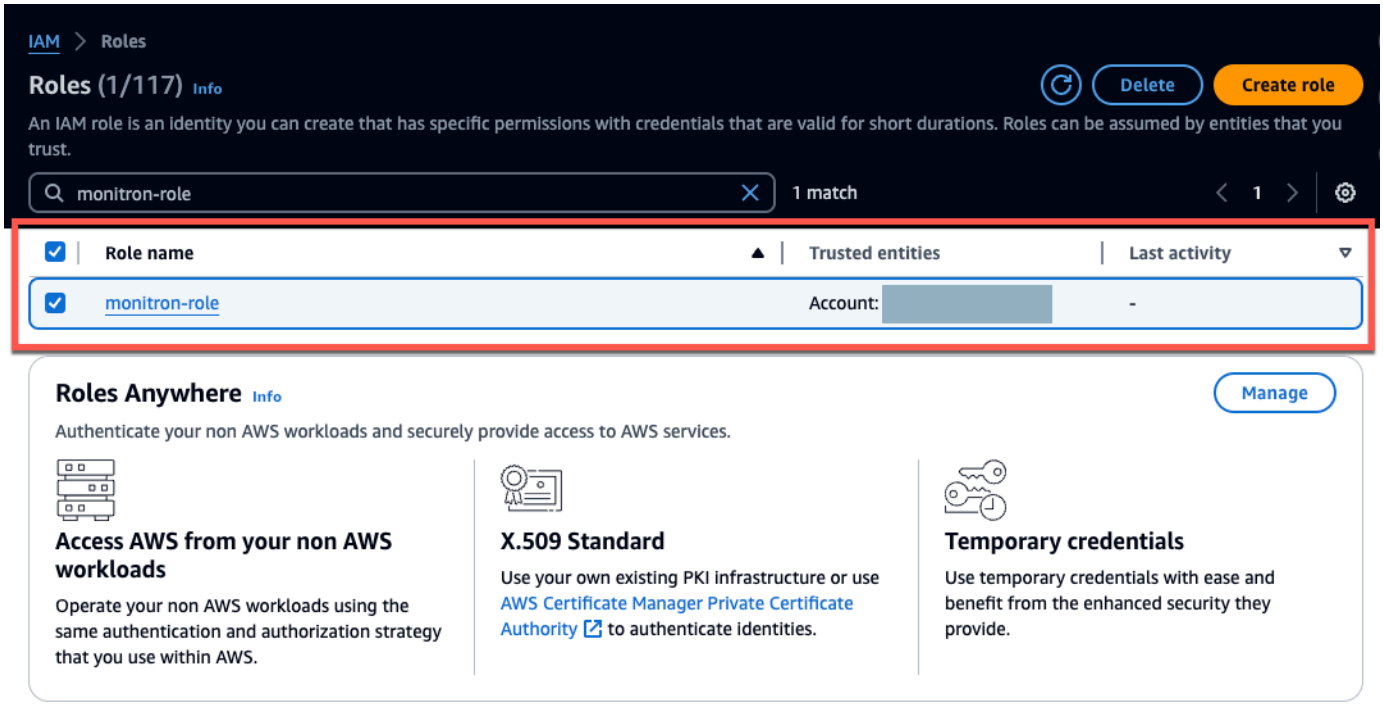
   c. For **Step 3: Add tags**, for **Add tags — *optional***, add optional tags to keep track of your resources.

8. Choose **Create role**.

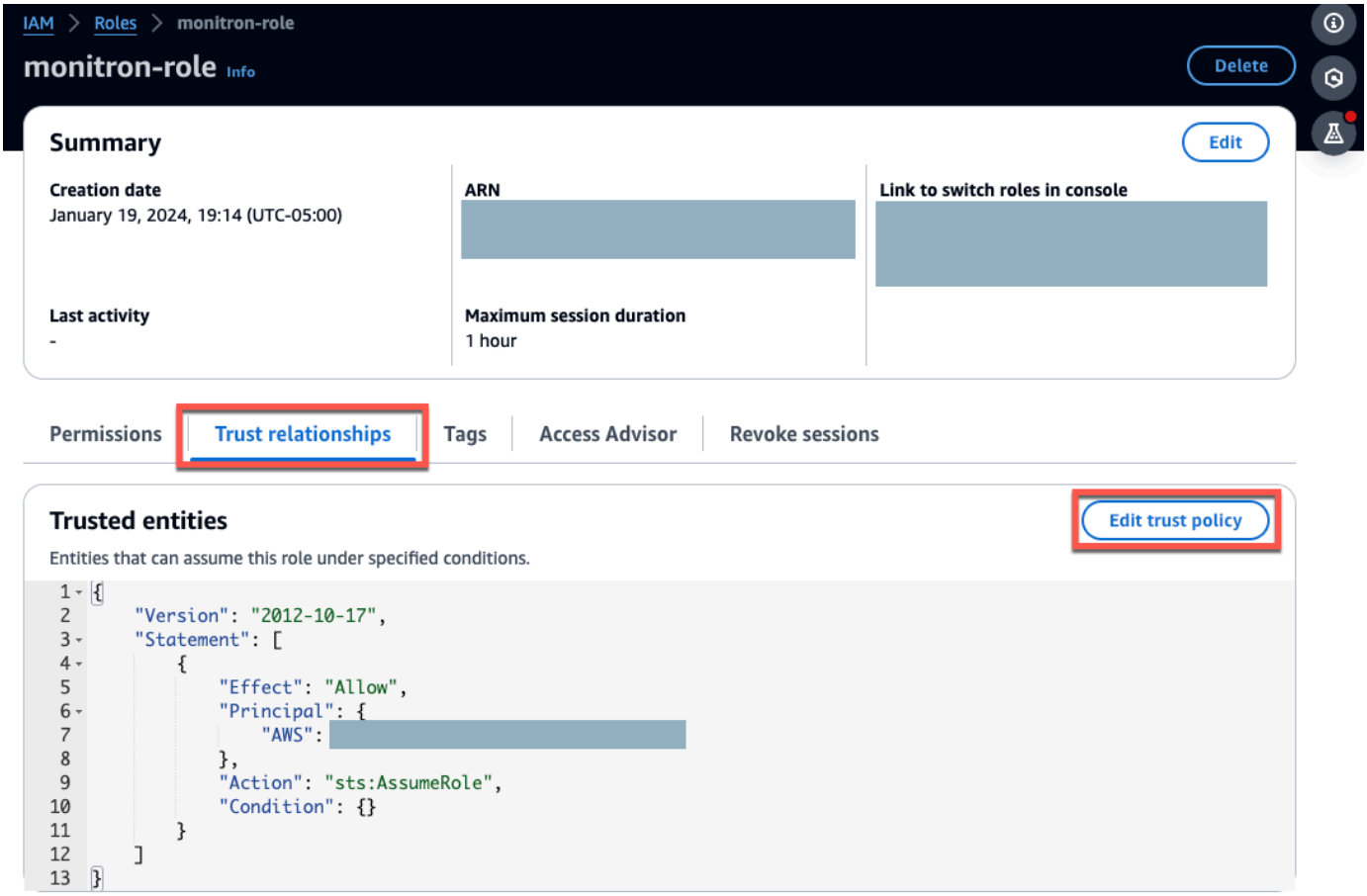

Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Step 1: Select trusted entities
Edit
Trust policy
Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
monitron-policy
Customer managed
Permissions policy

## Step 4: Create the trust policy

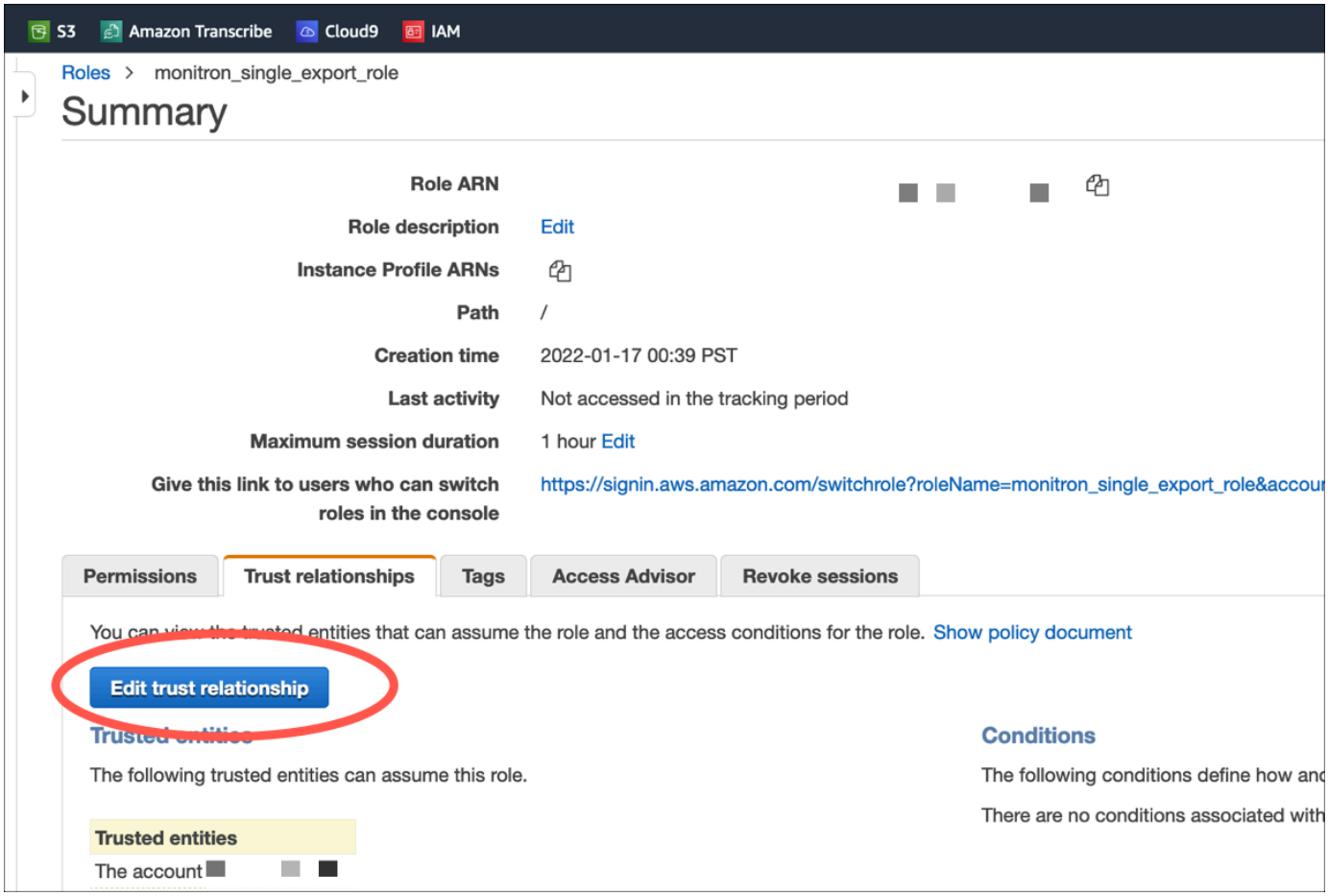
1. Search for the role you just created and choose the role.




2. Select the **Trust relationships** tab.

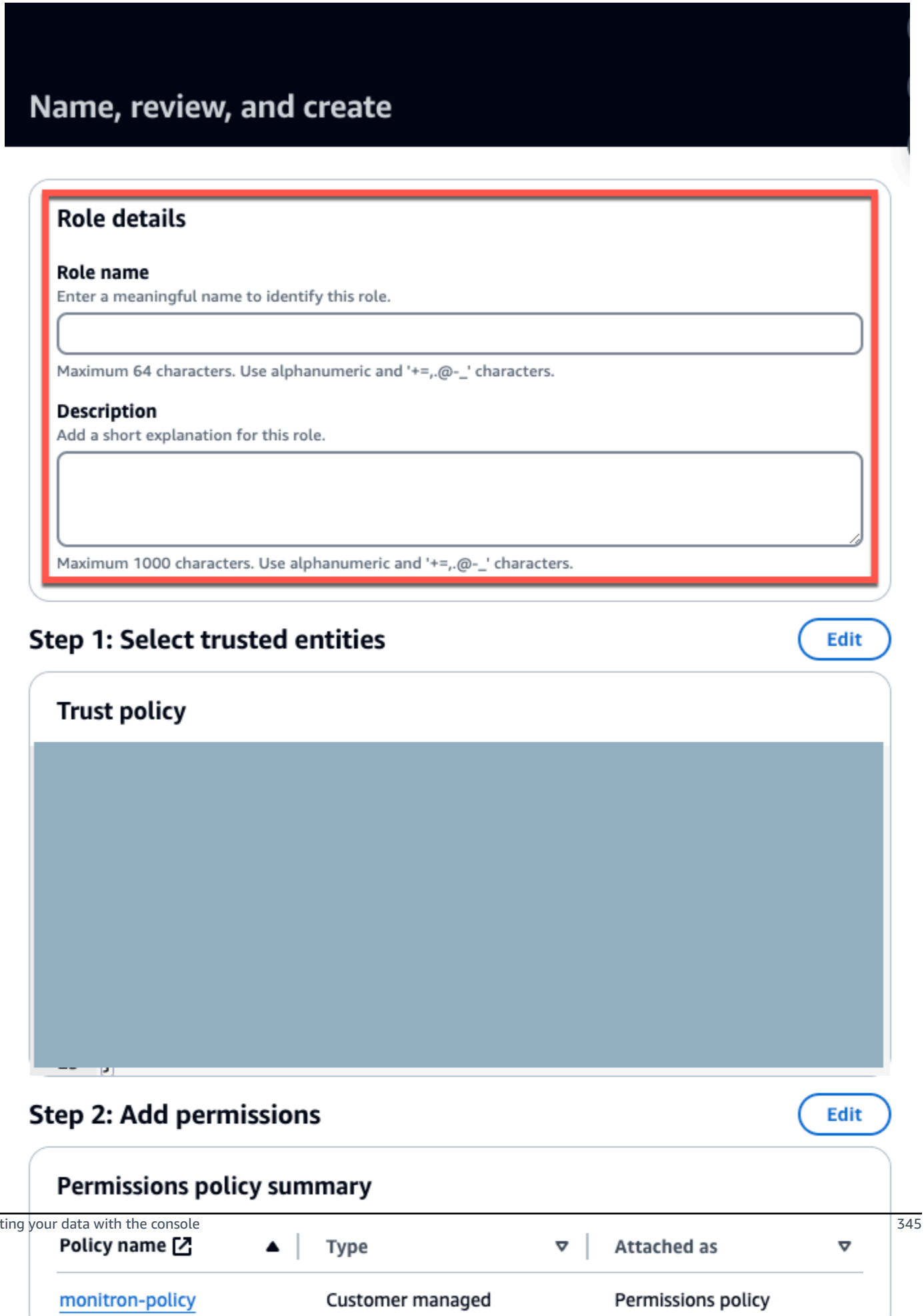



3. Choose **Edit trust relationship**.




4. Erase the default JSON text so that the form is empty.
5. Paste in the policy that allows Amazon Monitron to assume the role.

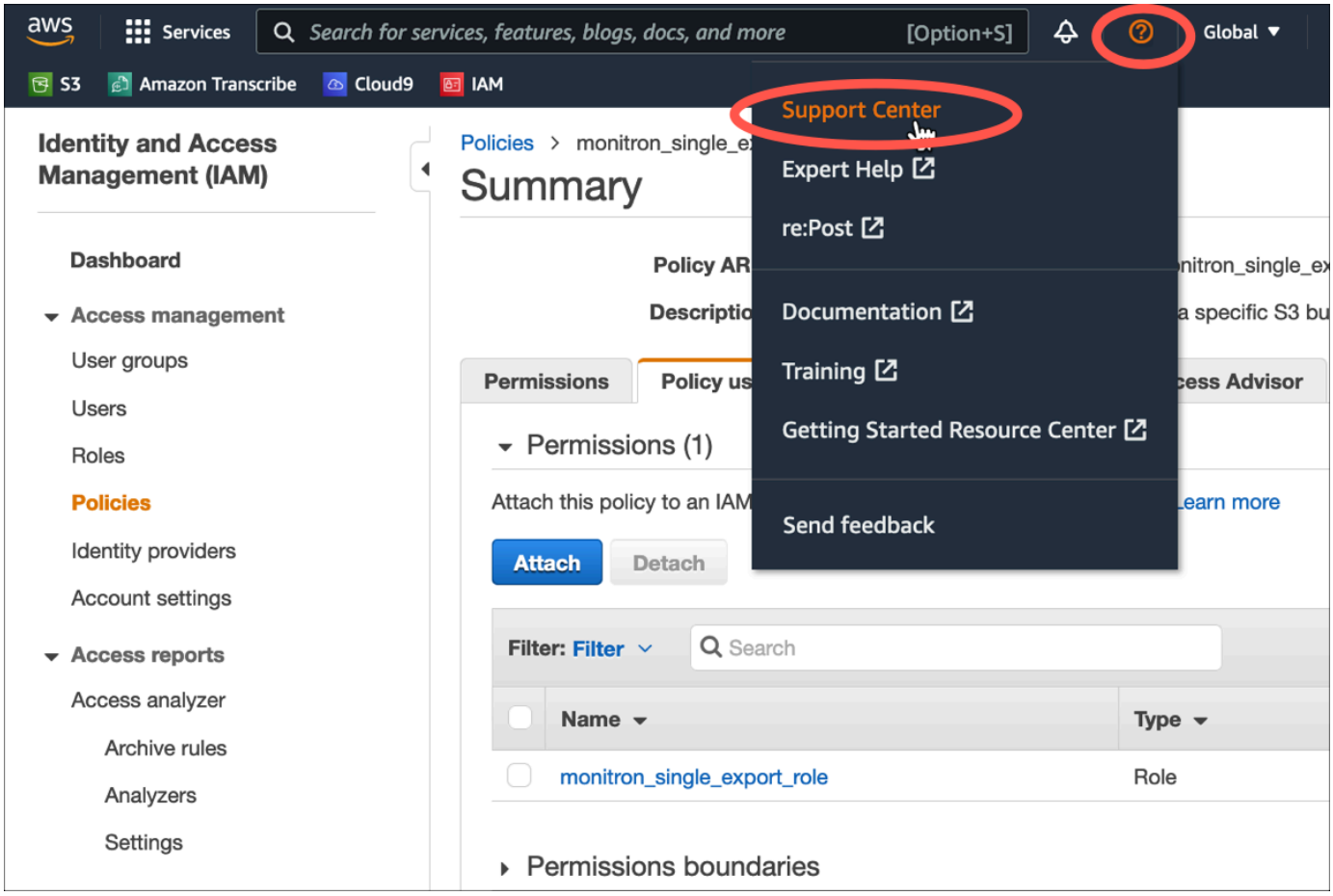
```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Principal": {
   "Service": ["monitron.amazonaws.com"]
  },
  "Action": "sts:AssumeRole"
 }]
}
```


Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Step 1: Select trusted entities
Edit
Trust policy
Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
monitron-policy
Customer managed
Permissions policy

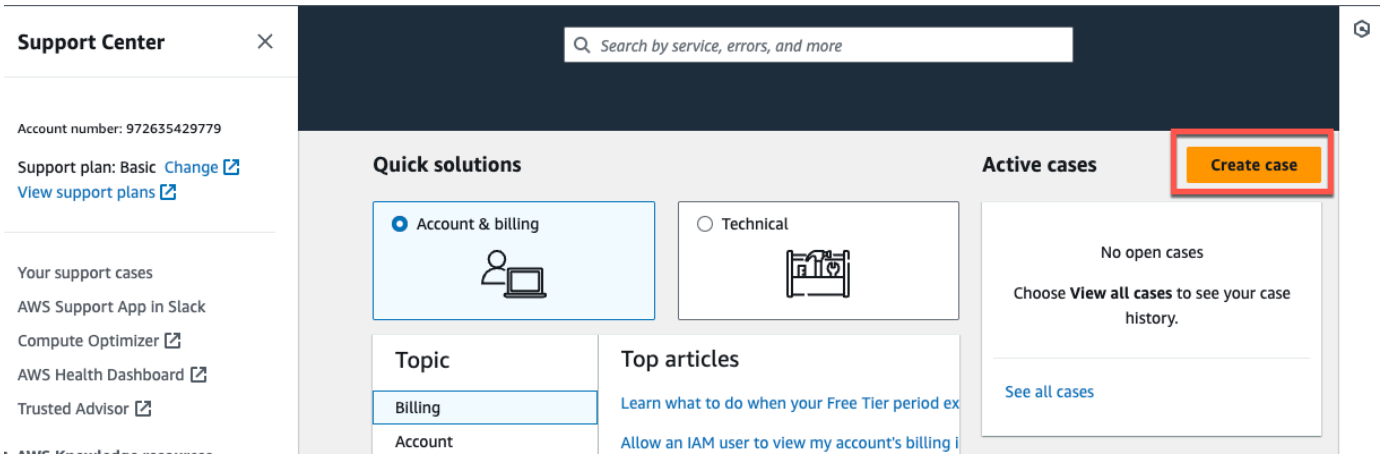
6. Choose **Update Trust Policy**.

## Step 5: Create the support case

1. From your AWS console, choose the question mark icon near the upper right corner of any page, then choose **Support Center**.




2. On the next page, choose **Create case**.



3. On the **How can we help?** page, do the following:

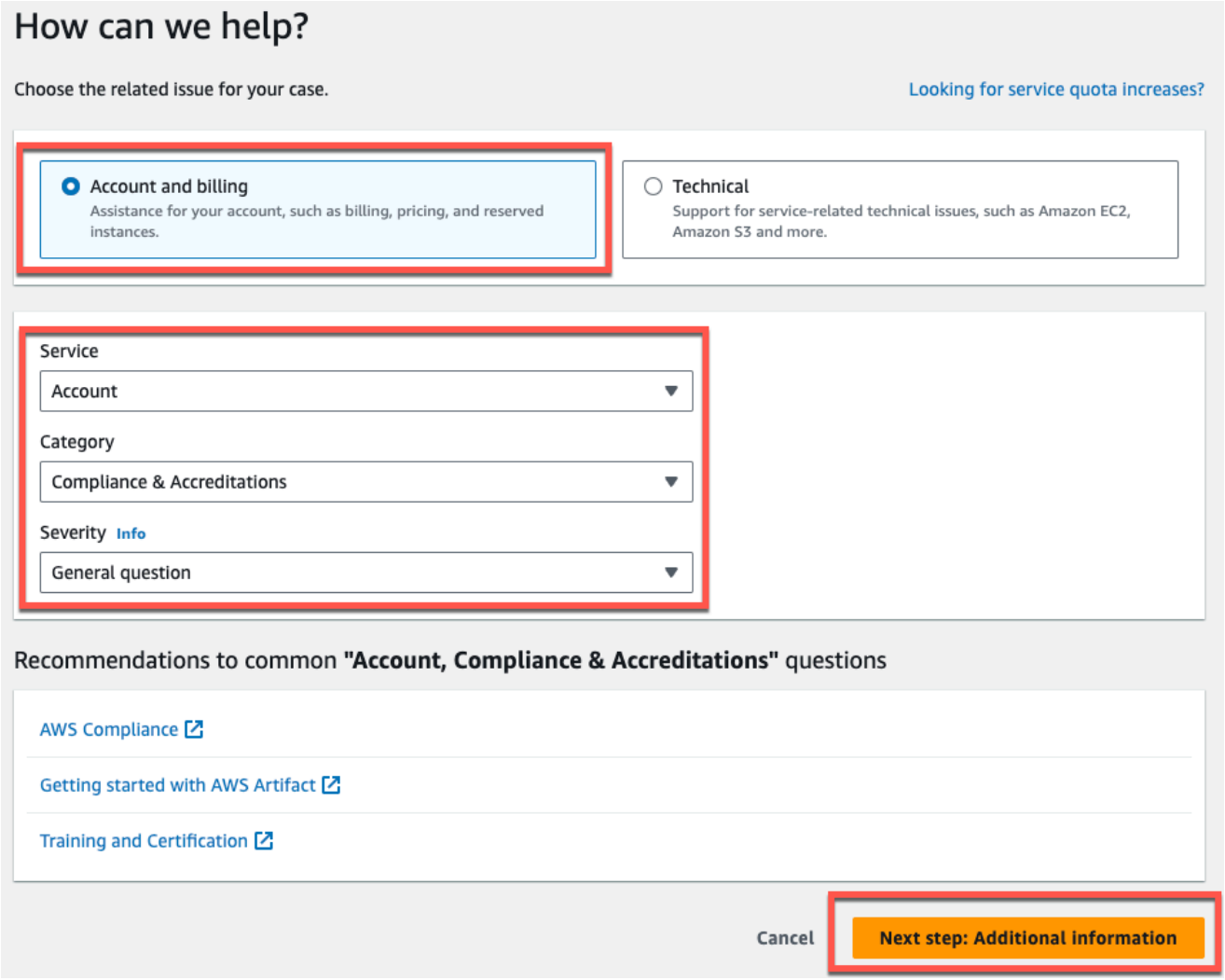
   a. Choose **Account and billing support**.

   b. Under **Service**, choose **Account**.

   c. Under **Category**, choose **Compliance & Accreditations**.

   d. Choose **Severity**, if that option is available to you based on your support subscription.

   e. Choose **Next step: Additional information**.



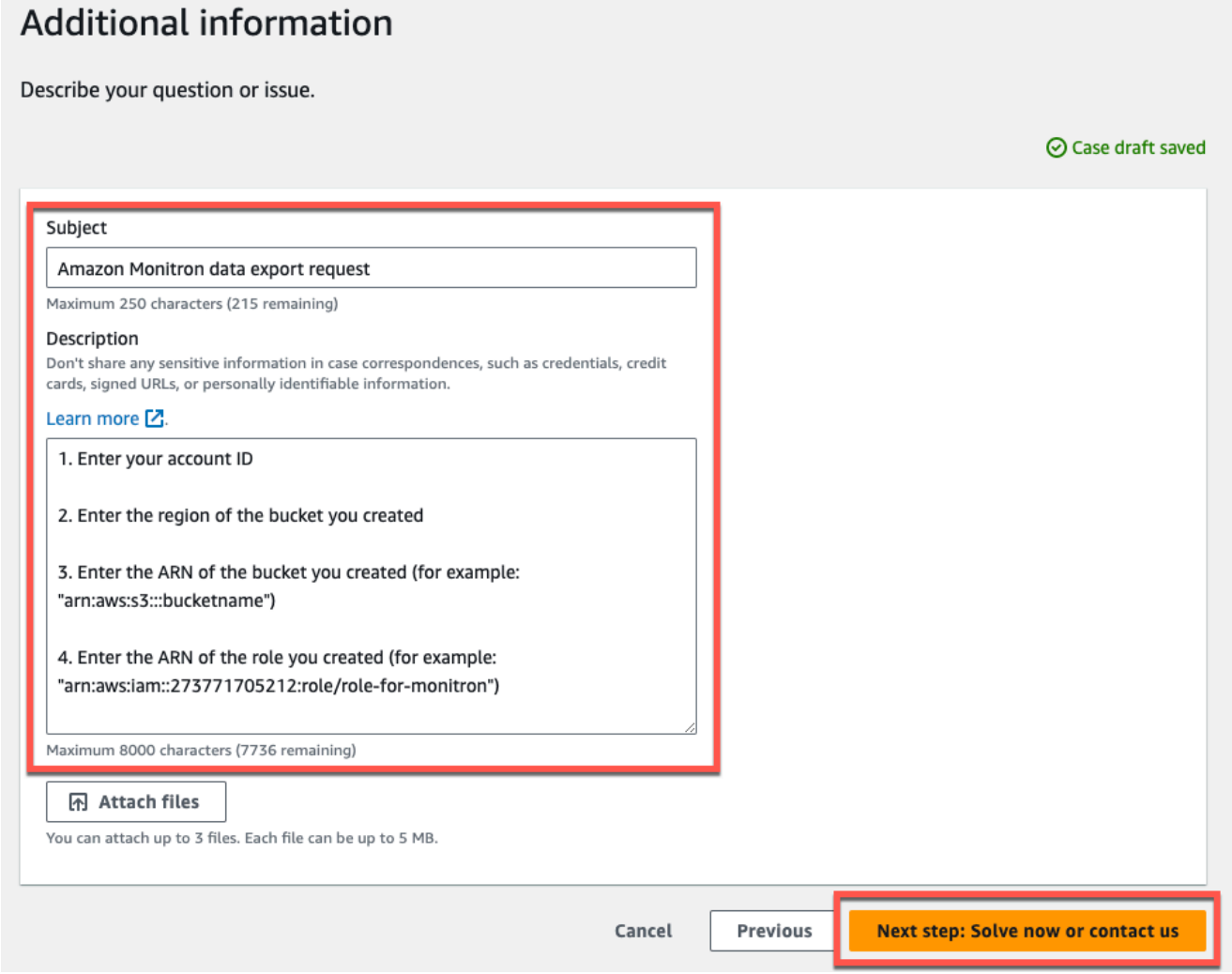

4. In **Additional information** do the following:

   a. Under **Subject**, enter **Amazon Monitron data export request**.

   b. In the **Description** field, enter:

      1. your account ID
      2. the region of the bucket you created

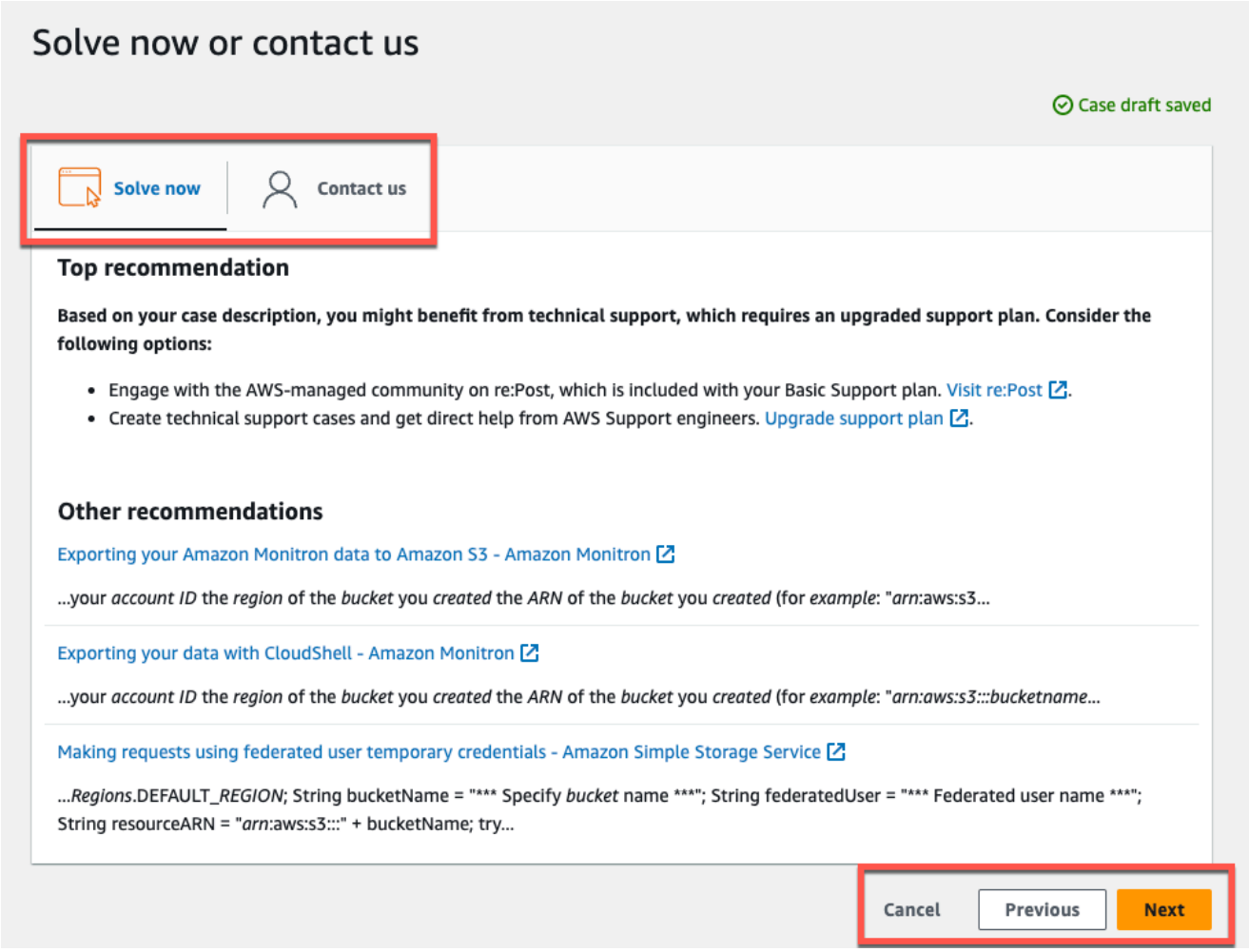
3. the ARN of the bucket you created (for example: "arn:aws:s3:::bucketname")
4. the ARN of the role you created (for example: "arn:aws:iam::273771705212:role/role-for-monitron")




c. Choose **Next step: Solve now or contact us**.

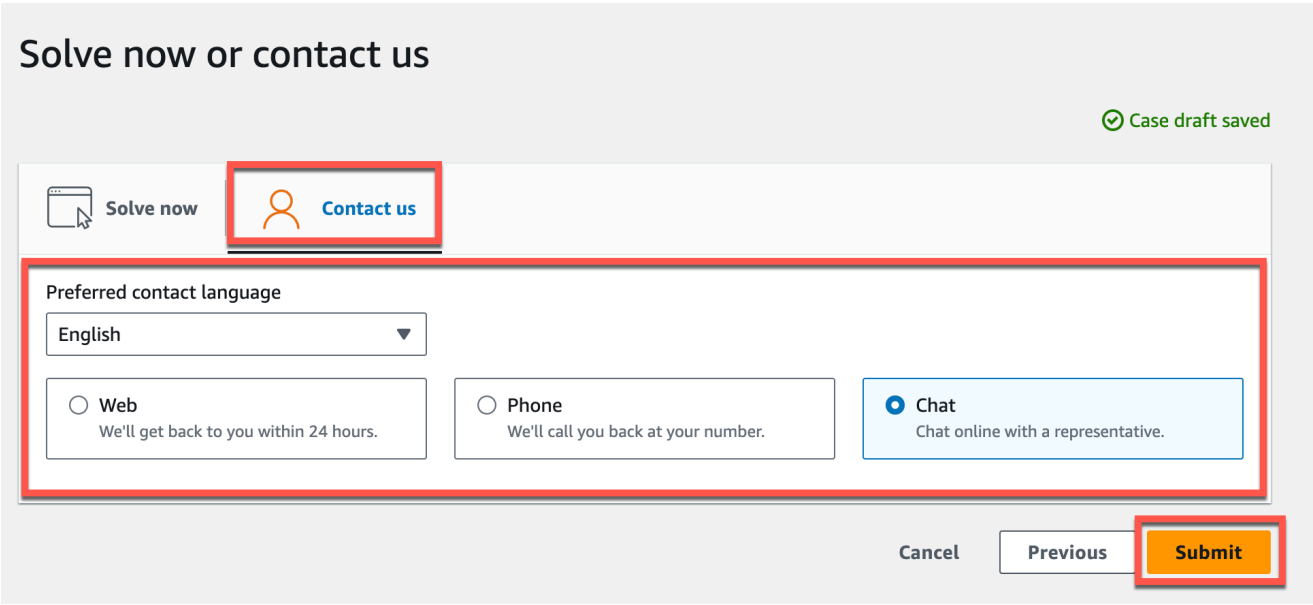
5. In **Solve now or contact us** do the following:

a. In **Solve now**, select **Next**.




b. In **Contact us**, choose your **Preferred contact language** and preferred method of contact.

c. Choose **Submit**. A confirmation screen with your case ID and details will be displayed.



An AWS customer support specialist will get back to you as soon as possible. If there are any issues with the steps listed, the specialist may ask you for more information. If all the necessary information has been provided, the specialist will let you know as soon as your data has been copied to the Amazon S3 bucket that you created above.

## Exporting your data with CloudShell

**Topics**


- Step 1: Creating an Amazon S3 bucket (with AWS CloudShell)
- Step 2: Granting Amazon Monitron access to your Amazon S3 bucket (with AWS CloudShell)
- Step 3: Creating your support ticket


### Step 1: Creating an Amazon S3 bucket (with AWS CloudShell)

1. Log in to the AWS Console.
2. Open AWS CloudShell

   AWS CloudShell is a command-line environment that operates inside your browser. Inside AWS CloudShell, you can use the AWS Command Line Interface to launch and configure many AWS services.
3. In AWS CloudShell, enter the following command, where bucketname is the name of the bucket you are creating:

   ```
   $ aws s3api create-bucket --bucket bucketname --region us-east-1
   ```

   This command creates an Amazon S3 bucket to store your raw data. You will be able to easily access your bucket from the console, and download your data at your convenience. For more information, see Creating, configuring, and working with Amazon S3 buckets.

   **Important**

   You are responsible for taking the appropriate steps to secure your data. We strongly recommend using server-side encryption and blocking public access to your bucket.

In the command above, the bucket is created in the US East (N. Virginia) Region. You can optionally specify a different Region in the request body. For more information, see Regions, Availability Zones, and Local Zones.

You should see output that looks something like this:

```
{ "Location": "/bucketname" }
```

4. Identify the Amazon Resource Name (ARN) of the bucket you created, which will be:

```
arn:aws:s3:::bucketname
```

## Step 2: Granting Amazon Monitron access to your Amazon S3 bucket (with AWS CloudShell)

1. Paste the code below into a text editor, and save it as: monitron-assumes-role.json. Do not use Microsoft Word, which will add extra characters. Use a simple text editor like Notepad or TextEdit.

   This policy gives Amazon Monitron permission to assume the role that will allow it to access your S3 bucket. For more information, see Policies and permissions in IAM.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Principal": {
   "Service": ["monitron.amazonaws.com"]
  },
  "Action": "sts:AssumeRole"
 }]
}
```

2. Paste the text below into a text editor, and save it as: monitron-role-accesses-s3.json

   This policy will allow Amazon Monitron (using the role created above) to access your Amazon S3 bucket.

```
{
    "Statement": [
        {
            "Action": [
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::bucketname"
            ]
        },
        {
            "Action": [
                "s3:PutObject",
                "s3:GetBucketAcl"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::bucketname/*"
            ]
        }
    ],
    "Version": "2012-10-17"
}
```

3. In the text file you just created, replace every occurrence of *bucketname* with the name of your bucket.

   For example, if the name of your bucket is relentless, then your file will look like this:

```
{
    "Statement": [
        {
            "Action": [
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
```

```
            "Resource": [
                "arn:aws:s3:::relentless"
            ]
        },
        {
            "Action": [
                "s3:PutObject",
                "s3:GetBucketAcl"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::relentless/*"
            ]
        }
    ],
    "Version": "2012-10-17"
}
```

4. Upload both of the json files that you just created to CloudShell in the home directory.

   To upload a file, choose Actions from the upper right hand corner of the CloudShell console page, then choose Upload file.

5. Enter the following on the command line in CloudShell:

   **aws iam create-role --role-name role-for-monitron --assume-role-policy-document "cat monitron-assumes-role.json"**

   This command creates the role and attaches the monitron-assumes-role policy.

   You should see output that looks something like this:

```
{
"Role": {
 "Path": "/",
 "RoleName": "role-for-monitron",
 "RoleId": "AROAT7PQQWN6BMTMASVPP",
 "Arn": "arn:aws:iam::273771705212:role/role-for-monitron",
 "CreateDate": "2021-07-14T02:48:15+00:00",
 "AssumeRolePolicyDocument": {
  "Version": "2012-10-17",
  "Statement": [{
   "Sid": "",
   "Effect": "Allow",
```

```
    "Principal": {
     "Service": [
      "monitron.amazonaws.com"
     ]
    },
    "Action": "sts:AssumeRole"
   }]
  }
 }
}
```

Take note of the ARN value for the role you just created. You will need it later.

In our example, the ARN value is: `arn:aws:iam::273771705212:role/role-for-monitron`

6. Enter the following on the command line in CloudShell:

**aws iam create-policy --policy-name role-uses-bucket --policy-document "cat role-uses-bucket.json"**

This command creates the monitron-role-accesses-s3 policy.

You should see output that looks something like this:

```
 {
 "Policy": {
  "PolicyName": "role-uses-bucket",
  "PolicyId": "ANPAT7PQQWN6I5KLORSDQ",
  "Arn": "arn:aws:iam::273771705212:policy/role-uses-bucket",
  "Path": "/",
  "DefaultVersionId": "v1",
  "AttachmentCount": 0,
  "PermissionsBoundaryUsageCount": 0,
  "IsAttachable": true,
  "CreateDate": "2021-07-14T02:19:23+00:00",
  "UpdateDate": "2021-07-14T02:19:23+00:00"
 }
}
```

Take note of the ARN value for the policy that you just created. You will need it for the next step.

In our example, the ARN value is:

```
arn:aws:iam::273771705212:policy/role-uses-bucket
```

7. Enter the following on the command line in CloudShell, replacing the ARN with the ARN for your role-uses-bucket policy:

```
aws iam attach-role-policy --role-name role-for-monitron --policy-arn
     arn:aws:iam::273771705212:policy/role-uses-bucket
```

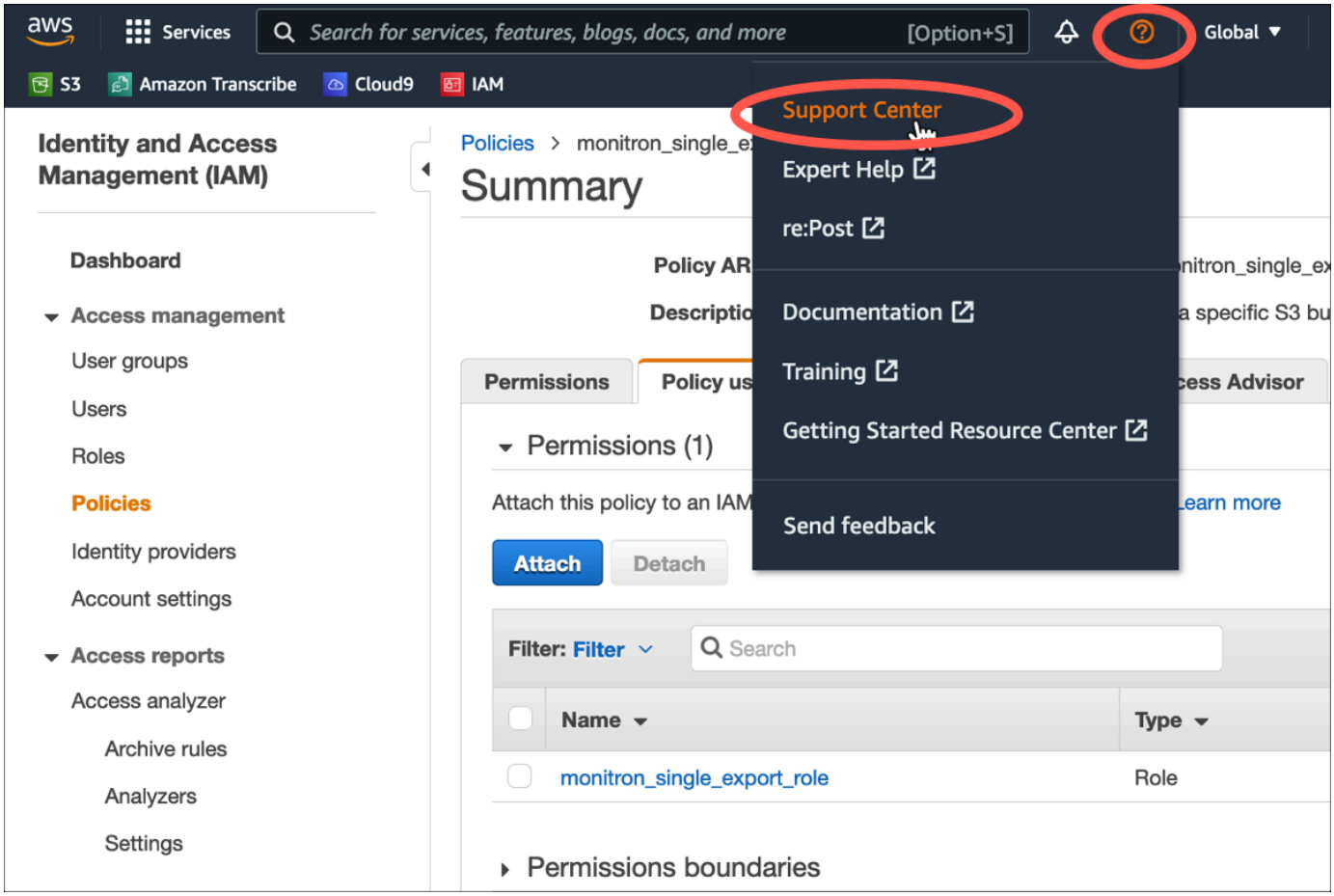
This command attaches the monitron-role-accesses-s3 policy to the role you just created.

Now you have created and provisioned an Amazon S3 bucket, a role that Amazon Monitron can assume, a policy that will allow Amazon Monitron to assume that role, and another policy that will allow the service using that role to use your Amazon S3 bucket.

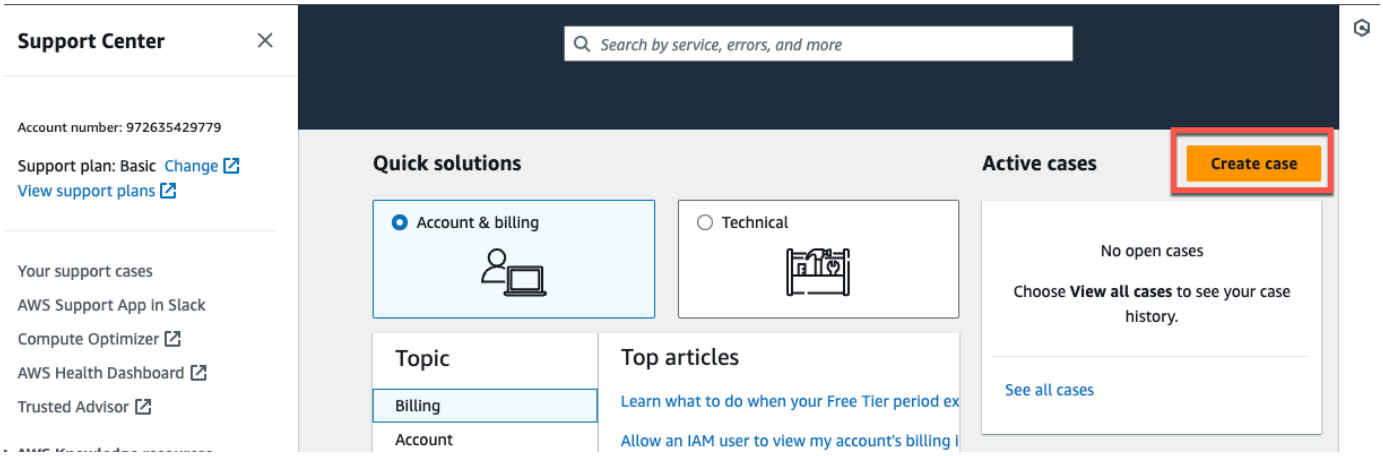
You are responsible for taking the appropriate steps to secure your data. We strongly recommend using server-side encryption and blocking public access to your bucket. For more information, see Blocking public access.

## Step 3: Creating your support ticket

1. From your AWS console, choose the question mark icon near the upper right corner of any page, then choose **Support Center**.




2. On the next page, choose **Create case**.




3. On the **How can we help?** page, do the following:

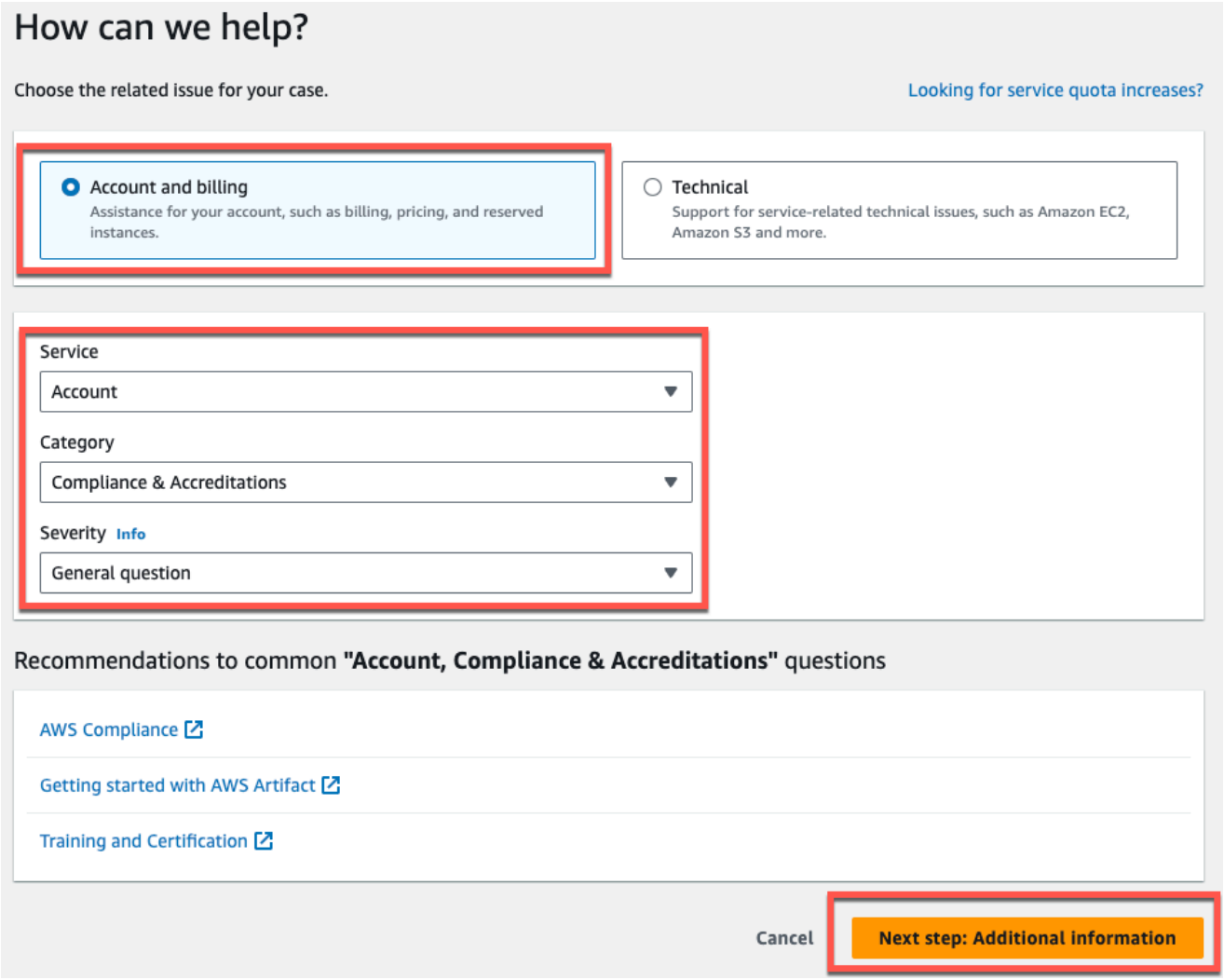
   a. Choose **Account and billing support**.

   b. Under **Service**, choose **Account**.

   c. Under **Category**, choose **Compliance & Accreditations**.

d. Choose **Severity**, if that option is available to you based on your support subscription.

e. Choose **Next step: Additional information**.

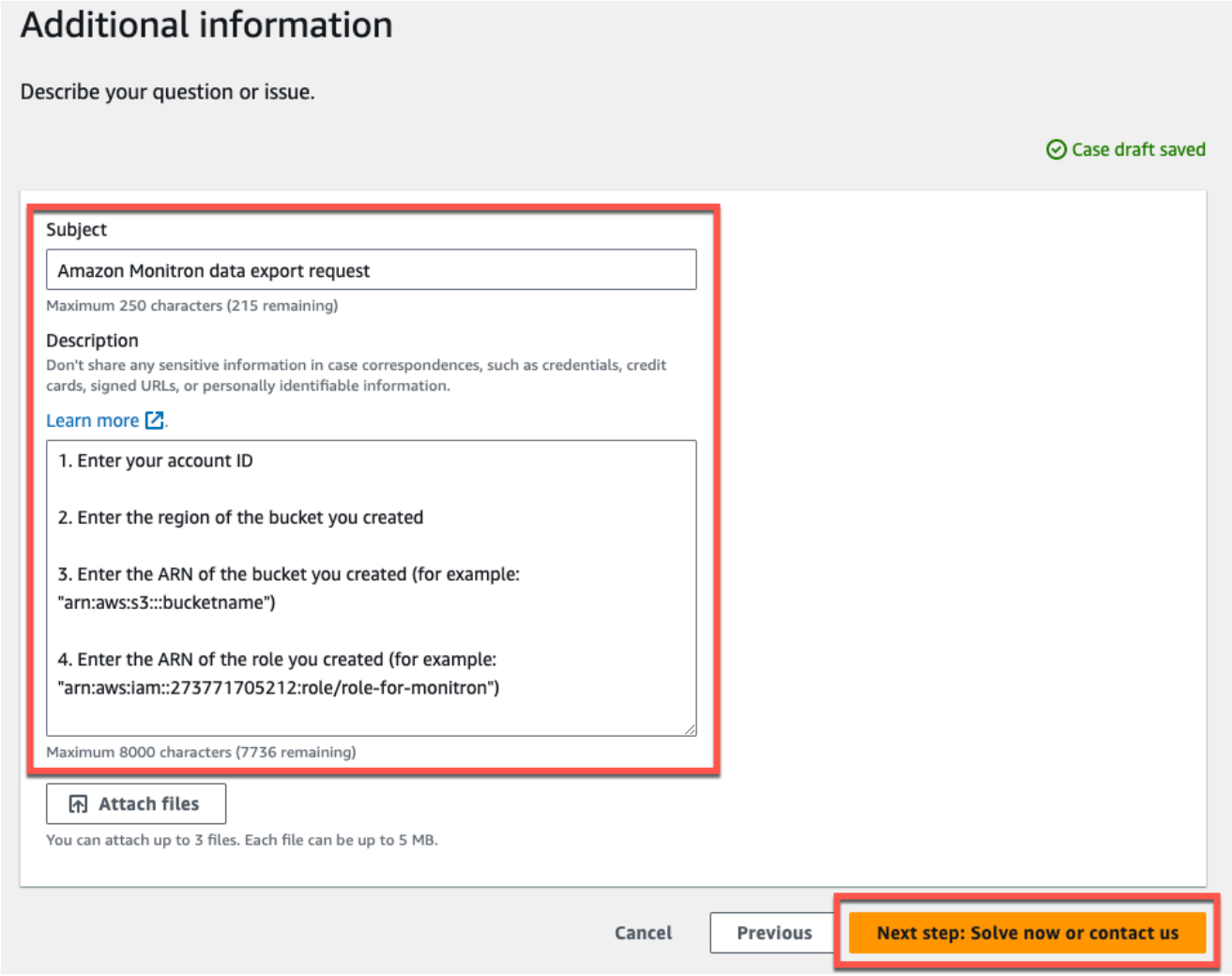



4. In **Additional information** do the following:

   a. Under **Subject**, enter **Amazon Monitron data export request**.

   b. In the **Description** field, enter:

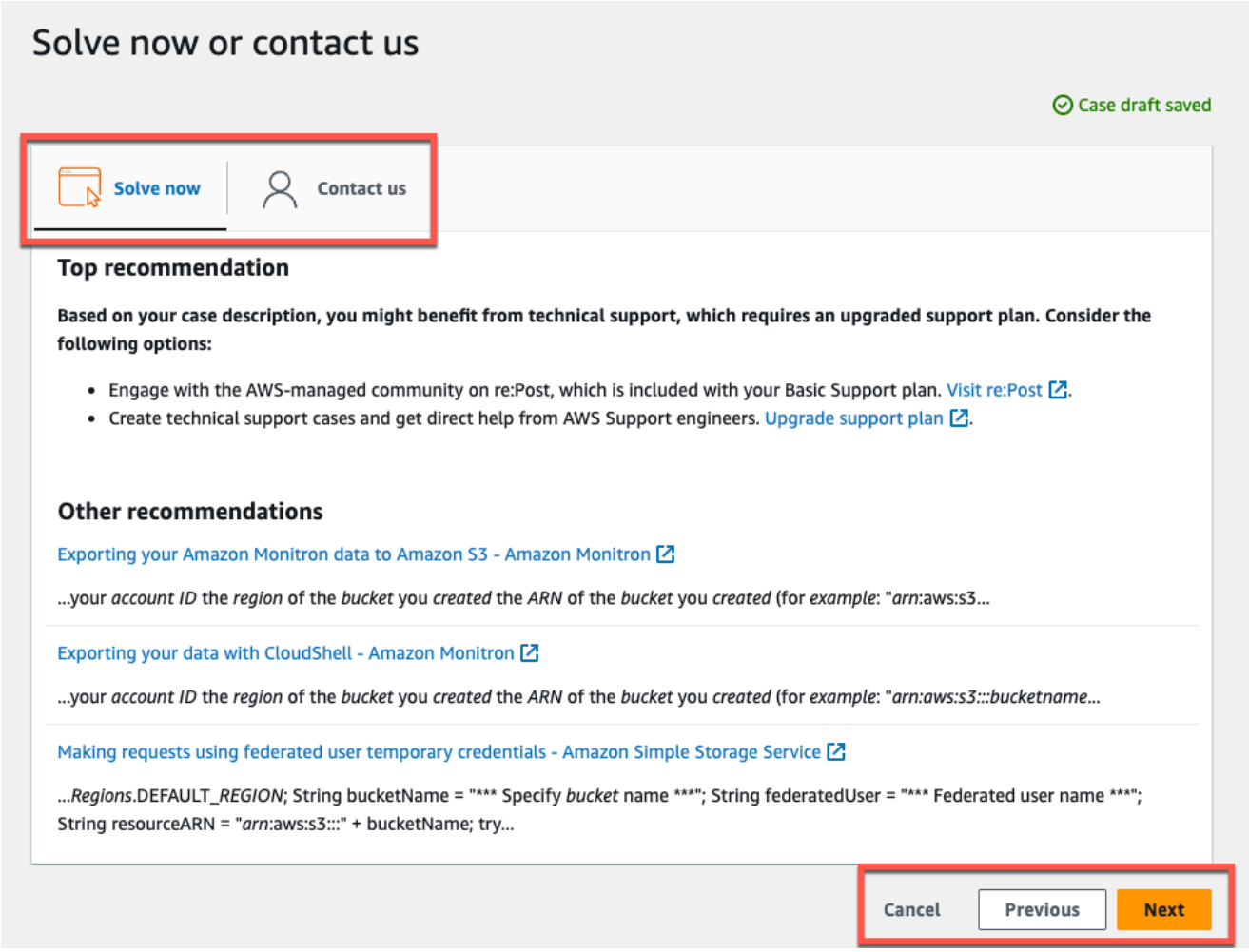
      1. your account ID
      2. the region of the bucket you created
      3. the ARN of the bucket you created (for example: "arn:aws:s3:::bucketname")
      4. the ARN of the role you created (for example: "arn:aws:iam::273771705212:role/role-for-monitron")




c. Choose **Next step: Solve now or contact us**.

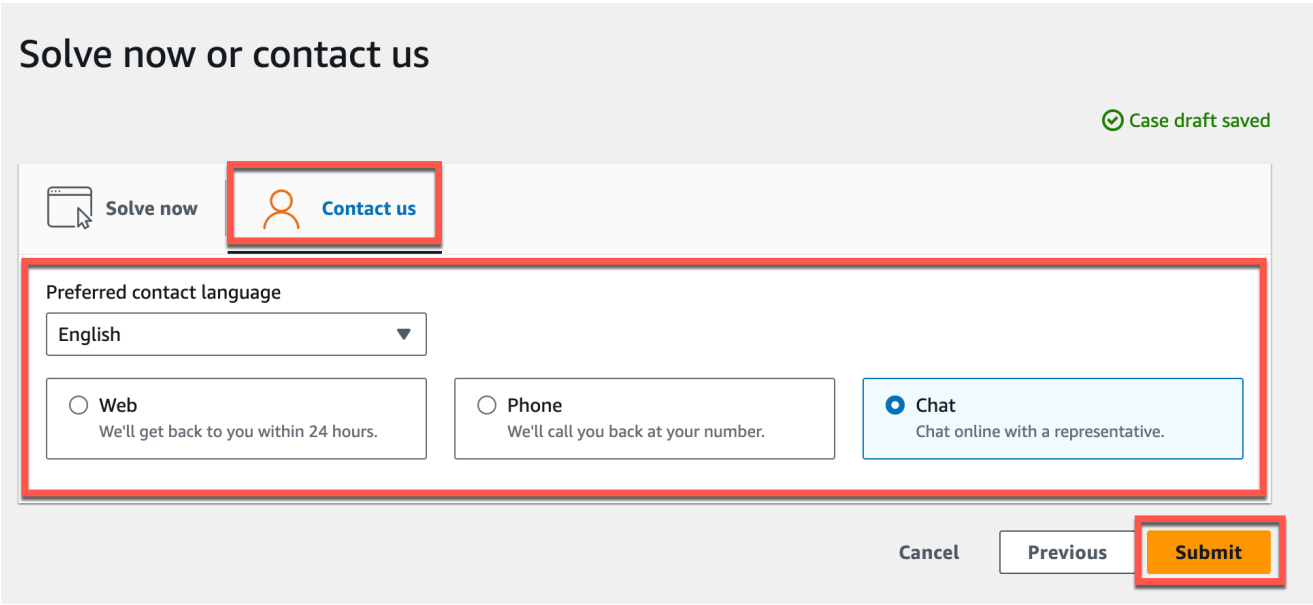
5. In **Solve now or contact us** do the following:

   a. In **Solve now**, select **Next**.




b. In **Contact us**, choose your **Preferred contact language** and preferred method of contact.

c. Choose **Submit**. A confirmation screen with your case ID and details will be displayed.



An AWS customer support specialist will get back to you as soon as possible. If there are any issues with the steps listed, the specialist may ask you for more information. If all the necessary information has been provided, the specialist will let you know as soon as your data has been copied to the Amazon S3 bucket that you created above.

# Amazon Monitron Kinesis data export v1

> **Note**
>
> Amazon Monitron Kinesis data export schema v1 has been deprecated. Learn more about the v2 data export schema.

You can export incoming measurement data and the corresponding inference results from Amazon Monitron and perform real-time analysis. Data export streams live data to Kinesis.

**Topics**


- Exporting your data to a Kinesis stream
- Editing live data export settings
- Stopping a live data export
- Viewing data export errors
- Using server-side encryption for the Kinesis stream
- Monitoring with Amazon CloudWatch Logs
- Storing exported data in Amazon S3
- Processing data with Lambda
- Understanding the v1 data export schema


## Exporting your data to a Kinesis stream

1. From your project's main page, near the bottom of the page, on the right, choose **Start live data export**.
2. Under **Select Amazon Kinesis data stream**, do one of the following:
   - Enter the name of an existing stream in the search box. Then skip to Step 5.

- Choose **Create a new data stream**.

3. On the **Create data stream** page, under **Data stream configuration**, enter your data stream name.
4. Under Data stream capacity, choose your capacity mode:

   - If your data stream's throughput requirements are unpredictable and variable, choose **On-demand**.
   - If you can reliably estimate the throughput requirements of your data stream, choose **Provisioned**. Then, under provisioned shards, enter the number of shards you want to create, or choose the **Shard estimator**.

5. Choose **Create data stream**.

## Editing live data export settings

To edit your live data export settings:

1. Open the Amazon Monitron console.
2. Choose **Projects** from the navigation pane.
3. If you have multiple projects, choose the project for which you want to edit the export settings.
4. From the main page for your project, under **Live data export**, from the **Actions** dropdown menu, choose **Edit live data export settings**.

## Stopping a live data export

1. Open the Amazon Monitron console.
2. Choose **Projects** from the navigation pane.
3. If you have multiple projects, choose the project for which you want to edit the export settings.
4. From the main page for your project, under **Live data export**, from the **Actions** dropdown menu, choose **Stop live data export**.
5. In the pop-up window, choose **Stop**.

## Viewing data export errors

To view the error messages in the CloudWatch Logs interface:

- On the Amazon Monitron console, from the main page for your project, under **Live data export**, choose **CloudWatch log group**.

## Using server-side encryption for the Kinesis stream

You can enable server-side encryption for your Kinesis stream before setting up Kinesis data export. However, if server-side encryption is enabled after Kinesis data export is set up, Amazon Monitron will not be able to publish to the stream. That's because Amazon Monitron will not have permission to call kms:GenerateDataKey so that it can encrypt data sent to Kinesis.

To work around this, follow the instructions under ???, but without changing the configuration. This will associate the encryption you have set up with your export configuration.

## Monitoring with Amazon CloudWatch Logs

You can monitor Amazon Monitron live data export using Amazon CloudWatch Logs. When a measurement fails to export, Amazon Monitron will send a log event to your CloudWatch Logs. You can also set up a metric filter on the error log to generate metrics and set up alarms. An alarm can watch for certain thresholds and send notifications or take actions when those thresholds are met. For more information, see the CloudWatch User Guide.

Amazon Monitron sends log events to the /aws/monitron/data-export/{HASH_ID} log group.

The log event has the following JSON format:

```
{
    "assetDisplayName": "string",
    "destination": "string",
    "errorCode": "string",
    "errorMessage": "string",
    "eventId": "string",
    "positionDisplayName": "string",
    "projectDisplayName": "string",
    "projectName": "string",
    "sensorId": "string",
    "siteDisplayName": "string",
```

```
    "timestamp": "string"
}
```

assetDisplayName

- The asset name displayed in the App
- Type: String

destination

- The ARN of the Kinesis data stream
- Type: String
- Pattern: arn:aws:kinesis:{{REGION}}:{{AWS_ACCOUNT_ID}}:stream/{{STREAM_NAME}}

errorCode

- The error code
- Type: String
- Valid Values: `INTERNAL_SEVER_ERROR | KINESIS_RESOURCE_NOT_FOUND | KINESIS_PROVISIONED_THROUGHPUT_EXCEEDED | KMS_ACCESS_DENIED | KMS_NOT_FOUND | KMS_DISABLED | KMS_INVALID_STATE | KMS_THROTTLING`

errorMessage

- The detailed error message
- Type: String

eventId

- The unique event ID corresponding to each measurement export
- Type: String

positionDisplayName

- The sensor position name displayed in the App
- Type: String

sensorId

- The physical ID of the sensor from which the measurement is sent
- Type: String

siteDisplayName

- The site name displayed in the App

- Type: String

timestamp

- The timestamp when the measurement is received by Amazon Monitron service in UTC
- Type: String
- Pattern: yyyy-mm-dd hh:mm:ss.SSS

## Storing exported data in Amazon S3

**Topics**


- Using a predefined CloudFormation template
- Configuring Kinesis manually in the console


### Using a predefined CloudFormation template

Amazon Monitron provides a predefined AWS CloudFormation template to help quickly set up the Firehose to deliver data from a Kinesis data stream to the Amazon S3 bucket. This template enables dynamic partitioning and the Amazon S3 objects delivered will use the following key format recommended by Amazon Monitron: `/project={projectName}/site={siteName}/time={yyyy-mm-dd 00:00:00}/{filename}`

1. Sign into your AWS account.
2. Open a new browser tab with the following URL:

   ```
   https://console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/create/review?templateURL=https://s3.us-east-1.amazonaws.com/monitron-cloudformation-templates-us-east-1/monitron_kinesis_data_export.yaml&stackName=monitron-kinesis-live-data-export
   ```

3. On the AWS CloudFormation page that opens, in the upper right corner, select the region in which you are using Amazon Monitron.
4. By default, the template will create a new Kinesis data stream and S3 bucket along with other resources needed to deliver data to Amazon S3. You can change the parameters to use existing resources.
5. Check the box that says *I acknowledge that AWS CloudFormation might create IAM resources.*
6. Choose **Create stack**.

7. On the next page, choose the refresh icon as often as you like until the status of the stack is CREATE_COMPLETE.

## Configuring Kinesis manually in the console

1. Sign in to the AWS Management Console and open the Kinesis console at https://console.aws.amazon.com/kinesis.
2. Choose **Delivery streams** in the navigation pane.
3. Choose **Create delivery stream**.
4. For Source, select **Amazon Kinesis Data Streams**.
5. For Destination, select **Amazon S3**.
6. Under **Source settings, Kinesis data stream**, enter the ARN of your Kinesis data stream.
7. Under **delivery stream name**, enter the name of your Kinesis data stream.
8. Under **Desination settings**, choose an Amazon S3 bucket or enter a bucket URI.
9. (optional) Enable dynamic partitioning using inline parsing for JSON. This option is appropriate if you want to partition streaming measurement data based on source information and timestamp. For example:
   - Choose **Enabled** for **Dynamic partitioning**.
   - Choose **Enabled** for **New line delimiter**.
   - Choose **Enabled** for **Inline parsing for JSON**.
   - Under **Dynamic partitioning keys**, add:

| Key name | JQ expression |
|---|---|
| project | .projectDisplayName\| "project=\(.)" |
| site | .siteDisplayName\| "site=\(.)" |
| time | .timestamp\| sub("[0-9]{2}:[0-9]{2}:[0-9]{2}.[0-9]{3}$"; "00:00:00")\| "time=\(.)" |

10. Choose **Apply dynamic partitioning keys** and confirm the generated Amazon S3 bucket prefix is `!{partitionKeyFromQuery:project}/!{partitionKeyFromQuery:site}/!{partitionKeyFromQuery:time}/`.

11. In Amazon S3, objects will use the following key format: `/project={projectName}/site={siteName}/time={yyyy-mm-dd 00:00:00}/{filename}`.
12. Choose **Create delivery stream**.
13. (optional) Use a more granular path.

    If you chose a dynamic partition, use the preceeding Amazon S3 key format if you plan to use AWS Glue and Athena to query the data. You can also choose a finer key format, but the Amazon Athena query will not be efficient. Here is an example of setting up a finer Amazon S3 key path.

    Under **Dynamic partitioning keys**, add:

| Key name | JQ expression |
|---|---|
| project | .projectDisplayName\| "project=\(.)" |
| site | .siteDisplayName\| "site=\(.)" |
| asset | .assetDisplayName\| "asset=\(.)" |
| position | .sensorPositionDisplayName\| "position=\(.)" |
| sensor | .sensor.physicalId \| "sensor=\(.)" |
| date | .timestamp\| sub(" [0-9]{2}:[0-9]{2}:[0-9]{2}.[0-9]{3}$"; "")\| "date=\(.)" |

    In Amazon S3, objects will use the following key format: `/project={projectName}/site={siteName}/asset={assetName}/position={positionName}/sensor={sensorId}/date={yyyy-mm-dd}/time={HH:MM:SS}/{filename}`

## Processing data with Lambda

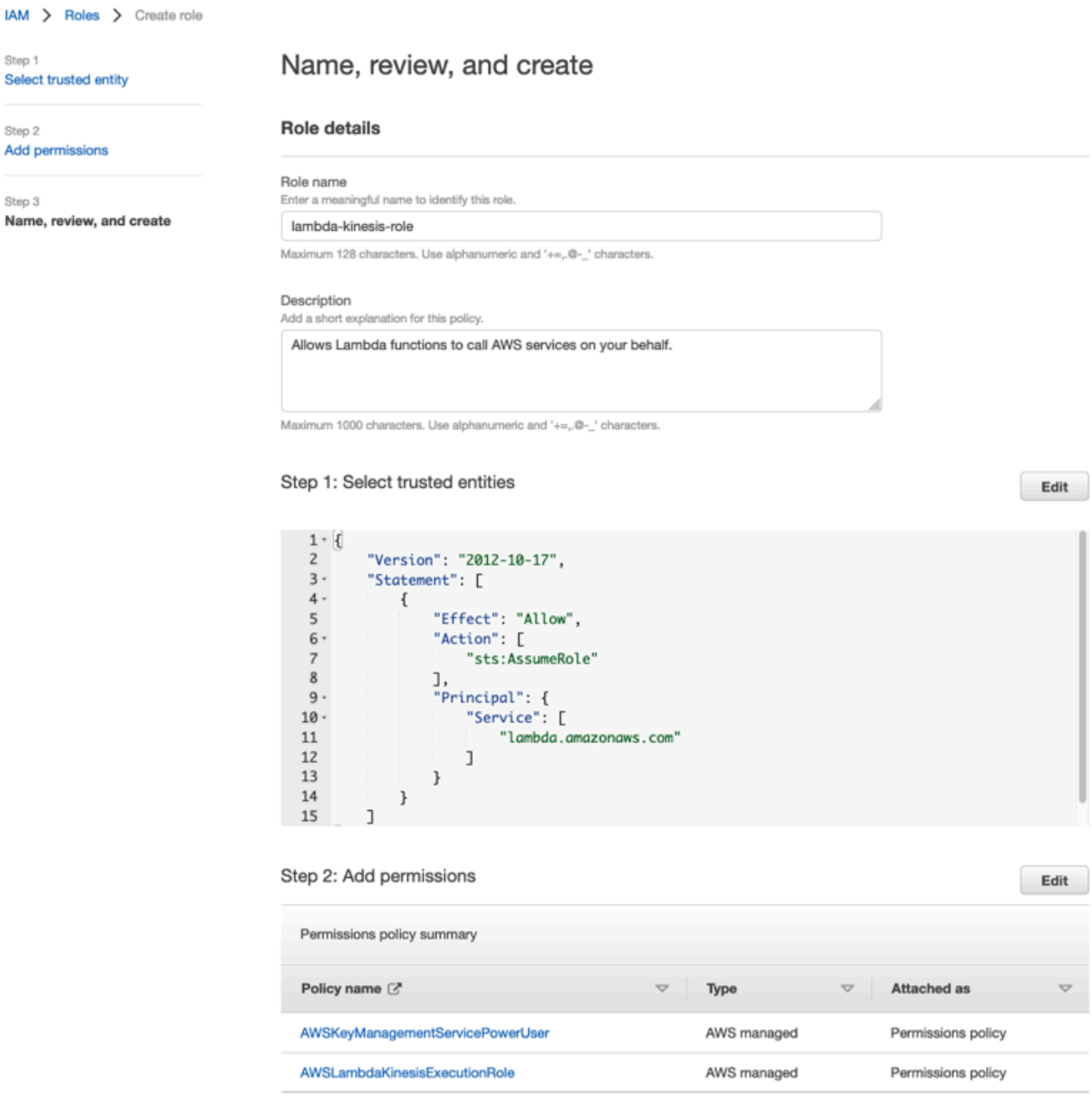
### Topics

- Step 1: Create the IAM role that gives your function permission to access AWS resources
- Step 2: Create the Lambda function

- Step 3: Configure the Lambda function
- Step 4: Enable Kinesis trigger in AWS Lambda console

## Step 1: Create the IAM role that gives your function permission to access AWS resources

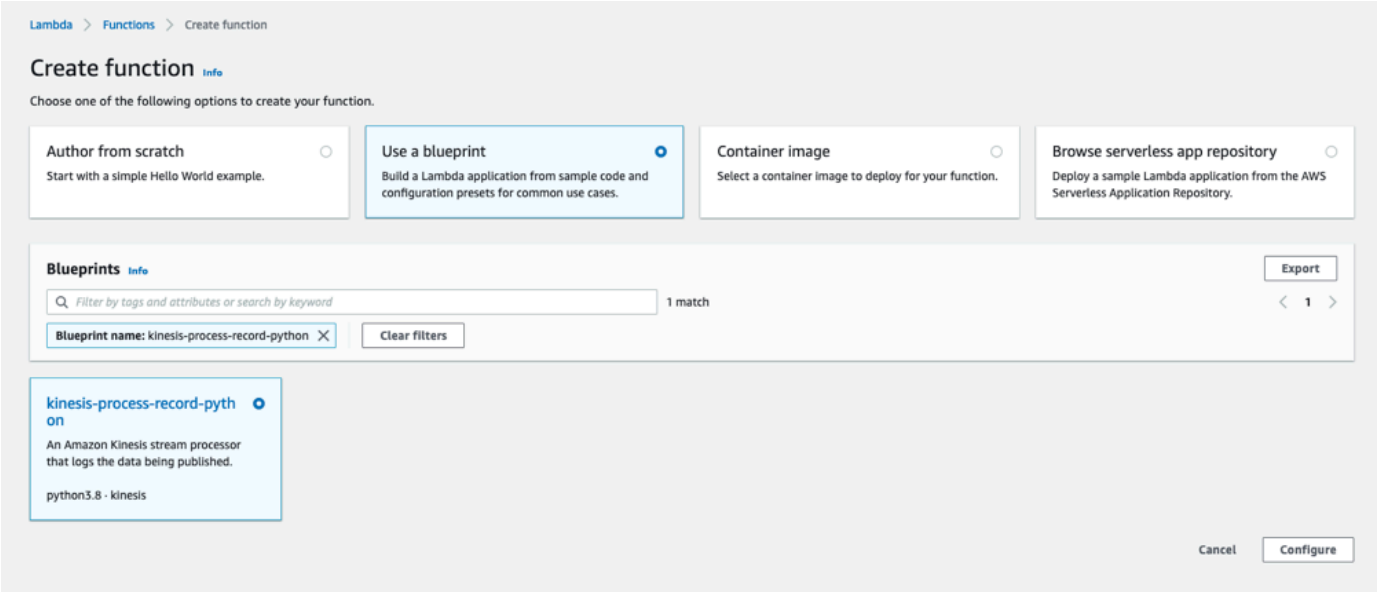
1. Open the roles page in the IAM console.
2. Choose **Create role**.
3. Create a role with the following properties.
   - Trusted entity: Lambda
   - Permissions: AWSLambdaKinesisExecutionRole (and AWSKeyManagementServicePowerUser if the Kinesis stream is encrypted)
   - Role name: lambda-kinesis-role




## Step 2: Create the Lambda function

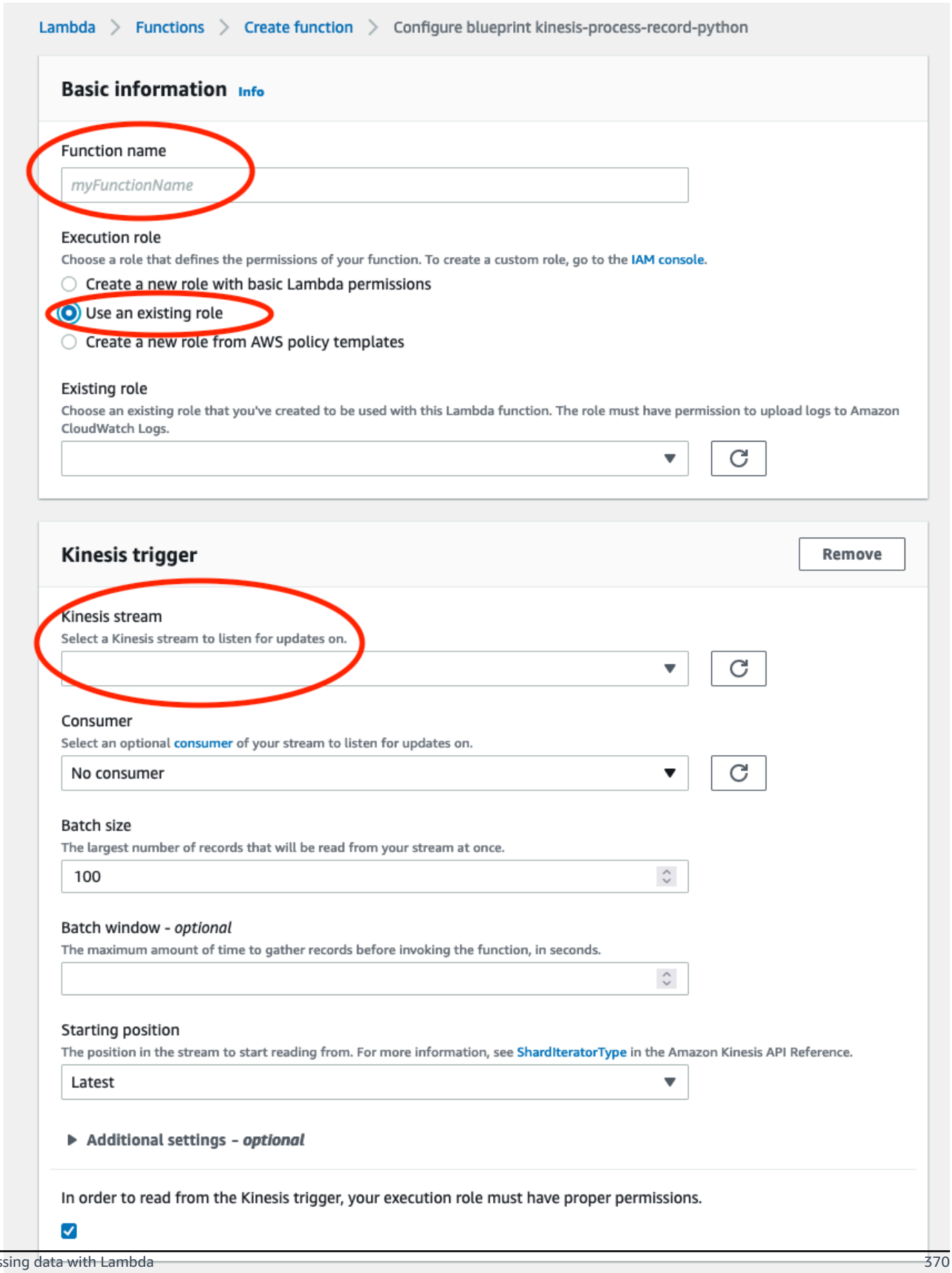
1. Open the **Functions** page in the Lambda console.
2. Choose **Create function**.
3. Choose **Use a blueprint**.

4. In the **Blueprints** search bar, search and choose **kinesis-process-record (nodejs)** or **kinesis-process-record-python**.
5. Choose **Configure**.



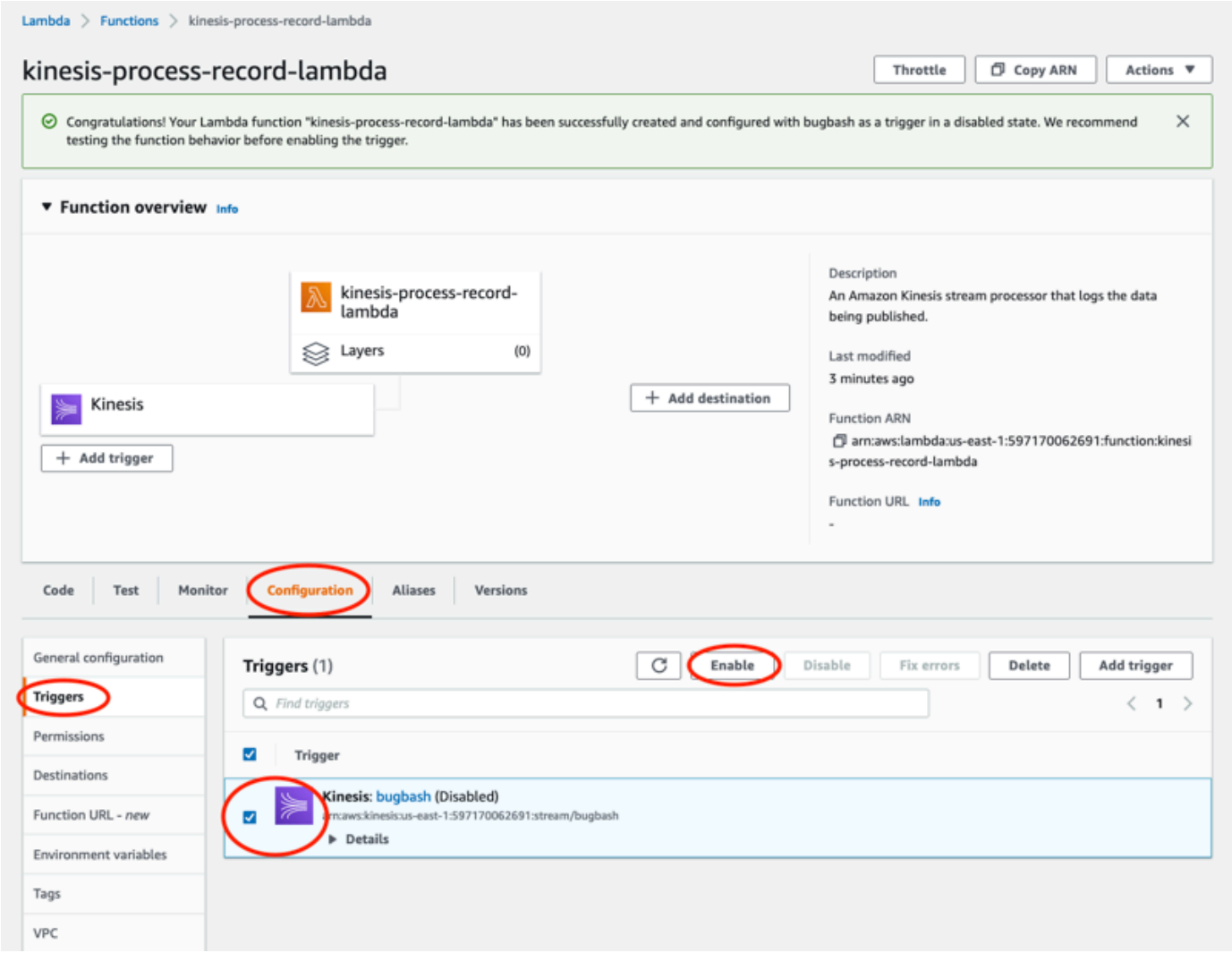

## Step 3: Configure the Lambda function

1. Choose **Function name**
2. Choose the role created in the first step as the **Execution role**.
3. Configure Kinesis trigger.
    1. Choose your Kinesis stream.
    2. Click **Create function**.


Lambda > Functions > Create function > Configure blueprint kinesis-process-record-python
Basic information Info
Function name
myFunctionName
Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console.
Create a new role with basic Lambda permissions
Use an existing role
Create a new role from AWS policy templates
Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.
Kinesis trigger
Remove
Kinesis stream
Select a Kinesis stream to listen for updates on.
Consumer
Select an optional consumer of your stream to listen for updates on.
No consumer
Batch size
The largest number of records that will be read from your stream at once.
100
Batch window - optional
The maximum amount of time to gather records before invoking the function, in seconds.
Starting position
The position in the stream to start reading from. For more information, see ShardIteratorType in the Amazon Kinesis API Reference.
Latest
Additional settings - optional
In order to read from the Kinesis trigger, your execution role must have proper permissions.

## Step 4: Enable Kinesis trigger in AWS Lambda console

1. On the **Configuration** tab, choose **Triggers**.
2. Check the box next to the name of the Kinesis stream and choose **Enable**.




The blueprint used in this example only consumes log data from the selected stream. You can further edit Lambda function code later to complete a more complicated task.

# Understanding the v1 data export schema

> **Note**
>
> Amazon Monitron Kinesis data export schema v1 has been deprecated. Learn more about the v2 data export schema.

Each measurement data and its corresponding inference result are exported as one Kinesis data stream record in JSON format.

### Topics


- v1 schema format
- v1 schema parameters


## v1 schema format

```
{
    "timestamp": "string",
    "eventId": "string",
    "version": "string",
    "projectDisplayName": "string",
    "siteDisplayName": "string",
    "assetDisplayName": "string",
    "sensorPositionDisplayName": "string",
    "sensor": {
        "physicalId": "string",
        "rssi": number
    },
    "gateway": {
        "physicalId": "string"
    },
    "measurement": {
        "features": {
            "acceleration": {
                "band0To6000Hz": {
                    "xAxis": {
                        "rms": number
                    },
                    "yAxis": {
```

```
                    "rms": number
                },
                "zAxis": {
                    "rms": number
                }
            },
            "band10To1000Hz": {
                "resultantVector": {
                    "absMax": number,
                    "absMin": number,
                    "crestFactor": number,
                    "rms": number
                },
                "xAxis": {
                    "rms": number
                },
                "yAxis": {
                    "rms": number
                },
                "zAxis": {
                    "rms": number
                }
            }
        },
        "temperature": number,
        "velocity": {
            "band10To1000Hz": {
                "resultantVector": {
                    "absMax": number,
                    "absMin": number,
                    "crestFactor": number,
                    "rms": number
                },
                "xAxis": {
                    "rms": number
                },
                "yAxis": {
                    "rms": number
                },
                "zAxis": {
                    "rms": number
                }
            }
        }
```

```
        },
        "sequenceNo": number
    },
    "models": {
        "temperatureML": {
            "persistentClassificationOutput": "string",
            "pointwiseClassificationOutput": "string"
        },
        "vibrationISO": {
            "isoClass": "string",
            "mutedThreshold": "string",
            "persistentClassificationOutput": "string",
            "pointwiseClassificationOutput": "string"
        },
        "vibrationML": {
            "persistentClassificationOutput": "string",
            "pointwiseClassificationOutput": "string"
        }
    },
    "assetState": {
        "newState": "string",
        "previousState": "string"
    }
}
```

## v1 schema parameters

timestamp

- The timestamp when the measurement is received by Monitron service in UTC
- Type: String
- Pattern: yyyy-mm-dd hh:mm:ss.SSS

eventId

- The unique data export event ID assigned for each measurement. Can be used to deduplicate the Kinesis stream records received.
- Type: String

version

- Schema version
- Type: String
- Current Value: 1.0

projectDisplayName

- The project name displayed in the App and console
- Type: String

siteDisplayName

- The site name displayed in the App
- Type: String

assetDisplayName

- The asset name displayed in the App
- Type: String

sensorPositionDisplayName

- The sensor position name displayed in the App
- Type: String

sensor.physicalId

- The physical ID of the sensor from which the measurement is sent
- Type: String

sensor.rssi

- The sensor bluetooth received signal strength indicator value
- Type: Number
- Unit: dBm

gateway.physicalId

- The physical ID of the gateway used to transmit data to Amazon Monitron service
- Type: String

measurement.features.acceleration.band0To6000Hz.xAxis.rms

- The root mean square of the acceleration observed in the frequency band 0–6000 Hz in the x axis
- Type: Number
- Unit: m/s^2

measurement.features.acceleration.band0To6000Hz.yAxis.rms

- The root mean square of the acceleration observed in the frequency band 0–6000 Hz in the y axis

- Type: Number
- Unit: m/s^2

measurement.features.acceleration.band0To6000Hz.zAxis.rms

- The root mean square of the acceleration observed in the frequency band 0–6000 Hz in the y axis
- Type: Number
- Unit: m/s^2

measurement.features.acceleration.band10To1000Hz.resultantVector.absMax

- The absolute maximum acceleration observed in the frequency band 10–1000 Hz
- Type: Number
- Unit: m/s^2

measurement.features.acceleration.band10To1000Hz.resultantVector.absMin

- The absolute minimum acceleration observed in the frequency band 10–1000 Hz
- Type: Number
- Unit: m/s^2

measurement.features.acceleration.band10To1000Hz.resultantVector.crestFactor

- The acceleration crest factor observed in the frequency band 10–1000 Hz
- Type: Number

measurement.features.acceleration.band10To1000Hz.resultantVector.rms

- The root mean square of the acceleration observed in the frequency band 10–1000 Hz
- Type: Number
- m/s^2

measurement.features.acceleration.band10To1000Hz.xAxis.rms

- The root mean square of the acceleration observed in the frequency band 10–1000 Hz in the x axis
- Type: Number
- m/s^2

measurement.features.acceleration.band10To1000Hz.yAxis.rms

- The root mean square of the acceleration observed in the frequency band 10–1000 Hz in the y axis
- Type: Number

- m/s^2

measurement.features.acceleration.band10To1000Hz.zAxis.rms

- The root mean square of the acceleration observed in the frequency band 10–1000 Hz in the z axis
- Type: Number
- m/s^2

measurement.features.temperature

- The temperature observed
- Type: Number
- °C/degC

measurement.features.velocity.band10To1000Hz.resultantVector.absMax

- The absolute maximum velocity observed in the frequency band 10–1000 Hz
- Type: Number
- mm/s

measurement.features.velocity.band10To1000Hz.resultantVector.absMin

- The absolute minimum velocity observed in the frequency band 10–1000 Hz
- Type: Number
- mm/s

measurement.features.velocity.band10To1000Hz.resultantVector.crestFactor

- The velocity crest factor observed in the frequency band 10–1000 Hz
- Type: Number

measurement.features.velocity.band10To1000Hz.resultantVector.rms

- The root mean square of the velocity observed in the frequency band 10–1000 Hz
- Type: Number
- mm/s

measurement.features.velocity.band10To1000Hz.xAxis.rms

- The root mean square of the velocity observed in the frequency band 10–1000 Hz in the x axis
- Type: Number
- mm/s

measurement.features.velocity.band10To1000Hz.yAxis.rms

- The root mean square of the velocity observed in the frequency band 10–1000 Hz in the y axis
- Type: Number
- mm/s

measurement.features.velocity.band10To1000Hz.zAxis.rms

- The root mean square of the velocity observed in the frequency band 10–1000 Hz in the z axis
- Type: Number
- mm/s

measurement.sequenceNo

- The measurement sequence number
- Type: Number

models.temperatureML.persistentClassificationOutput

- The persistent classification output from the machine learning based temperature model
- Type: Number
- Valid Values: `UNKNOWN | HEALTHY | WARNING | ALARM`

models.temperatureML.pointwiseClassificationOutput

- The point–wise classification output from the machine learning based temperature model
- Type: String
- Valid Values: `UNKNOWN | INITIALIZING | HEALTHY | WARNING | ALARM`

models.vibrationISO.isoClass

- The ISO 20816 class (a standard for measurement and evaluation of machine vibration) used by the ISO based vibration model
- Type: String
- Valid Values: `CLASS1 | CLASS2 | CLASS3 | CLASS4 | FAN_BV2`

models.vibrationISO.mutedThreshold

- The threshold to mute the notification from the ISO based vibration model
- Type: String
- Valid Values: `WARNING | ALARM`

models.vibrationISO.persistentClassificationOutput

- The persistent classification output from the ISO based vibration model
- Type: String
- Valid Values: `UNKNOWN | HEALTHY | WARNING | ALARM`

models.vibrationISO.pointwiseClassificationOutput

- The point–wise classification output from the the ISO based vibration model
- Type: String
- Valid Values: `UNKNOWN | HEALTHY | WARNING | ALARM | MUTED_WARNING | MUTED_ALARM`

models.vibrationML.persistentClassificationOutput

- The persistent classification output from the machine learning based vibration model
- Type: String
- Valid Values: `UNKNOWN | HEALTHY | WARNING | ALARM`

models.vibrationML.pointwiseClassificationOutput

- The point–wise classification output from the machine learning based vibration model
- Type: String
- Valid Values: `UNKNOWN | INITIALIZING | HEALTHY | WARNING | ALARM`

assetState.newState

- The machine status after processing the measurement
- Type: String
- Valid Values: `UNKNOWN | HEALTHY | NEEDS_MAINTENANCE | WARNING | ALARM`

assetState.previousState

- The machine status before processing the measurement
- Type: String
- Valid Values: `UNKNOWN | HEALTHY | NEEDS_MAINTENANCE | WARNING | ALARM`

# Amazon Monitron Kinesis data export v2

You can export incoming measurement data and the corresponding inference results from Amazon Monitron and perform real-time analysis. Data export streams live data to Kinesis.

**Topics**

- Exporting your data to a Kinesis stream
- Editing live data export settings
- Stopping a live data export
- Viewing data export errors
- Using server-side encryption for the Kinesis stream
- Monitoring with Amazon CloudWatch Logs
- Storing exported data in Amazon S3
- Processing data with Lambda
- Understanding the v2 data export schema
- Migration from Kinesis v1 to v2


## Exporting your data to a Kinesis stream

1. From your project's main page, near the bottom of the page, on the right, choose **Start live data export**.
2. Under **Select Kinesis data stream**, do one of the following:
   - Enter the name of an existing stream in the search box. Then skip to Step 5.
   - Choose **Create a new data stream**.
3. On the **Create data stream** page, under **Data stream configuration**, enter your data stream name.
4. Under Data stream capacity, choose your capacity mode:
   - If your data stream's throughput requirements are unpredictable and variable, choose **On-demand**.
   - If you can reliably estimate the throughput requirements of your data stream, choose **Provisioned**. Then, under provisioned shards, enter the number of shards you want to create, or choose the **Shard estimator**.
5. Choose **Create data stream**.

## Editing live data export settings

To edit your live data export settings:

1. Open the Amazon Monitron console.
2. Choose **Projects** from the navigation pane.
3. If you have multiple projects, choose the project for which you want to edit the export settings.
4. From the main page for your project, under **Live data export**, from the **Actions** dropdown menu, choose **Edit live data export settings**.

## Stopping a live data export

1. Open the Amazon Monitron console.
2. Choose **Projects** from the navigation pane.
3. If you have multiple projects, choose the project for which you want to edit the export settings.
4. From the main page for your project, under **Live data export**, from the **Actions** dropdown menu, choose **Stop live data export**.
5. In the pop-up window, choose **Stop**.

## Viewing data export errors

To view the error messages in the CloudWatch Logs interface:

- On the Amazon Monitron console, from the main page for your project, under **Live data export**, choose **CloudWatch log group**.

## Using server-side encryption for the Kinesis stream

You can enable server-side encryption for your Kinesis stream before setting up Kinesis data export. However, if server-side encryption is enabled after Kinesis data export is set up, Amazon Monitron will not be able to publish to the stream. That's because Amazon Monitron will not have permission to call kms:GenerateDataKey so that it can encrypt data sent to Kinesis.

To work around this, follow the instructions under ???, but without changing the configuration. This will associate the encryption you have set up with your export configuration.

# Monitoring with Amazon CloudWatch Logs

You can monitor Amazon Monitron live data export using Amazon CloudWatch Logs. When a measurement fails to export, Amazon Monitron will send a log event to your CloudWatch Logs. You can also set up a metric filter on the error log to generate metrics and set up alarms. An alarm can watch for certain thresholds and send notifications or take actions when those thresholds are met. For more information, see the CloudWatch User Guide.

Amazon Monitron sends log events to the /aws/monitron/data-export/{HASH_ID} log group.

The log event has the following JSON format:

```
{
    "assetName": "string",
    "destination": "string",
    "errorCode": "string",
    "errorMessage": "string",
    "eventId": "string",
    "eventType": "string",
    "positionName": "string",
    "projectName": "string",
    "projectId": "string",
    "sensorId": "string",
    "gatewayId": "string",
    "siteName": "string",
    "timestamp": "string"
}
```

assetName

- The asset name displayed in the app
- Type: String

destination

- The ARN of the Kinesis data stream
- Type: String
- Pattern: arn:aws:kinesis:{{REGION}}:{{AWS_ACCOUNT_ID}}:stream/{{STREAM_NAME}}

errorCode

- The error code
- Type: String

- Valid Values: `INTERNAL_SEVER_ERROR | KINESIS_RESOURCE_NOT_FOUND | KINESIS_PROVISIONED_THROUGHPUT_EXCEEDED | KMS_ACCESS_DENIED | KMS_NOT_FOUND | KMS_DISABLED | KMS_INVALID_STATE | KMS_THROTTLING`

errorMessage

- The detailed error message
- Type: String

eventId

- The unique event ID corresponding to each measurement export
- Type: String

eventType

- The current event type
- Type: String
- Valid values: `measurement | gatewayConnected | gatewayDisconnected | sensorConnected | sensorDisconnected | assetStateTransition`

positionName

- The sensor position name displayed in the app
- Type: String

projectName

- The project name displayed in the app and console
- Type: String

projectID

- The unique project ID corresponding to the Amazon Monitron project
- Type: String

sensorID

- The physical ID of the sensor from which the measurement is sent
- Type: String

gatewayID

- The physical ID of the gateway used to transmit data to the Amazon Monitron service
- Type: String

siteName

- The site name displayed in the app
- Type: String

timestamp

- The timestamp when the measurement is received by the Amazon Monitron service in UTC
- Type: String
- Pattern: yyyy-mm-dd hh:mm:ss.SSS

## Storing exported data in Amazon S3

If you want to store your exported data in Amazon S3, use the following procedure.

**Topics**


- Configuring Kinesis manually in the console


### Configuring Kinesis manually in the console

1. Sign in to the AWS Management Console and open the Kinesis console at https://console.aws.amazon.com/kinesis.
2. Choose **Delivery streams** in the navigation pane.
3. Choose **Create delivery stream**.
4. For Source, select **Amazon Kinesis Data Streams**.
5. For Destination, select **Amazon S3**.
6. Under **Source settings, Kinesis data stream**, enter the ARN of your Kinesis data stream.
7. Under **delivery stream name**, enter the name of your Kinesis data stream.
8. Under **Desination settings**, choose an Amazon S3 bucket or enter a bucket URI.
9. (optional) Enable dynamic partitioning using inline parsing for JSON. This option is appropriate if you want to partition streaming measurement data based on source information and timestamp. For example:

    - Choose **Enabled** for **Dynamic partitioning**.
    - Choose **Enabled** for **New line delimiter**.
    - Choose **Enabled** for **Inline parsing for JSON**.

- Under **Dynamic partitioning keys**, add:

| Key name | JQ expression |
| --- | --- |
| project | .projectName\| "project=\(.)" |
| site | .eventPayload.siteName\| "site=\(.)" |
| time | .timestamp\| sub("[0-9]{2}:[0-9]{2}:[0-9]{2}.[0-9]{3}$"; "00:00:00")\| "time=\(.)" |

10. Choose **Apply dynamic partitioning keys** and confirm the generated Amazon S3 bucket prefix is `!{partitionKeyFromQuery:project}/!{partitionKeyFromQuery:site}/!{partitionKeyFromQuery:time}/`.
11. In Amazon S3, objects will use the following key format: `/project={projectName}/site={siteName}/time={yyyy-mm-dd 00:00:00}/{filename}`.
12. Choose **Create delivery stream**.

## Processing data with Lambda

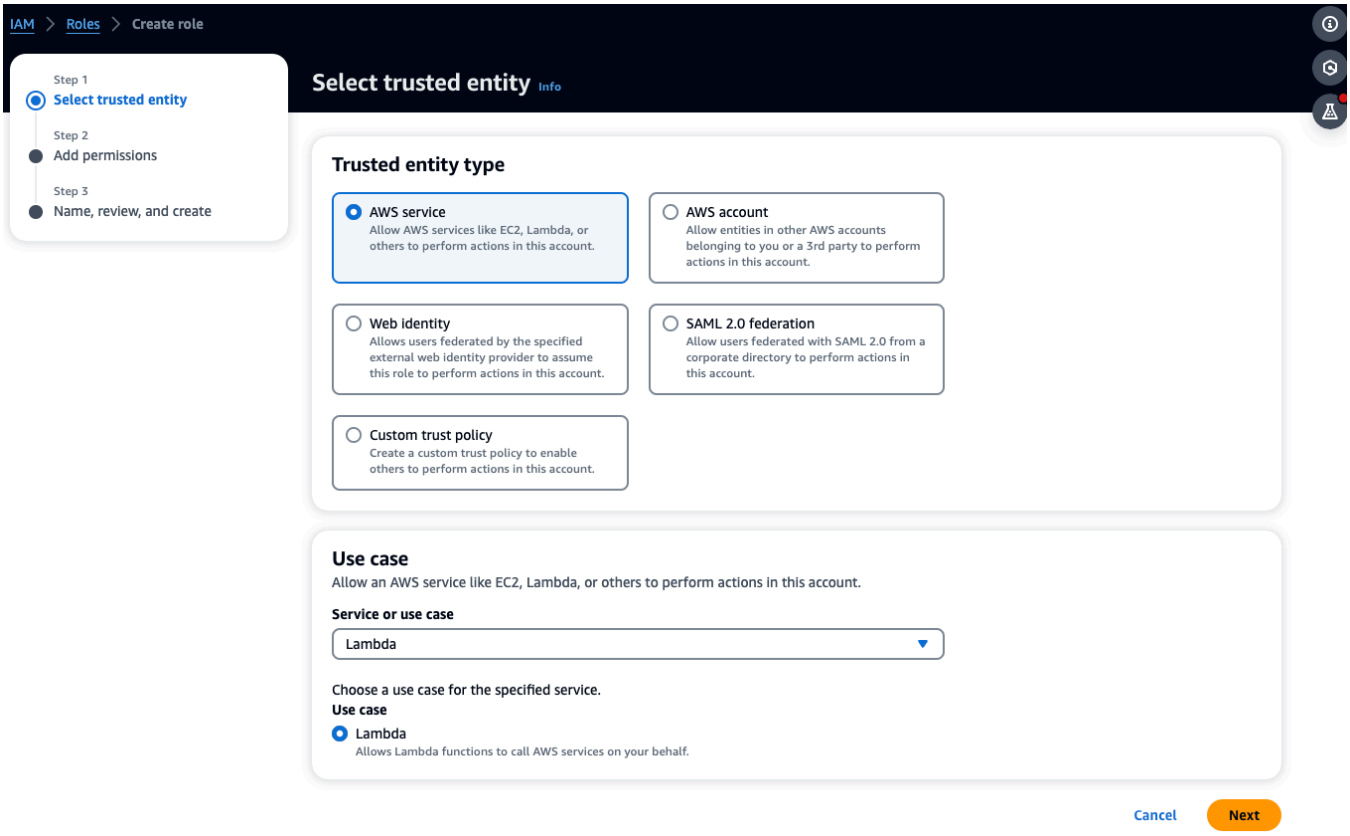
**Topics**


- Step 1: Create the IAM role that gives your function permission to access AWS resources
- Step 2: Create the Lambda function
- Step 3: Configure the Lambda function
- Step 4: Enable Kinesis trigger in AWS Lambda console


### Step 1: Create the IAM role that gives your function permission to access AWS resources

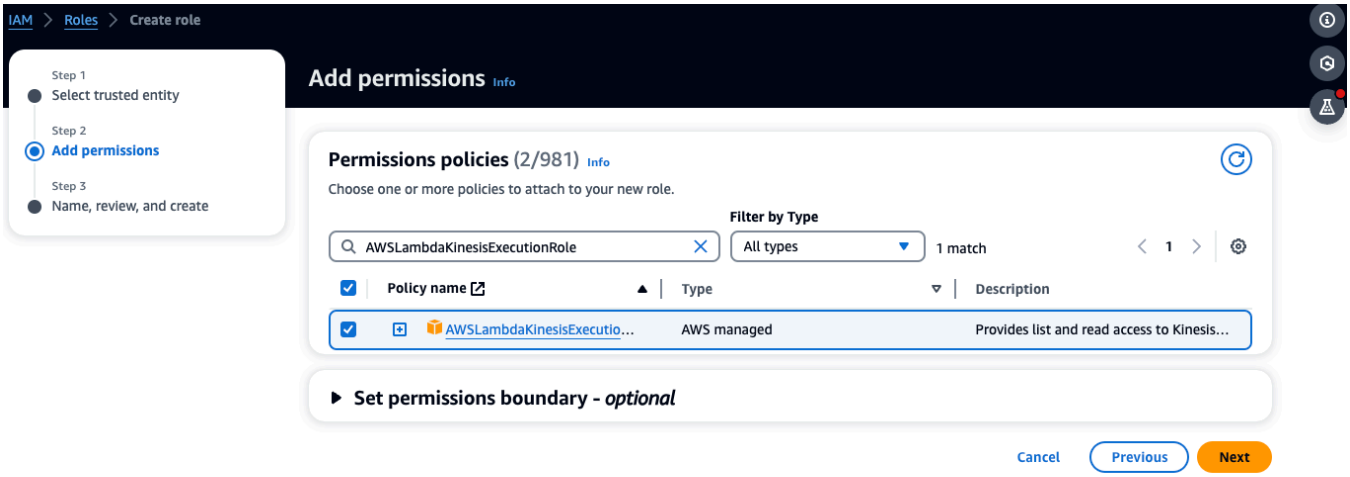
1. Open the roles page in the IAM console.
2. Choose **Create role**.
3. On the **Select trusted entity** page, do the following:
   - In **Trusted entity type**, choose **AWS service**.
   - In **Use case**, for **Service or use case** choose **Lambda**.

- Choose **Next**.



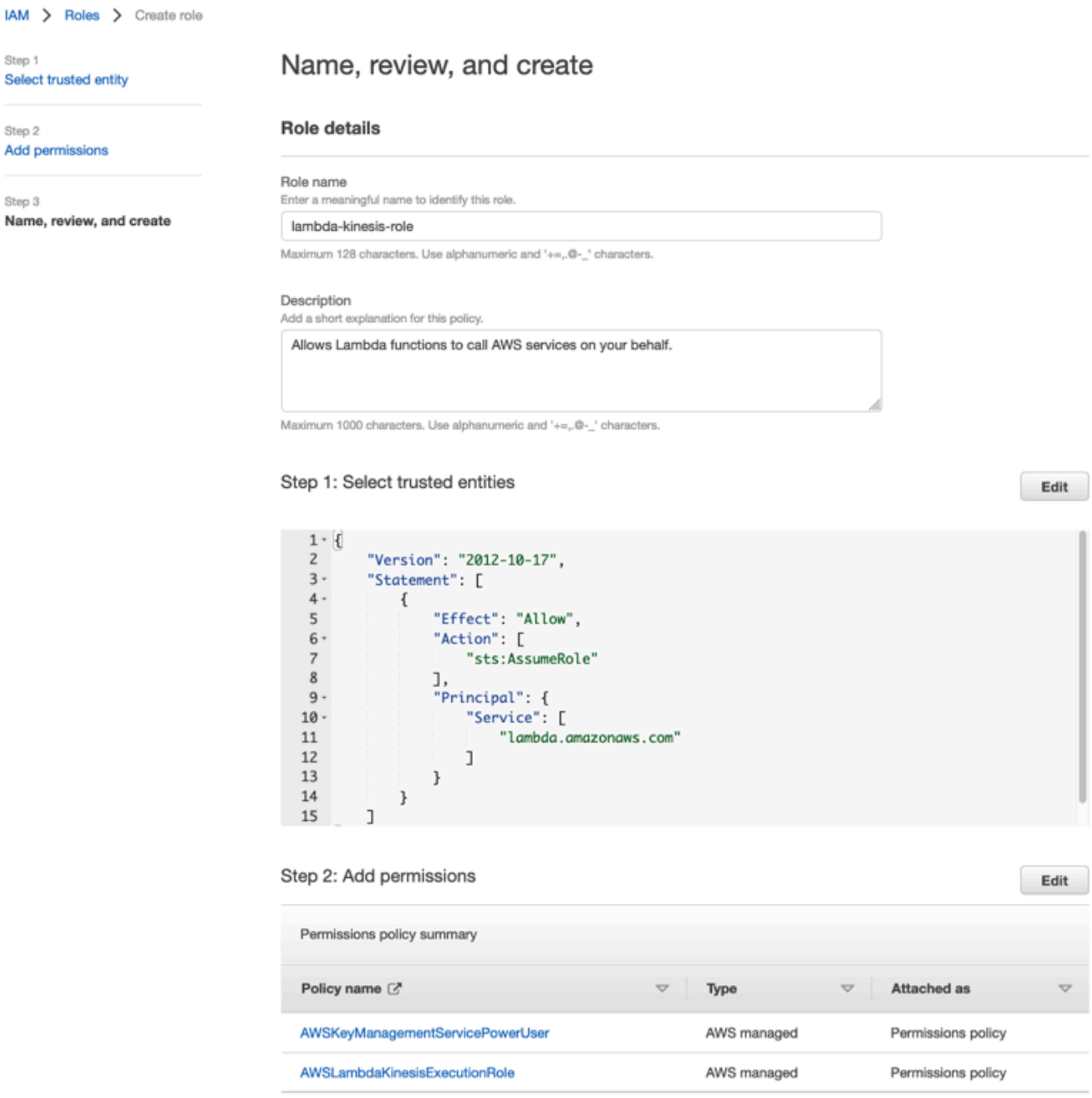

4. In the **Add permissions** page, do the following:

   - In **Permissions policies**, choose AWSLambdaKinesisExecutionRole (and AWSKeyManagementServicePowerUser if the Kinesis stream is encrypted).
   - Leave the configurations in **Set permissions boundary** as is.
   - Choose **Next**.




5. In the **Name, review, and create** page, do the following:

   - In **Role details**, for **Role name**, enter a name for your role. For example *`lambda-kinesis-role`*. You can also choose to add an optional **Description**.
   - Leave the settings for **Step 1: Select trusted entities** and **Step 2: Add permissions** as is. You can choost to add tags in **Step 3: Add tags** to keep track of your resources.

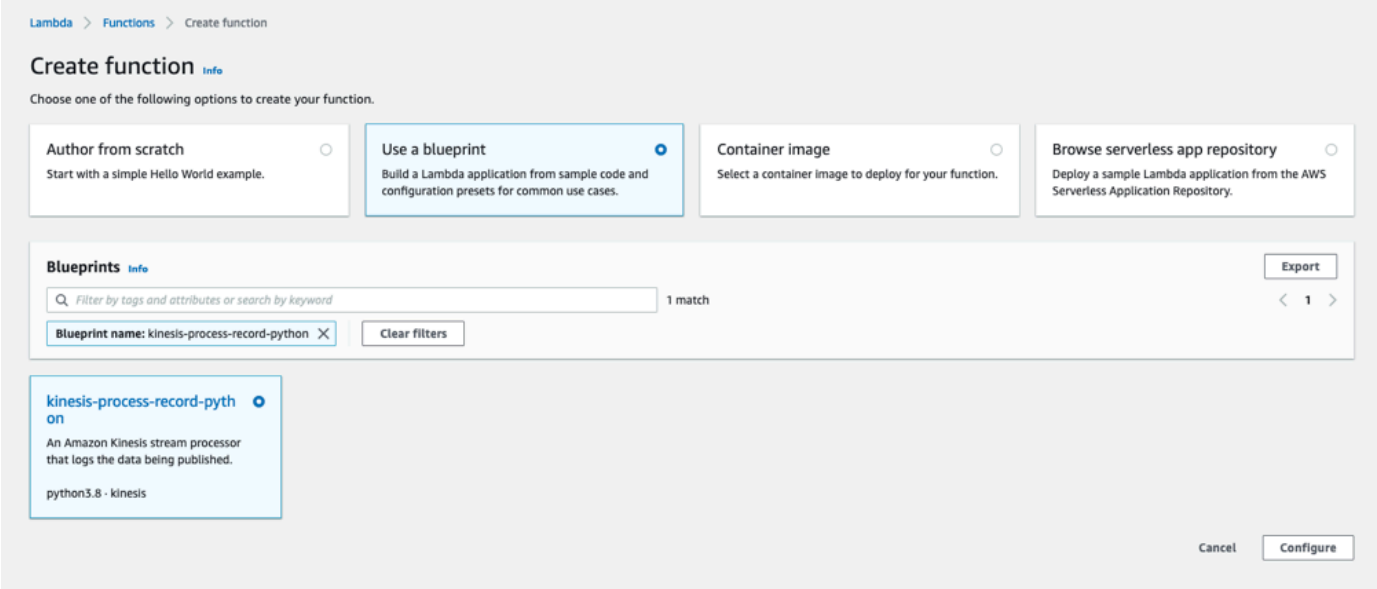



6. Select **Create role**.

## Step 2: Create the Lambda function

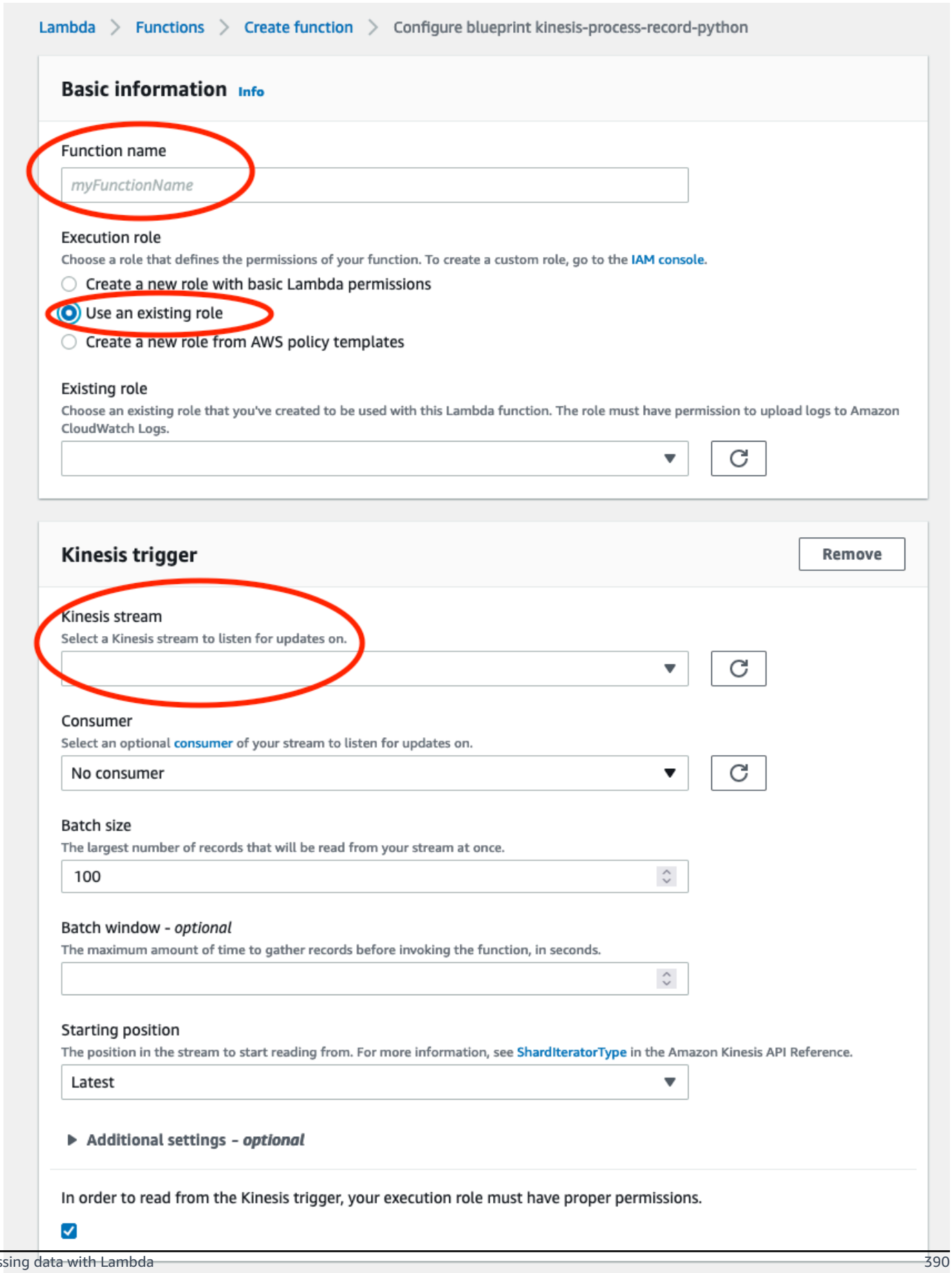
1. Open the **Functions** page in the Lambda console.
2. Choose **Create function**.

3. Choose **Use a blueprint**.
4. In the **Blueprints** search bar, search and choose **kinesis-process-record (nodejs)** or **kinesis-process-record-python**.
5. Choose **Configure**.



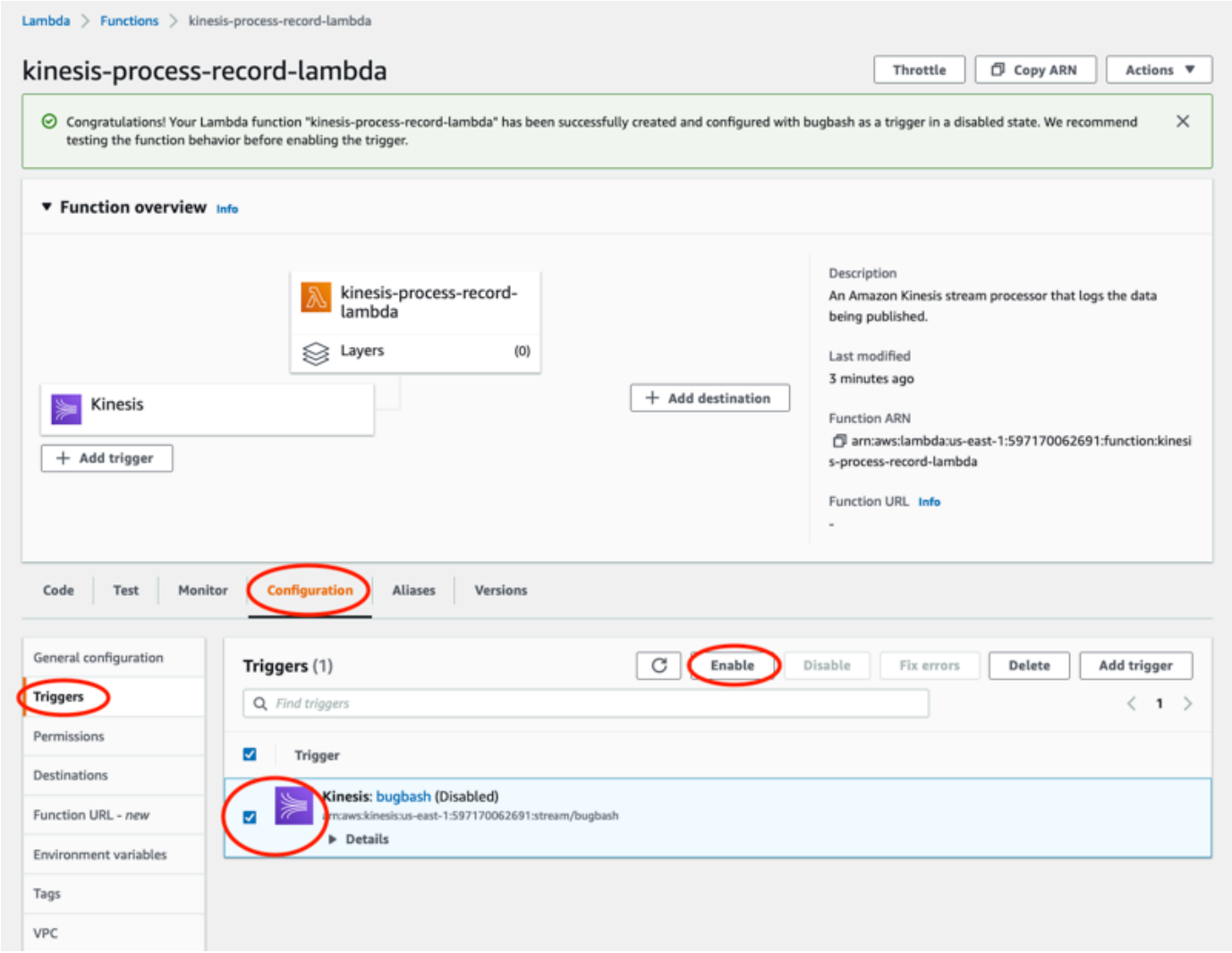

## Step 3: Configure the Lambda function

1. Choose **Function name**
2. Choose the role created in the first step as the **Execution role**.
3. Configure Kinesis trigger.
    1. Choose your Kinesis stream.
    2. Click **Create function**.


Lambda > Functions > Create function > Configure blueprint kinesis-process-record-python
Basic information Info
Function name
myFunctionName
Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console.
Create a new role with basic Lambda permissions
Use an existing role
Create a new role from AWS policy templates
Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.
Kinesis trigger
Remove
Kinesis stream
Select a Kinesis stream to listen for updates on.
Consumer
Select an optional consumer of your stream to listen for updates on.
No consumer
Batch size
The largest number of records that will be read from your stream at once.
100
Batch window - optional
The maximum amount of time to gather records before invoking the function, in seconds.
Starting position
The position in the stream to start reading from. For more information, see ShardIteratorType in the Amazon Kinesis API Reference.
Latest
Additional settings - optional
In order to read from the Kinesis trigger, your execution role must have proper permissions.

### Step 4: Enable Kinesis trigger in AWS Lambda console

1. On the **Configuration** tab, choose **Triggers**.
2. Check the box next to the name of the Kinesis stream and choose **Enable**.




The blueprint used in this example only consumes log data from the selected stream. You can further edit Lambda function code later to complete a more complicated task.

## Understanding the v2 data export schema

Each measurement data, its corresponding inference result, gateway connect/disconnect, and sensor connect/disconnect events are exported as one Kinesis data stream record in JSON format.

### Topics

- v2 schema format
- v2 schema parameters


## v2 schema format

```
{
    "timestamp": "string",
    "eventId": "string",
    "version": "2.0",
    "accountId": "string",
    "projectName": "string",
    "projectId": "string",
    "eventType": "measurement|gatewayConnected|gatewayDisconnected|sensorConnected|
sensorDisconnected|assetStateTransition",
    // measurement
    "eventPayload": {
        "siteName": "string",
        "assetName": "string",
        "positionName": "string",
        "companyName": "string",
        "geoLocation": {
            "latitude": number,
            "longitude": number
        },
        "address": "string",
        "serialNumber": "string",
        "make": "string",
        "model": "string",
        "assetPositionURL": "string",
        "sensor": {
            "physicalId": "string",
            "rssi": number
        },
        "gateway": {
            "physicalId": "string"
        },
        "sequenceNo": number,
        "features": {
            "acceleration": {
                "band0To6000Hz": {
                    "xAxis": {
                        "rms": number
```

```
                    },
                    "yAxis": {
                        "rms": number
                    },
                    "zAxis": {
                        "rms": number
                    }
                },
                "band10To1000Hz": {
                    "totalVibration": {
                        "absMax": number,
                        "absMin": number,
                        "crestFactor": number,
                        "rms": number
                    },
                    "xAxis": {
                        "rms": number
                    },
                    "yAxis": {
                        "rms": number
                    },
                    "zAxis": {
                        "rms": number
                    }
                }
            },
            "velocity": {
                "band10To1000Hz": {
                    "totalVibration": {
                        "absMax": number,
                        "absMin": number,
                        "crestFactor": number,
                        "rms": number
                    },
                    "xAxis": {
                        "rms": number
                    },
                    "yAxis": {
                        "rms": number
                    },
                    "zAxis": {
                        "rms": number
                    }
                }
```

```
            },
            "temperature": number
        }
        "models": {
            "temperatureML": {
                "previousPersistentClassificationOutput": "string",
                "persistentClassificationOutput": "string",
                "pointwiseClassificationOutput": "string"
            },
            "vibrationISO": {
                "isoClass": "string",
                "mutedThreshold": "string",
                "previousPersistentClassificationOutput": "string",
                "persistentClassificationOutput": "string",
                "pointwiseClassificationOutput": "string"
            },
            "vibrationML": {
                "previousPersistentClassificationOutput": "string",
                "persistentClassificationOutput": "string",
                "pointwiseClassificationOutput": "string"
            }
        },
        "assetPositionId": "string"
    }

    // sensorConnected
    "eventPayload": {
        "siteName": "string",
        "assetName": "string",
        "positionName": "string",
        "companyName": "string",
        "geoLocation": {
            "latitude": number,
            "longitude": number
        },
        "address": "string",
        "serialNumber": "string",
        "make": "string",
        "model": "string",
        "assetPositionURL": "string",
        "sensor": {
            "physicalId": "string"
        },
        "assetPositionId": "string"
```

```
    }

    // sensorDisconnected
    "eventPayload": {
        "siteName": "string",
        "assetName": "string",
        "positionName": "string",
        "companyName": "string",
        "geoLocation": {
            "latitude": number,
            "longitude": number
        },
        "address": "string",
        "serialNumber": "string",
        "make": "string",
        "model": "string",
        "assetPositionURL": "string",
        "sensor": {
            "physicalId": "string"
        },
        "assetPositionId": "string"
    }

    // gatewayConnected
    "eventPayload": {
        "siteName": "string",
        "gatewayName": "string",
        "gatewayListURL": "string",
        "companyName": "string",
        "geoLocation": {
            "latitude": number,
            "longitude": number
        },
        "address": "string",
        "gateway": {
            "physicalId": "string"
        }
    }

    // gatewayDisconnected
    "eventPayload": {
        "siteName": "string",
        "gatewayName": "string",
        "gatewayListURL": "string",
```

```
        "companyName": "string",
        "geoLocation": {
            "latitude": number,
            "longitude": number
        },
        "address": "string",
        "gateway": {
            "physicalId": "string"
        }
    }

    // assetStateTransition
    "eventPayload": {
        "siteName": "string",
        "assetName": "string",
        "positionName": "string",
        "companyName": "string",
        "geoLocation": {
            "latitude": number,
            "longitude": number
        },
        "address": "string",
        "serialNumber": "string",
        "make": "string",
        "model": "string",
        "assetPositionURL": "string",
        "sensor": {
            "physicalId": "string"
        },
        "assetTransitionType": "measurement|userInput",
        "assetState": {
            "newState": "string",
            "previousState": "string"
        },
        "closureCode": {
            "failureMode": "string",
            "failureCause": "string",
            "actionTaken": "string",
            "resolvedModels": list<"string">
        },
        "assetPositionId": "string"
    }
}
```

## v2 schema parameters

The Amazon Monitron Kinesis data export schema v2 includes the following schema parameters. Some parameters are updates from v1 and some are unique to v2. For example, `siteName` was a first-level parameter in v1. In v2, it is a second-level parameter that can be found under the `eventPayload` entity.

timestamp

- The timestamp when the measurement is received by Amazon Monitron service in UTC
- Type: String
- Pattern: yyyy-mm-dd hh:mm:ss.SSS

eventId

- The unique data export event ID assigned for each measurement. Can be used to deduplicate the Kinesis stream records received.
- Type: String

version

- Schema version
- Type: String
- Value: 1.0 or 2.0

accountId

- The 12-digit AWS account ID for your Monitron project
- Type: String

projectName

The project name displayed in the app and console.

Type: String

projectId

The unique ID of your Amazon Monitron project.

Type: String

eventType

- The current event stream. Each event type will have a dedicated `eventPayload` format.

- Type: String
- Possible values: `measurement`, `gatewayConnected`, `gatewayDisconnected`, `sensorConnected`, `sensorDisconnected`, `assetStateTransition`.

### `eventType: measurement`

eventPayload.features.acceleration.band0To6000Hz.xAxis.rms

- The root mean square of the acceleration observed in the frequency band 0–6000 Hz in the x axis
- Type: Number
- Unit: m/s^2

eventPayload.features.acceleration.band0To6000Hz.yAxis.rms

- The root mean square of the acceleration observed in the frequency band 0–6000 Hz in the y axis
- Type: Number
- Unit: m/s^2

eventPayload.features.acceleration.band0To6000Hz.zAxis.rms

- The root mean square of the acceleration observed in the frequency band 0–6000 Hz in the z axis
- Type: Number
- Unit: m/s^2

eventPayload.features.acceleration.band10To1000Hz.resultantVector.absMax

- The absolute maximum acceleration observed in the frequency band 10–1000 Hz
- Type: Number
- Unit: m/s^2

eventPayload.features.acceleration.band10To1000Hz.resultantVector.absMin

- The absolute minimum acceleration observed in the frequency band 10–1000 Hz
- Type: Number
- Unit: m/s^2

eventPayload.features.acceleration.band10To1000Hz.resultantVector.crestFactor

- The acceleration crest factor observed in the frequency band 10–1000 Hz
- Type: Number

eventPayload.features.acceleration.band10To1000Hz.resultantVector.rms

- The root mean square of the acceleration observed in the frequency band 10–1000 Hz
- Type: Number
- m/s^2

eventPayload.features.acceleration.band10To1000Hz.xAxis.rms

- The root mean square of the acceleration observed in the frequency band 10–1000 Hz in the x axis
- Type: Number
- m/s^2

eventPayload.features.acceleration.band10To1000Hz.yAxis.rms

- The root mean square of the acceleration observed in the frequency band 10–1000 Hz in the y axis
- Type: Number
- m/s^2

eventPayload.features.acceleration.band10To1000Hz.zAxis.rms

- The root mean square of the acceleration observed in the frequency band 10–1000 Hz in the z axis
- Type: Number
- m/s^2

eventPayload.features.temperature

- The temperature observed
- Type: Number
- °C/degC

eventPayload.features.velocity.band10To1000Hz.resultantVector.absMax

- The absolute maximum velocity observed in the frequency band 10–1000 Hz
- Type: Number
- mm/s

eventPayload.features.velocity.band10To1000Hz.resultantVector.absMin

- The absolute minimum velocity observed in the frequency band 10–1000 Hz
- Type: Number

- mm/s

eventPayload.features.velocity.band10To1000Hz.resultantVector.crestFactor

- The velocity crest factor observed in the frequency band 10–1000 Hz
- Type: Number

eventPayload.features.velocity.band10To1000Hz.resultantVector.rms

- The root mean square of the velocity observed in the frequency band 10–1000 Hz
- Type: Number
- mm/s

eventPayload.features.velocity.band10To1000Hz.xAxis.rms

- The root mean square of the velocity observed in the frequency band 10–1000 Hz in the x axis
- Type: Number
- mm/s

eventPayload.features.velocity.band10To1000Hz.yAxis.rms

- The root mean square of the velocity observed in the frequency band 10–1000 Hz in the y axis
- Type: Number
- mm/s

eventPayload.features.velocity.band10To1000Hz.zAxis.rms

- The root mean square of the velocity observed in the frequency band 10–1000 Hz in the z axis
- Type: Number
- mm/s

eventPayload.sequenceNo

- The measurement sequence number
- Type: Number

eventPayload.assetPositionId

- The identifier of the sensor position for which the measurement is sent.
- Type: String

eventPayload.companyName

- The name of the company using the asset.

- Type: String

eventPayload.geoLocation.latitude

- The latitude of the site's physical location.
- Type: Number

eventPayload.geoLocation.longitude

- The longitude of the site's physical location.
- Type: Number

eventPayload.address

- The address of the site.
- Type: String

eventPayload.serialNumber

- The serial number of the asset.
- Type: String

eventPayload.make

- The make of the asset.
- Type: String

eventPayload.model

- The model of the asset.
- Type: String

### `eventType: sensorConnected`

siteName

- The site name displayed in the app
- Type: String

assetName

- The asset name displayed in the app
- Type: String

positionName

- The sensor position name displayed in the app

- Type: String

assetPositionURL

- The sensor URL displayed in the app
- Type: String

physicalID

- The physical ID of the sensor from which the measurement is sent
- Type: String

eventPayload.assetPositionId

- The identifier of the sensor position whose state changed.
- Type: String

eventPayload.companyName

- The name of the company using the asset.
- Type: String

eventPayload.geoLocation.latitude

- The latitude of the site's physical location.
- Type: Number

eventPayload.geoLocation.longitude

- The longitude of the site's physical location.
- Type: Number

eventPayload.address

- The address of the site.
- Type: String

eventPayload.serialNumber

- The serial number of the asset.
- Type: String

eventPayload.make

- The make of the asset.
- Type: String

eventPayload.model

- The model of the asset.

- Type: String

### `eventType: sensorDisconnected`

siteName

- The site name displayed in the app
- Type: String

assetName

- The asset name displayed in the app
- Type: String

positionName

- The sensor position name displayed in the app
- Type: String

assetPositionURL

- The sensor URL displayed in the app
- Type: String

physicalID

- The physical ID of the sensor from which the measurement is sent
- Type: String

eventPayload.assetPositionId

- The identifier of the sensor position whose state changed.
- Type: String

eventPayload.companyName

- The name of the company using the asset.
- Type: String

eventPayload.geoLocation.latitude

- The latitude of the site's physical location.
- Type: Number

eventPayload.geoLocation.longitude

- The longitude of the site's physical location.
- Type: Number

eventPayload.address

- The address of the site.
- Type: String

eventPayload.serialNumber

- The serial number of the asset.
- Type: String

eventPayload.make

- The make of the asset.
- Type: String

eventPayload.model

- The model of the asset.
- Type: String

### `eventType: gatewayConnected`

eventPayload.siteName

- The site name displayed in the app
- Type: String

eventPayload.gatewayName

- The name of the gateway as displayed in the app
- Type: String

eventPayload.gatewayListURL

- The gateway URL displayed in the app
- Type: String

eventPayload.gateway.physicalID

- The physical ID of the gateway just connected to transmit data to the Amazon Monitron service
- Type: String

eventPayload.companyName

- The name of the company using the asset.
- Type: String

eventPayload.geoLocation.latitude

- The latitude of the site's physical location.
- Type: Number

eventPayload.geoLocation.longitude

- The longitude of the site's physical location.
- Type: Number

eventPayload.address

- The address of the site.
- Type: String

### `eventType: gatewayDisconnected`

siteName

- The site name displayed in the app
- Type: String

gatewayName

- The name of the gateway as displayed in the app
- Type: String

gatewayListURL

- The gateway URL displayed in the app
- Type: String

physicalID

- The physical ID of the gateway just connected to transmit data to the Amazon Monitron service
- Type: String

eventPayload.companyName

- The name of the company using the asset.
- Type: String

eventPayload.geoLocation.latitude

- The latitude of the site's physical location.
- Type: Number

eventPayload.geoLocation.longitude

- The longitude of the site's physical location.
- Type: Number

eventPayload.address

- The address of the site.
- Type: String

### `eventType: assetStateTransition`

eventPayload.siteName

- The site name displayed in the app
- Type: String

eventPayload.assetName

- The asset name displayed in the app
- Type: String

eventPayload.positionName

- The sensor position name displayed in the app
- Type: String

eventPayload.assetPositionURL

- The sensor URL displayed in the app
- Type: String

eventPayload.sensor.physicalID

- The physical ID of the sensor from which the measurement is sent
- Type: String

eventPayload.assetTransitionType

- The reason behind the asset state transition
- Type: String
- Possible values: `measurement` or `userInput`

eventPayload.assetState.newState

- The new state of the asset

- Type: String

eventPayload.assetState.previousState

- The previous state of the asset
- Type: String

eventPayload.closureCode.failureMode

- The failure mode selected by the user when acknowledging this failure
- Type: String
- Possible values: `NO_ISSUE` | `BLOCKAGE` | `CAVITATION` | `CORROSION` | `DEPOSIT` | `IMBALANCE` | `LUBRICATION` | `MISALIGNMENT` | `OTHER` | `RESONANCE` | `ROTATING_LOOSENESS` | `STRUCTURAL_LOOSENESS` | `TRANSMITTED_FAULT` | `UNDETERMINED`

eventPayload.closureCode.failureCause

- The cause of the failure as selected by the user in the app dropdown when acknowledging a failure.
- Type: String
- Possible values: `ADMINISTRATION` | `DESIGN` | `FABRICATION` | `MAINTENANCE` | `OPERATION` | `OTHER` | `QUALITY` | `UNDETERMINED` | `WEAR`

eventPayload.closureCode.actionTaken

- The action taken when closing this anomaly, as selected by the user in the app dropdown.
- Type: String
- Possible values: `ADJUST` | `CLEAN` | `LUBRICATE` | `MODIFY` | `NO_ACTION` | `OTHER` | `OVERHAUL` | `REPLACE`

eventPayload.closureCode.resolvedModels

- The set of models which called out the issue.
- Type: List of Strings
- Possible values: `vibrationISO` | `vibrationML` | `temperatureML`

eventPayload.assetPositionId

- The identifier of the asset position whose state changed.
- Type: String

models.temperatureML.persistentClassificationOutput

- The persistent classification output from the machine learning based temperature model

- Type: Number
- Valid Values: `UNKNOWN | HEALTHY | WARNING | ALARM`

models.temperatureML.pointwiseClassificationOutput

- The point–wise classification output from the machine learning based temperature model
- Type: String
- Valid Values: `UNKNOWN | INITIALIZING | HEALTHY | WARNING | ALARM`

models.vibrationISO.isoClass

- The ISO 20816 class (a standard for measurement and evaluation of machine vibration) used by the ISO based vibration model
- Type: String
- Valid Values: `CLASS1 | CLASS2 | CLASS3 | CLASS4`

models.vibrationISO.mutedThreshold

- The threshold to mute the notification from the ISO based vibration model
- Type: String
- Valid Values: `WARNING | ALARM`

models.vibrationISO.persistentClassificationOutput

- The persistent classification output from the ISO based vibration model
- Type: String
- Valid Values: `UNKNOWN | HEALTHY | WARNING | ALARM`

models.vibrationISO.pointwiseClassificationOutput

- The point–wise classification output from the the ISO based vibration model
- Type: String
- Valid Values: `UNKNOWN | HEALTHY | WARNING | ALARM | MUTED_WARNING | MUTED_ALARM`

models.vibrationML.persistentClassificationOutput

- The persistent classification output from the machine learning based vibration model
- Type: String
- Valid Values: `UNKNOWN | HEALTHY | WARNING | ALARM`

models.vibrationML.pointwiseClassificationOutput

- The point–wise classification output from the machine learning based vibration model

- Type: String
- Valid Values: `UNKNOWN | INITIALIZING | HEALTHY | WARNING | ALARM`

assetState.newState

- The machine status after processing the measurement
- Type: String
- Valid Values: `UNKNOWN | HEALTHY | NEEDS_MAINTENANCE | WARNING | ALARM`

assetState.previousState

- The machine status before processing the measurement
- Type: String
- Valid Values: `UNKNOWN | HEALTHY | NEEDS_MAINTENANCE | WARNING | ALARM`

eventPayload.companyName

- The name of the company using the asset.
- Type: String

eventPayload.geoLocation.latitude

- The latitude of the site's physical location.
- Type: Number

eventPayload.geoLocation.longitude

- The longitude of the site's physical location.
- Type: Number

eventPayload.address

- The address of the site.
- Type: String

eventPayload.serialNumber

- The serial number of the asset.
- Type: String

eventPayload.make

- The make of the asset.
- Type: String

eventPayload.model

- The model of the asset.

- Type: String

# Migration from Kinesis v1 to v2

If you are currently using the v1 data schema, you may already be sending data to Amazon S3, or further processing the data stream payload with Lambda.

**Topics**


- Updating the data schema to v2
- Updating data processing with Lambda


## Updating the data schema to v2

If you have already configured a data stream with the v1 schema, you can update your data export process by doing the following:

1. Open your Amazon Monitron console.
2. Navigate to your project.
3. Stop the current live data export.
4. Start the live data export to create a new data stream.
5. Select the newly created data stream.
6. Choose **start live data export**. At this point, the new schema will send your payload through the data stream.
7. (Optional) Go to the Kinesis console and delete your old data stream.
8. Configure a new delivery method for your newly created data stream with the v2 schema.

Your new stream now delivers payloads conforming to the v2 schema to your new bucket. We recommend using two distinct buckets to have a consistent format in case you want to process all the data in these buckets. For example, using other services such as Athena and AWS Glue.

> **Note**
>
> If you were delivering your data to Amazon S3, learn how to store exported data in Amazon S3 for details on how to deliver your data to Amazon S3 with the v2 schema.

> **Note**
>
> If you were using a Lambda function to process your payloads, learn how to process data with Lambda. You can also refer to the updating with Lambda section for more information.

## Updating data processing with Lambda

Updating the data processing with Lambda requires you to consider that the v2 data stream is now event-based. Your initial v1 Lambda code may have been similar to the following:

```
import base64

def main_handler(event):
    # Kinesis "data" blob is base64 encoded so decode here:
    for record in event['Records']:
        payload = base64.b64decode(record["kinesis"]["data"])

        measurement = payload["measurement"]
        projectDisplayName = payload["projectDisplayName"]

        # Process the content of the measurement
        # ...
```

Since the v1 data schema is on a deprecation path, the previous Lambda code won't work with all the new data streams.

The following Python sample code will process events from Kinesis stream with the data schema v2. This code uses the new `eventType` parameter to orient the processing to the appropriate handler:

```
import base64

handlers = {
    "measurement": measurementEventHandler,
    "gatewayConnected": gatewayConnectedEventHandler,
    "gatewayDisconnected": gatewayDisconnectedEventHandler,
    "sensorConnected": sensorConnectedEventHandler,
    "sensorDisconnected": sensorDisconnectedEventHandler,
}
```

```
def main_handler(event):
    # Kinesis "data" blob is base64 encoded so decode here:
    for record in event['Records']:
        payload = base64.b64decode(record["kinesis"]["data"])

        eventType = payload["eventType"]
        if eventType not in handler.keys():
            log.info("No event handler found for the event type: {event['eventType']}")
            return

        # Invoke the appropriate handler based on the event type.
        eventPayload = payload["eventPayload"]
        eventHandler = handlers[eventType]
        eventHandler(eventPayload)

def measurementEventHandler(measurementEventPayload):
    # Handle measurement event
    projectName = measurementEventPayload["projectName"]

    # ...

def gatewayConnectedEventHandler(gatewayConnectedEventPayload):
    # Handle gateway connected event

# Other event handler functions
```

# Monitoring costs

Amazon Monitron assigns AWS–generated tags to each sensor: a project tag and a site tag. If you use AWS Cost Explorer, you can use these assigned tag values to get cost reports filtered to specific Amazon Monitron projects and sites.

**Topics**


- Conceptual overview
- Billing tag keys and tag values
- Retrieving project tag values
- Retrieving site tag values
- Activating billing tags
- Viewing cost reports


## Conceptual overview

When you set up Amazon Monitron, you create a project in which you configure and install your Amazon Monitron resources. Every project, in turn, can be linked to mutliple sites, or organized collections of assets, gateways, and sensors linked together based on either a common location or function.

Each site can contain multiple Amazon Monitron sensors, attached to multiple assets or machines, transmitting the asset data collected through multiple gateways.

While all your sites, assets, gateways, and sensors exist conveniently within one project, your Amazon Monitron setup might be more distributed in practice. For example, your company may own one project to monitor sites located in different geographical locations, or grouped together by different business use cases and needs. Or you may own multiple projects, each with its own specific configuration. Partners who integrate Amazon Monitron, may also wish to assign a project to each of their own customers

While getting an overall understanding of your Amazon Monitron costs is useful, what your business may need is a more granular understanding of the usage and costs attached to each project, location, or business use case. This may also be necessary for internal cost allocation purpose between different divisions.

In these situations, using Amazon Monitron assigned AWS–generated tags in AWS Cost Explorer can help you understand and plan your business resources better.

## Billing tag keys and tag values

Amazon Monitron uses AWS–generated tags to internally assign project and site level tag values. You can use these tags to find your projects and sites on the AWS Cost Explorer console. The tag keys are of the following format:

- **Project** – `aws:monitron:project`
- **Site** – `aws:monitron:location_level4`

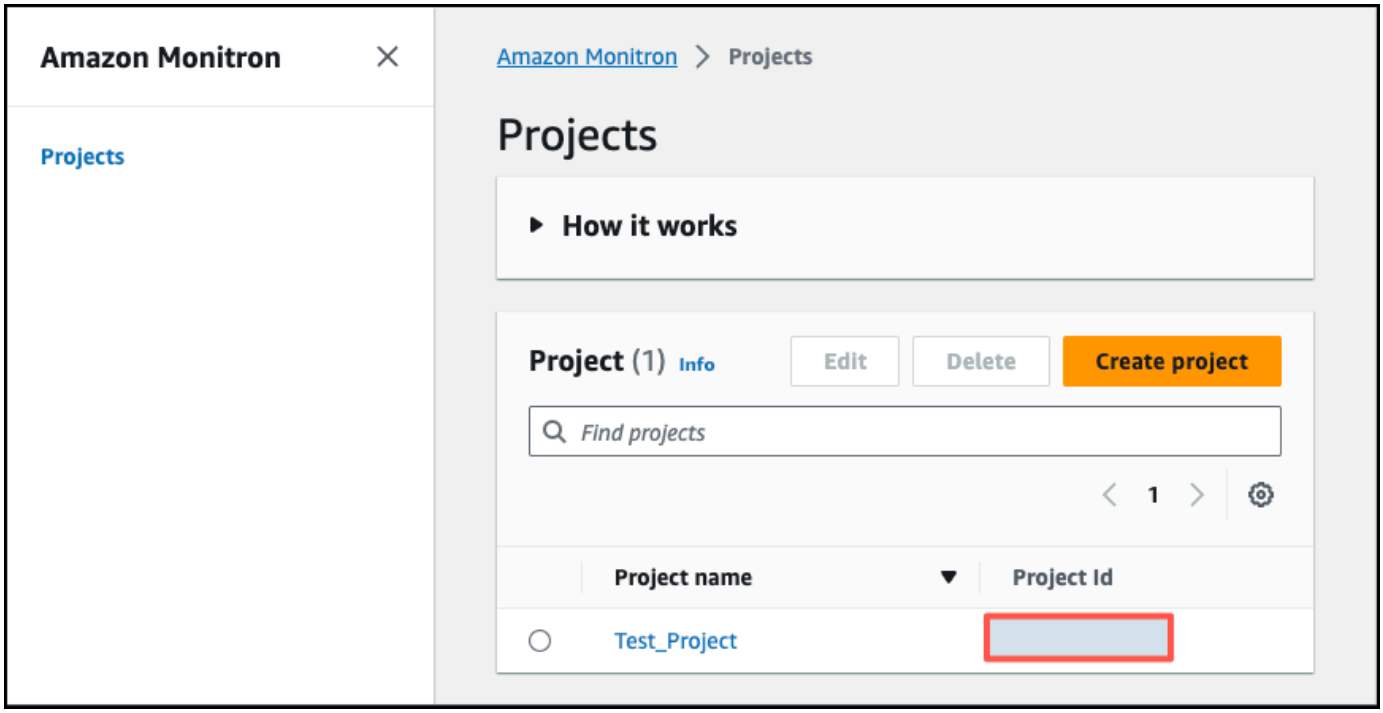
## Retrieving project tag values

You can retrieve your assigned project value using your Amazon Monitron web app. The tag value for your project is the project ID.

**To retrieve the specific tag value assigned to your Amazon Monitron 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.
5. Copy the tag value from your **Project Id**.

   You can use this project id to filter costs in AWS Cost Explorer console.

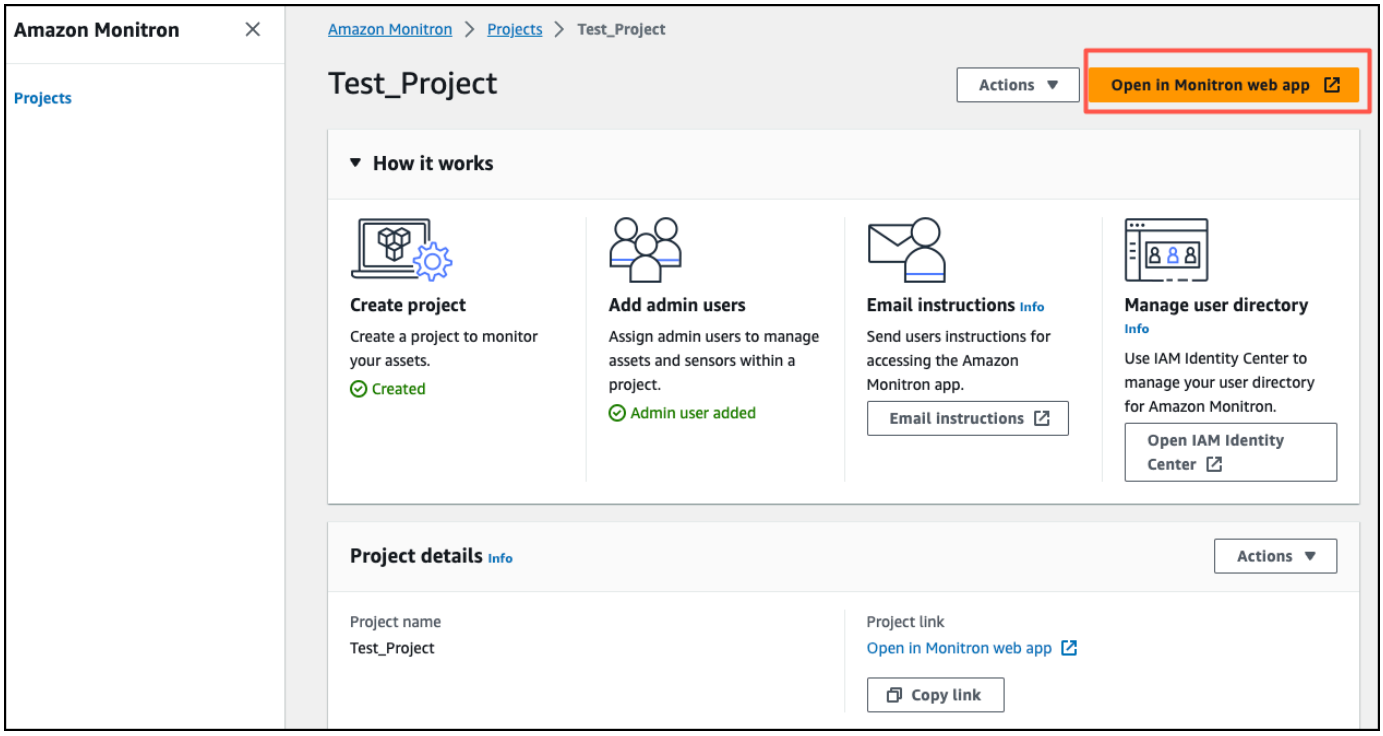
## Retrieving site tag values

You can retrieve your assigned site tag value using your Amazon Monitron web app. The tag value for your site is the Id.

**To retrieve the specific tag value assigned to your Amazon Monitron site:**

1. Open the Amazon Monitron console at https://console.aws.amazon.com/monitron.
2. Choose **Create project**.
3. If you're creating a project for the first time, follow the steps outlined in Creating a project.

   If you're choosing an existing project, from the left navigation menu, select **Projects**, and then select the project you want to create custom asset classes for.
4. From the project details page, choose **Open in Amazon Monitron web app**.




5. From the left navigation pane, choose **Sites**.

   The list of sites is displayed.




6. Choose the site that you want to get details on.
7. Copy the tag value from your **Id**.

   You can use this id to filter costs in AWS Cost Explorer console.

# Activating billing tags

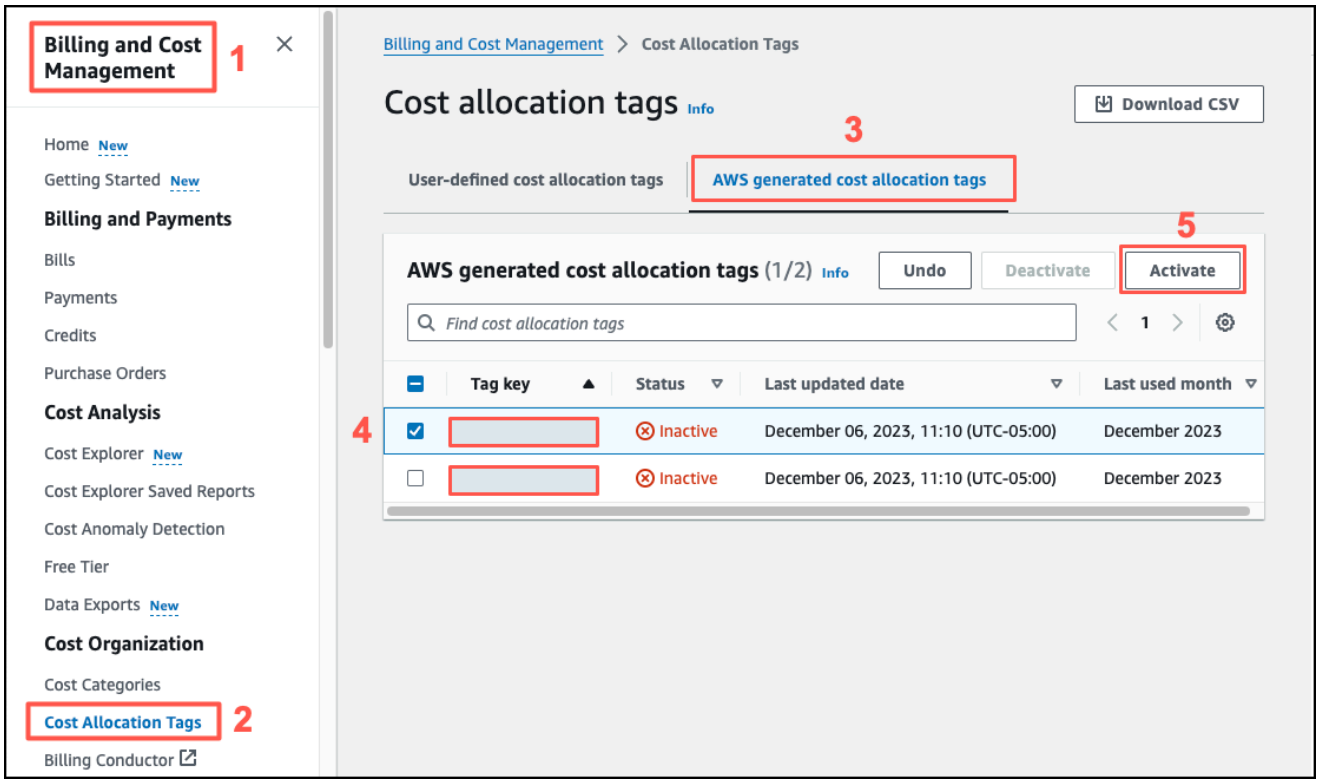
To begin using project and site level cost tracker tags, you must do the following:

1. **Prerequisite** – You must activate AWS Cost Explorer on the AWS Management Console. This requires minimal setup. We recommend you follow the steps outlined in the AWS Cost Management guide.
2. **Activate the Amazon Monitron AWS–generated tags** in your AWS billing account.

   **From your AWS Billing and Cost Management left navigation pane:**

   a. From **Cost Organization**, select **Cost allocation tags**. You will find the **AWS generated cost allocation tags** in this section.

   b. Select the tags you want to use and choose **Activate**.




> **Note**
>
> It takes up to 96 hours for the tags to be activated. The billing data starts being tagged only after the tags are active.

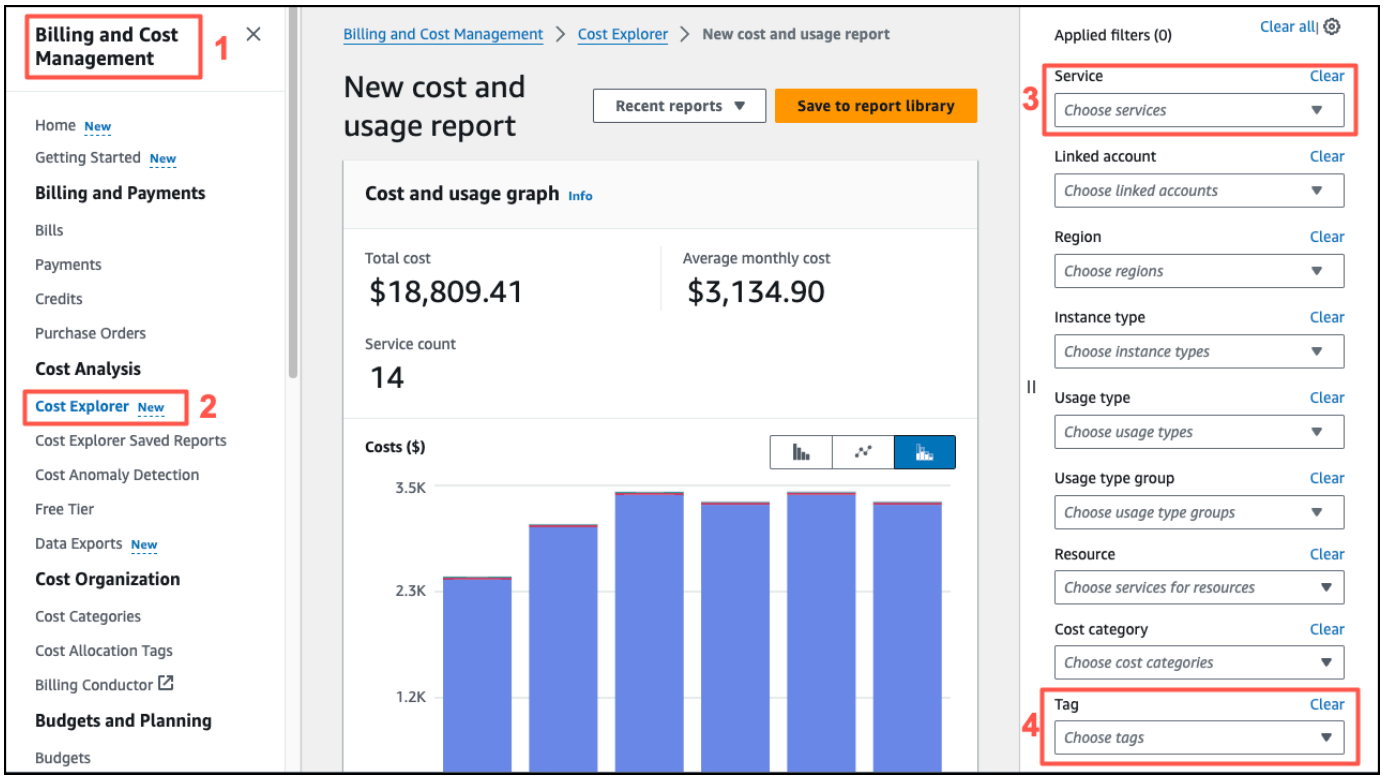
# Viewing cost reports

After your Amazon Monitron AWS generated tags have been activated and are active, you can view usage and cost reports filtered by these tags using AWS Cost Explorer on the AWS Cost Management console.

You can filter usage and cost history by choosing a tag key value pair. For example, if you want to view usage reports a particular project, you would first choose a tag value `aws:monitron:project` and then select the project id value from the options available.

**To generate cost and usage reports**

1. Open the AWS Cost Management console at https://console.aws.amazon.com/costmanagement.
2. From the left navigation pane, select **Cost Explorer**.
3. From the **New cost and usage report** page, from the right navigation menu, in **Filters**, choose Amazon Monitron as the **Service**.
4. From the right navigation menu, for **Tags** choose the assigned tag key for your project or site from the dropdown options.
5. Then, choose the Amazon Monitron assigned tag value for your project or site.



**Note**

You can save the report with the filters selected to the report library to easily review it later. You can also adjust and customize your report further, including the date range and granularity of your report.

# App settings

This section shows you how to change your Amazon Monitron app and console settings.

**Topics**


- Localization settings


# Localization settings

The Amazon Monitron app detects your device's location from your web browser or phone and uses this information to populate default settings in the app. Default settings for the Amazon Monitron include: language, date/time format, and number format (commas vs. decimals).

Languages currently supported by Amazon Monitron include:

- English
- French
- Spanish
- Portuguese (BR)

Any languages supported in the application are also supported in the console.

When a language is not available for a particular area, the Amazon Monitron app will default to English, and US units/number format. The app will detect your location once and then use these defaults until you manually change them.

## Changing localization settings

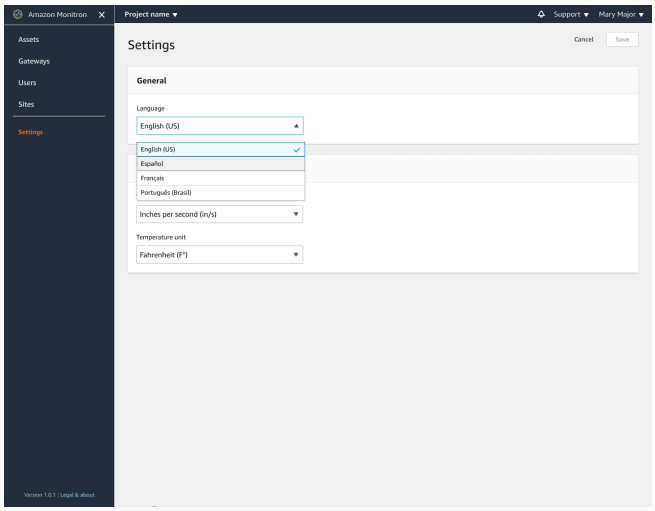
You can change your Amazon Monitron language settings for both the web and mobile apps, and the console.

**To change localization settings**

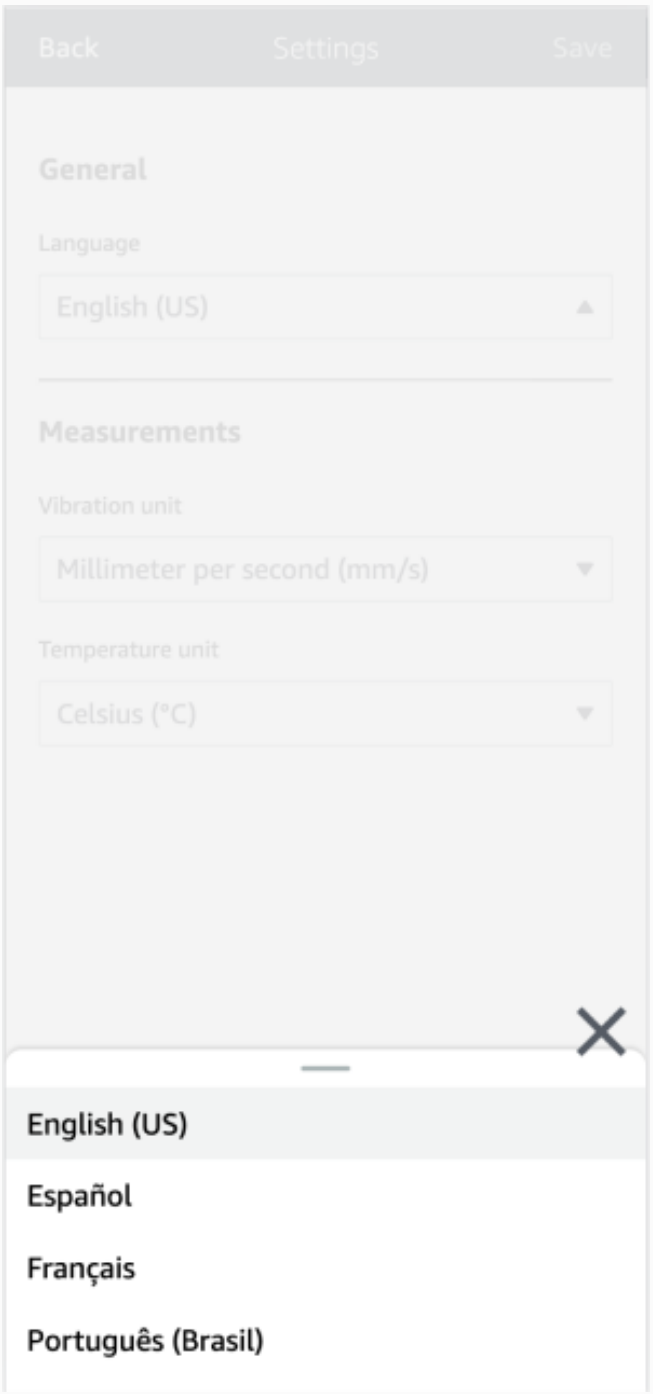
1. Update and save your language, measurement, and temperature settings in the **Settings** menu of the app.

**Important**

Any changes you make to the language or units setting will be saved locally in the browser and will be applied to any project you open in the same browser. These changes are not shared across devices.

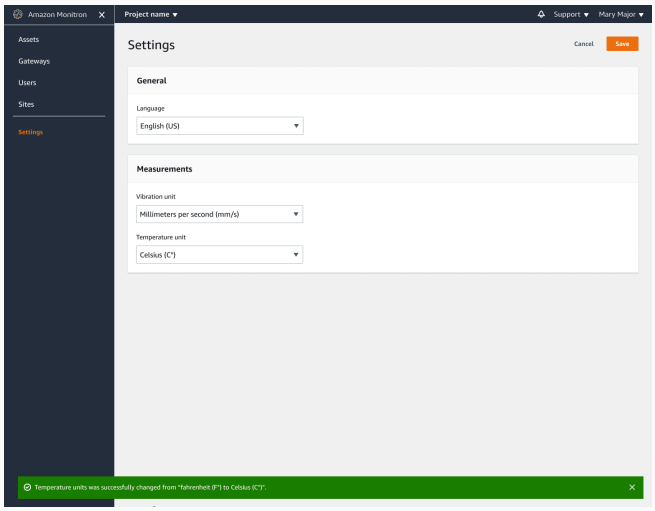



a web app view

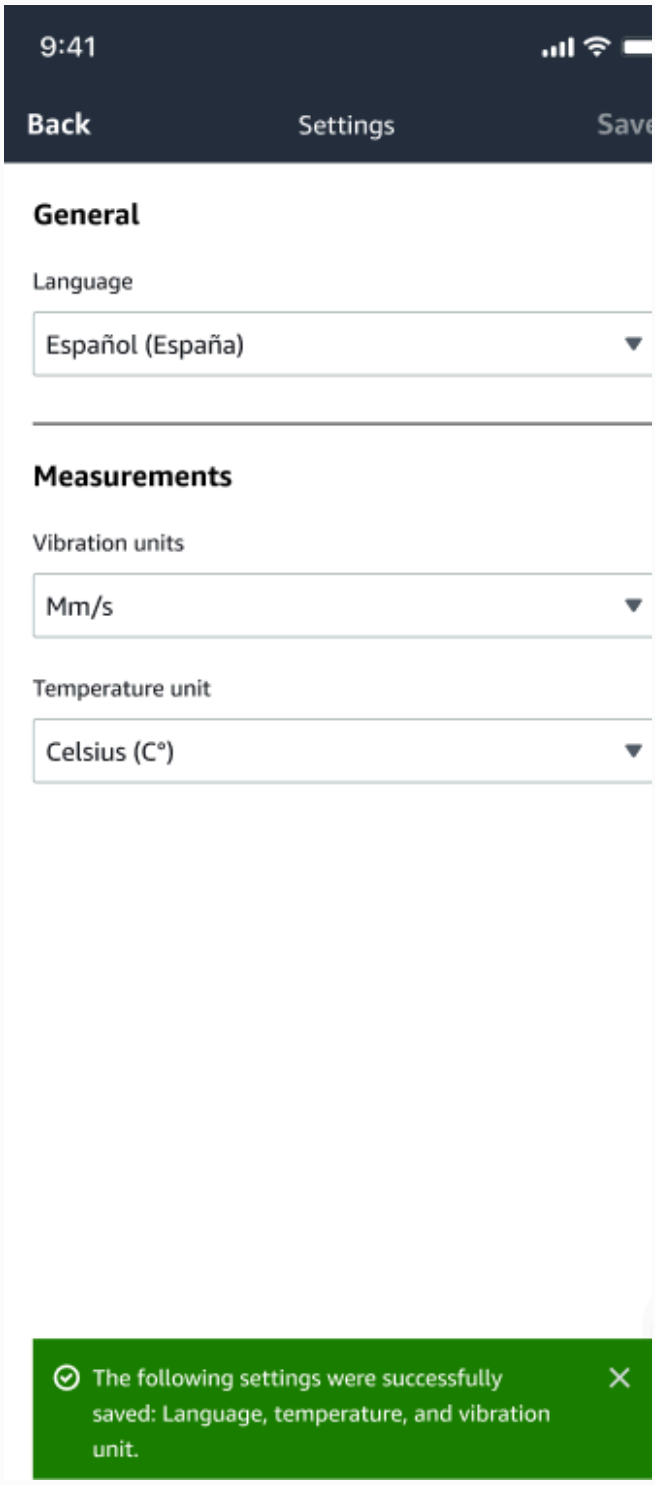



a mobile app view

2. Choose **Save**.
3. You will see the following alert banner if you change two or more settings:

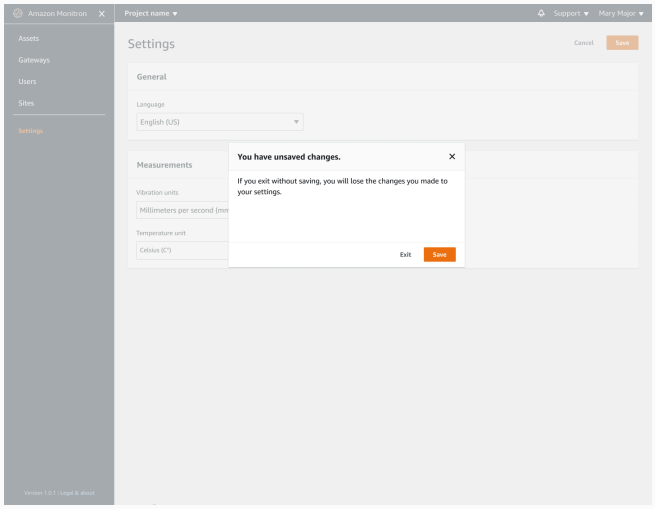



a web app view

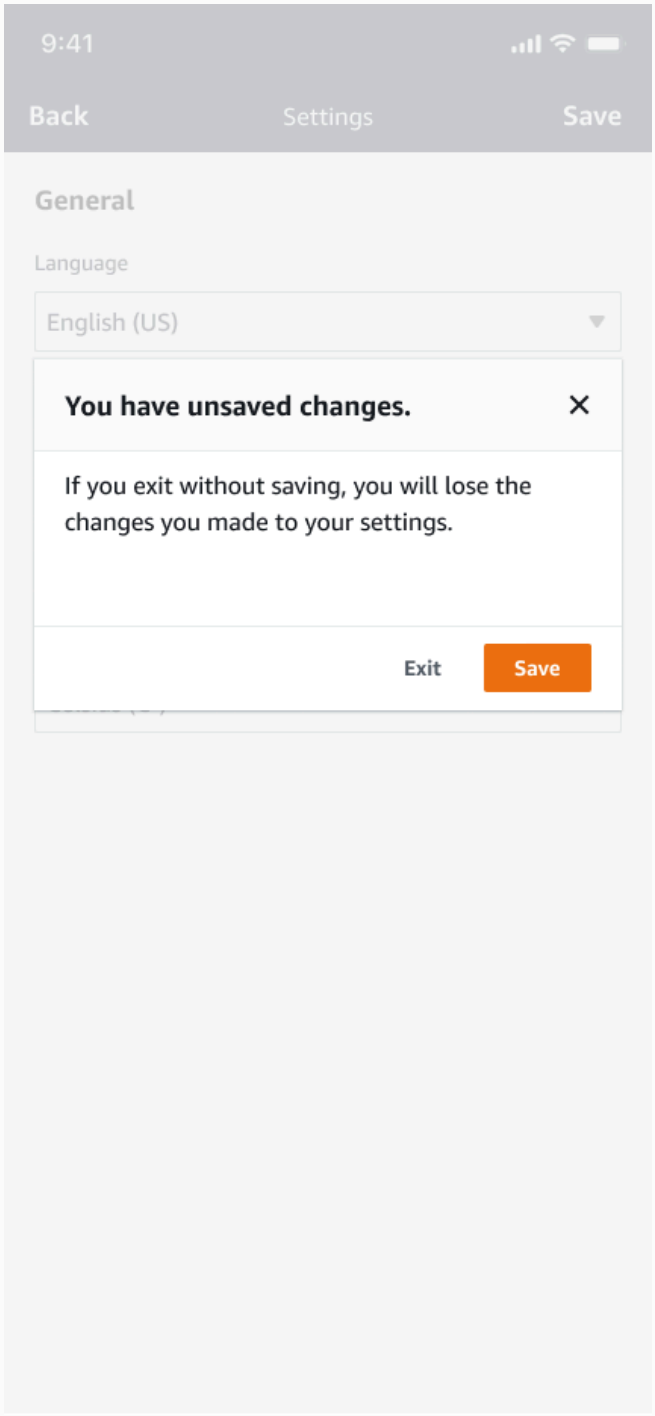



a mobile app view

4. You will see the following alert if you leave the settings menu without saving:




a web app view




a mobile app view

# 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
- Example: Amazon Monitron log file entries


## Amazon Monitron information in CloudTrail

CloudTrail is enabled for your AWS users when you create your 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
- CreateSensor
- UpdateSensor
- DeleteSensor
- CreateGateway
- DeleteGateway
- CreateSite
- UpdateSite
- DeleteSite
- CreateAsset

- UpdateAsset
- DeleteAsset
- CreateAssetStateTransition
- CreateUserAccessRoleAssociation
- UpdateUserAccessRoleAssociation
- DeleteUserAccessRoleAssociation
- FinishSensorCommissioning
- StartSensorCommissioning

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.

**Topics**

- Successful DeleteProject action

- Failed DeleteProject action (authorization error)
- Failed DeleteProject action (conflict exception error)

## 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
- Identity and Access Management for Amazon Monitron
- Logging and Monitoring in Amazon Monitron
- Compliance Validation for Amazon Monitron
- Infrastructure Security in Amazon Monitron
- Security Best Practices for Amazon Monitron


# 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 users 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*.

**Topics**

- Data at rest
- Data in transit
- AWS KMS and data encryption in Amazon Monitron

## 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.

See also ???.

## Data in transit

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

## AWS 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
- Authenticating with Identities
- Managing Access Using Policies
- How Amazon Monitron Works with IAM
- Using service-linked roles for Amazon Monitron

## 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.

**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 service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Amazon Monitron, see How Amazon Monitron Works with IAM.

**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.

## Authenticating with Identities

Authentication is how you sign in to AWS using your identity credentials. You must be *authenticated* (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

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

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

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the

recommended method to sign requests yourself, see AWS Signature Version 4 for API requests in the *IAM User Guide*.

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

**Topics**

- AWS account root user
- IAM users and Groups
- IAM Roles

## AWS account root user

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the *IAM User Guide*.

## IAM users and Groups

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

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

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see Use cases for IAM users 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. To temporarily assume an IAM role in the AWS Management Console, you can switch from a user to an IAM role (console). 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 Methods to assume a role in the *IAM User Guide*.

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

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see Create a role for a third-party identity provider (federation) in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see Permission sets in the *AWS IAM Identity Center User Guide*.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see Cross account resource access in IAM 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.
  - **Forward access sessions (FAS)** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the

principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see Forward access sessions.

- **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 Create 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 AWS 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 Use an IAM role to grant permissions to applications running on Amazon EC2 instances in the *IAM User Guide*.

## Managing Access Using Policies

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

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

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

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.

**Topics**


- Identity-Based Policies
- Other Policy Types
- Multiple Policy Types


## 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 Define custom IAM permissions with customer managed 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 Choose 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 an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a

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

- **Resource control policies (RCPs)** – RCPs are JSON policies that you can use to set the maximum available permissions for resources in your accounts without updating the IAM policies attached to each resource that you own. The RCP limits permissions for resources in member accounts and can impact the effective permissions for identities, including the AWS account root user, regardless of whether they belong to your organization. For more information about Organizations and RCPs, including a list of AWS services that support RCPs, see Resource control policies (RCPs) 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
- Amazon Monitron Resource-Based Policies
- Authorization Based on Amazon Monitron Tags
- Amazon Monitron IAM Roles

- Amazon Monitron Identity-Based Policy Examples
- Troubleshooting Amazon Monitron Identity and Access

## 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*.

### Topics

- Actions
- Resources
- Condition Keys
- Examples

### 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 IAM Identity Center (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 Actions defined by Amazon Monitron in the *IAM User Guide*. To learn with which actions and resources you can use a condition key, see Condition keys for Amazon Monitron.

#### Examples

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

### 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 give permissions to the IAM users, groups, or roles that require them. Then these users, groups, or roles can perform the 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
- Using the Amazon Monitron Console
- Example: List All Amazon Monitron Projects
- Example: List Amazon Monitron Projects Based on Tags


### Policy Best Practices

Identity-based policies 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 with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see AWS managed policies or AWS managed policies for job functions in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as AWS CloudFormation. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see Validate policies with IAM Access Analyzer in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Secure API access with MFA in the *IAM User Guide*.

For more information about best practices in IAM, see Security best practices in IAM in the *IAM User Guide*.

### Using the Amazon 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 IAM Identity Center. 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
- I Want to Allow People Outside of My AWS Account to Access My Amazon Monitron Resources

#### I Am Not Authorized to Perform an Action in Amazon Monitron

If you receive an error that you're not authorized to perform an action, your policies must be updated to allow you to perform the action.

The following example error occurs when the `mateojackson` IAM user tries to use the console to view details about a fictional *`my-example-widget`* resource but doesn't have the fictional `monitron:`*`GetWidget`* permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 monitron:GetWidget on resource: my-example-widget
```

In this case, the policy for the `mateojackson` user must be updated to allow access to the *`my-example-widget`* resource by using the `monitron:`*`GetWidget`* action.

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

#### I Want to 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.
- 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 Cross account resource access in IAM in the *IAM User Guide*.

## Using service-linked roles for Amazon Monitron

Amazon Monitron 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 Monitron. Service-linked roles are predefined by Amazon Monitron 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 Monitron easier because you don't have to manually add the necessary permissions. Amazon Monitron defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon Monitron 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.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have **Yes** in the **Service-linked roles** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

### Topics

- Service-linked role permissions for Amazon Monitron
- Creating a service-linked role for Amazon Monitron
- Editing a service-linked role for Amazon Monitron

- Deleting a service-linked role for Amazon Monitron
- Supported regions for Amazon Monitron service-linked roles
- AWS managed policies for Amazon Monitron
- Amazon Monitron updates to AWS managed policies

## Service-linked role permissions for Amazon Monitron

Amazon Monitron uses the service-linked role named **AWSServiceRoleForMonitron[_{SUFFIX}]** – Amazon Monitron uses AWSServiceRoleForMonitron to access other AWS services, including Cloudwatch Logs, Kinesis Data Streams, KMS keys, and SSO. For more information about the policy, see AWSServiceRoleForMonitronPolicy in the *AWS Managed Policy Reference Guide*

The AWSServiceRoleForMonitron[_{SUFFIX}] service-linked role trusts the following services to assume the role:

- `monitron.amazonaws.com` or `core.monitron.amazonaws.com`

The role permissions policy named MonitronServiceRolePolicy allows Amazon Monitron to complete the following actions on the specified resources:

- Action: Amazon CloudWatch Logs `logs:CreateLogGroup`, `logs:CreateLogStream` and `logs:PutLogEvents` on the CloudWatch log group, log stream, and log events under /aws/monitron/* path

The role permissions policy named MonitronServiceDataExport-KinesisDataStreamAccess allows Amazon Monitron to complete the following actions on the specified resources:

- Action: Amazon Kinesis `kinesis:PutRecord`, `kinesis:PutRecords`, and `kinesis:DescribeStream` on the Kinesis data stream specified for live data export.
- Action: Amazon AWS KMS `kms:GenerateDataKey` for the AWS KMS key used by the specified Kinesis data stream for live data export
- Action: Amazon IAM `iam:DeleteRole` to delete the service-linked role itself when not used

The role permissions policy named AWSServiceRoleForMonitronPolicy allows Amazon Monitron to complete the following actions on the specified resources:

- Action: IAM Identity Center `sso:GetManagedApplicationInstance`, `sso:GetProfile`, `sso:ListProfiles`, `sso:AssociateProfile`, `sso:ListDirectoryAssociations`, `sso:ListProfileAssociations`, `sso-directory:DescribeUsers`, `sso-directory:SearchUsers`, `sso:CreateApplicationAssignment`, and `sso:ListApplicationAssignments` to access IAM Identity Center users associated with the project

> **Note**
>
> Add `sso:ListProfileAssociations` to allow Amazon Monitron to list associations with the application instance underlying the Amazon Monitron Project.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the *IAM User Guide*.

## Creating a service-linked role for Amazon Monitron

You don't need to manually create a service-linked role. When you enable a feature requiring your permissions to call other AWS services on your behalf in Amazon Monitron in the AWS Management Console, Amazon Monitron creates the service-linked role for you.

## Editing a service-linked role for Amazon Monitron

Amazon Monitron does not allow you to edit the AWSServiceRoleForMonitron[_{SUFFIX}] 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 Monitron

You don't need to manually delete the AWSServiceRoleForMonitron[_{SUFFIX}] role. When you delete a Amazon Monitron project that you created through Amazon Monitron in the AWS Management Console, Amazon Monitron cleans up the resources and deletes the service-linked role for you.

You can also use the IAM console, the AWS CLI or the AWS API to manually delete the service-linked role. To do this, you must first manually clean up the resources for your service-linked role and then you can manually delete it.

> **Note**
>
> If the Amazon Monitron 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 Monitron resources used by the AWSServiceRoleForMonitron[_{SUFFIX}]**

- Delete Amazon Monitron projects using this service-linked role.

**To manually delete the service-linked role using IAM**

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForMonitron[_{SUFFIX}] service-linked role. For more information, see Deleting a service-linked role in the *IAM User Guide*.

## Supported regions for Amazon Monitron service-linked roles

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

Amazon Monitron does not support using service-linked roles in every region where the service is available. You can use the AWSServiceRoleForMonitron[_{SUFFIX}] role in the following regions.

| Region name | Region identity | Support in Amazon Monitron |
|---|---|---|
| US East (N. Virginia) | us-east-1 | Yes |
| US East (Ohio) | us-east-2 | No |
| US West (N. California) | us-west-1 | No |
| US West (Oregon) | us-west-2 | No |

| Region name | Region identity | Support in Amazon Monitron |
|---|---|---|
| Asia Pacific (Mumbai) | ap-south-1 | No |
| Asia Pacific (Osaka) | ap-northeast-3 | No |
| Asia Pacific (Seoul) | ap-northeast-2 | No |
| Asia Pacific (Singapore) | ap-southeast-1 | No |
| Asia Pacific (Sydney) | ap-southeast-2 | Yes |
| Asia Pacific (Tokyo) | ap-northeast-1 | No |
| Canada (Central) | ca-central-1 | No |
| Europe (Frankfurt) | eu-central-1 | No |
| Europe (Ireland) | eu-west-1 | Yes |
| Europe (London) | eu-west-2 | No |
| Europe (Paris) | eu-west-3 | No |
| South America (São Paulo) | sa-east-1 | No |
| AWS GovCloud (US) | us-gov-west-1 | No |

## AWS managed policies for Amazon Monitron

You can attach AmazonMonitronFullAccess to your IAM entities. This policy grants *administrative* permissions that allow access to all Amazon Monitron resources and operations.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "monitron.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "monitron:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:ListKeys",
                "kms:DescribeKey",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "monitron.*.amazonaws.com"
                    ]
                },
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        },
        {
            "Sid": "AWSSSOPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "ds:DescribeDirectories",
```

```
                "ds:DescribeTrusts"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:DescribeStream",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:GetLogEvents",
                "logs:CreateLogGroup"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/monitron/*"
        },
    ]
}
```

## Amazon Monitron updates to AWS managed policies

View details about updates to AWS managed policies for Amazon Monitron since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Amazon Monitron document history page.

| Change | Description | Date |
| --- | --- | --- |
| AWSServiceRoleForMonitronPolicy - Update to an existing policy | Added `sso:CreateApplicationAssignment` and `sso:ListApplicationAssignments` to role permissions policy. | September 30, 2024 |

| Change | Description | Date |
| --- | --- | --- |
| AmazonMonitronFullAccess - Update to an existing policy | Amazon Monitron added permissions to describe and list Kinesis Data Streams, and describe get, and create CloudWatch log groups, log streams, and log events.<br><br>You must use these permissions to use the Amazon Monitron console to display information about Kinesis Data Streams and CloudWatch Logs. | June 8, 2022 |

# 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.

# Compliance Validation for Amazon Monitron

To learn whether an AWS service is within the scope of specific compliance programs, see AWS services in Scope by Compliance Program and choose the compliance program that you are interested in. 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 Compliance & Governance – These solution implementation guides discuss architectural considerations and provide steps for deploying security and compliance features.
- HIPAA Eligible Services Reference – Lists HIPAA eligible services. Not all AWS services are HIPAA eligible.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- AWS Customer Compliance Guides – Understand the shared responsibility model through the lens of compliance. The guides summarize the best practices for securing AWS services and map the guidance to security controls across multiple frameworks (including National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI), and International Organization for Standardization (ISO)).
- 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. Security Hub uses security controls to evaluate your AWS resources and to check your compliance against security industry standards and best practices. For a list of supported services and controls, see Security Hub controls reference.
- Amazon GuardDuty – This AWS service detects potential threats to your AWS accounts, workloads, containers, and data by monitoring your environment for suspicious and malicious activities. GuardDuty can help you address various compliance requirements, like PCI DSS, by meeting intrusion detection requirements mandated by certain compliance frameworks.
- 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 AWS global network security. For information about AWS security services and how AWS protects infrastructure, see AWS Cloud Security. To design your AWS environment using the best practices for infrastructure security, see Infrastructure Protection in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access Amazon Monitron through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). 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 IAM Identity Center (IAM Identity Center) 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.

# Troubleshooting Amazon Monitron device issues

If you have problems with one of your Amazon Monitron devices, use these suggestions to troubleshoot the problem. Then, if you're still having trouble, contact AWS Support.

> **Note**
>
> We recommend Safari as a default browser for iOS and Chrome as a default browser for Android.

**Topics**


- Troubleshooting Issues with Amazon Monitron Sensors
- Troubleshooting issues with Amazon Monitron gateways


# Troubleshooting Issues with Amazon Monitron Sensors

As a completely self-contained unit, there aren't many things that are likely to go wrong with a sensor. However, some issues can still occur.

**Topics**


- If you can't commission your sensors
- If your sensor is offline
- If your sensor falls off


## If you can't commission your sensors

Consider the following questions.

- **Does the mobile phone running the Amazon Monitron App have a stable internet connection?**

  For commissioning a sensor, the mobile phone running the Amazon Monitron App should have internet connectivity.

- **Are you holding your smartphone close to the sensor?**



At the moment of commissioning, your phone should be within two centimeters of the sensor. Don't move your phone while the sensor is being commissioned.

- **Does your smartphone have NFC activated?**

  Some iOS devices require that NFC Tag Reader be manually turned on in Control Center. To see if your device is one of them, check the iPhone User Guide.

- **Are you holding your NFC antenna close to the sensor?**

  On an iPhone, the NFC antenna is close to the top of the device. On an Android device, it could be in a different location. Check the documentation for Samsung, Google Pixel, or your device's manufacturer.

- **Does the commissioning progress bar show up? (Android only)**



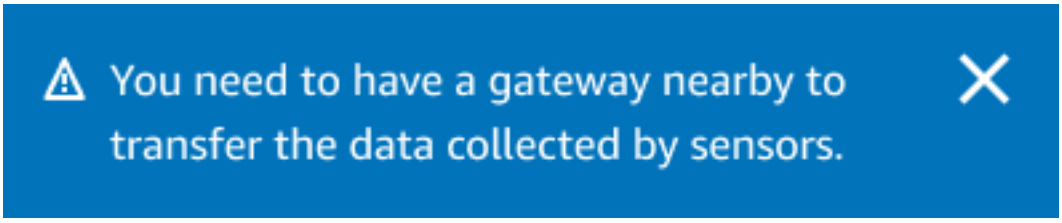

If the commissioning progress bar doesn't show up (Android only), or resets to the beginning, then the NFC communication between the sensor and your smartphone is weak or can't be established. Move your smartphone around to try and establish the NFC connection. Smartphones often have different locations for transmitting NFC, depending on the brand. Check the hardware specifications of your smartphone and tap the sensor specifically with that part of your phone. Confirm that NFC is turned on and broadcasting.

- **Do you get an error saying that the sensor is already in use?**

  Delete the sensor from its previous asset or position, and then retry the commissioning process. If that doesn't work, try and commission another sensor that is not currently in use.

## If your sensor is offline

Once a sensor has been paired to an asset, Amazon Monitron will make two attempts (over the course of 30 seconds) to take the initial measurement. If neither of those attempts is successful, then an alert like the one below will appear in the app.




If your sensor has stopped sending data, try the following:

- Try taking a one-time measurement. If you can do so, then the sensor is working. If you cannot, then the sensor is not working, and may have run out of battery power. Replace it with a new sensor.
- Confirm that an available gateway is within range. Amazon Monitron sensors and gateways communicate using Bluetooth Low Energy (BLE), with a typical range of 20 to 30 meters. In a completely open space, a sensor and a gateway may communicate with each other at greater distances.
- Check for obstacles. Concrete walls and metal objects attenuate the signals.
- Check for signal interference. The Bluetooth signal that sensors and gateways use to communicate occupies the 2.4GHz ISM (industrial, scientific and medical) band. Other devices that may use that band include wireless headsets and mice, wireless cameras, microwave ovens, and garage door openers.
- If the measurement action starts (you see a loading bar), but does not complete, try to retake the measurement. If the same thing happens again, try to delete the sensor and recommission it.
- If the measurement action fails, or you are not able to commission the sensor, contact customer support.

## If your sensor falls off

Re-mount it.

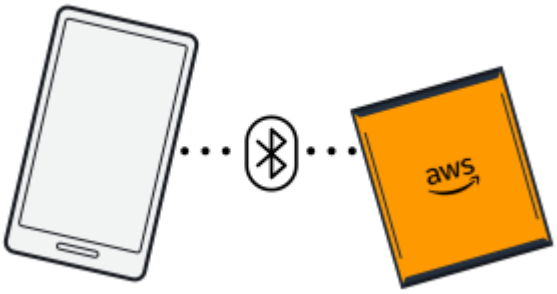
# Troubleshooting issues with Amazon Monitron gateways

**Topics**

- If your mobile app can't pair with the gateway
- If commissioning the gateway fails
- If your gateway goes offline

# If your mobile app can't pair with the gateway

If you choose **Add gateway** in your mobile app, but the app can't find the gateway, try the following.




Bluetooth pairing with a Wi-Fi gateway



Bluetooth pairing with an Ethernet gateway.

- **Make sure that the gateway is turned on.**

  Check the lights on the front of the gateway. If at least one of them is on, then the gateway has power. If the gateway has no power, check the following:

  - Is the power cord firmly attached to the back of the gateway and the power outlet?
  - Is the power outlet functioning properly?
  - Is the gateway power cable working? To test this, try using the cable with another gateway.
  - Is the outlet where the cable plugs into the gateway clean, with no debris stuck inside? Be sure to check the outlet in the gateway and the connecting end of the cable.
- **Make sure that the gateway is in commissioning mode.**

  See Commissioning a Wi-Fi gateway or Commissioning an Ethernet gateway.
- **Make sure your smartphone's Bluetooth is working.**
  - Try switching it off and on. If that doesn't help, restart your phone and check again.
  - Are you within your smartphone's Bluetooth range? Bluetooth range is typically less than 10 meters.
  - Is there anything that might be interfering electronically with the Bluetooth signal? See If your sensor is offline.

If none of these actions resolves the issue, try the following:

- Log out of the mobile app and restart it.
- Reset your Wi-Fi gateway or reset your Ethernet gateway.

## If commissioning the gateway fails

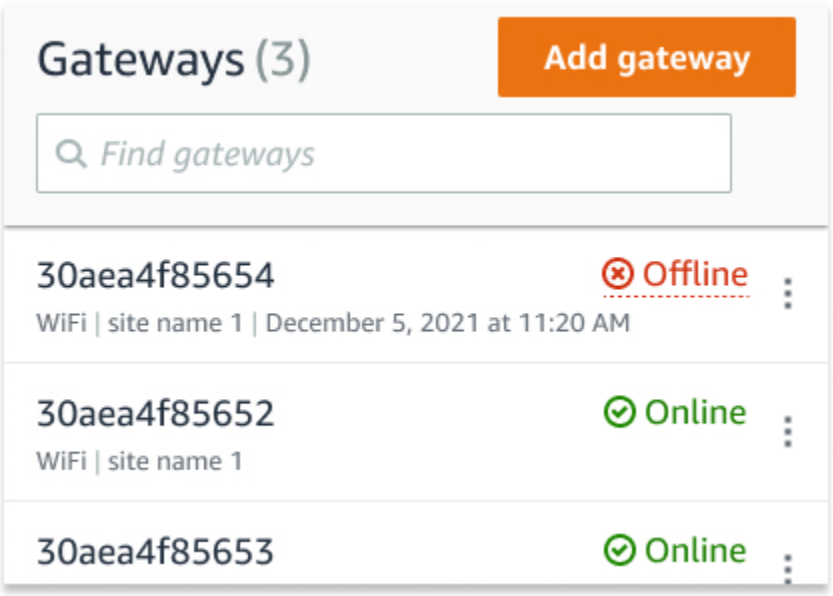
If the Amazon Monitron gateway commissioning process fails, try the following:

- Check that the mobile phone running Amazon Monitron App has internet connectivity.
- If commissioning of a Wi-Fi gateway fails, try commissioning it using a mobile hotspot provided by your mobile device. If that succeeds, it suggests a configuration issue with the Wi-Fi network or in firewall settings.

## If your gateway goes offline

Your mobile or web app may tell you that your gateway is offline, or not connected to the network. In such cases, try the following:

- If you recently added the gateway to your configuration, wait for its status to update. A newly commissioned gateway may take up to 20 seconds to go online.
- Be sure that you aren't trying to configure a Wi-Fi gateway with static IPs. The Wi-Fi gateway does not currently support static IPs. However, you can configure your network to always assign the same IP address to the same device.
- Make sure that your firewall is not blocking the gateway. Amazon Monitron gateways use TCP port 8883. You must allow connections to TCP port 8883 for amazonaws.com subdomains in order to provide firewall access to Amazon Monitron gateways.
- Confirm that the issue is not network congestion. There are two ways in which Amazon Monitron may notify you that a gateway is offline:
  - When looking at information about your gateways in the mobile or web app, you may notice that a gateway is listed as offline.




The timestamp for an offline gateway marks the last time Amazon Monitron recieved a signal from that gateway.

In this case, you may not have received a notification about the gateway's offline status. Amazon Monitron will not issue a notification every single time a gateway appears to be offline. A newly commissioned gateway is considered offline until it connects to the internet. A gateway on a congested network is considered offline if Amazon Monitron hasn't heard from that gateway in 15 minutes.

- Confirm that you're not dealing with a newly commissioned gateway or a newly paired sensor. If so, wait an hour. Sensors send data once per hour. If you don't want to wait, you can take a one-time measurement.
- Confirm that your gateway is connected to a power source. If it is, unplug the gateway and then plug it back in.
- If it's a Wi-Fi gateway, check the Wi-Fi connection. If the password for the Wi-Fi network has been changed since the gateway was added, it won't be able to connect. To reconnect, you'll have to delete the gateway and add it again, connecting to the Wi-Fi network using the new password. For more information about how to add a gateway, see Commissioning a Wi-Fi gateway or Commissioning an Ethernet gateway.
- If it's an Ethernet gateway, check the network configuration.
- Delete the gateway using the Amazon Monitron mobile app, do a factory reset of the gateway, and then install the gateway again. For more information, see Resetting the Wi-Fi gateway to factory settings or Resetting the Ethernet gateway to factory settings.

If none of these suggestions helps to get your Amazon Monitron device working again, contact AWS Support.

# Amazon Monitron devices

Amazon Monitron Starter Kits, sensors, and gateways are available for purchase at Amazon.com or Amazon Business. Amazon Monitron devices are available in the US, the UK, and the EU.

# Quotas in Amazon Monitron

You can request an increase for 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. You can also contact your IT Manager for assistance with requesting a quota increase.

## Supported Regions

Amazon Monitron is currently supported in the following regions:

- US East (N. Virginia): us-east-1
- Europe (Ireland): eu-west-1
- Asia Pacific (Sydney): ap-southeast-2

## Quotas

All Amazon Monitron operations have the following quotas.

| Description | Quota |
|---|---|
| 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 |
| Maximum number of custom classes per project | 25 |
| Maximum number of positions per custom class | 500 |

# Document history for the Amazon Monitron User Guide

- **Latest documentation update:** Oct 31, 2024

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

| Change | Description | Date |
| --- | --- | --- |
| Amazon Monitron is no longer open to new customers . Existing customers can continue to use the service as normal. For capabilities similar to Amazon Monitron, see our blog post. | Amazon Monitron is no longer open to new customers . Existing customers can continue to use the service as normal. For capabilities similar to Amazon Monitron, see our blog post. | October 31, 2024 |
| Amazon Monitron will no longer be open to new customers starting October 31, 2024. If you would like to use the service, sign up prior to that date. Existing customers can continue to use the service as normal. For capabilities similar to Amazon Monitron, see our blog post. | Amazon Monitron will no longer be open to new customers starting October 31, 2024. If you would like to use the service, sign up prior to that date. Existing customers can continue to use the service as normal. For capabilities similar to Amazon Monitron, see our blog post. | October 1, 2024 |
| Updated service-linked role policy | Added `sso:CreateApplicationAssignment` and `sso:ListApplicationAssignments` to role permissions policy. | September 30, 2024 |

| | | |
|---|---|---|
| User management | You can view and manage user assignments and permissions as an admin across a project. See Managing users for more details. | March 19, 2024 |
| Moving assets between sites | You can move Amazon Monitron assets between sites. See Moving an asset for more details. | March 19, 2024 |
| Amazon Monitron gateway updates | You can now retrieve Amazon Monitron gateway MAC address details by scanning device QR codes. See Retrieving MAC address details for Ethernet Gateways and Retrieving MAC address details for Wi-Fi Gateways for more details. | February 22, 2024 |
| Unmuting ISO alerts | You can now unmute ISO alerts (alarms and warnings) . See Muting and unmuting alerts for more details. | January 31, 2024 |
| Static IP address for gateways | Amazon Monitron now supports new static IP addresses for gateways. See Securing your network for more details. | January 25, 2024 |

| | | |
|---|---|---|
| Amazon Monitron billing monitoring updates | You can now use Amazon Monitron AWS–generated tags to monitor billing. See Monitoring costs for more details. | December 13, 2023 |
| Amazon Monitron custom machine classes | You can now create custom machine classes in Amazon Monitron. See Creating custom classes for more information. | December 7, 2023 |
| Amazon Monitron safety updates | Updated Amazon Monitron sensor safety information. | November 26, 2023 |
| Amazon Monitron IT Manager's Guide deprecated | Amazon Monitron IT Manager's Guide has been merged into the Amazon Monitron Amazon Monitron User Guide. | October 24, 2023 |
| Amazon Monitron CloudTrail event name updates | Amazon Monitron CloudTrail event names updated. See Amazon Monitron information in CloudTrail for more details. | October 2, 2023 |
| New region supported | Amazon Monitron is now available in the Asia Pacific (Sydney) Region. For all supported Regions, see Supported Regions. | August 17, 2023 |

| | | |
|---|---|---|
| View gateway details in mobile app | You can now view your Amazon Monitron gateway details from the mobile app. See Viewing Ethernet gateway details and Viewing Wi-Fi gateway details. | July 20, 2023 |
| Switching between projects | You can now switch between your Amazon Monitron projects in your AWS account. See Switching between projects for more details. | June 15, 2023 |
| Edit gateway name | You can now edit gateway names for your Amazon Monitron gateways. See Editing ethernet gateway and Editing Wi-Fi gateway for more details. | June 15, 2023 |
| Create position from web app | You can now create a position for your Amazon Monitron sensor from the web app. See Adding a sensor position. | June 15, 2023 |
| Sensor battery life status | Amazon Monitron now displays sensor battery states to help you keep track of sensor health. See Sensor battery status for more details. | May 22, 2023 |
| Scatter plot view for sensor measurements | You can now view your Amazon Monitron sensor data in scatter plot format. | May 22, 2023 |

| | | |
|---|---|---|
| Editing machine class updates | Each Amazon Monitron sensor can now be assigned a machine class. | May 22, 2023 |
| Added Kinesis data export schema v2 | Added Amazon Monitron Kinesis data export schema v2 and v1 deprecation instructions. | April 4, 2023 |
| Vibration ISO image updates | Updated several images to show new measurement functionality and filtering tools in the mobile and web UI. | March 16, 2023 |
| Sensor position info added | Overview of how to identify a sensor's position details. | January 24, 2023 |
| In-app updates | Added a note and updates on the in-app update feature, which users should monitor to be sure they have the latest Amazon Monitron features. | December 15, 2022 |
| Edit gateway name | Users have the ability to edit a gateway name once it's created. | December 15, 2022 |
| Device offline | This update explains the behavior of sensors that go offline. | December 15, 2022 |
| Updated Kinesis data export instructions | Updated Kinesis configurations and settings instructions. | December 5, 2022 |

| | | |
|---|---|---|
| Updated service-linked role policy | Added `sso:ListProfileAssociations` to role permissions policy. | September 30, 2022 |
| Networking information added | You can now read details about how Amazon Monitron connects to your local network. | July 5, 2022 |
| Web app supported | Amazon Monitron now has a web app. | November 18, 2021 |
| Ethernet gateways added | Amazon Monitron Ethernet gateways can now be purchased and integrated with the existing Amazon Monitron system. | September 7, 2021 |
| New region supported | Amazon Monitron is now available in the Europe (Ireland) Region. For all supported Regions, see Supported Regions . | May 5, 2021 |
| One-off downloads supported | You can download your data to Amazon S3 using either the CLI or the console. | January 21, 2021 |
| New guide and service | This is the first release of the Amazon Monitron User Guide and service. | December 1, 2020 |