aws

ユーザーガイド

Amazon Monitron

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

Amazon Monitron: ユーザーガイド

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

Amazon の商標およびトレードドレスはAmazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

.... x
とは Amazon Monitron 1
Amazon Monitron デバイス 1
Amazon Monitron ソフトウェア 3
の利点 Amazon Monitron 7
Amazon Monitron の料金 7
関連リソース 7
を初めてお使いになる方 Amazon Monitron向けの情報 8
の Amazon Monitron 仕組み 11
Amazon Monitron ワークフロー 11
Amazon Monitron の概念 12
Amazon Monitron コンポーネント 16
Amazon Monitron アラート 22
入門 25
プロジェクトのセットアップ 25
ステップ 1: アカウントを作成する 26
ステップ 2: プロジェクトを作成する 28
ステップ 3: 管理者ユーザーを作成する 29
ステップ 4: (オプション) Amazon Monitron ユーザーをプロジェクトに追加する 30
ステップ 5: ユーザーをプロジェクトに招待する 34
アセットの追加とデバイスの設置 35
ステップ 1: ゲートウェイを追加する 36
ステップ 2: アセットを追加する 41
ステップ 3: センサーを取り付ける 48
ステップ 4: センサーをアセットにペアリングする 50
警告とアラートの把握 53
ステップ 1: アセットの健全性を把握する 54
ステップ 2: アセットの状態を表示する 58
ステップ 3: 機械の異常を表示して確認する 60
ステップ 4: 機械の異常を解決する 64
ステップ 5: アラートのミュートとミュート解除 64
プロジェクト 76
プロジェクトの作成 76
プロジェクトでのタグの使用 77

プロジェクト作成時のタグの追加 78
プロジェクト作成後のタグの追加 80
タグの変更または削除 81
プロジェクトの更新 82
プロジェクトの切り替え 83
ウェブアプリでのプロジェクトの切り替え 83
モバイルアプリでのプロジェクトの切り替え 86
プロジェクトの削除 90
プロジェクトのその他のタスク 91
サイト 93
プロジェクトのサイトへの整理 93
プロジェクトやサイトへのアクセスの制御 94
サイトの作成 94
モバイルアプリを使用してサイトを追加するには 94
ウェブアプリを使用して新しいサイトを追加するには 95
サイト名の変更 96
モバイルアプリを使用してサイト名を変更するには 97
ウェブアプリを使用してサイト名を変更するには 97
サイトの削除 97
モバイルアプリを使用してサイトを削除するには 98
ウェブアプリを使用してサイトを削除するには 99
モバイルアプリを使用したプロジェクトとサイト間の移動 99
プロジェクトレベルからサイトレベルへの切り替え 100
サイトレベルからプロジェクトレベルへの切り替え 100
ゲートウェイ 102
イーサネットゲートウェイ 102
イーサネットゲートウェイの LED ライトの読み取り 104
イーサネットゲートウェイの取り付けと設置 106
イーサネットゲートウェイのコミッショニング 112
イーサネットゲートウェイ検出のトラブルシューティング 116
..... 117
イーサネットゲートウェイの工場出荷時設定へのリセット 118
ゲートウェイのリストの表示 119
イーサネットゲートウェイの詳細の表示 120
イーサネットゲートウェイの名前の編集 125
インターネットゲートウェイの削除 130

MAC アドレスの詳細の取得 131
Wi-Fi ゲートウェイ 136
Wi-Fi ゲートウェイの LED ライトの読み取り 137
Wi-Fi ゲートウェイの取り付けと設置 139
Wi-Fi ゲートウェイのコミッショニング 147
Wi-Fi ゲートウェイ検出のトラブルシューティング 149
Bluetooth ペアリングのトラブルシューティング 151
Wi-Fi ゲートウェイの工場出荷時設定へのリセット 151
ゲートウェイのリストの表示 152
Wi-Fi ゲートウェイの詳細の表示 154
Wi-Fi ゲートウェイの名前の編集 158
Wi-Fi ゲートウェイの削除 163
MAC アドレスの詳細の取得 164
アセット 170
アセットクラスの作成 171
カスタムクラスの作成 172
カスタムクラスの更新 176
カスタムクラスの削除 179
アセットの管理 183
アセットのリストの表示 185
アセットリストを開くには。 185
アセットの追加 185
モバイルアプリを使用したアセットの追加 42
ウェブアプリを使用したアセットの追加 46
アセット名の変更 191
モバイルアプリでアセット名を変更するには 191
ウェブアプリでアセット名前を変更するには 191
アセットの移動 192
ウェブアプリでアセットを移動するには 193
モバイルアプリでアセットを移動するには 195
アセットの削除 201
アセットを削除するには 201
センサー 203
センサーの配置 203
センサーを取り付ける 207
センサーのポジションを追加する 208

ウェブアプリでセンサーのポジションを追加するには 209
モバイルアプリでセンサーのポジションを追加するには 210
センサーをアセットにペアリングする 216
センサーをアセットにペアリングするには 216
センサーのポジション名を変更する 222
モバイルアプリでセンサーのポジション名を変更する 223
ウェブアプリでセンサーのポジション名を変更する 223
機械のクラスを編集する 224
モバイルアプリで機械のクラスを編集するには 225
ウェブアプリで機械のクラスを編集するには 231
ポジションの詳細ページから機械クラスを編集するには 232
センサーを削除する 232
モバイルアプリでセンサーを削除するには 233
ウェブアプリでセンサーを削除するには 234
センサーポジションを削除する 235
モバイルアプリでセンサーポジションを削除するには 235
ウェブアプリでセンサーポジションを削除するには 236
センサーの詳細を理解する 237
センサーの詳細を表示する 238
センサーの接続ステータス 240
センサーのバッテリーステータス 241
センサーポジションを識別する 243
ペアリングされたセンサーを識別する 244
センサーが見当たらない、または読み取れない 247
権限とサイトコミッショニングの問題 248
別のサイトからセンサーをスキャンする 250
定格超過センサー 251
測定値とマシンの異常 255
測定値を表示するプラットフォームの選択 255
アプリ内更新 256
センサーの測定値の表示 260
センサーの測定値について 262
アセットステータスについて 266
アセットリスト 266
アセットとポジションのステータス 268
通知 270

マシンの異常の確認 ... 272
マシンの異常を表示して確認するには ... 272
異常の解決 ... 274
障害モード ... 274
失敗の原因 ... 275
モバイルアプリを使ってマシンの異常を解決するには ... 275
ワンタイム測定の実施 ... 276
ワンタイム測定を行うには (モバイルアプリのみ) ... 277
ユーザーの管理 ... 292
管理者ユーザーの管理 ... 292
ユーザーディレクトリのセットアップ ... 293
ユーザーを管理者として追加する ... 302
管理者ユーザーとしてのユーザーの管理 ... 305
管理者ユーザーの削除 ... 309
招待 E メールの送信 ... 310
管理者以外のユーザーの管理 ... 312
ユーザーのリストの表示 ... 312
ユーザーの追加 ... 315
ユーザーロールの変更 ... 319
ユーザーの削除 ... 321
ネットワーク ... 323
モバイルデバイスとのネットワーキング ... 323
モバイルアプリでの Monitron ネットワーク基盤のセットアップ ... 323
ゲートウェイのセットアップ ... 324
センサーのセットアップ ... 324
ネットワークのセキュリティ強化 ... 325
データへのアクセス ... 327
Amazon S3 へデータをエクスポートする ... 327
前提条件 ... 328
AWS CloudFormation (推奨オプション) を使用してデータをエクスポートする ... 328
コンソールを使用してデータをエクスポートする ... 335
CloudShell を使用してデータをエクスポートする ... 355
Kinesis v1 を使ってデータをエクスポートする ... 365
Kinesis ストリームへデータをエクスポートする ... 365
ライブデータエクスポート設定を編集する ... 366
ライブデータエクスポートを停止する ... 366

データエクスポートのエラーを表示する 366
Kinesis ストリームへのサーバー側の暗号化の使用 367
Amazon CloudWatch Logs による のモニタリング 367
エクスポートしたデータを Amazon S3 に保存する 369
Lambda でデータを処理する 371
v1 データエクスポートスキーマを理解する 377
Kinesis v2 を使ってデータをエクスポートする 384
Kinesis ストリームへデータをエクスポートする 385
ライブデータエクスポート設定を編集する 385
ライブデータエクスポートを停止する 385
データエクスポートのエラーを表示する 386
Kinesis ストリームへのサーバー側の暗号化の使用 386
Amazon CloudWatch Logs による のモニタリング 386
エクスポートしたデータを Amazon S3 に保存する 388
Lambda でデータを処理する 390
v2 データエクスポートスキーマを理解する 395
Kinesis v1 から v2 への移行 413
コストのモニタリング 417
概念の概要 417
請求タグキーとタグ値 418
プロジェクトタグ値の取得 418
サイトタグ値の取得 419
請求タグのアクティブ化 421
コストレポートを表示する 422
アプリ設定 424
ローカリゼーション設定 424
ローカリゼーション設定の変更 424
を使用したアクションのログ記録 AWS CloudTrail 429
CloudTrail 内の Amazon Monitron 情報 429
例: Amazon Monitron ログファイルのエントリ 431
DeleteProject アクション成功 432
DeleteProject アクション失敗 (認可エラー) 433
DeleteProject アクション失敗 (競合の例外エラー) 434
セキュリティ 436
データ保護 437
保管中のデータ 438

転送中のデータ 438
AWS KMS および データ暗号化 438
Identity and Access Management 439
対象者 440
アイデンティティを使用した認証 440
ポリシーを使用したアクセスの管理 444
Amazon Monitron で IAM を使用する方法 446
サービスにリンクされたロールの使用 454
ログ記録とモニタリング 461
コンプライアンス検証 462
インフラストラクチャセキュリティ 463
Amazon Monitron のセキュリティベストプラクティス 463
トラブルシューティング 465
Amazon Monitron に関する問題のトラブルシューティング 465
センサーをコミッショニングできない場合 465
センサーがオフラインの場合 467
センサーが外れた場合 468
..... 468
..... 469
ゲートウェイのコミッショニングに失敗した場合 470
..... 470
利用可能なデバイス 473
クォータ 474
サポート対象の リージョン 474
クォータ 474
ドキュメント履歴 475

Amazon Monitron は新規顧客に公開されなくなりました。既存のお客様は、通常どおりサービスを引き続き使用できます。Amazon Monitron に似た機能については、ブログ記事を参照してください。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。

とは Amazon Monitron

Amazon Monitron は、機器内の潜在的な障害を検出する機械学習ベースのend-to-endの条件モニタリングシステムです。これを使用することで、予知保全プログラムを実装し、計画外の機械のダウンタイムによる生産性の低下を低減できます。

Amazon Monitron には、振動と温度のデータをキャプチャするための専用のセンサーと、 AWS クラウドにデータを自動的に転送するためのゲートウェイが含まれています。Amazon Monitron は、データを分析して機器の潜在的な障害の兆候を検出し、障害の発生を通知します。これにより、問題を深刻化する前に解決できます。Amazon Monitron を使用すると、修正メンテナンスをより効果的にスケジュールして生産性の低下を抑え、機器の致命的な故障によって発生する可能性のある修理コストを最小限に留めることができます。

Amazon Monitron には、2 つのバージョンのアプリケーションが付属しています。モバイルアプリケーションは、機器の状態を追跡する際のシステムセットアップ、分析、通知を処理します。ウェブアプリケーションは、セットアップを除き、モバイルアプリと同じ機能をすべて提供します。

信頼性マネージャーは、開発作業や専門的なトレーニングを行わずに、迅速にデプロイ Amazon Monitron して、ベアリング、モーター、ギアボックス、ポンプなどの産業機器の機械の状態を追跡できます。

Amazon Monitronとは?

Amazon Monitron デバイス

Amazon Monitron には、機器からデータを収集するためのセンサーと、そのデータを送信するためのゲートウェイの 2 種類のデバイスが含まれています Amazon Monitron。どちらも Amazon.com または Amazon Business から購入できます。

モニタリングする機械 (つまりアセット) にセンサーを直接取り付けます。1 つのアセットに最大 20 のセンサーを設置できます。

Amazon Monitron センサー

各センサーはアセットからデータを収集し、ファクトリーウォールにマウントされ、標準のコンセントに接続されたゲートウェイ Amazon Monitron を使用して、 AWS クラウド経由で に送信します。

Amazon Monitron Starter Kit は、Amazon.com://Amazon Business」で入手でき、5 つのセンサーと 1 つの Wi-Fi ゲートウェイが含まれています。必要に応じて、センサーとゲートウェイをさらに追加できます。

Amazon Monitron ゲートウェイ

Amazon Monitron ソフトウェア

Amazon Monitron にはコンソールが含まれています。これは、IT アカウントマネージャーがプロジェクトを作成し、それを管理する管理者ユーザーを追加するために使用します。このプロジェクトとは、チームの他のメンバーが機器をモニタリングするために行うあらゆる Amazon Monitron タスクのフレームワークです。プロジェクトをセットアップするまで、Amazon Monitron を使用して他の機器のモニタリングを行うことはできません。IT マネージャーのタスクには以下の内容が含まれます。

- Amazon Monitron にユーザーを提供するためのユーザーディレクトリのセットアップ
- サイトの作成、センサーのペアリング、アセットの追加など、チームのすべての Amazon Monitron モニタリングタスクを含むプロジェクトの作成
- プロジェクトを管理する管理者ユーザーの追加

プロジェクトの初期設定を除き、チームのすべてのモニタリングタスクは、スマートフォンにインストールした Amazon Monitron モバイルアプリ、またはブラウザで使用できるウェブアプリを使用して実行できます。工場の信頼性マネージャーは、モバイルアプリを使用して、サイトのセットアップ、ユーザーの管理、アセットの追加、センサーのインストールを行うことができます。ウェブアプリでは、センサーとゲートウェイのインストールを除き、同じタスクを実行できます。技術者はアプリを使用して機器の健全性をモニタリングし、潜在的な障害を追跡してドキュメント化できます。

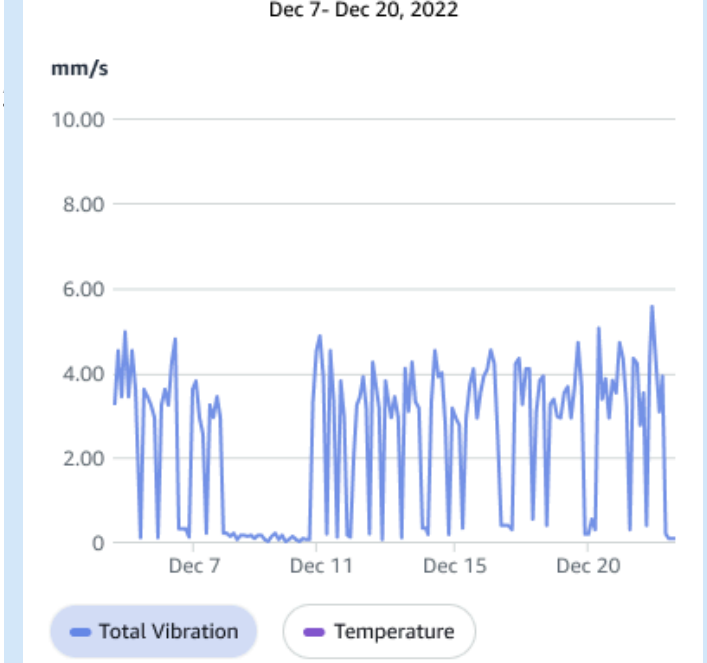
モバイルアプリでは各アセットにアイコンが表示されるため、アセットの状態が一目でわかります。

アラートのアイコン	アラートの定義
	正常: マシンは正常に動作しています。
	アラーム: このアセットのいずれかのポジションでアラームが発せられました。このポジションではマシンの振動と温度が正常範囲外であることを示しています。できるだけ早く問題を調査することが推奨されます。問題が解決されないと、機器に障害が発生する可能性があります。

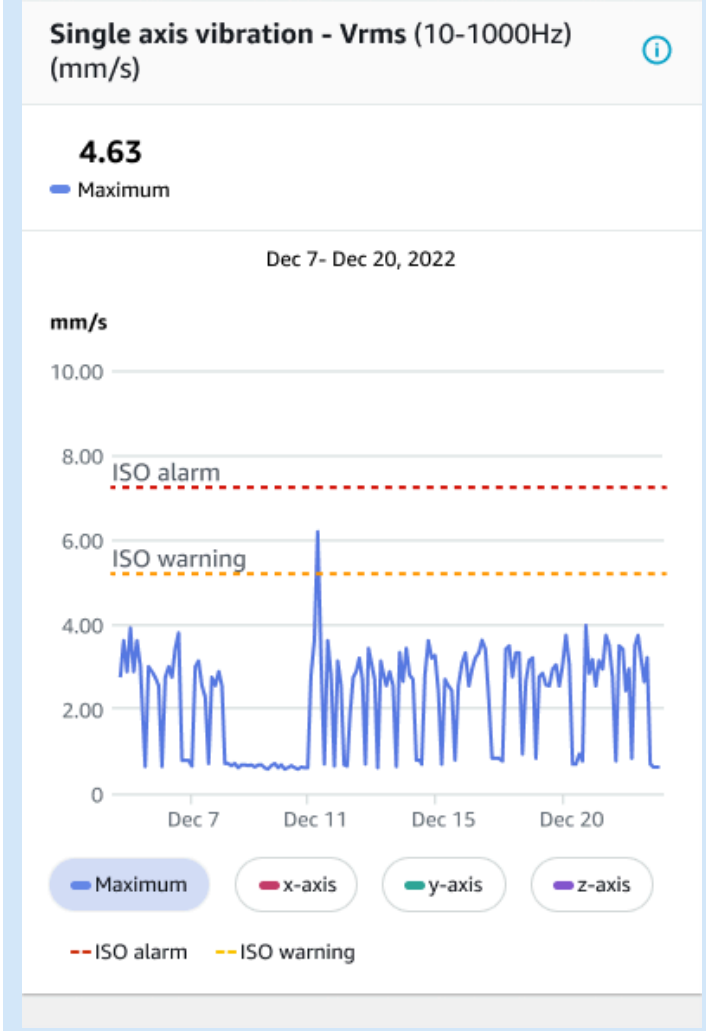
アラートのアイコン	アラートの定義
	警告: このアセットの位置の 1 つに対して警告がトリガーされました。これは、 Amazon Monitron が潜在的な障害の初期兆候を検出したことを示します。 は、機械学習と ISO 振動標準を組み合わせて、機器の振動と温度を分析することで警告条件 Amazon Monitron を識別します。
	メンテナンス: アラームが確認され、問題を調査しています。
	アセット正常 - オフライン: センサーはオフラインで、最後に記録された状態は [正常] でした。センサーがオンラインに戻るまで、新しいアラートは生成されません。
	ポジション正常 - オフライン: センサーはオフラインで、最後に記録された状態は [正常] でした。ポジションがオンラインに戻るまで、新しいアラートは生成されません。
	アセットアラーム - オフライン: センサーはオフラインで、最後に記録された状態は [アラーム] でした。センサーがオンラインに戻るまで、新しいアラートは生成されません。
	ポジションアラーム - オフライン: センサーはオフラインで、最後に記録された状態は [アラーム] でした。ポジションがオンラインに戻るまで、新しいアラートは生成されません。

アラートのアイコン	アラートの定義
	アセット警告 - オフライン: センサーはオフラインで、最後に記録された状態は [警告] でした。センサーがオンラインに戻るまで、新しいアラートは生成されません。
	ポジション警告 - オフライン: センサーはオフラインで、最後に記録された状態は [警告] でした。ポジションがオンラインに戻るまで、新しいアラートは生成されません。
	アセットメンテナンス - オフライン: センサーはオフラインで、最後に記録された状態は [メンテナンス] でした。センサーがオンラインに戻るまで、新しいアラートは生成されません。
	ポジションメンテナンス-オフライン: センサーはオフラインで、最後に記録された状態は [メンテナンス] でした。ポジションがオンラインに戻るまで、新しいアラートは生成されません。
センサーなし	センサーなし: アセット上の少なくとも 1 つのポジションでセンサーがペアリングされていません。

詳細については、データをドリルダウンできます。



正常なアセットのセンサーによる読み取り。



異常のあるアセットのセンサーによる読み取り。

Amazon Monitron はより多くのデータを収集するため、機械学習 (ML) モデルを改善し、潜在的なマシン異常をより正確に推定する方法を学習します。

の利点 Amazon Monitron

Amazon Monitron には、次の主な利点があります。

- すぐに機能 – Amazon Monitron センサーとゲートウェイは、 Amazon Monitron ソフトウェアで動作するように事前設定されています。信頼性マネージャーはアプリを使用してこれらのデバイスをインストールし、わずか数時間で機器のモニタリングを開始できます。セットアップは簡単で、開発作業、ML の知識、統合はほとんど必要ありません。
- Amazon Monitron アプリ内の即時通知 – 異常なマシンパターンを検出すると、アプリ内のユーザー通知 Amazon Monitron を送信します。技術者は、 Amazon Monitron アプリでこれらの異常なマシンの状態を表示、追跡、フィードバックできます。
- ISO および ML ベースの分析 - Amazon Monitron は、機械の異常な動作状態を自動的に検出します。これを行うために、 Amazon Monitron は振動信号と温度信号を分析し、国際標準化機構 (ISO 20816) 規格のしきい値や ML 対応モデルと比較します。
- アプリに ML フィードバックを追加するためのサポート - 技術者が app. Amazon Monitron learns にアラートの精度に関するフィードバックを入力するシンプルなワークフロー Amazon Monitron を提供し、そのフィードバックから学習し、時間の経過とともに改善し続けます。

Amazon Monitron の料金

Amazon Monitron には、センサーとゲートウェイの 1 回限りのデバイス購入コストと、使用中の Amazon Monitron センサーごとの継続的なpay-as-you-goの両方が含まれます。追加の前払い料金や長期契約はありません。

詳細については、「Amazon Monitron の料金」を参照してください。

関連リソース

Amazon Monitronについては、以下のドキュメントとその他のリソースを利用できます。

- Amazon Monitron 入門ガイド – IT マネージャー、信頼性マネージャー、技術者向けのこのガイドでは、 の使用を開始します Amazon Monitron。ここでは Amazon Monitron、 のセットアップ、アセットの作成、センサーのセットアップ、および機器のモニタリングの開始方法について説明します。

- Amazon Monitron ユーザーガイド – この詳細なガイドでは、信頼性マネージャー (管理者ユーザー) と技術者に、 を使用して機器にマシンの異常がないかモニタリング Amazon Monitron する方法の詳細を説明します。また、プライマリ Amazon Monitron ツールである アプリの使用方法についても説明します。

を初めてお使いになる方 Amazon Monitron向けの情報

の操作方法は、 Amazon Monitron ユーザーとしてのロール Amazon Monitron によって異なります。以下のオプションから自分に最も適したロールを選択すると、 Amazon Monitronの詳細を学ぶのに役立つ推奨トピックが表示されます。

IT マネージャー

IT マネージャーは、 Amazon Monitron プロジェクトをセットアップし、ユーザーを追加するように Amazon Monitron ユーザーディレクトリを設定し、サイト管理者ユーザーをマネージャープロジェクトに追加します。また、 で Amazon Monitron AWS ログを確認することもできます CloudTrail。

の IT Manager を初めて使用する場合は Amazon Monitron、次のセクションを順番に読むことをお勧めします。

1	2	3	4	5	6	7
の Amazon Monitron 仕組み	プロジェクトのセットアップ	プロジェクト	管理者ユーザーの管理	Amazon Monitron のネットワーキングについて	データへのアクセス	セキュリティ
Amazon Monitron コンポーネントを紹介し、Amazon Monitron の仕組みについて説明します。	プロジェクトを作成 Amazon Monitron するための AWS コンソールの設定方法について説明します。	Amazon Monitron プロジェクトを管理する方法について説明します。	管理者ユーザーを Amazon Monitron プロジェクトに追加したり、プロジェクトから削除したりする方法	Amazon Monitron ハードウェアネットワークについて説明します。	Kinesis を使用して Amazon Monitron データをエクスポートする方法、または Amazon S3 にダウ	セキュリティとコンプライアンスの目的を満たす Amazon Monitron ように を設定する方法につい

1	2	3	4	5	6	7
の Amazon Monitron 仕組み	プロジェクトのセットアップ	プロジェクト	管理者ユーザーの管理	Amazon Monitron のネットワーキングについて	データへのアクセス	セキュリティ
			を説明します		ンロードする方法を説明します。	て説明します。

信頼性マネージャー/管理ユーザー

信頼性マネージャー/管理者ユーザーは、 Amazon Monitron プロジェクトまたはサイト内のすべてのリソースにフルアクセスできます。信頼性マネージャーまたはサイト管理者ユーザーは、他のユーザーの追加、アセットの作成、センサーとアセットのペアリング、アセットのモニタリング、アラートの確認、異常の解決を行うことができます。

初めての信頼性マネージャーまたは管理者ユーザーの場合は Amazon Monitron、次のセクションを順番に読むことをお勧めします。

1	2	3	4	5	6	7
の Amazon Monitron 仕組み	アセットの追加とデバイスの設置	サイト	イーサネットゲートウェイ	Wi-Fi ゲートウェイ	アセット	ユーザーの管理
Amazon Monitron コンポーネントを紹介し、Amazon Monitron の仕組みに	Amazon Monitron ゲートウェイのインストール、アセットの追加、センサーのアタッチ方法	サイトの作成および管理方法を説明します	イーサネットゲートウェイをセットアップして設定する方法を説明します	Wi-Fi ゲートウェイをセットアップして設定する方法を説明します	アセットとセンサーの管理方法を説明します	管理者ユーザーの管理方法を説明します

1	2	3	4	5	6	7
の Amazon Monitron 仕組み	アセットの追加とデバイスの設置	サイト	イーサネットゲートウェイ	Wi-Fi ゲートウェイ	アセット	ユーザーの管理
ついて説明します。	について説明します。					

技術者

技術者ユーザーには、追加された Amazon Monitron プロジェクトまたはサイトに対する読み取り専用アクセス許可があります。また、アセットをモニタリングしたり、異常を認識して解決したりするアクセス許可も付与されています。

の技術者を初めて使用する場合は Amazon Monitron、次のセクションを順番に読むことをお勧めします。

1	2	3	4	5	6
の Amazon Monitron 仕組み	アセット	センサーの測定値とマシンの異常のモニタリングについて	イーサネットゲートウェイ	Wi-Fi ゲートウェイ	Amazon Monitron デバイスの問題のトラブルシューティング
Amazon Monitron コンポーネントを紹介し、 Amazon Monitron の仕組みについて説明します。	アセットとセンサーの管理方法を説明します	センサーの測定値を理解し、機械の異常をモニタリングする方法を説明します	イーサネットゲートウェイをセットアップして設定する方法を説明します	Wi-Fi ゲートウェイをセットアップして設定する方法を説明します	Amazon Monitron デバイスの問題のトラブルシューティング方法について説明します。

の Amazon Monitron 仕組み

Amazon Monitron は、機械学習end-to-endの条件モニタリングソリューションシステムで、機械内の障害の発生を検出し、予測メンテナンスプログラムを実装して、予期しない機械のダウンタイムによる生産性の低下を軽減できます。

Amazon Monitron には、振動と温度のデータをキャプチャするための専用のセンサー、 AWS クラウドにデータを自動的に転送するためのゲートウェイ、および機器の状態を追跡する際のシステムのセットアップ、分析、通知用のアプリケーションが含まれています。

Amazon Monitron センサーは ISO しきい値モデルと機械学習 (ML) モデルを使用して振動をモニタリングします。ISO モデルは振動の大きさ (マシンの状態) の解析に使用されます。ML モデルは振動の変化 (マシンの状態の変化) の検出に使用されます。

信頼性マネージャーは をデプロイ Amazon Monitron して、開発作業や専門的なトレーニングを行わずに、ベアリング、モーター、ギアボックス、ポンプなどの産業機器の機械の状態を追跡できます。

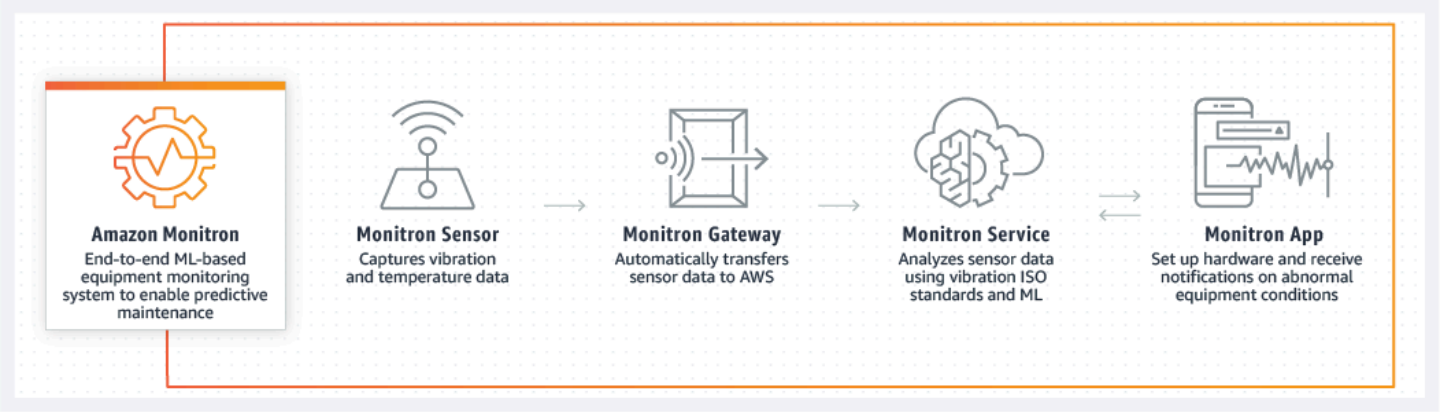
> **Tip**
>
> Amazon Monitron アプリの更新と最新の機能へのアクセスを定期的に確認します。

トピック

- Amazon Monitron ワークフロー
- Amazon Monitron の概念
- Amazon Monitron コンポーネント
- Amazon Monitron アラート

Amazon Monitron ワークフロー

次の図は、 の基本的なワークフローを示しています Amazon Monitron。



1. Amazon Monitron センサーは、機器 (アセット) から温度と振動のデータをキャプチャし、ゲートウェイに送信します。
2. Amazon Monitron ゲートウェイは、ファクトリーの AWS インターネット接続を使用してデータを クラウドに送信します。
3. AWS クラウドの Amazon Monitron ML ベースのサービスは、センサーデータを分析します。
   a. Amazon Monitron は、障害の発生を示す可能性のあるデータの異常を探します。
   b. が潜在的な障害 Amazon Monitron を検出した場合、信頼性マネージャーと技術者に Amazon Monitron アプリを通じて通知し、適切なアクションを実行できるようにします。
   c. 技術者はアラートに基づいて調査し、発生している障害を解決します。アラートの精度に関するフィードバックを入力し、このフィードバックから app. Amazon Monitron learns で実行された障害モード、原因、アクションを報告し、継続的に改善します。
4. アプリでは、現在と過去の温度と振動のデータをグラフでわかりやすく表示でき、問題を調査する際に活用できます。

Amazon Monitron の概念

Amazon Monitron 実装は、次の方法で構造化されます。

```
プロジェクト → サイト → アセット → センサー → ポジション
```

次の表は、使用を開始するために知っておくべき Amazon Monitron 概念と用語を示しています Amazon Monitron。

概念の名称	概念の定義	重要な事実	一般的なユーザー
プロジェクト	• Amazon Monitron が使用するゲートウェイ、アセット、センサーのセットアップを行います • 機器の障害につながる可能性のある Amazon Monitron 検出されたマシン異常の詳細をキャプチャします	• リソースはプロジェクト間で共有できません • Amazon Monitron コンソール上でのみ作成できます • IT 管理者または Amazon Monitron コンソールにアクセスできるユーザーのみが作成および管理できます	• IT 管理者/マネージャー
サイト	• 同じ目的を共有するアセット、ゲートウェイ、センサーの集まりです • プロジェクトを整理して管理しやすくするために使用します	• プロジェクトに大量のアセット、ゲートウェイ、センサーがある場合の整理に役立ちます • アクセスと権限の制御に使用できます • 1 つのプロジェクト内に最大 50 のサイトを作成でき、各サイトには最大 100 のアセットと 200 のゲートウェイを追加できます • サイトをプロジェクトに追加するには、プロジェクトレベルの管理者	• IT 管理者/マネージャー • 信頼性マネージャー

概念の名称	概念の定義	重要な事実	一般的なユーザー
		ユーザーである必要があります • モバイルアプリとウェブアプリの両方から設定できます	
ゲートウェイ	• Amazon Monitron センサーによって収集されたデータを AWS クラウドに転送する Wi-Fi またはイーサネットデバイス。	• センサーデータが正しく クラウドに転送されているかどうかを追跡するのに役立ちます。 • モバイルアプリを使用してコミッショニングする必要があります	• 信頼性マネージャー • 技術者

アセット	• 工場の現場に設置されている各機器です
	• 例:
	  • 個々のマシン
	  • 大型機器の一部
	  • 工業プロセスの一部
	  • 製造モデルの要素
		• マシンの状態を確認する上での基盤となるものです
		• Amazon Monitron センサーはアセットとそのパーツとペアリングされます
		• 1 つのアセットで最大 20 のポジションにセンサーを設置できます
		• モバイルアプリとウェブアプリの両方から設定できます
			• 信頼性マネージャー
			• 技術者

概念の名称	概念の定義	重要な事実	一般的なユーザー
センサー	• 機器から温度と振動のデータを収集します • Amazon Monitron はデータを使用して開発中の問題を検出します	• 各アセットで最大 20 のポジションにセンサーを設置できます • 設置されているマシンの部位に対応するマシンクラスを割り当てることができます • モバイルアプリからのみ設定できます	• 技術者 • 信頼性マネージャー

概念の名称	概念の定義	重要な事実	一般的なユーザー
ポジション	• アセットでセンサーを取り付ける場所です • データの収集と分析において重要です	• 各アセットで最大 20 のポジションにセンサーを設置できます • 同じアセット上の位置には、マシンの状態をきめ細かく表示するために異なるマシンクラスを割り当てることができます。 **Important** 複数の潜在的な障害点がある複雑な機械では、複数のポジションからデータを収集することを推奨します。	• 技術者 • 信頼性マネージャー

Amazon Monitron コンポーネント

Amazon Monitron には、振動データと温度データをキャプチャする専用のセンサーと、 クラウドにデータを自動的に転送するゲートウェイが含まれています AWS 。また、2 つのバージョンのアプリケーションも付属しています。モバイルアプリケーションは、機器の状態を追跡する際のシステムセットアップ、分析、通知を処理します。ウェブアプリケーションは、セットアップを除き、モバイルアプリと同じ機能をすべて提供します。

Amazon Monitron Starter Kit は、Amazon.com://Amazon Business」で入手でき、5 つのセンサーと 1 つの Wi-Fi ゲートウェイが含まれています。必要に応じて、センサーとゲートウェイを購入して追加できます。詳細については、「Amazon Monitron のFAQs」を参照してください。

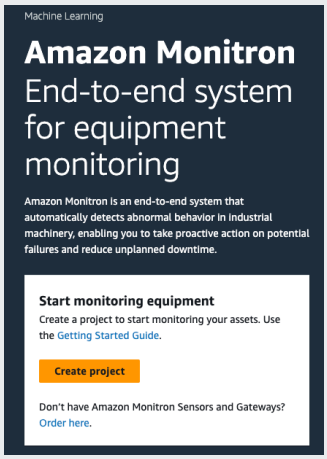
次の表は、 Amazon Monitron コンポーネント、その関数、およびそれらのユースケースを示しています。

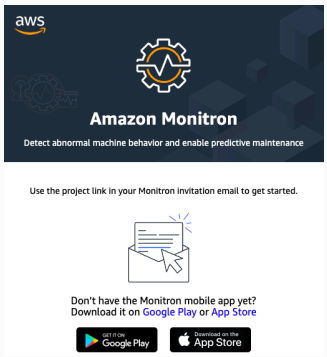
> **Note**
>
> 振動は、km (mm) と インチで測定されます。温度は華氏 (F) と摂氏 (C) で測定されます。

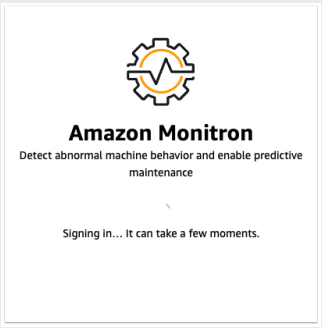
コンポーネント名	コンポーネントの詳細	関数	一般的なユーザー
センサー 	• ハードウェア • 温度: -20C – +80C/ -4F – +176F • 寸法： 52.8x43.0 x24.9mm/2 .08x1.69x0.98 インチ • 重み： 54 gms • IP 評価： IP65 • ワイヤレスプロトコル： Bluetooth Low Energy 5 • 振動センサー： 3 軸 MEMs 加速度計、範囲 +/-16g、最大 6kHz の周波数応答、サンプリング周波数 26.7 kHz • 電源： 充電不可能なリチウム金属バッテリー	• 機械 (アセット) から直接振動と温度のデータをキャプチャします。 • Wi-Fi ゲートウェイまたはイーサネットゲートウェイを使用して、収集したデータを AWS クラウドに送信します。 • 最大 20 個の をマシン (アセット) に配置することができます • 各センサーには、配置されているマシン (アセット) パーツに対応するマシンクラスを割	• 技術者 • 信頼性マネージャー

コンポーネント名	コンポーネントの詳細	関数	一般的なユーザー
	• バッテリー寿命：推定 5 年 • デフォルトのデータキャプチャ：1 時間に 1 回	り当てることができます。	
イーサネットゲートウェイ 	• ハードウェア • 温度： -20C ~ +60C /-4F ~ +140F • 寸法: 13.9X10.7 X4.1cm/5. 5X4.2X1.6 インチ • 重み： 230 gms/8.20 oz • IP 評価： IP65 • インターネット接続： RJ45 10/100Mbps • 電力： IEEE 802.3at type1 (15.4 Watt クラス)	• マシン (アセット) から収集された振動と温度のデータを AWS クラウドに送信します。 • RJ-45 ソケットに接続されたイーサネット Cat 5e または Cat 6 コードを搭載 • アセット (マシン) に直接アタッチする必要はありません • 動作するには Power over Ethernet (POE) 対応ルーターまたは POE パワーインジェクターが必要です	• 技術者 • 信頼性マネージャー

コンポーネント名	コンポーネントの詳細	関数	一般的なユーザー
Wi-Fi ゲートウェイ 	• ハードウェア • 温度： 0C ~ 40C/32 F ~ 104F • 寸法： 90x78x38 mm/3.6x3.1x1.5 インチ • 重み： 95 gms • IP 評価： IP65 • インターネット接続： WiFi、802.11b/g/n、ISM 2.4GHz のみ • 電源： 5.0V ~ 2.0 DC、米国、英国、欧州の国 (屋内のみ) 用の AC アダプター付属	• マシン (アセット) から収集された振動と温度のデータを AWS クラウドに送信します。 • Wi-Fi (標準ソケットに接続) **Note** Wi-Fi ゲートウェイはすべてのサイトでサポートされているわけではありません。 Amazon Monitron イーサネットゲートウェイはグローバル標準です。	• 技術者 • 信頼性マネージャー

コンポーネント名	コンポーネントの詳細	関数	一般的なユーザー
コンソール 	ソフトウェア	• にサインアップする AWS • Amazon Monitron プロジェクトの作成 • プロジェクトを管理する管理者ユーザーを作成して最初に割り当てる **Important** が機能 Amazon Monitron するには、最初に設定する必要があります。	• IT マネージャー • IT 管理者 • 信頼性マネージャー

コンポーネント名	コンポーネントの詳細	関数	一般的なユーザー
モバイルアプリ 	ソフトウェア	• Amazon Monitron プロジェクトの管理 • （プロジェクトレベルの管理者ユーザーのみ) サイトの作成 • アセットを作成する • 機器の状態のモニタリング • （モバイルアプリのみ) センサーとゲートウェイのセットアップ	• 技術者 • 信頼性マネージャー

コンポーネント名	コンポーネントの詳細	関数	一般的なユーザー
ウェブアプリ  	ソフトウェア	• Amazon Monitron プロジェクトの管理 • (プロジェクトレベルの管理者ユーザーのみ) サイトの作成 • アセットを作成する • 機器の状態のモニタリング **Important** ウェブアプリは、センサーとゲートウェイのインストールを除き、モバイルアプリでサポートされているすべてのタスクをサポートします。	• 技術者 • 信頼性マネージャー

Amazon Monitron アラート

機器の状態を追跡するために、 Amazon Monitron モバイルアプリには各アセットのアイコンが表示されるため、その状態を一目で確認できます。

次の表は、アセットのステータスアイコンを示しています。

アラートのアイコン	アラートの定義
	正常: マシンは正常に動作しています。
	アラーム: このアセットのいずれかのポジションでアラームが発せられました。このポジションではマシンの振動と温度が正常範囲外であることを示しています。できるだけ早く問題を調査することが推奨されます。問題が解決されないと、機器に障害が発生する可能性があります。
	警告: このアセットの位置の 1 つに対して警告がトリガーされました。これは、 Amazon Monitron が潜在的な障害の初期兆候を検出したことを示します。 は、機械学習と ISO 振動標準を組み合わせて、機器の振動と温度を分析することで警告条件 Amazon Monitron を識別します。
	メンテナンス: アラームが確認され、問題を調査しています。
	アセット正常 - オフライン: センサーはオフラインで、最後に記録された状態は [正常] でした。センサーがオンラインに戻るまで、新しいアラートは生成されません。
	ポジション正常 - オフライン: センサーはオフラインで、最後に記録された状態は [正常] でした。ポジションがオンラインに戻るまで、新しいアラートは生成されません。

アラートのアイコン	アラートの定義
	アセットアラーム - オフライン: センサーはオフラインで、最後に記録された状態は [アラーム] でした。センサーがオンラインに戻るまで、新しいアラートは生成されません。
	ポジションアラーム - オフライン: センサーはオフラインで、最後に記録された状態は [アラーム] でした。ポジションがオンラインに戻るまで、新しいアラートは生成されません。
	アセット警告 - オフライン: センサーはオフラインで、最後に記録された状態は [警告] でした。センサーがオンラインに戻るまで、新しいアラートは生成されません。
	ポジション警告 - オフライン: センサーはオフラインで、最後に記録された状態は [警告] でした。ポジションがオンラインに戻るまで、新しいアラートは生成されません。
	アセットメンテナンス - オフライン: センサーはオフラインで、最後に記録された状態は [メンテナンス] でした。センサーがオンラインに戻るまで、新しいアラートは生成されません。
	ポジションメンテナンス-オフライン: センサーはオフラインで、最後に記録された状態は [メンテナンス] でした。ポジションがオンラインに戻るまで、新しいアラートは生成されません。

入門

この章では、Amazon Monitron の使用を開始するための基本的なステップを説明します。

1. プロジェクトのセットアップ - チームの他のメンバーが機器をモニタリングするためのフレームワークを説明します。これには、Amazon Monitron コンソールを使用します。選択したプロジェクトの数に応じて、時々実行するか、1 回だけ実行します。その他のタスクはすべて Amazon Monitron モバイルアプリを通じて実行されます。
2. アセットの追加とデバイスの設置 - ここでのセットアップタスクはすべて、モバイルアプリを使用して実行できます。これはプロジェクト開始時に行う主要なアクティビティです。初めにいくつかのアセットを追加して、数台のデバイスを設置します。後からアセットを追加して、同じタスクを行うことができます。
3. アラートの把握 - Amazon Monitron の日常的な使い方を説明します。これには、モバイルアプリを使用します。日常的なモニタリングと、Amazon Monitron が機械の異常の可能性を発見したときに対処する必要があるタスクを紹介します。

Amazon Monitron の詳細については、「Amazon Monitron の製品詳細ページ」をご覧ください。

トピック

- プロジェクトのセットアップ
- アセットの追加とデバイスの設置
- 警告とアラートの把握

プロジェクトのセットアップ

Amazon Monitron の最初のステップは、Amazon Monitron コンソールでプロジェクトをセットアップすることです。プロジェクトとは、チームが Amazon Monitron モバイルアプリでゲートウェイ、アセット、センサーをセットアップする場所です。

トピック

- ステップ 1: アカウントを作成する
- ステップ 2: プロジェクトを作成する
- ステップ 3: 管理者ユーザーを作成する
- ステップ 4: (オプション) Amazon Monitron ユーザーをプロジェクトに追加する

- ステップ 5: ユーザーをプロジェクトに招待する

ステップ 1: アカウントを作成する

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、日常的なタスクにルートユーザーを使用しないように AWS アカウントのルートユーザー、 のセキュリティを確保し AWS IAM Identity Center、 を有効にして管理ユーザーを作成します。

を保護する AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドのルートユーザーとしてサインインするを参照してください。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、IAM ユーザーガイドの AWS アカウント 「ルートユーザー (コンソール) の仮想 MFA デバイスを有効にする」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 AWS IAM Identity Center ユーザーガイド」の「デフォルトを使用してユーザーアクセスを設定する IAM アイデンティティセンターディレクトリ」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、AWS サインイン「 ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの結合」を参照してください。

> **Important**
>
> Amazon Monitron は、オプトインリージョンと政府リージョンを除くすべての IAM アイデンティティセンターリージョンをサポートします。サポートされているリージョンのリストについては、「SSO 要件の理解」を参照してください。

ステップ 2: プロジェクトを作成する

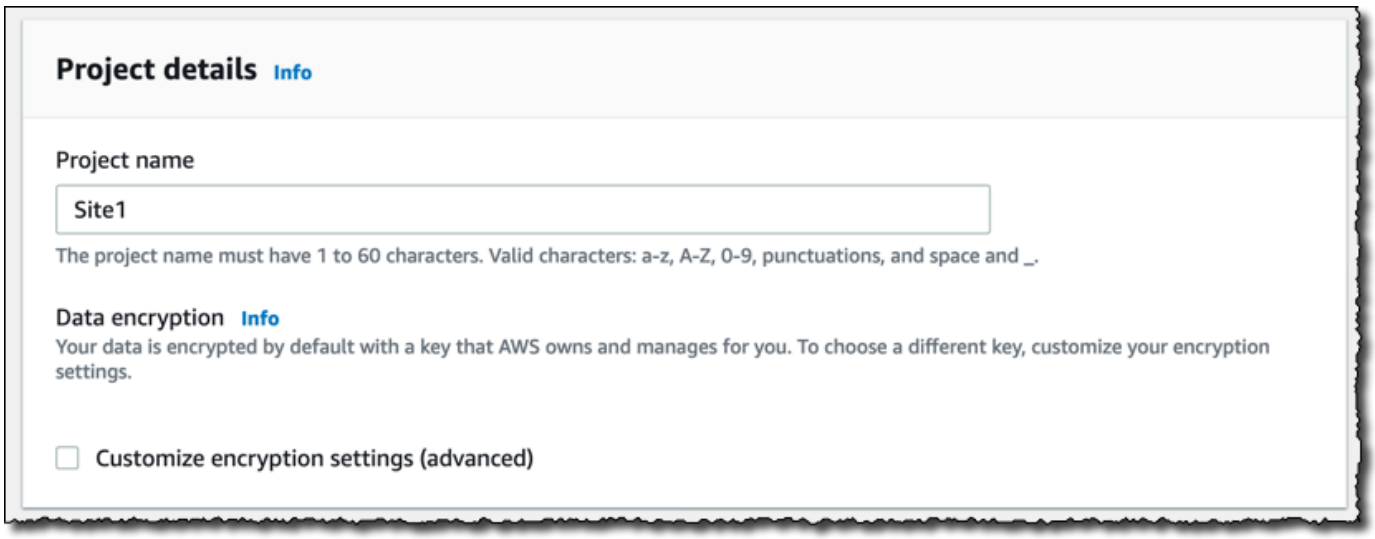
にサインインしたので AWS Management Console、Amazon Monitron コンソールを使用してプロジェクトを作成できます。

プロジェクトを作成するには

1. AWS リージョンセレクタで使用するリージョンを選択します。Amazon Monitron は米国東部 (バージニア北部)、欧州 (アイルランド)、およびアジアパシフィック (シドニー) リージョンでのみ利用できます。
2. Amazon Monitron コンソール (https://console.aws.amazon.com/monitron) を開きます。
3. [プロジェクトを作成] を選択します。
4. [プロジェクトの詳細] の [プロジェクト名] に、プロジェクトの名前を入力します。
5. (オプション) データ暗号化では、 がある場合はカスタム暗号化設定 (詳細) を確認できます AWS KMS key AWS Key Management Service。Amazon Monitron は、保管中および転送中のすべてのデータを暗号化します。独自の CMK を提供しない場合、データは Amazon Monitron が所有および管理する CMK によって暗号化されます。

   プロジェクトの暗号化の詳細については、「KMS and Data Encryption in Amazon Monitron」を参照してください。
6. (オプション) プロジェクトにタグを追加するには、[タグ] にキーと値のペアを入力し、[タグを追加] をクリックします。

   タグの詳細については、「Tags in Amazon Monitron」を参照してください。
7. [次へ] をクリックしてプロジェクトを作成します。



最初のプロジェクトを作成すると、 AWS アカウントの所有者は AWS Organizations から E メールを受け取ります。この E メールによってアクションを要求されることはありません。

ステップ 3: 管理者ユーザーを作成する

組織内の 1 人以上のユーザー (信頼性マネージャーなど) に管理者ユーザーとしてアクセス許可を付与します。管理者ユーザーとは、Amazon Monitron プロジェクトに属しており、プロジェクトに他のユーザーを追加できる人のことです。

管理者ユーザーを追加すると、Amazon Monitron は AWS IAM Identity Centerにそのユーザーのアカウントを作成します。IAM Identity Center は、組織内の AWS アカウントとアプリケーションへの SSO アクセスを管理するのに役立つサービスです。Amazon Monitron は IAM アイデンティティセンターを使用して、Amazon Monitron モバイルアプリのユーザーを認証します。

AWS アカウントで IAM アイデンティティセンターを有効にしていない場合、最初の Amazon Monitron 管理者ユーザーを作成するときに Amazon Monitron によって有効にされます。アカウントで既に IAM アイデンティティセンターを使用している場合、IAM アイデンティティセンターのユーザーが Amazon Monitron コンソールに表示されます。

このセクションのステップを実行すると、自分自身を管理者ユーザーとしてプロジェクトに追加できます。作成する追加の管理者ユーザーごとに、このステップを繰り返します。

管理者ユーザーを作成するには

AWS アカウントで IAM Identity Center を既に使用していない限り、Amazon Monitron を使用して管理者ユーザーを作成します。これらのユーザーが既に IAM アイデンティティセンターに存在する場合は、ユーザーの作成を省略して、そのユーザーに管理者ロールを割り当てることができます。

1. Amazon Monitron コンソール (https://console.aws.amazon.com/monitron) を開きます。
2. [プロジェクト管理者ユーザーを追加] ページで [ユーザーを作成] を選択します。
3. [ユーザーを作成] セクションで、管理者ユーザーの E メールアドレスと名前を入力します。
4. [ユーザーを作成] を選択します。

   Amazon Monitron が IAM アイデンティティセンターにユーザーを作成します。IAM アイデンティティセンターは、アカウントをアクティブ化するためのリンクを含む E メールをユーザーに送信します。リンクは最大 7 日間有効です。この期間内に、各ユーザーは E メールを開いて招待を承諾する必要があります。

管理者ロールを管理ユーザーに割り当てるには

1. [プロジェクト管理者ユーザーを追加] ページで、作成した各管理者ユーザーのチェックボックスをオンにします。
2. [追加] を選択します。

   管理者ユーザーが IAM アイデンティティセンターのアカウントへの招待をまだ承諾していない場合でも、管理者ユーザーをプロジェクトに追加できます。

ステップ 4: (オプション) Amazon Monitron ユーザーをプロジェクトに追加する

管理者ユーザーに加えて、管理者権限のないユーザーも追加できます。例えば、そのユーザーは、Amazon Monitron モバイルアプリを使用してアセットの監視、通知の確認、クロージャーコードの入力のみを行う技術者の場合があります。

管理者ユーザーではないユーザーの場合

- ユーザーアカウントを作成するには、Amazon Monitron ではなく IAM アイデンティティセンターを使用します。

- ユーザーをプロジェクトに追加するには、Amazon Monitron コンソールではなく、Amazon Monitron モバイルアプリを使用します。

トピック

- IAM アイデンティティセンターにユーザーを追加するには
- モバイルアプリを使用してユーザーを追加するには
- ウェブアプリを使用してユーザーを追加する方法

IAM アイデンティティセンターにユーザーを追加するには

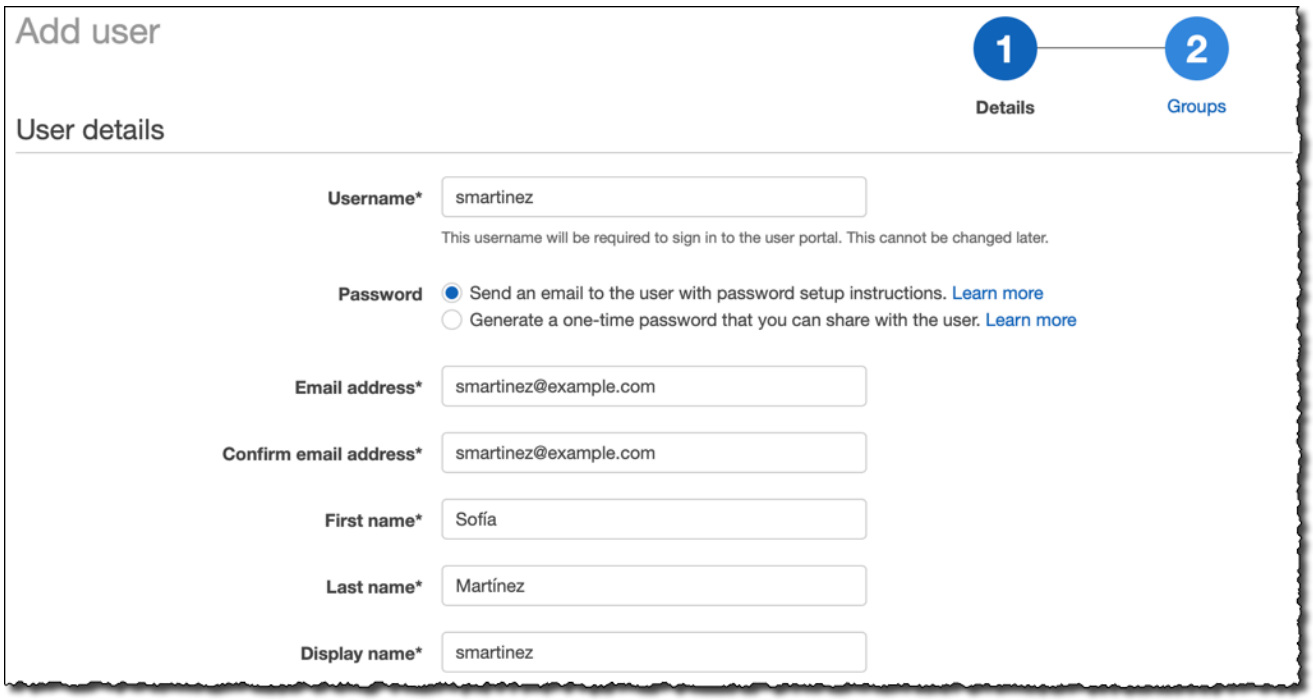
アカウントに IAM Identity Center の AWS アカウントが既にある場合は、この手順をスキップできます。モバイルアプリのプロジェクトにユーザーを追加する準備が整っている状態です。それ以外の場合は、以下のステップを実行して IAM アイデンティティセンターにユーザーを追加します。

> **Note**
>
> すべてのユーザーが管理者ユーザーである場合、以下のステップは不要です。

1. https://console.aws.amazon.com/singlesignon/ で AWS IAM Identity Center コンソールを開きます。
2. IAM アイデンティティセンターで [ユーザー] をクリックします。
3. Amazon Monitron モバイルアプリでプロジェクトにアクセスするユーザーごとに、以下のステップを繰り返します。

    a. [ユーザー] ページで [ユーザーを追加] をクリックします。

    b. [ユーザーの詳細] セクションで、ユーザー名と連絡先情報を入力します。[パスワード] は [パスワードの設定手順を記載した E メールをユーザーに送信します] のままにしておきます。

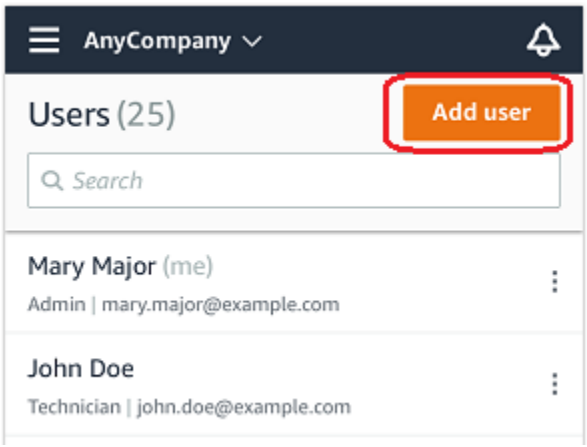


c. [次: グループ] を選択します。

d. [ユーザーを追加] を選択します。IAM アイデンティティセンターでは、IAM アイデンティティセンターのユーザーをアクティブ化するためのリンクを含む E メールをユーザーに送信します。リンクは最大 7 日間有効です。Amazon Monitron モバイルアプリでプロジェクトにアクセスする前に、各ユーザーは E メールを開いて招待を承諾する必要があります。

モバイルアプリを使用してユーザーを追加するには

1. スマートフォンで Amazon Monitron モバイルアプリにログインします。
2. ユーザーを追加するプロジェクトまたはサイトに移動し、[ユーザー] のリストに移動します。
3. [ユーザーを追加] を選択します。



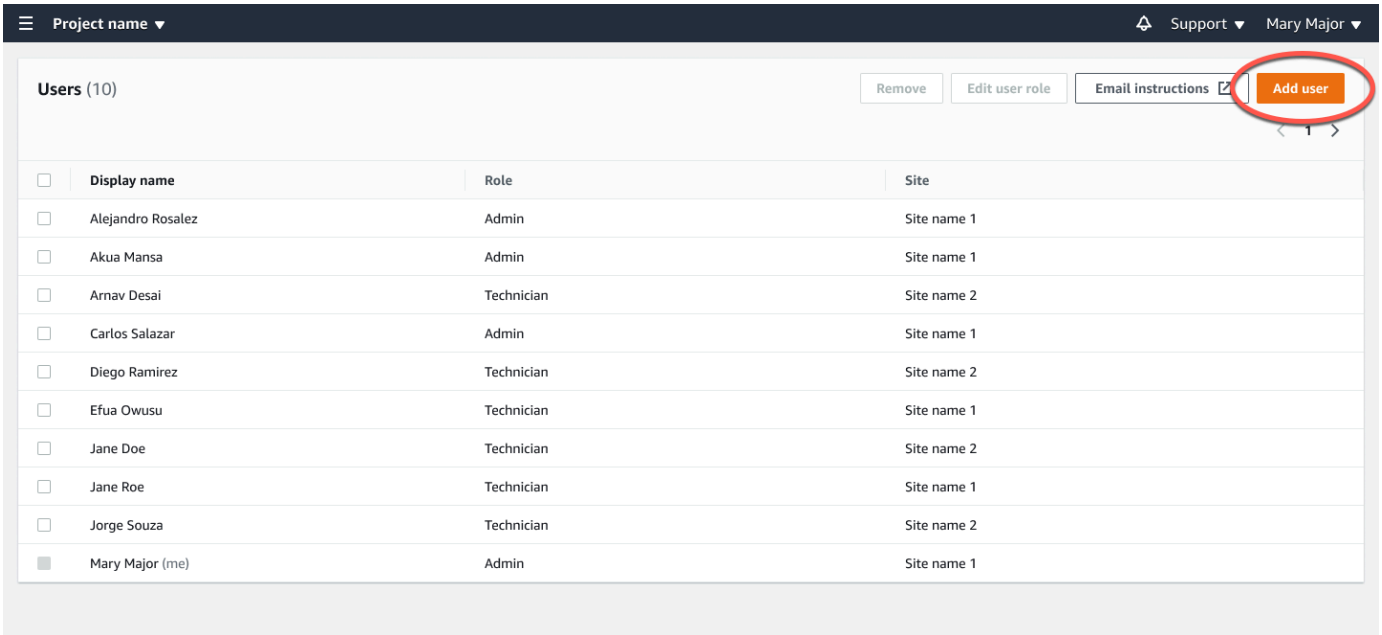
4. ユーザー名を入力します。

   Amazon Monitron がユーザーディレクトリでユーザーを検索します。
5. リストからユーザーを選択します。
6. ユーザーに割り当てるロールを [管理者]、[技術者]、[閲覧者] から選択します。
7. [追加] を選択します。

   新しいユーザーが [ユーザー] のリストに表示されます。
8. 新しいユーザーに、プロジェクトにアクセスして Amazon Monitron モバイルアプリをダウンロードするためのリンクを含む、招待 E メールを送信します。詳細については、「Sending an email invitation」を参照してください。

ウェブアプリを使用してユーザーを追加する方法

1. ナビゲーションペインで [ユーザー] を選択します。
2. [ユーザーを追加] を選択します。

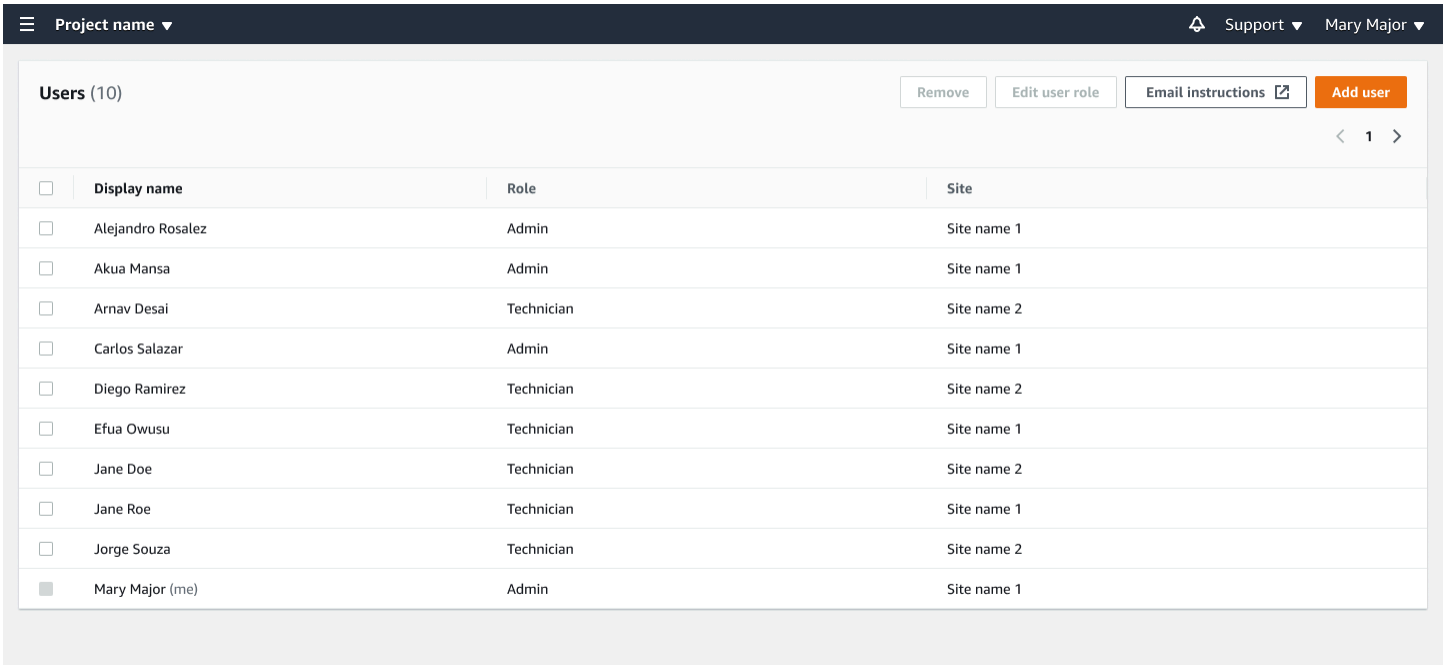


3. ユーザー名を入力します。

   Amazon Monitron がユーザーディレクトリでユーザーを検索します。
4. リストからユーザーを選択します。
5. ユーザーに割り当てるロールを [管理者]、[技術者]、[読み取り専用] から選択します。
6. [追加] を選択します。

新しいユーザーが [ユーザー] のリストに表示されます。

7. 新しいユーザーに、プロジェクトにアクセスして Amazon Monitron モバイルアプリをダウンロードするためのリンクを含む、招待 E メールを送信します。詳細については、「Sending an email invitation」を参照してください。

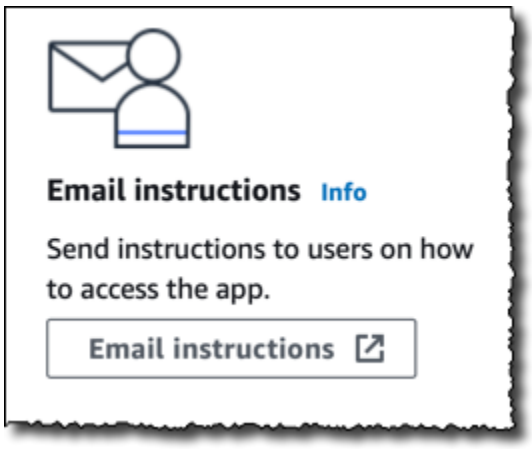


ステップ 5: ユーザーをプロジェクトに招待する

Amazon Monitron プロジェクトに、追加したユーザーを招待します。

1. Amazon Monitron コンソール (https://console.aws.amazon.com/monitron) を開きます。
2. ナビゲーションペインで、[プロジェクト] を選択します。
3. [プロジェクト] ページでプロジェクト名を選択し、詳細ページを開きます。
4. 編集するユーザーごとに、以下のステップを繰り返します。

   a. [仕組み] で、[E メールによる指示] を選択します。



E メールクライアントが立ち上がり、Amazon Monitron プロジェクトへの招待を含む下書きが表示されます。これには、Google Play ストアから Amazon Monitron モバイルアプリをダウンロードするためのリンクと、プロジェクトを開くためのリンクの両方が含まれています。

b. このメッセージをユーザーに送信します。

アセットの追加とデバイスの設置

プロジェクトを作成したら、お客様またはチームの信頼性マネージャーや技術者は、Amazon Monitron モバイルアプリを使用してゲートウェイを追加し、アセットを作成し、それらにセンサーをペアリングして、機器のモニタリングを開始できます。Amazon Monitron は、近距離無線通信 (NFC) と Bluetooth を備える Android 8.0 以降または iOS 14 以降を搭載したスマートフォンのみをサポートしています。

IT マネージャーまたは信頼性マネージャーは、初めてログインしてプロジェクトに接続する方法を記載した E メールを生成し、送信します。初めてログインしたら、ステップに従ってゲートウェイを追加し、デバイスを設置します。

トピック

- ステップ 1: ゲートウェイを追加する
- ステップ 2: アセットを追加する
- ステップ 3: センサーを取り付ける
- ステップ 4: センサーをアセットにペアリングする

ステップ 1: ゲートウェイを追加する

Amazon Monitron では、センサーが機械からデータを収集してゲートウェイに渡します。ゲートウェイはそのデータを AWS クラウドに送信し、Amazon Monitron が分析します。これらのゲートウェイは通常、センサーから 20～30 メートル以内の工場内の壁に取り付けられ、ローカル Wi-Fi ネットワークを使用して AWS クラウドに接続します。

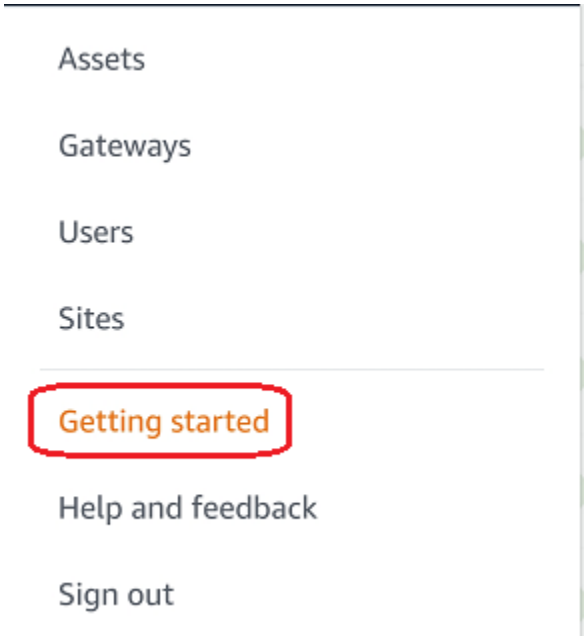
ゲートウェイを追加する前に、スマートフォンの Bluetooth がオンになっていることを確認してください。モバイルアプリを使用してのみゲートウェイを追加できます。

トピック

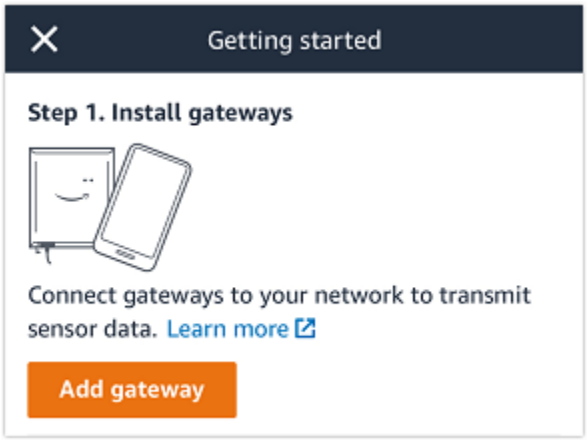
- Wi-Fi ゲートウェイを追加するには
- イーサネットゲートウェイを追加するには

Wi-Fi ゲートウェイを追加するには

1. メニューアイコン (☰) をクリックし、[開始方法] を選択します。



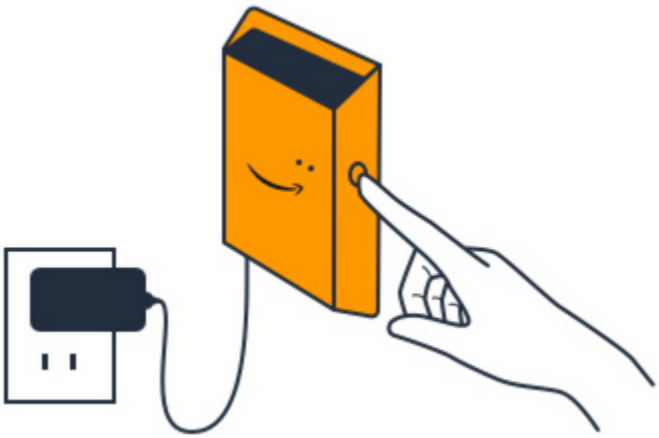
2. [ゲートウェイを追加] を選択します。



3. 工場では、センサーとの通信に最適な場所にゲートウェイを配置してください。

   ゲートウェイを取り付ける最適な場所は、センサーよりも高く、20～30 メートル以内の距離です。ゲートウェイの位置決めの詳細については、「Amazon Monitron ユーザーガイド」の「Where to Install Your Gateway」を参照してください。

4. ゲートウェイを接続し、上部の LED ライトが黄色と青色に交互に点滅することを確認します。



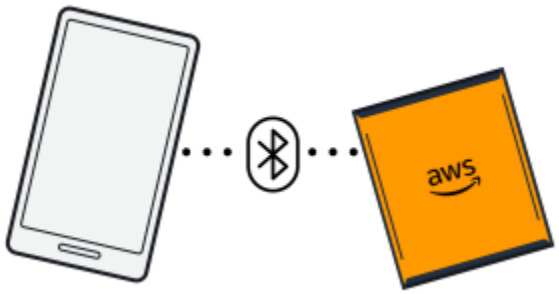
5. ゲートウェイの側面にあるボタンを押して、コミッショニングモードにします。ライトがすばやく点滅し始めます。
6. モバイルアプリで [次へ] をクリックします。
7. [ゲートウェイを追加] を選択します。

   Amazon Monitron がゲートウェイを検索します。これには少し時間がかかることがあります。ゲートウェイが検出されると、ゲートウェイのリストにそのゲートウェイが表示されます。

   ゲートウェイが検出されない場合は、「Amazon Monitron ユーザーガイド」の「Setting Up Gateways」を参照して、考えられる解決策を確認してください。

8. 新しいゲートウェイがリストに表示されたら、そのゲートウェイを選択します。

   Amazon Monitron が新しいゲートウェイに接続するまでに少し時間がかかることがあります。



9. ゲートウェイに接続すると、Amazon Monitron は Wi-Fi ネットワークをスキャンします。使用する Wi-Fi ネットワークを選択します。

   > **Note**
   >
   > ゲートウェイが正常に接続されると、Amazon Monitron はモバイルアプリにゲートウェイデバイス ID と MAC ID を表示します。

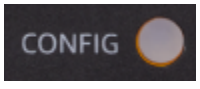
10. Wi-Fi パスワードを入力して [接続] をクリックします。

    ゲートウェイのコミッショニングに数分かかる場合があります。

イーサネットゲートウェイを追加するには

1. スマートフォンの Bluetooth がまだオンになっていない場合は、オンにしてください。
2. ゲートウェイは、センサーとの通信に最適な場所に配置してください。

   ゲートウェイをマウントする最適な場所は、センサーよりも高く、20～30 メートル以内です。ゲートウェイを見つけるためのその他のヘルプについては、「」を参照してください[イーサネットゲートウェイの取り付けと設置](#)。
3. ゲートウェイを接続し、ゲートウェイの正面にあるネットワークライト (黄色) と Bluetooth ライト (青色) が交互に点滅していることを確認します。
4. ゲートウェイの [設定] ボタンを押してコミッショニングモードにします。Bluetooth とネットワークの LED ライトがすばやく点滅し始めます。



5. スマートフォンでモバイルアプリを開きます。
6. [開始方法] ページまたは [ゲートウェイ] ページで、[ゲートウェイを追加] を選択します。

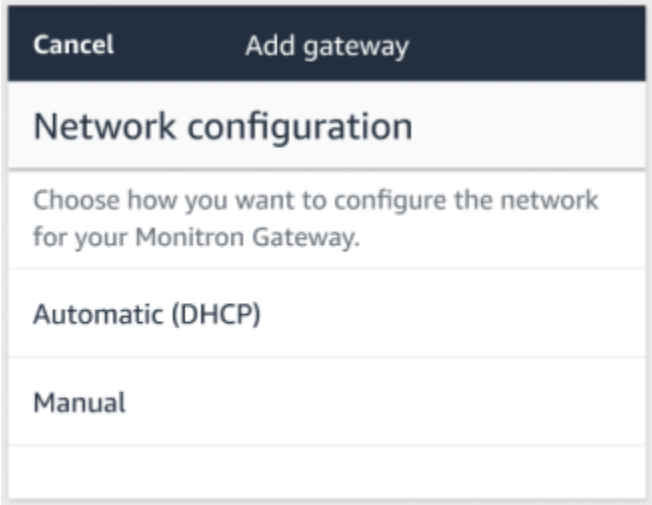
   Amazon Monitron がゲートウェイをスキャンします。これには少し時間がかかることがあります。Amazon Monitron がゲートウェイを検出すると、ゲートウェイのリストにそのゲートウェイが表示されます。
7. 表示されたゲートウェイを選択します。

   Amazon Monitron が新しいゲートウェイに接続するまでに少し時間がかかることがあります。

   モバイルアプリケーションがゲートウェイへの接続を引き続き試みても成功しない場合は、「イーサネットゲートウェイ検出のトラブルシューティング」を参照してください。

> **Note**
>
> ゲートウェイが正常に接続されると、Amazon Monitron はモバイルアプリにゲートウェイデバイス ID と MAC ID を表示します。

8. ゲートウェイに接続されると、Amazon Monitron にはゲートウェイのネットワーク接続を設定するための 2 つのオプションが表示されます。



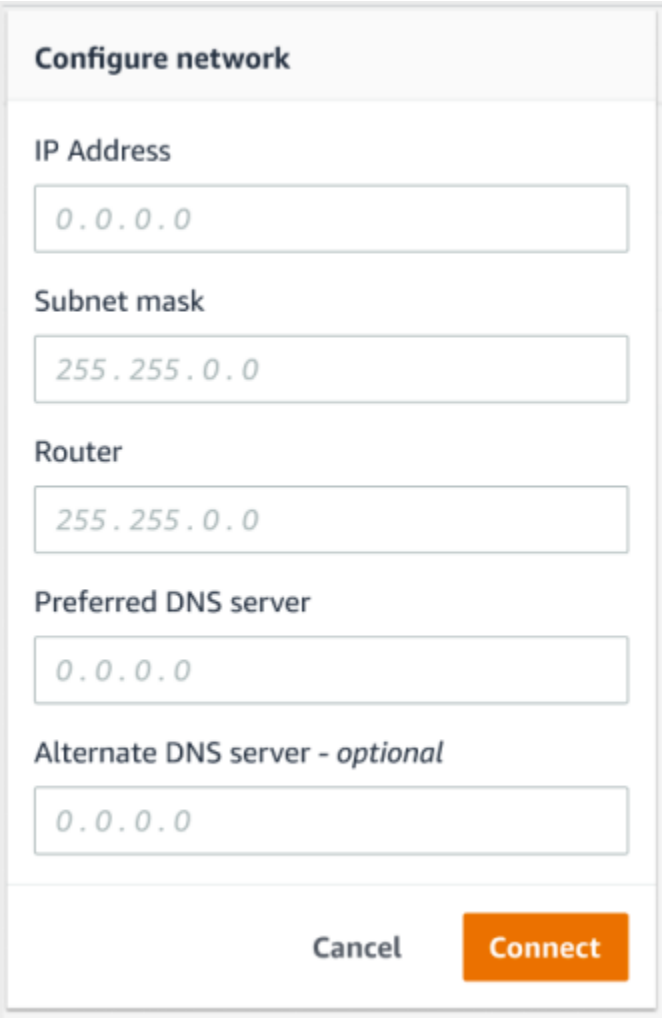
9. お使いのネットワーク設定を選択します。

   ゲートウェイのコミッショニングが行われ、ネットワークに接続されるまでには、数分かかる場合があります。

   ゲートウェイの動作に他の問題がある場合は、リセットすると役立つ場合があります。詳細については、「???」を参照してください。

   a. [自動 (DHCP)] を選択した場合、Amazon Monitron はゲートウェイに接続するようにネットワークを自動的に設定します。

   b. [手動] を選択した場合は、[IP アドレス]、[サブネットマスク]、[ルーター]、[優先 DNS サーバー]、[代替 DNS サーバー (オプション)] の情報を入力します。次に、[接続] を選択します。



ステップ 2: アセットを追加する

Amazon Monitron では、モニタリングする機械をアセットと呼びます。通常、アセットは個々の機械ですが、機器の特定のセクションである場合もあります。アセットはセンサーとペアリングされており、センサーは温度と振動を直接モニタリングして、潜在的な故障がないかを確認します。Amazon Monitron ウェブアプリと Amazon Monitron モバイルアプリの両方を使用してアセットを追加できます。

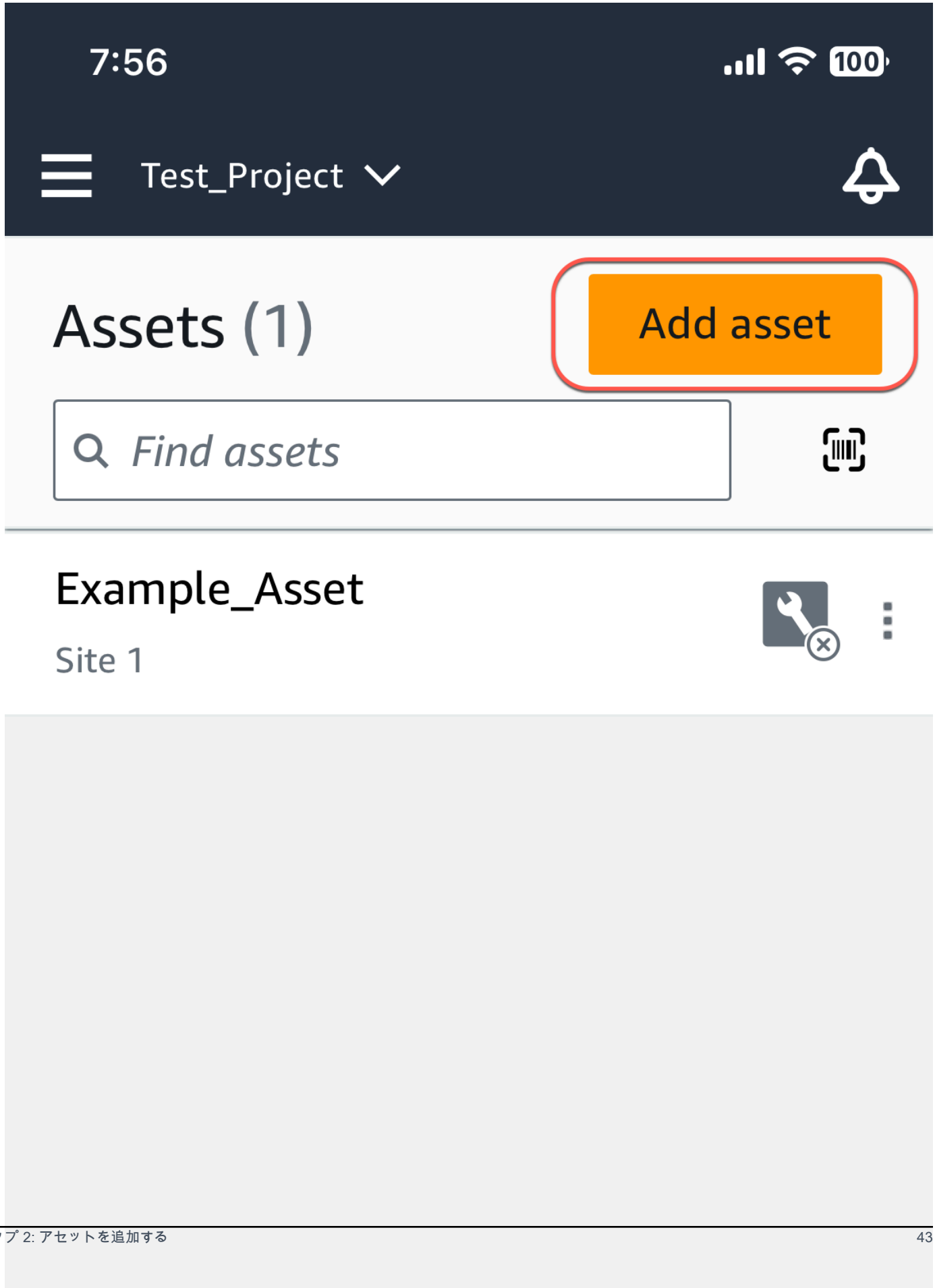
トピック

- モバイルアプリを使用したアセットの追加
- ウェブアプリを使用したアセットの追加

モバイルアプリを使用したアセットの追加

モバイルアプリを使用してアセットを追加するには

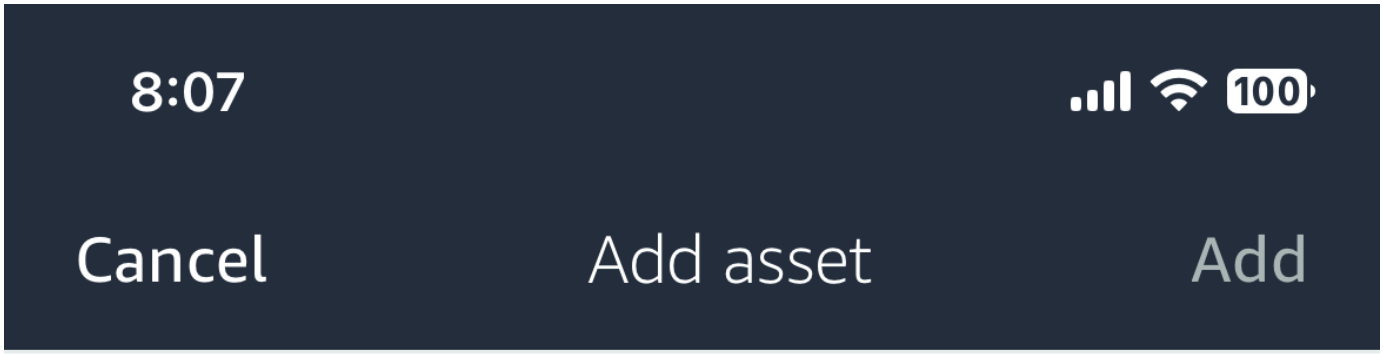
1. モバイルアプリにサインインし、アセットを追加するプロジェクトを選択します。


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

2. アセットを追加するプロジェクトが正しいサイトにいることを確認します。プロジェクト名またはサイト名は、アプリ内でそのレベルにいることを示しています。

サイトレベルからプロジェクトレベルへの変更、またはその逆の変更の詳細については、「モバイルアプリを使用したプロジェクトとサイト間の移動」を参照してください。

3. アセットページから、アセットの追加を選択します。
4. アセットの追加ページで、アセット名に、作成するアセットの名前を追加し、追加を選択します。



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.

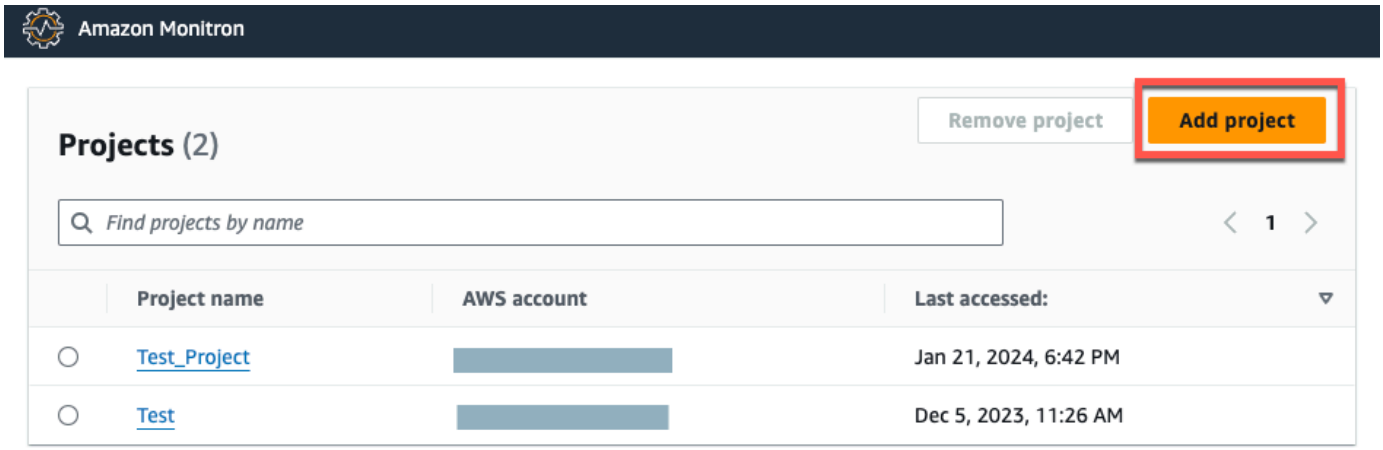
> **Note**
>
> アセット名を特定する QR コードがある場合は、その QR コードを選択してスキャンできます。

最初のアセットを追加すると、[アセット] ページのリストにそのアセットが表示されます。

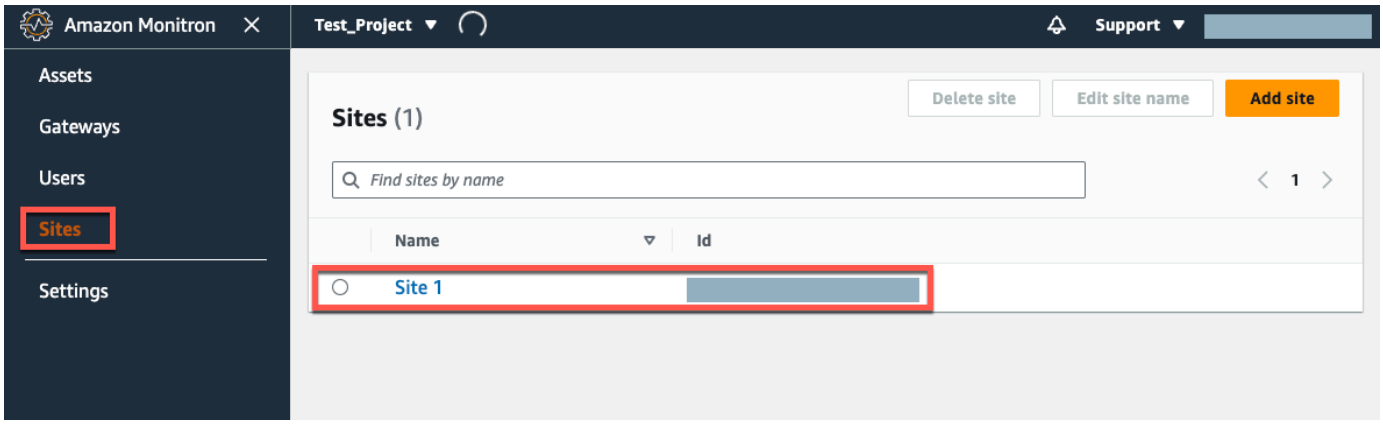
ウェブアプリを使用したアセットの追加

ウェブアプリを使用してアセットを追加するには

1. ウェブアプリにサインインし、アセットを追加するプロジェクトを選択します。

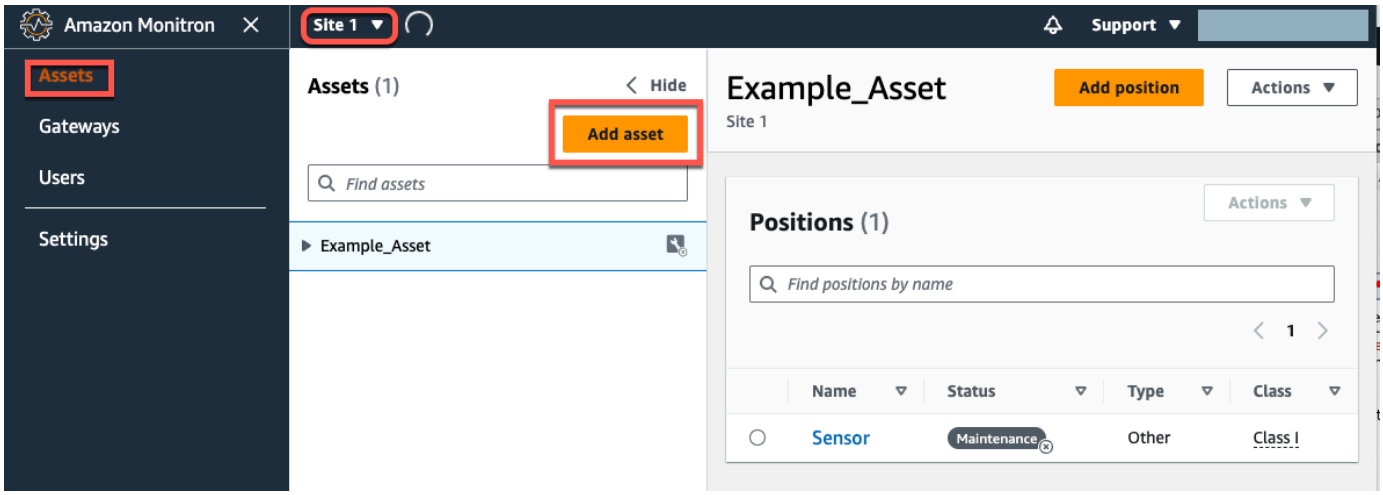


2. 左側のナビゲーションメニューから、サイトを選択し、アセットの対象となるサイトを選択します。

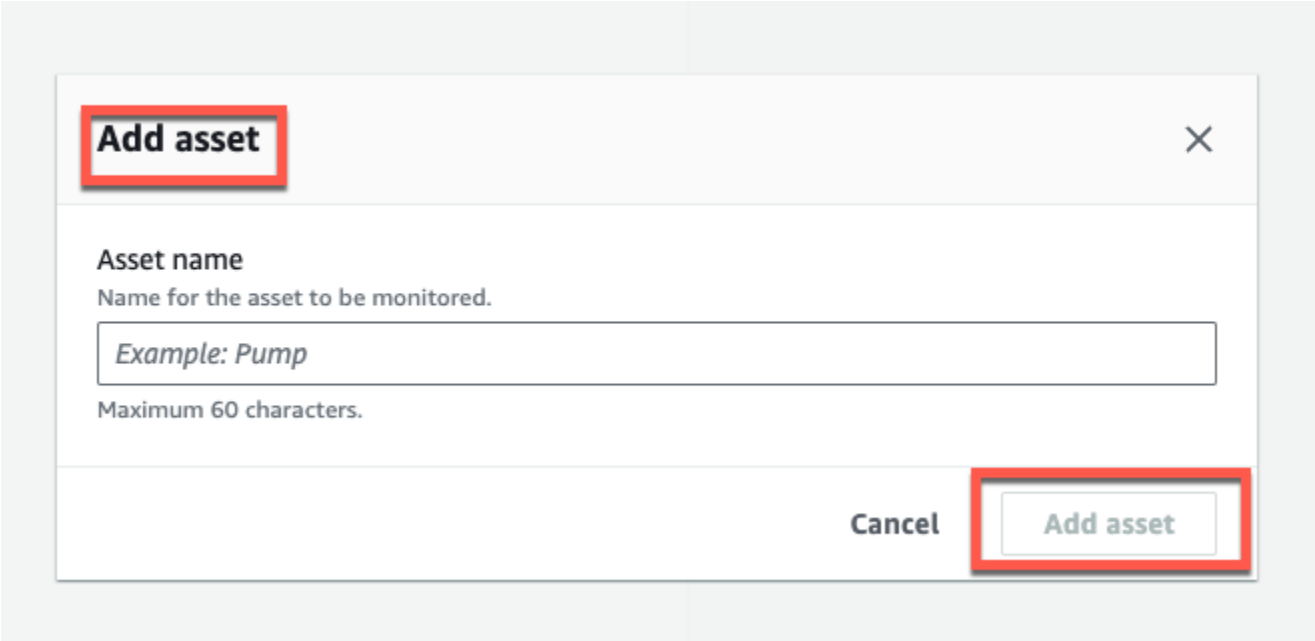


> **Note**
>
> アセットをプロジェクトに直接追加することもできます。

3. アセットページから、アセットの追加を選択します。



4. アセットの追加ページで、アセット名に、作成するアセットの名前を追加し、アセットの追加を選択します。



最初のアセットを追加すると、[アセット] ページのリストにそのアセットが表示されます。

ステップ 3: センサーを取り付ける

アセットはセンサーとペアリングされており、センサーはアセットの状態を直接モニタリングします。各センサーを、アセット上のモニタリングする場所に取り付けます。各アセットには 1 つ以上のセンサーを取り付けることができます。各センサーは、ペアリングされた位置で振動と温度の測定値を取得し、ゲートウェイを使用してそのデータを AWS クラウドに送信し、機械の状態を分析します。

センサーの取り付け場所

センサーを設置するときは、機械の温度や振動を正確に検出できる場所を選択します。

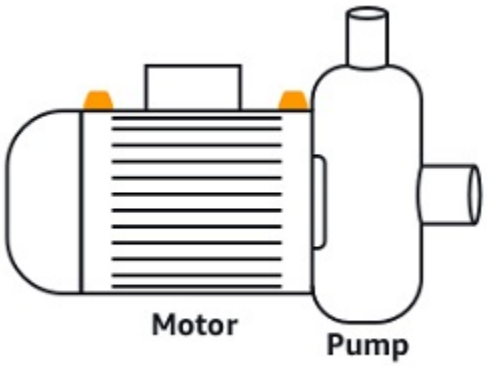
精度を最大限に高めるには:

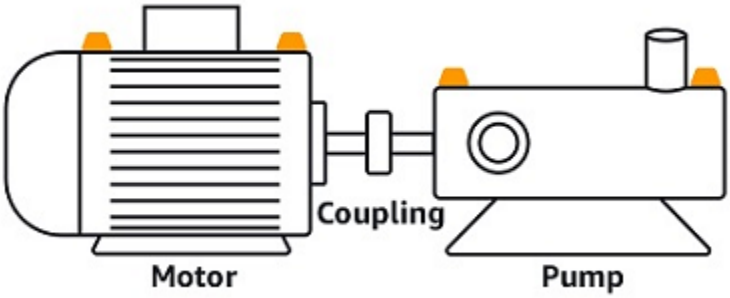
- センサーをターゲットコンポーネントのハウジングに直接取り付けます。
- 振動伝達経路の長さ (振動発生源とセンサーの間の距離) を最小限にします。
- 板金カバーなど、固有周波数によって振動する可能性のある場所にセンサーを取り付けることは避けてください。

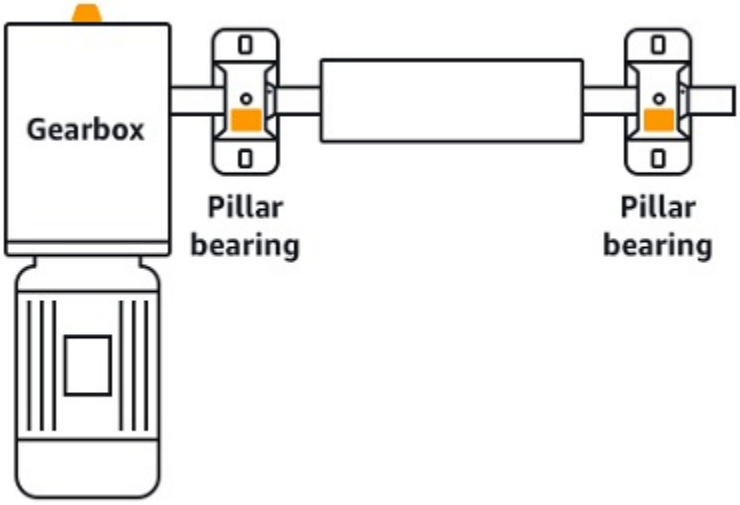
振動は、発生源から 30 ~ 36 インチ (75 ~ 90 cm) より遠くなると減衰します。振動伝達経路に以下のような属性があると、振動伝達経路の長さを短縮させることができます。

- 多数の取り付け面 (信号反射をもたらすことが可能)
- ゴムやプラスチックなど、振動を吸収する材料

以下の例は、センサーを取り付ける場所を示しています。詳細と例については、「Amazon Monitron ユーザーガイド」の「Where to Place Your Sensors」を参照してください。

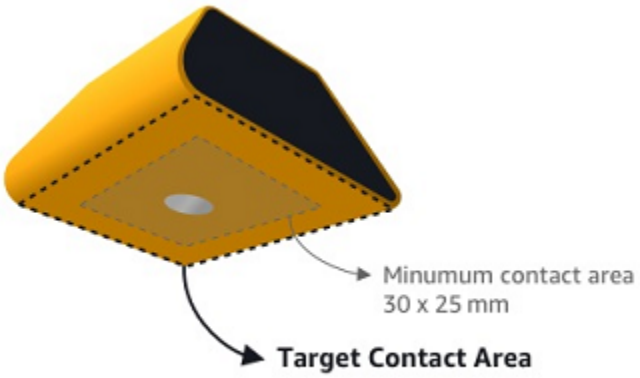






センサーの取り付け方法

アセットのどこにセンサーを取り付けるかを決めたら、センサーベースの少なくとも 3 分の 1 がアセットに固定されることを確認します。センサーは、センサーの底面全体で振動と温度の測定値を検出します。ただし、以下の画像に示すように、アセットの対象エリアを、センサーのできるだけ中央に配置することが重要です。



センサーを工業用接着剤で取り付けます。シアノアクリレート系のエポキシ樹脂をお勧めします。アセットへのセンサー取り付けの詳細については、「Amazon Monitron ユーザーガイド」の「How to Place the Sensors」を参照してください。

> **Warning**
>
> Amazon Monitron センサーは、工業用接着剤を使用して機器に取り付けることができます。接着剤を選ぶ前に、取り付け面を確認することをお勧めします。最大 5 mm の粗さ/ギャップの表面では、LOCTITE® 3090 や LOCTITE® 4070 など、ギャップを埋める接着剤を選択できます。取り付け面が平ら (粗さが 0.1 mm 未満) の場合は、LOCTITE® 454 などの一般的な接着剤が利用できます。接着剤ベンダーによる処理ガイドラインを必ず確認し、それに従ってください。
> 接着剤の安全な使用の詳細については、必要に応じて「Loctite 454 技術情報」、「Loctite 3090 技術情報」、または「Loctite 4070 技術情報」を参照してください。

Amazon Monitron センサーを取り付けるには

1. センサーの底面に接着剤を薄く塗布し、接触面積を最大化します。
2. センサーを機械部品の取り付け位置に固定し、接着剤の説明書に記載されている時間を守ってしっかりと押し付けます。

ステップ 4: センサーをアセットにペアリングする

アセットとペアリングする各センサーはポジションが指定されており、アセットの特定の部分をモニタリングするように設定されています。例えば、コンベアベルト上のベアリングをモニタリングするように設定されたセンサーは、「Left Bearing 1」というポジション名と、「ベアリング」というポジションのタイプを持っている場合があります。

Amazon Monitron は、2 つの電子デバイス間の通信に短距離 (4 cm 以下) ワイヤレステクノロジーである近距離無線通信 (NFC) を使用しています。Amazon Monitron を使用するには、NFC がネイティブにインストールされた iOS または Android 8.0 以降のスマートフォンが必要です。

> **Important**
>
> モニタリングする機器は、センサーとペアリングする前に正常な状態でなければなりません。Amazon Monitron は、通常の状態に基づいて機器のベースラインを確立する必要があり、これによって後から異常を判断できます。

センサーをアセットとペアリングするには

1. 「ステップ 3: センサーを取り付ける」の説明に従って、センサーを正しい場所に取り付けます。このステップ 4 では、センサーをアセットとペアリングした後で取り付けることもできます。
2. スマートフォンの NFC 機能がオンになっていて、機能していることを確認します。
3. Amazon Monitron モバイルアプリを開き、センサーを追加するプロジェクトを選択します。
4. ナビゲーションメニューから、正しいサイトにいることを確認し、アセットを選択します。
5. [アセット] のリストから、先ほど作成したアセットを選択します。
6. アセットページで、位置の追加を選択します。
7. 位置の追加ページで、次の操作を行います。

   a. 名前 に、ポジションの名前を追加します。

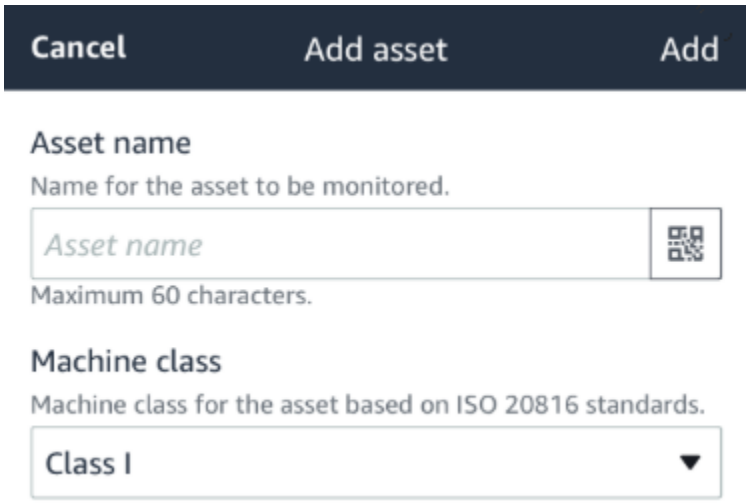
   b. Type で、モニタリングする場所に最適な位置のタイプを選択します。

      - ベアリング
      - コンプレッサー
      - ファン
      - ギアボックス
      - モーター
      - ポンプ
      - その他

> **Note**
>
> センサーをペアリングした後で、ポジションのタイプを変更することはできません。

c. クラス では、使用可能な 4 つの からアセットのマシンクラスを選択します。

> **Note**
>
> アセットの機械のクラスは ISO 20816 規格に基づいています。Amazon Monitron 管理者は、プロジェクト内のすべてのポジションにカスタムマシンアセットクラスを作成することもできます。マシンクラスとそのカスタマイズの詳細については、「アセット」を参照してください。



8. [次へ] を選択します。センサーを追加するように求められます。センサーを追加する方法については、「センサー」を参照してください。
9. [センサーをペアリング] をクリックします。
10. スマートフォンをセンサーに近づけて、センサーを登録します。登録が完了すると、進行状況バーが表示されます。

センサーのコミッショニングに数分かかる場合があります。センサーのペアリングに問題がある場合は、「センサーのペアリング」で詳細を確認してください。

> **Tip**
>
> スマートフォンがセンサーを検出できない場合は、NFC アンテナがセンサーに接近するようにスマートフォンを近づけてみてください。iPhone モデルの場合、アンテナはデバイスの上端にあります。Android モデルの場合、アンテナの位置は異なります。Android デバイスで NFC アンテナを見つけるには、以下のリソースを参照してください。
>
> - NFC detection area (Samsung)
> - Google Pixel のハードウェアの図

[アセット] ページでセンサーがアセットとペアリングされ、ポジションによって識別されるようになります。

警告とアラートの把握

> **Note**
>
> このセクションでは、Amazon Monitron モバイルアプリの使用に焦点を当てています。Amazon Monitron ウェブアプリの詳細については、「Amazon Monitron ユーザーガイド」の「Understanding sensor measurements」を参照してください。

センサーがアセットとペアリングされると、Amazon Monitron はアセットの状態のモニタリングを開始します。機械の異常状態を検出すると通知 ( ) を送信し、アセットの状態を変更します。アラート通知は、機械学習と機械の振動に関する ISO 20816 規格を組み合わせて生成されます。

データをモニタリングし、異常に関するアラートに対応するには、Amazon Monitron モバイルアプリを使用します。

管理者から、初めてログインしてプロジェクトに接続する方法を記載した E メールが送信されます。

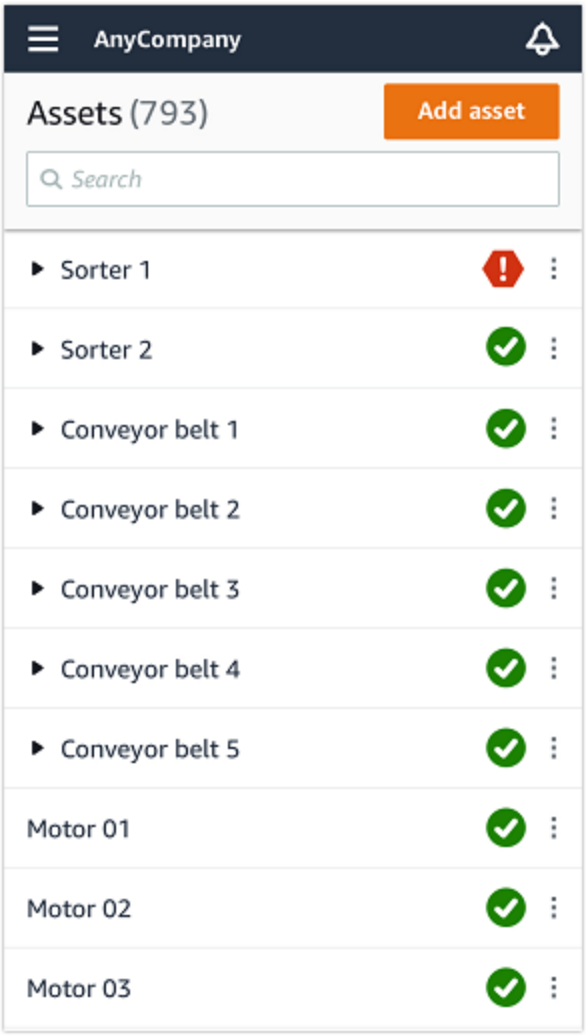
トピック

- ステップ 1: アセットの健全性を把握する

- ステップ 2: アセットの状態を表示する
- ステップ 3: 機械の異常を表示して確認する
- ステップ 4: 機械の異常を解決する
- ステップ 5: アラートのミュートとミュート解除

ステップ 1: アセットの健全性を把握する

Amazon Monitron モバイルアプリを使用してアセットをモニタリングするには、まず [アセット] のリストから始めます。このリストは、モバイルアプリを開くと表示されます。



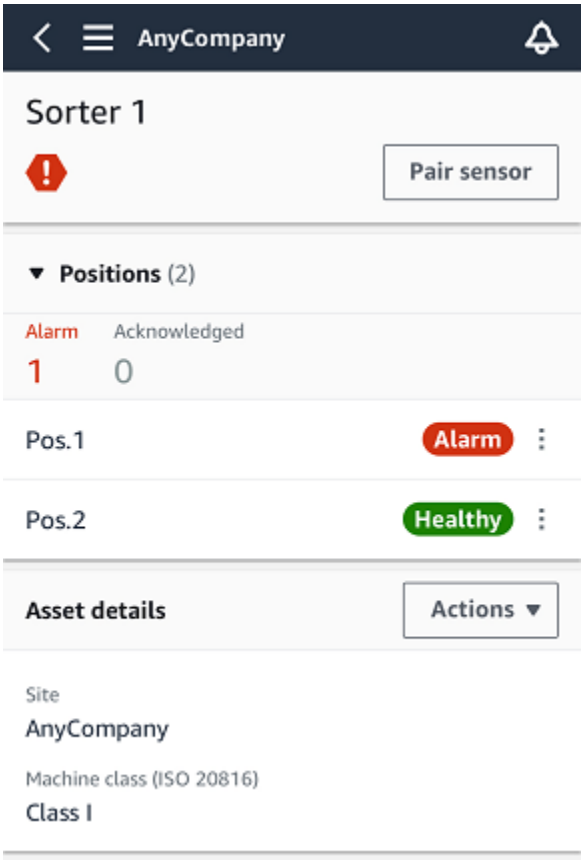
[アセット] のリストには、プロジェクトまたはサイトの各アセットが一覧表示されています。

[アセット] ページのリストには、各アセットに状態を示すアイコンが示されています。以下の表では、そのアイコンについて説明します。

アイコン	ヘルスステータス
	正常状態: アセット内のすべてのセンサーポジションのステータスは正常です。
	警告状態: アセットのポジションの 1 つで警告がトリガーされています。これは、Amazon Monitron が潜在的な障害の初期兆候を検出したことを示しています。Amazon Monitron は、機械学習と ISO 振動規格を組み合わせて機器の振動と温度を分析し、警告状態を特定します。
	アラーム状態: アセットが警告状態になると、Amazon Monitron は引き続きそのアセットをモニタリングします。繰り返しになりますが、Amazon Monitron は機械学習と ISO 振動規格を組み合わせてデータを分析しています。アセットの状態が著しく悪化した場合、Amazon Monitron は機器の状態が著しく悪化したことを検出し、[アラーム] 通知を送信してエスカレーションを行います。できるだけ早く問題を調査することをお勧めします。問題が解決されないと、機器に障害が発生する可能性があります。

アイコン	ヘルスステータス
	メンテナンス状態: アセットのセンサーの 1 つがメンテナンス状態です。アラーム状態は技術者によって確認されましたが、まだ問題が解決されていません。
センサーなし	センサーなし: アセット上の少なくとも 1 つのポジションで、センサーがペアリングされていません。

アセットを選択すると、アプリにはアセット上の各センサーポジションのヘルスステータスが表示されます。



以下の表では、ポジションステータスのインジケータについて説明します。

ステータス	State
	このポジションは正常で、測定値はすべて正常範囲内です。
	このポジションでは、潜在的な故障状態の初期兆候を示す警告がトリガーされています。機器を注意深くモニタリングし、計画メンテナンスの際に調査を開始することをお勧めします。
	このポジションでは、機械の振動または温度が正常範囲外であることを示すアラームがトリガーされています。できるだけ早く問題を調査することをお勧めします。問題が解決されないと、機器に障害が発生する可能性があります。
	このポジションのアラーム状態は技術者によって確認されましたが、まだ問題が解決されていません。
センサーなし	このポジションではセンサーがペアリングされていません。

個々のポジションで問題が発生すると、そのポジションとアセット全体のステータスが変更されます。

ステップ 2: アセットの状態を表示する

アセットを表示すると、単にアセットとポジションのヘルスステータスを示すアイコンを把握できるだけではありません。センサーによって収集されたデータを自分で確認できるため、とても便利です。

Amazon Monitron モバイルアプリでセンサーデータを表示するには

1. [アセット] のリストで表示するアセットを選択します。
2. 表示させたいデータを持つポジションを選択します。
3. [振動] タブと [温度] タブで、確認したい最近のセンサーデータのグラフと、詳細レベルを選択します。

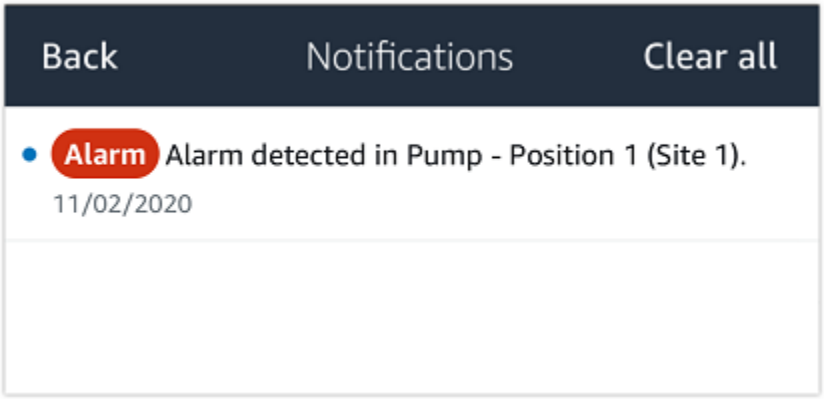
   各期間 (1 日、1 週間、2 週間、1 か月など) で別々のバージョンを選択できます。

ステップ 3: 機械の異常を表示して確認する

Amazon Monitron では、ポジションを長くモニタリングするほどベースラインが微調整され、精度が向上します。

[アラーム] または [警告] がトリガーされると、Amazon Monitron はモバイルアプリに通知を送信します。この通知は、画面右上にアイコン
( )
として表示されます。

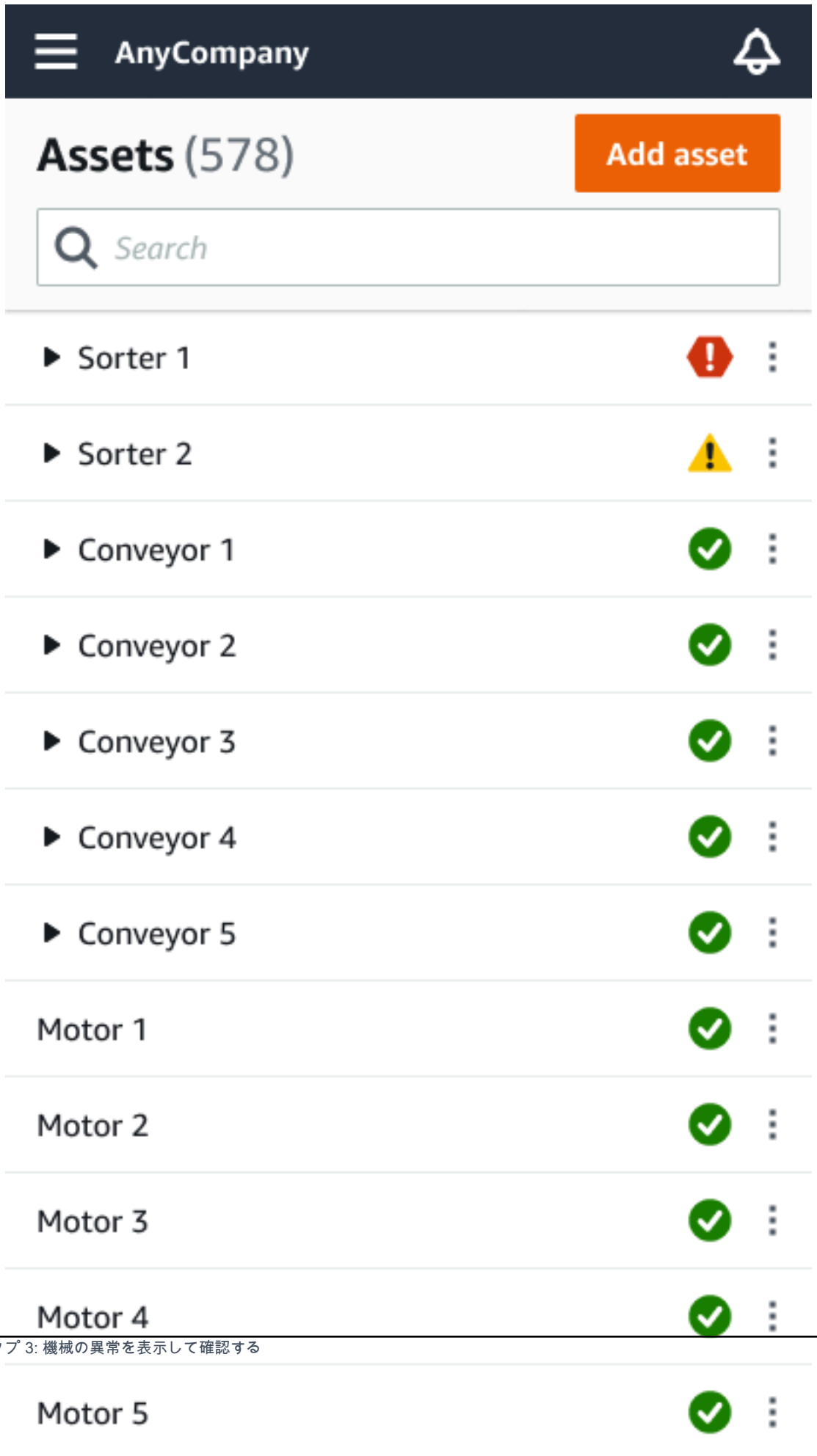
通知アイコンをクリックすると [通知] ページが開き、保留中の通知がすべて一覧表示されます。



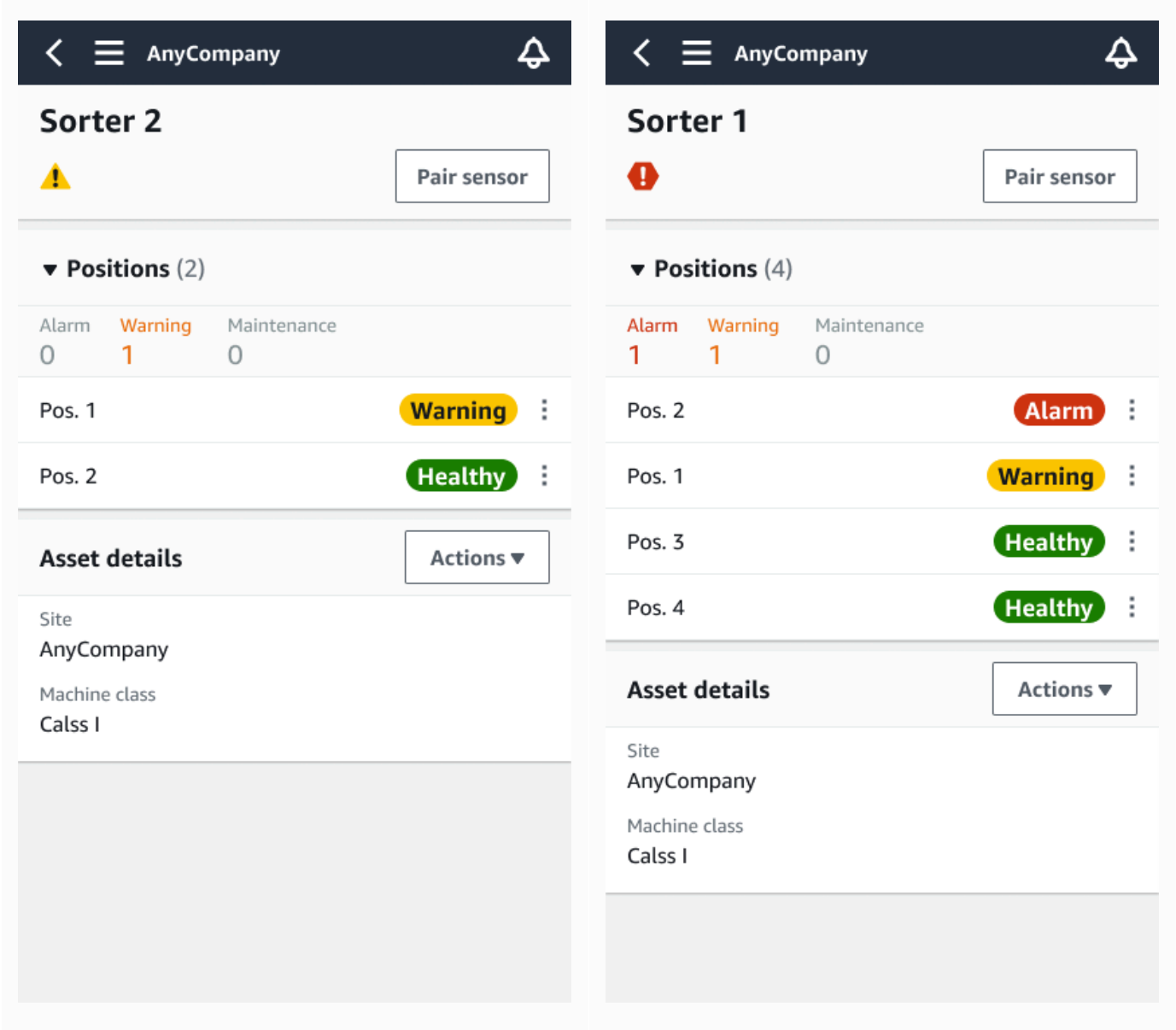
通知を受け取ったら、それを表示して確認する必要があります。これによってアセットの問題が解決されるわけではなく、Amazon Monitron に確認したことを知らせるだけです。

異常を表示して確認するには

1. [アセット] のリストで、アラームが発生しているアセットを選択します。

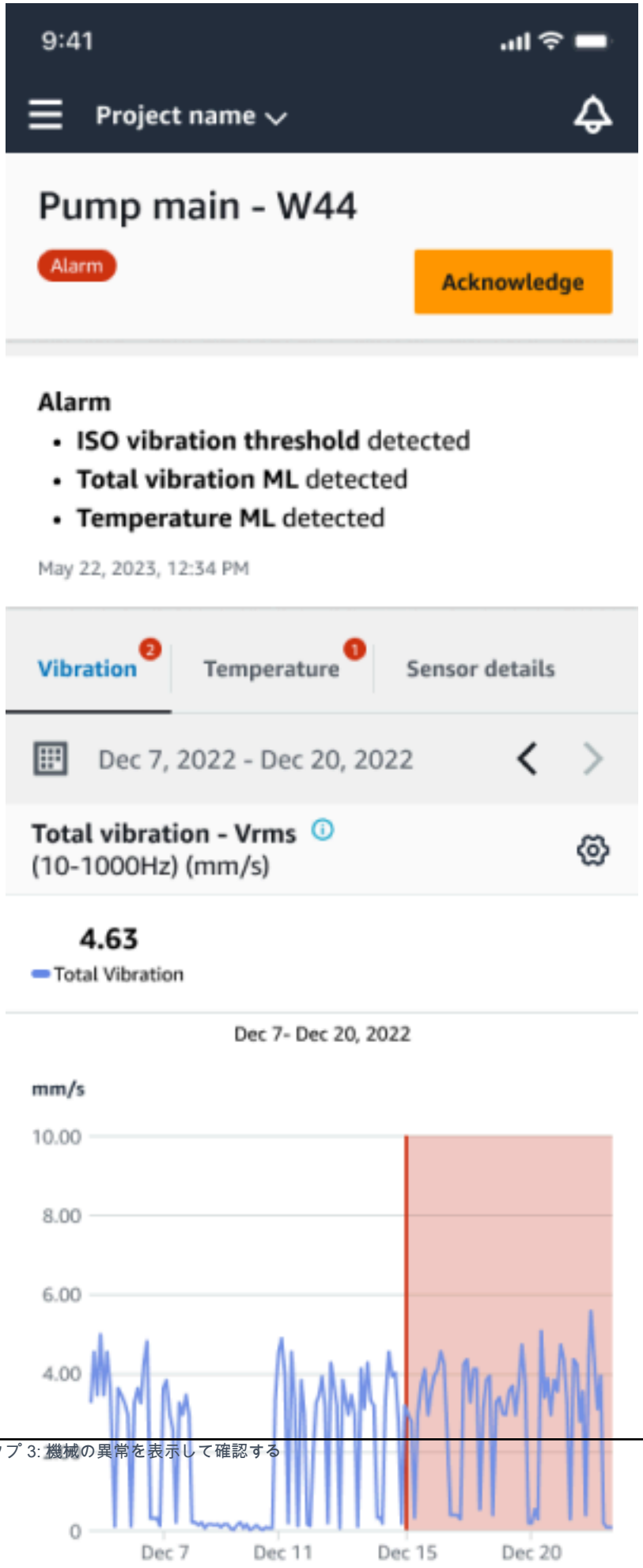

AnyCompany
Assets (578)
Add asset
Search
Sorter 1
Sorter 2
Conveyor 1
Conveyor 2
Conveyor 3
Conveyor 4
Conveyor 5
Motor 1
Motor 2
Motor 3
Motor 4
Motor 5

2. アラームが発生しているポジションを選択すると、問題が表示されます。



3. 問題を認識していることを知らせるには、[確認] をクリックします。

以下の画面のテキストに注目してください。ここには、アラート通知が機器の振動または温度に基づいてトリガーされたのか、あるいは振動の ISO しきい値または機械学習モデルによってトリガーされたのかが示されています。この情報は、技術者が問題を調査して解決する際に使用できます。異常を確認して修復したら、モバイルアプリで問題を解決します。


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

アセットの状態が以下のように変更されます。

アラームを確認したら、異常を調査し、必要に応じて解決します。

ステップ 4: 機械の異常を解決する

異常が解決されると、センサーは正常状態に戻り、問題に関する情報が Amazon Monitron に提供されます。そのため、今後いつ障害が発生する可能性があるかをより正確に判断できます。

障害モードと障害の原因、および異常の解決方法については、「Amazon Monitron ユーザーガイド」の「Resolving a Machine Abnormality」を参照してください。

異常を解決するには

1. [アセット] のリストで、問題が発生しているアセットを選択します。
2. 異常が解決されたポジションを選択します。
3. [解決] を選択します。
4. [障害モード] で、使用可能なタイプから 1 つを選択します。
5. [障害の原因] で、原因を選択します。
6. [実行されたアクション] で、実行したアクションを選択します。
7. [送信] を選択します。

   [アセット] のリストで、アセットのステータスが [正常] に戻ります。

ステップ 5: アラートのミュートとミュート解除

ポジションのアラート (アラームと警告) をミュートまたはミュート解除することを選択できます。

トピック

- アラートのミュート
- アラートのミュート解除

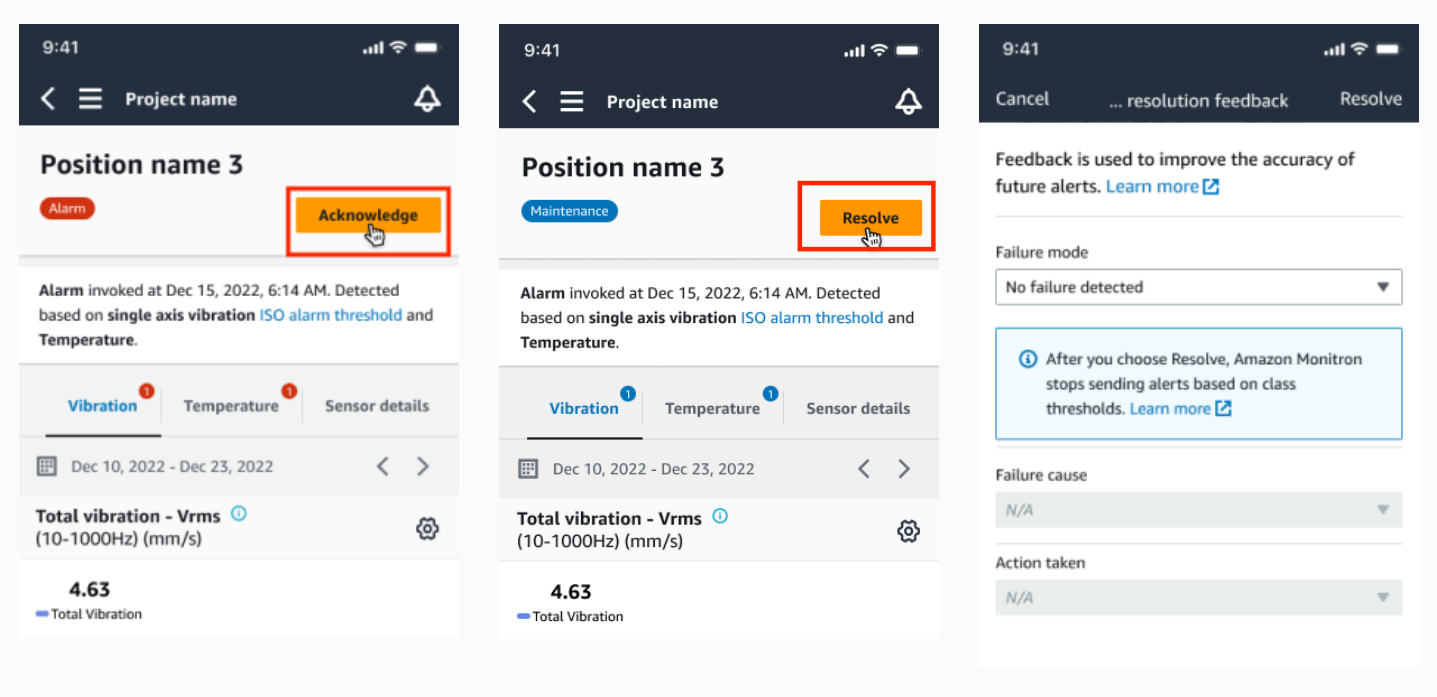
アラートのミュート

ISO しきい値は大規模なクラスの機器に広く適用されています。そのため、特定のアセットの潜在的な障害を検出する際には、他の要因も考慮する必要があります。例えば、アラートが発生した時点で機器がまだ正常であると判断した場合、ISO 振動しきい値によって生成された通知をミュートできます。

また、アラートを閉じるときに「失敗モードに」の「失敗が検出されない」フィードバックを提供することで、アラート (アラームと警告) をミュートすることもできます。Amazon Monitron は、ISO しきい値に基づく通知がミュートされている場合でも、機械学習に基づいて検出された潜在的な障害を引き続きユーザーに通知します。

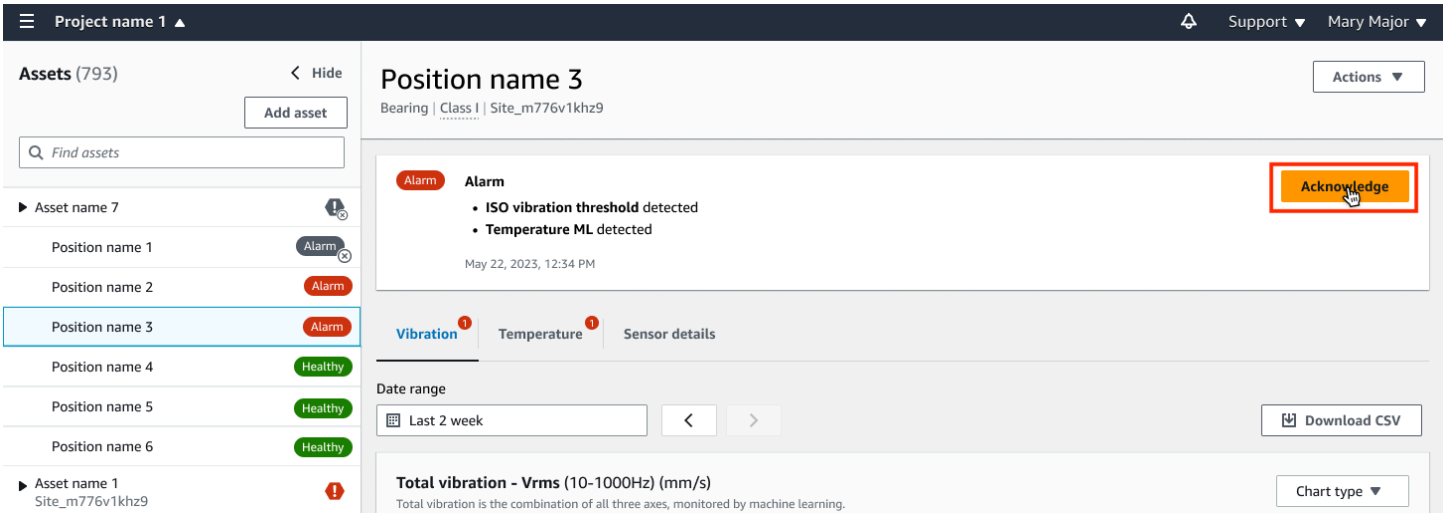
モバイルアプリでのアラートのミュート

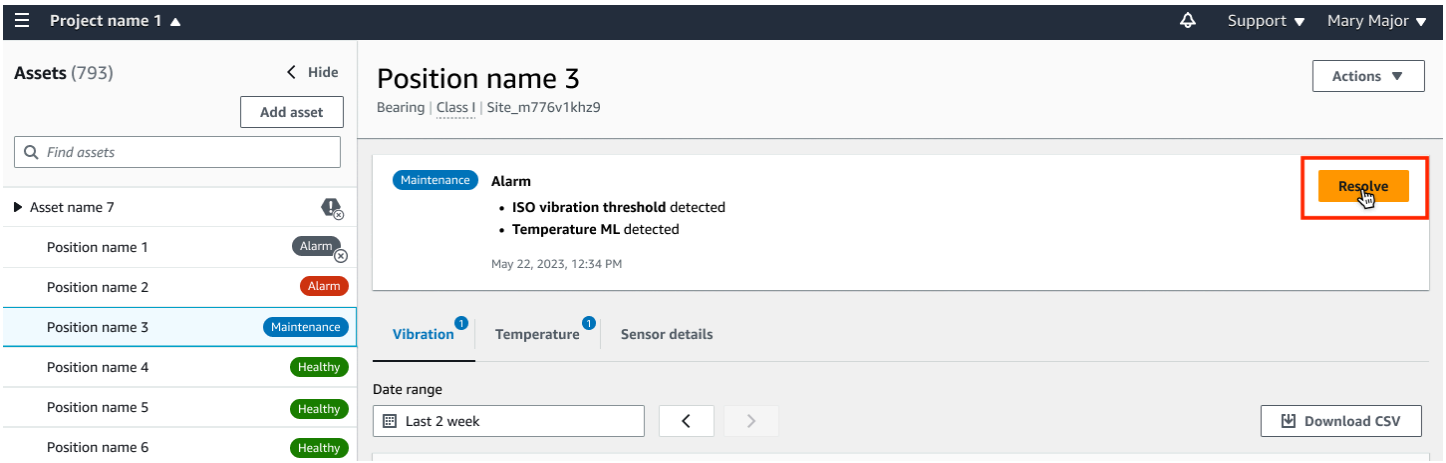
次の画像は、Amazon Monitron モバイルアプリでアラートをミュートする方法を示しています。

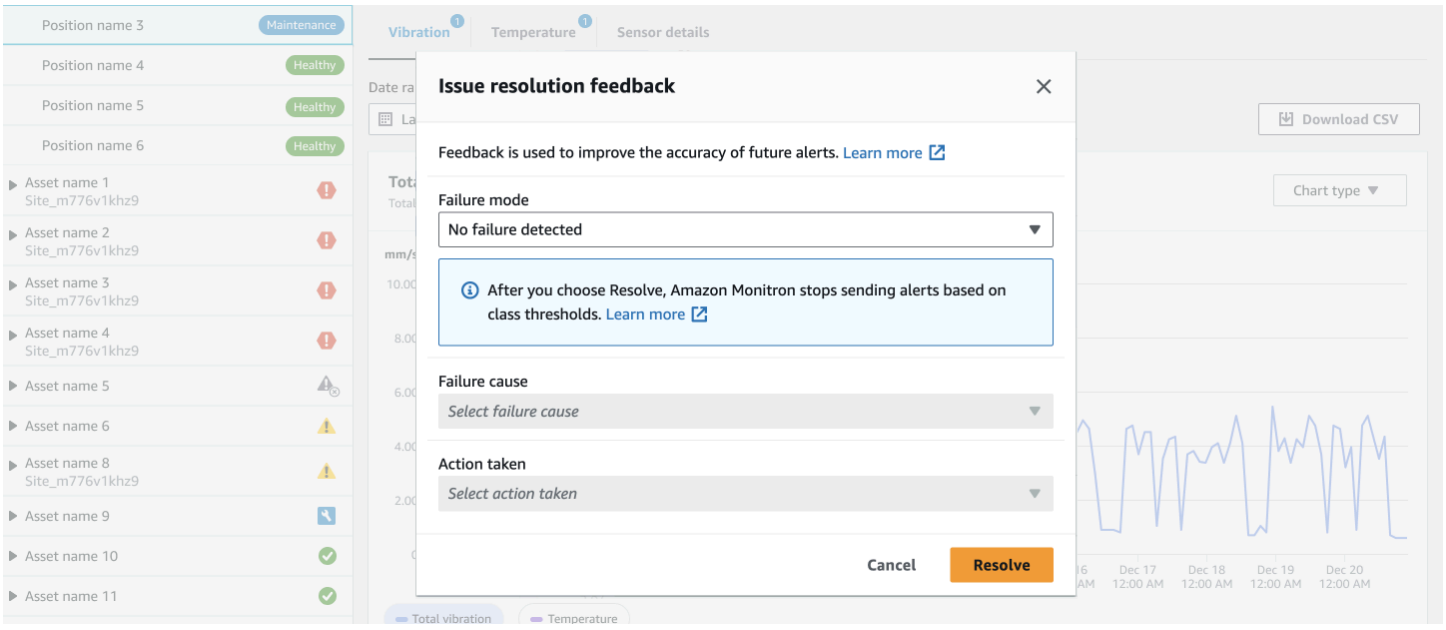


ウェブアプリでのアラートのミュート

次の画像は、Amazon Monitron ウェブアプリでアラートをミュートする方法を示しています。


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
Total vibration
Temperature

アラートのミュート解除

アラート (アラームと警告) はいつでもミュート解除できます。アラートをミュート解除するときは、次のオプションから選択できます。

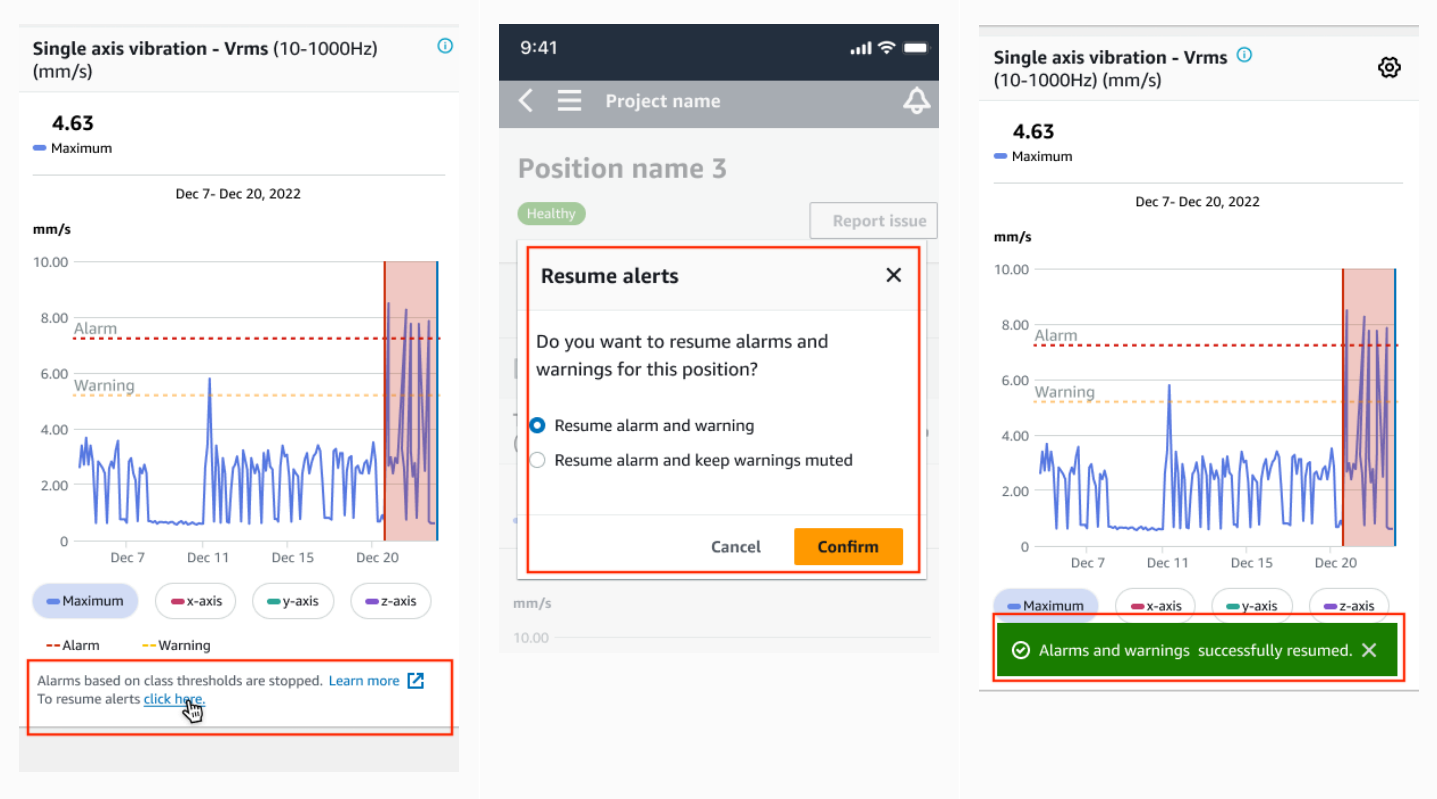
利用可能なオプション

- すべてのアラート (アラームと警告) を再開する
- アラームを再開し、警告をミュート状態にする
- アラームのみを再開する
- 警告のみを再開する

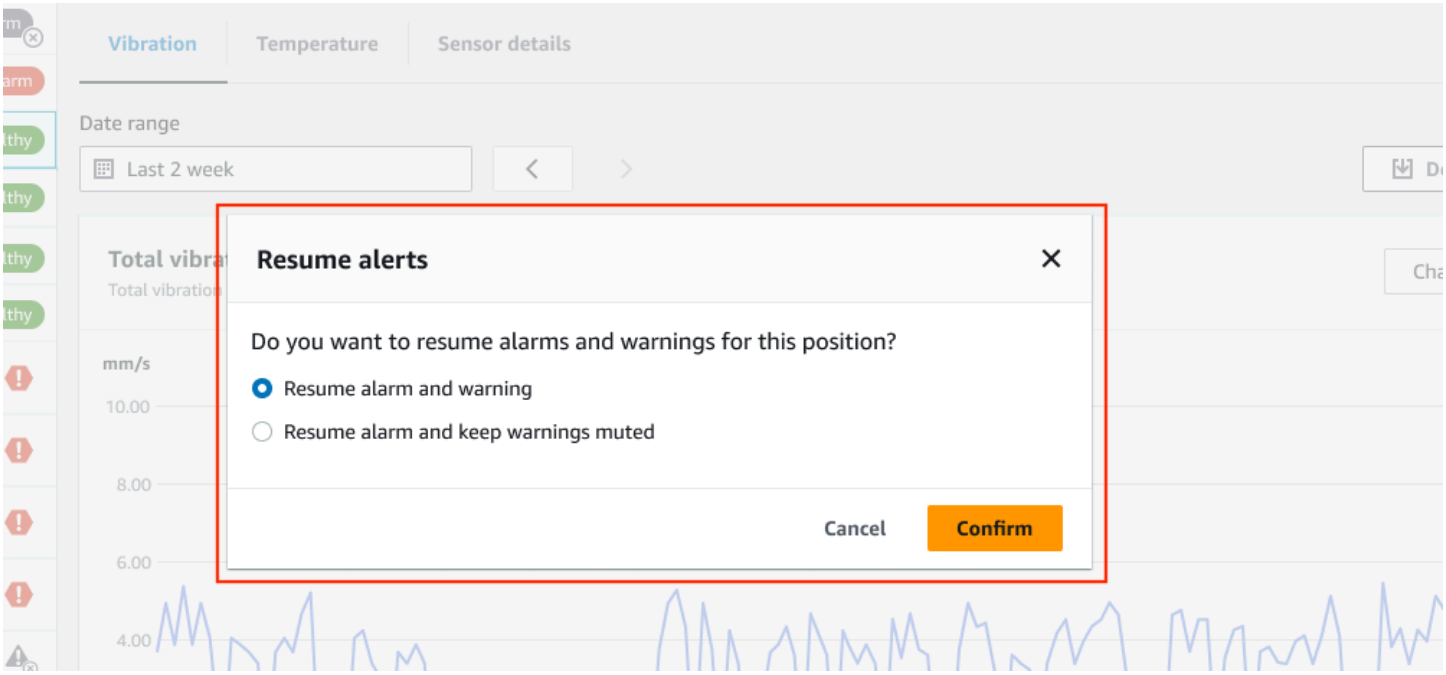
すべてのアラート (アラームと警告) を再開する

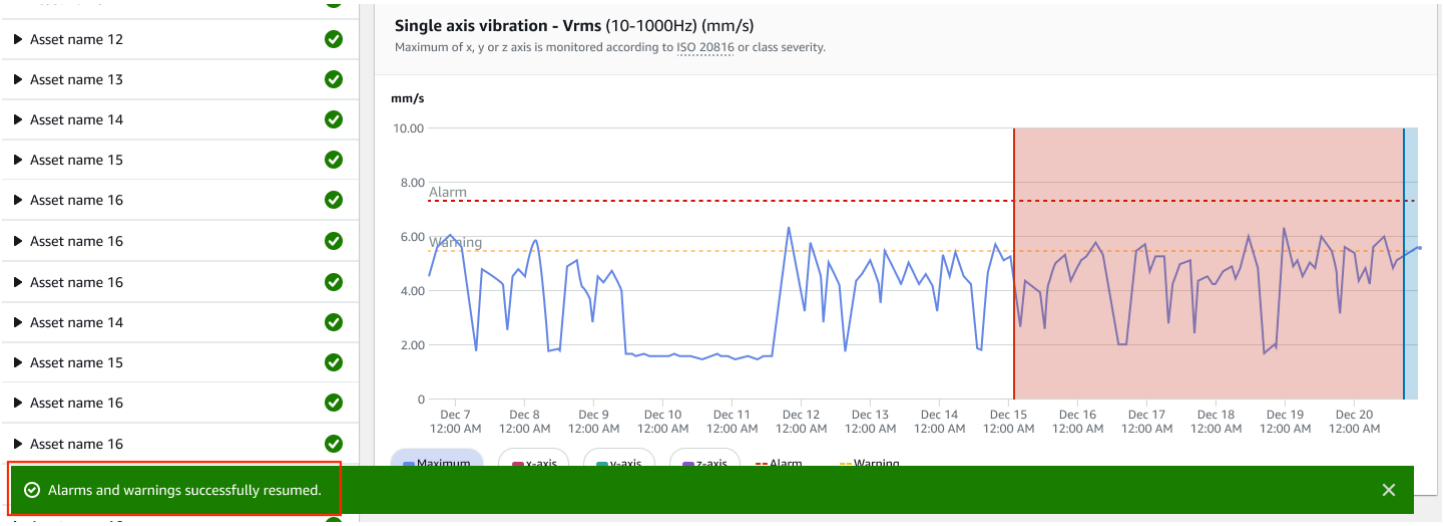
アラームと警告の両方をミュートしている場合は、ミュートを解除できます。

モバイルですべてのアラートを再開する



ウェブ上のすべてのアラートを再開する

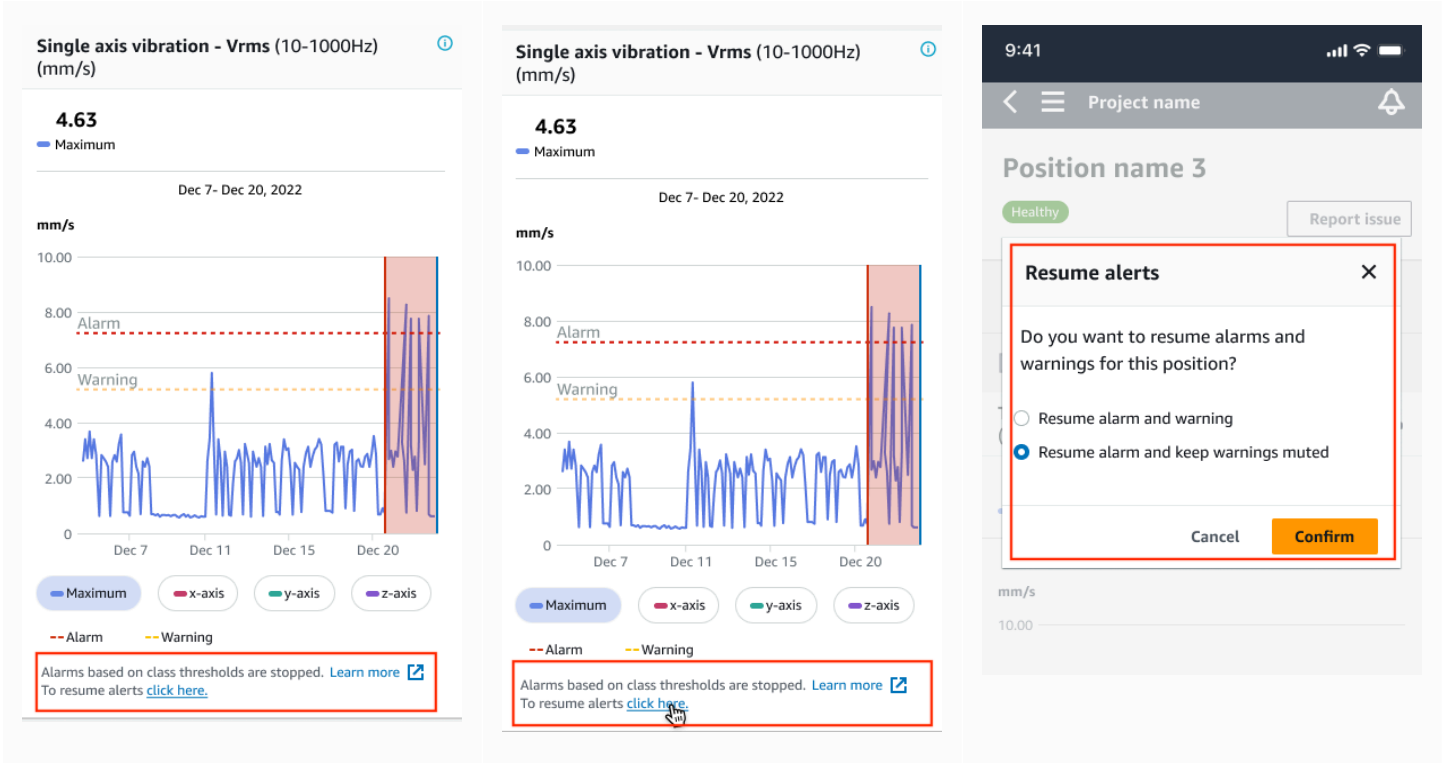




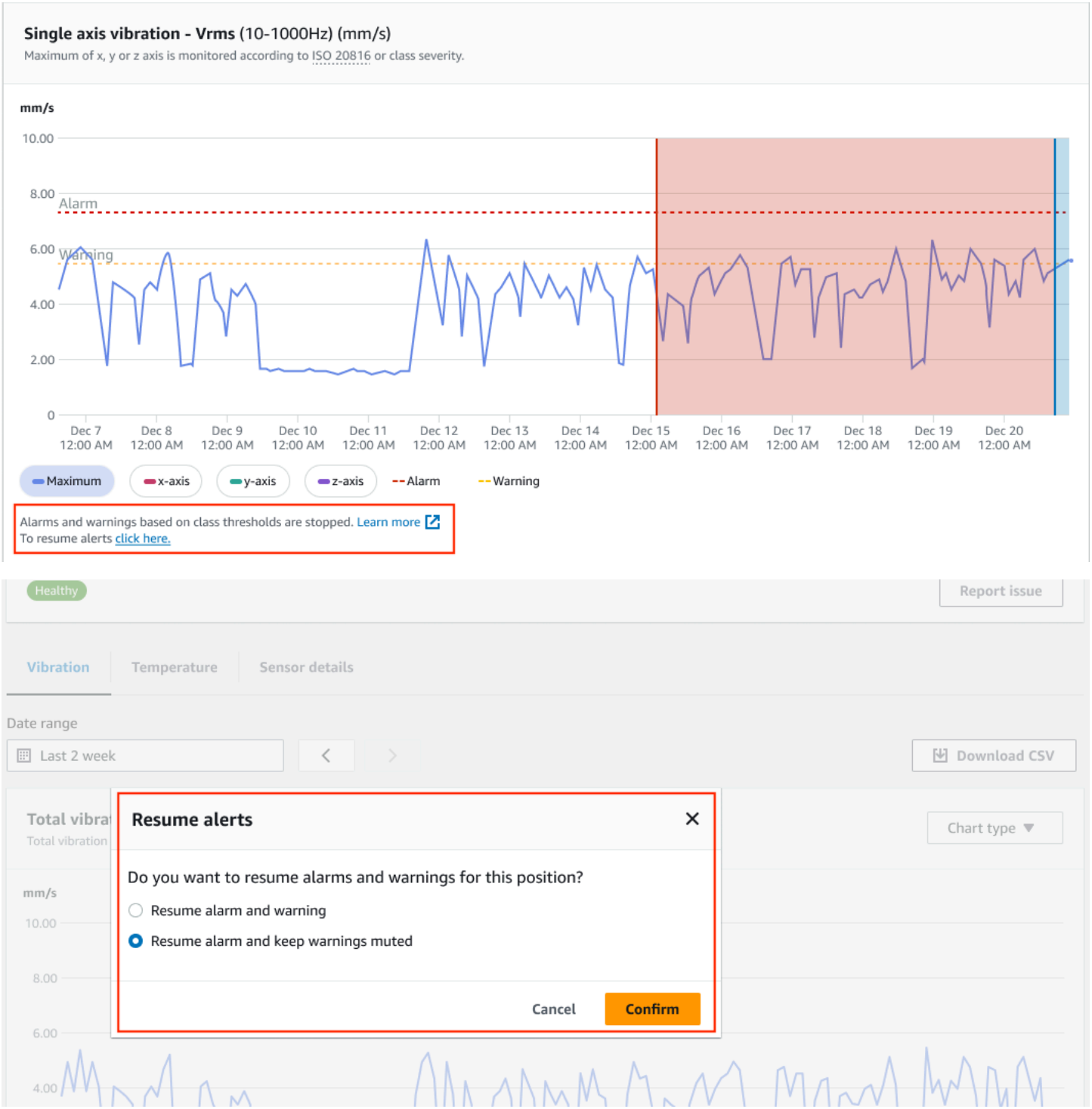
アラームを再開し、警告をミュート状態にする

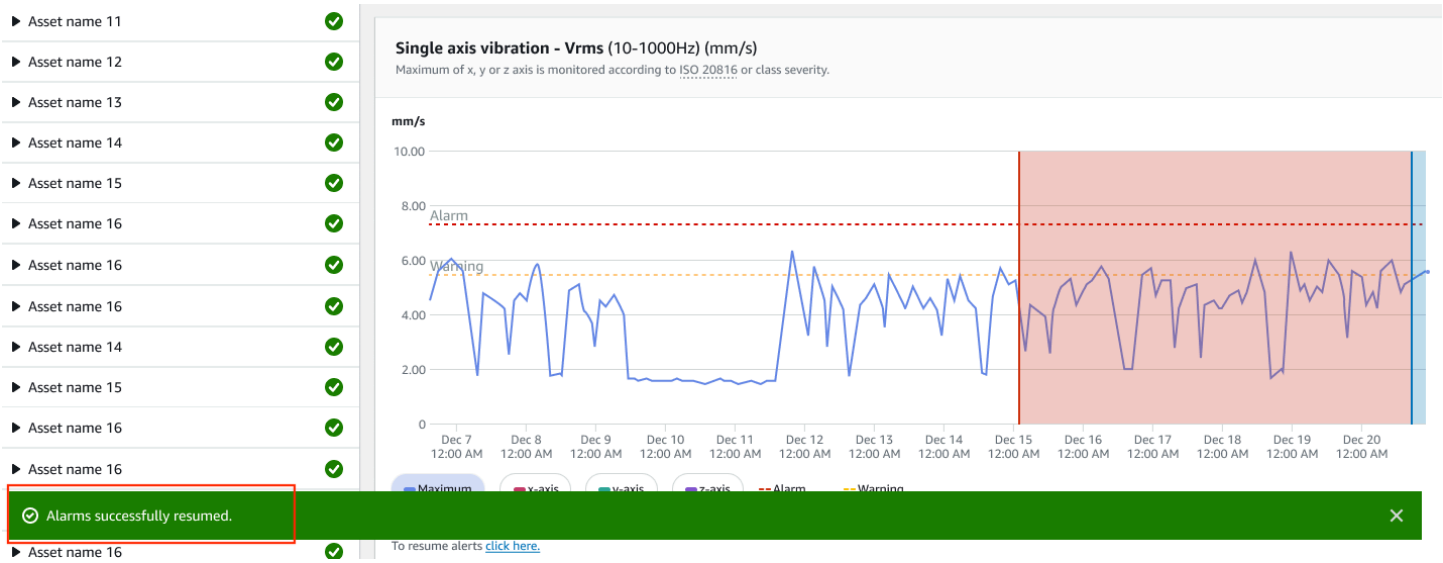
アラームと警告の両方をミュートしている場合は、アラームのミュートを解除し、警告をミュート状態に保つことができます。

モバイルアプリで警告をミュートしたままアラームを再開する



ウェブアプリで警告をミュートしたままアラームを再開する

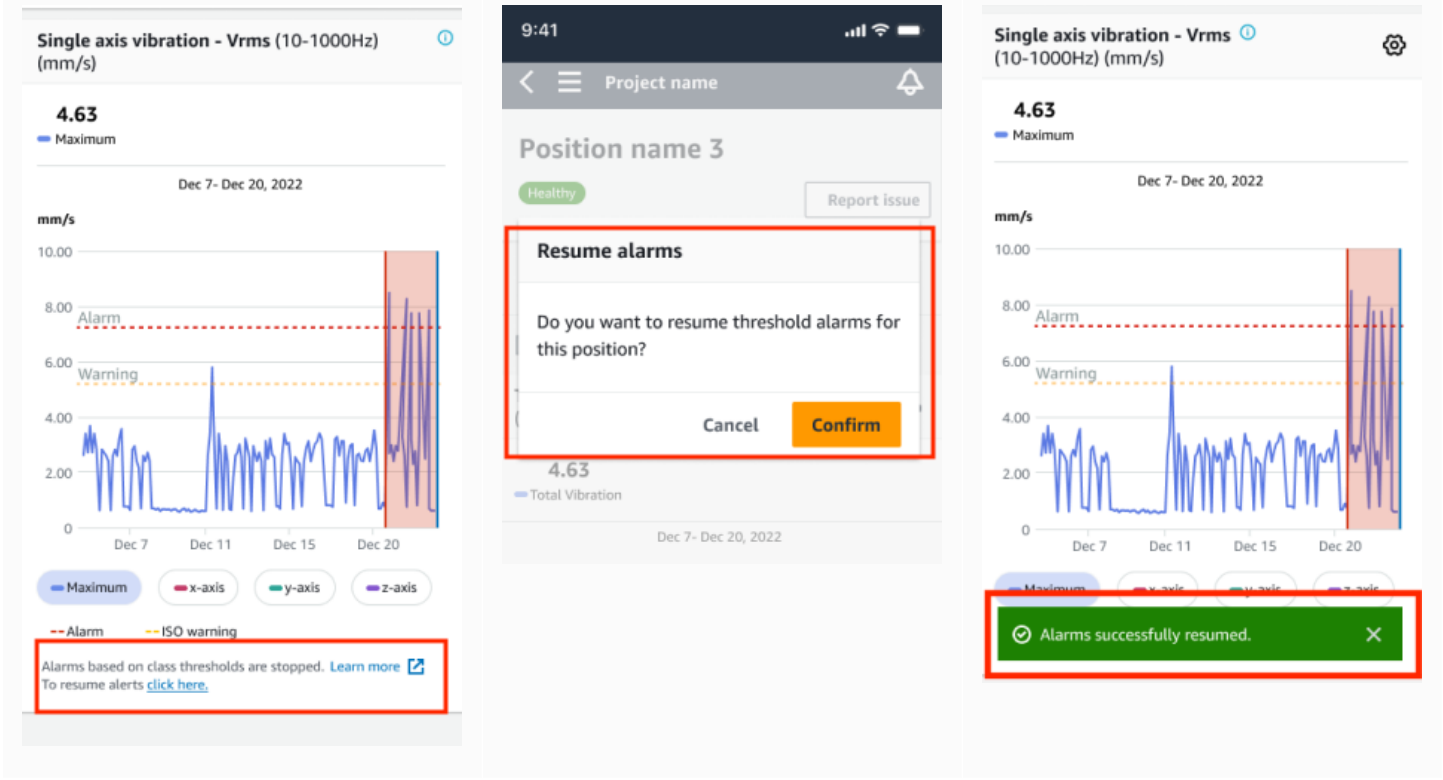




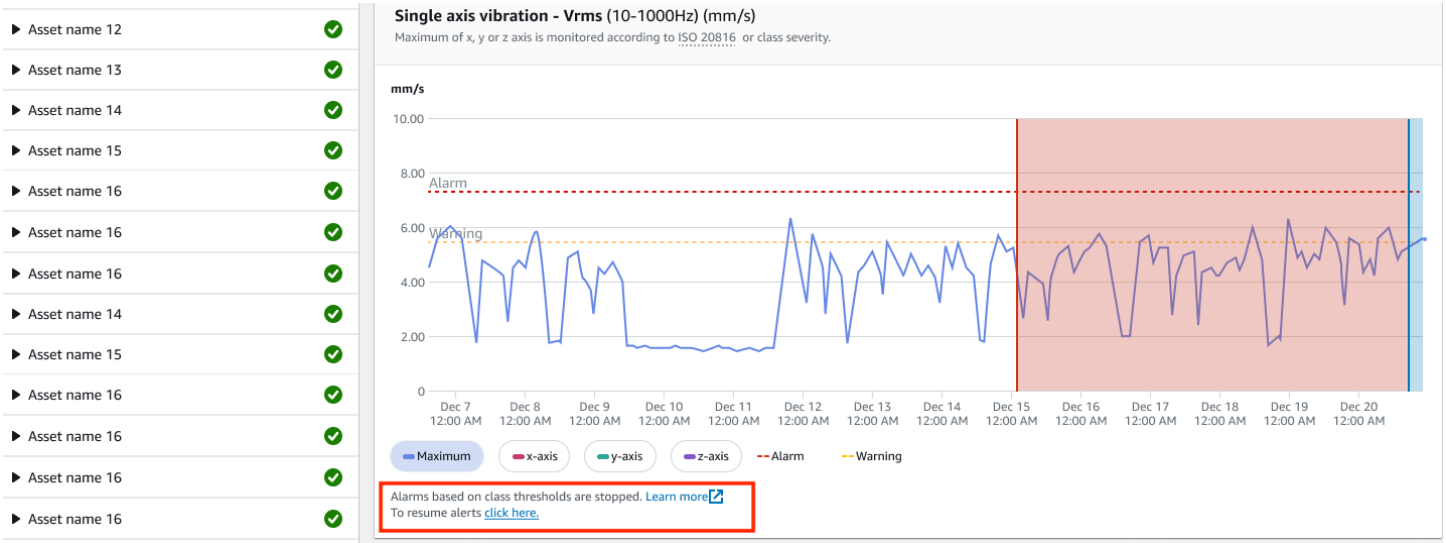
アラームのみを再開する

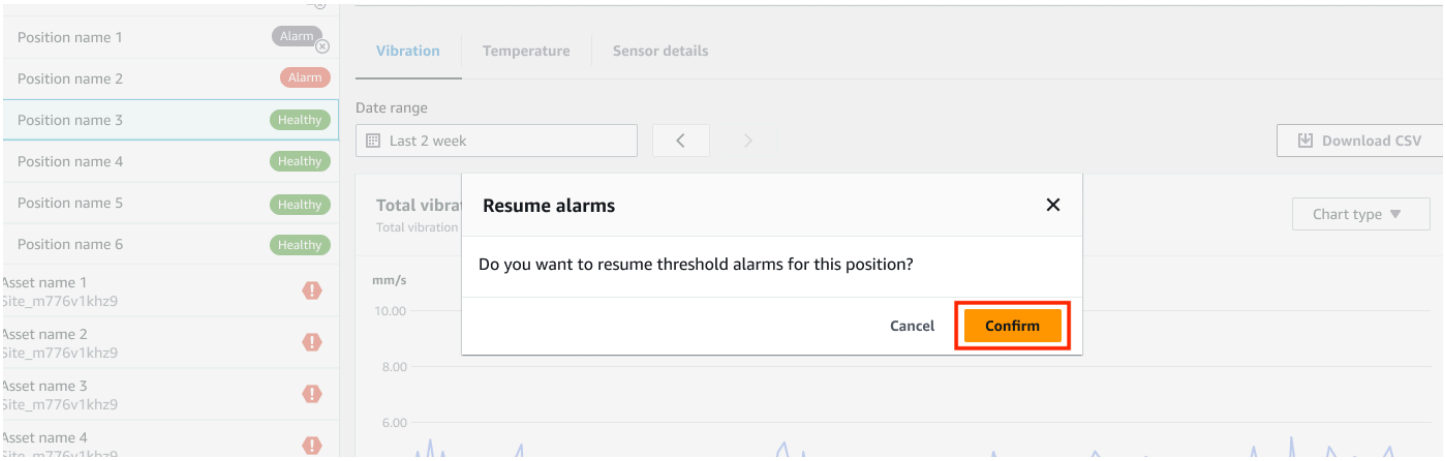
アラームをミュートしている場合は、ミュートを解除できます。

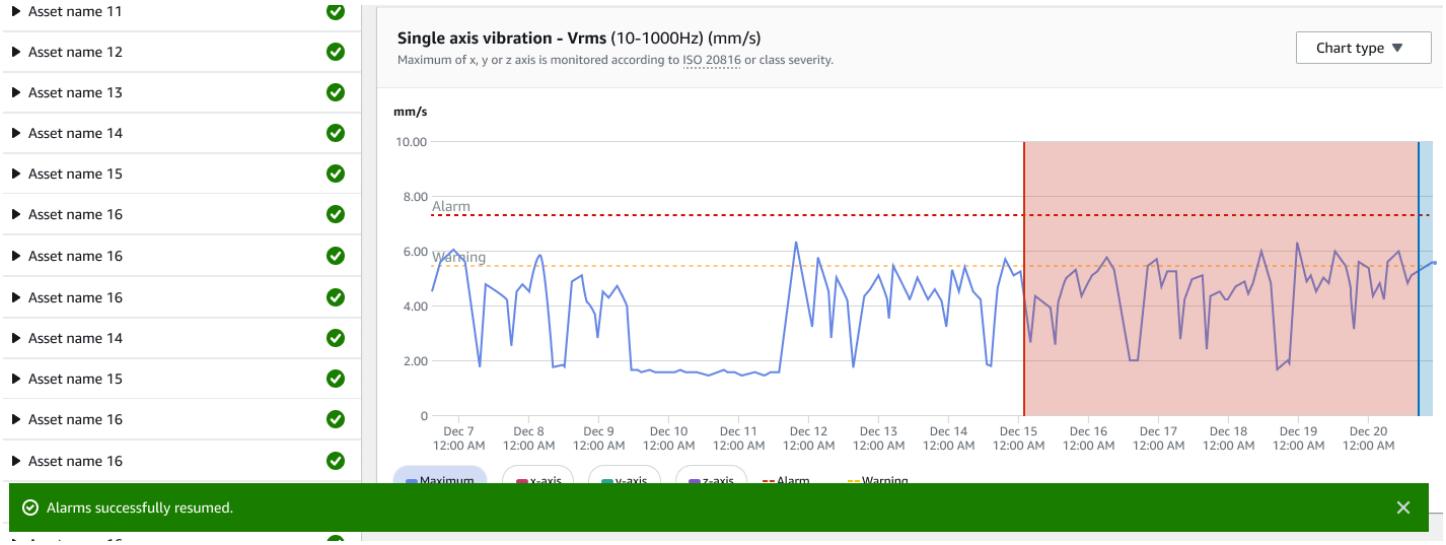
モバイルアプリでアラームを再開する



ウェブアプリでアラームを再開する



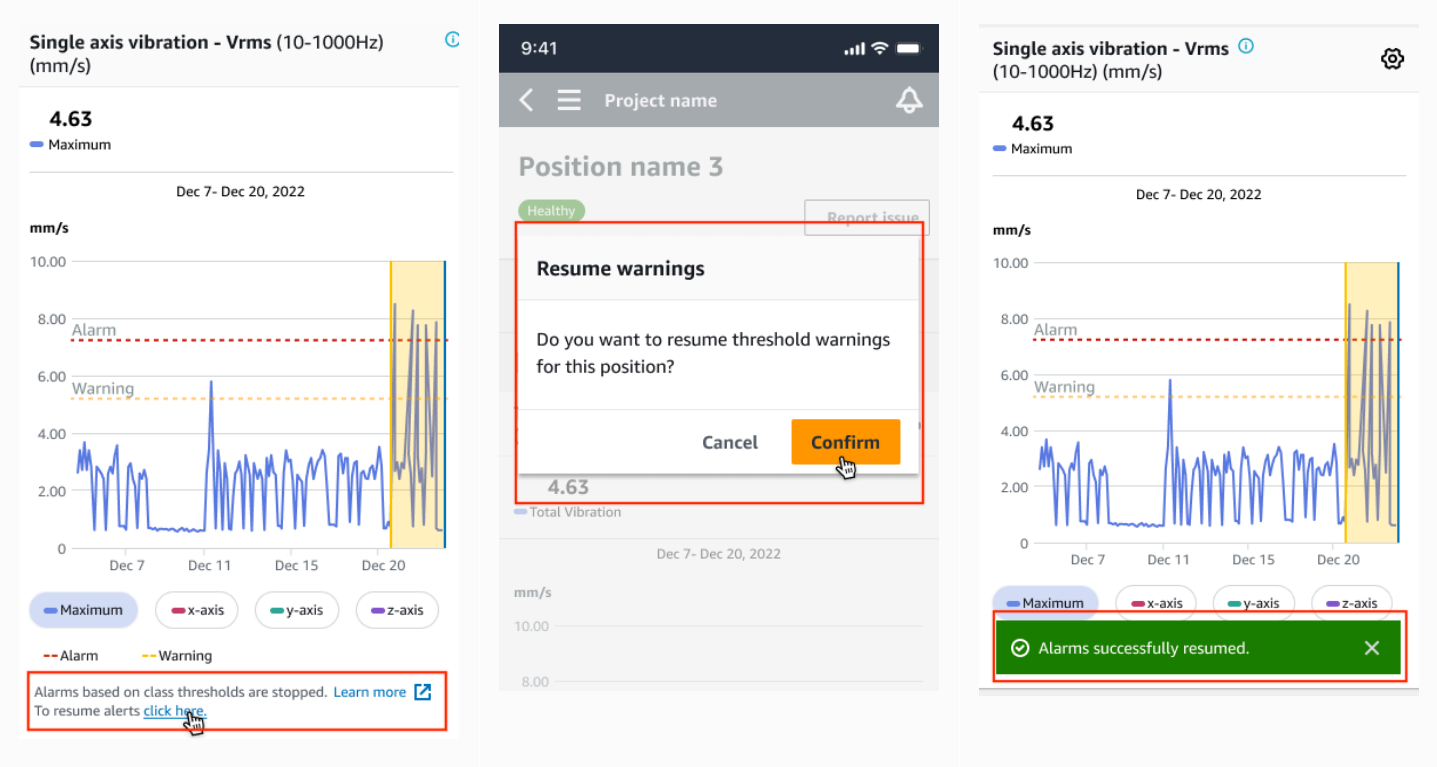




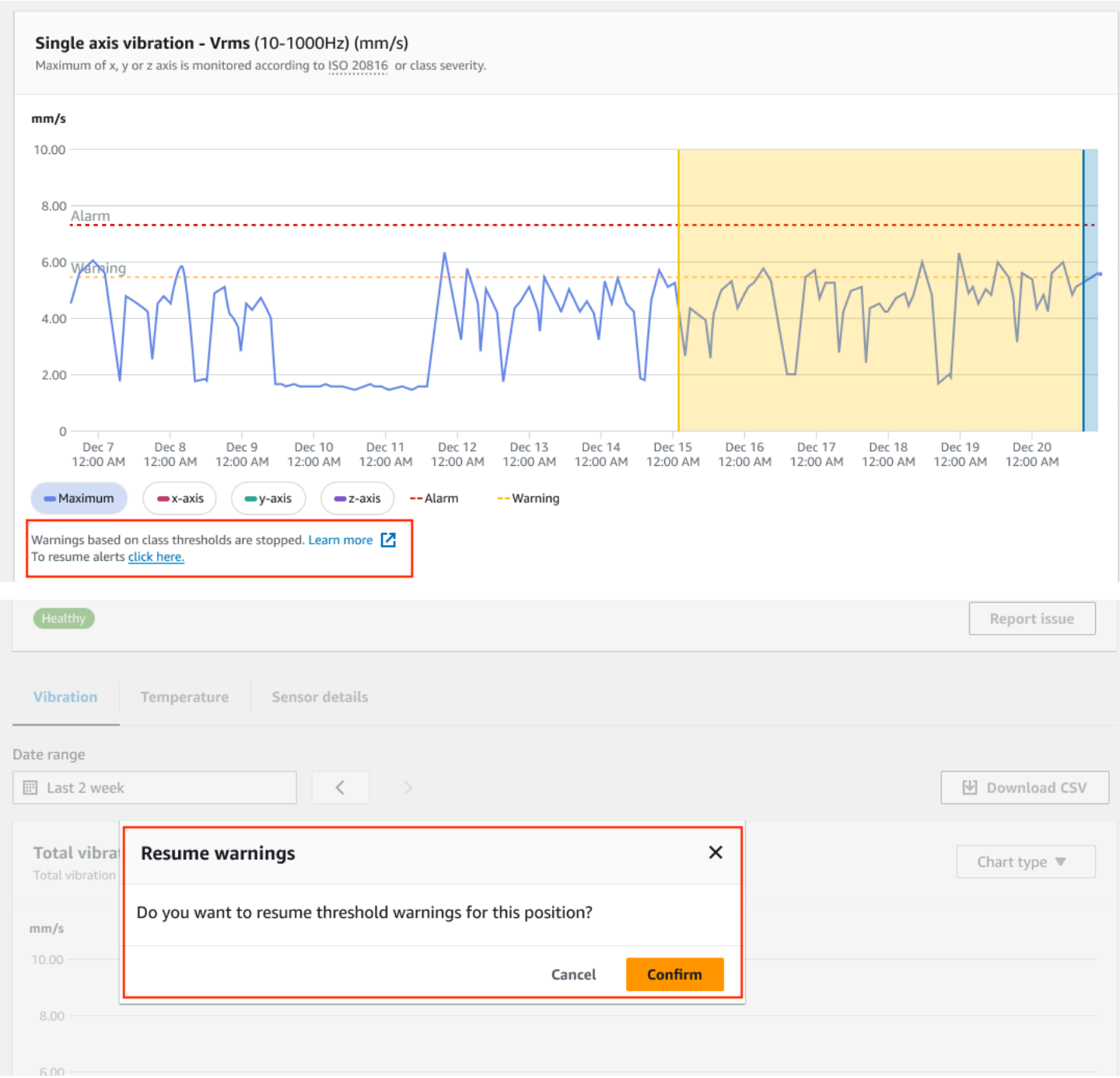
警告のみを再開する

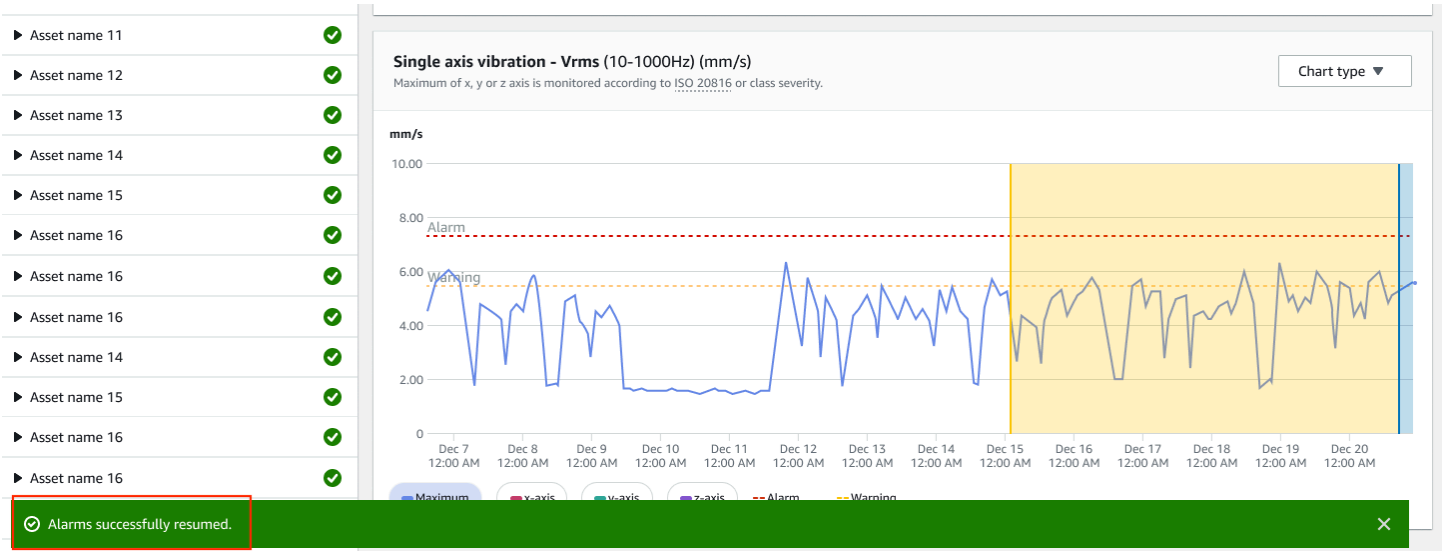
警告をミュートした場合は、再開することを選択できます。

モバイルアプリで警告を再開する



ウェブアプリで警告を再開する




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.

プロジェクト

プロジェクトは を使用するための基盤です Amazon Monitron。プロジェクトとは、 Amazon Monitron が機器の障害につながる可能性のある異常な状態を検出するために使用するゲートウェイ、アセット、センサーをチームがセットアップする場所です。

Amazon Monitron プロジェクトは次のように構成されています。

プロジェクト → サイト → アセット → ポジション → センサー

プロジェクト間でこれらのリソースを共有することはできません。プロジェクトの作成を開始する前に、プロジェクトのニーズを検討することを推奨します。プロジェクトには、すべてのアセットのメンテナンスニーズを予測するのに必要なリソースがすべて含まれているようにしてください。

プロジェクトレベルの管理者ユーザーまたは IT マネージャーのみが、プロジェクトを作成、更新、削除し、それらのタスクに Amazon Monitron コンソールを使用できます。

トピック

- プロジェクトの作成
- プロジェクトでのタグの使用
- プロジェクトの更新
- プロジェクトの切り替え
- プロジェクトの削除
- プロジェクトのその他のタスク

プロジェクトの作成

AWS アカウントには複数の Amazon Monitron プロジェクトを含めることができますが、通常はアカウントごとに 1 つあります。プロジェクト名は、 AWS アカウントと AWS リージョンで一意である必要があります。

プロジェクトを作成するには

1. Amazon Monitron コンソールを https://console.aws.amazon.com/monitron://https://https://https://https://https://https
2. [プロジェクトの作成] を選択します。

3. [プロジェクトの詳細] の下の [プロジェクト名] に、次の条件で名前を入力します。

   - 現在のアカウント内で一意
   - 大文字、小文字、数字、句読点、スペースが使用可能
   - 1 ~ 60 文字以内

4. デフォルトでは、 Amazon Monitron は () AWS 所有のキー を使用してプロジェクトを暗号化します AWS Key Management Service AWS KMS。別の AWS KMS キーを使用する場合は、データ暗号化でカスタム暗号化設定 (アドバンスド) を選択し、次のいずれかを実行します。

   - 使用する AWS KMS キーが既にある場合は、 AWS AWS KMS 「キーの選択」でキーを選択するか、キーの Amazon リソースネーム (ARN) を入力します。
   - キーを作成する場合は、 AWS AWS KMS キーの作成を選択します。 AWS KMS コンソールが開くので、そこでカスタムキーをセットアップします。

5. (オプション) プロジェクトにタグを追加するには、[タグ] にキーと値のペアを入力し、[タグを追加] をクリックします。プロジェクトを作成する前にこのタグを削除するには、[タグを削除する] を選択します。
6. [次へ] をクリックしてプロジェクトを作成します。

プロジェクトでのタグの使用

タグはキーと値のペアであり、プロジェクトの分類に使用できます。例えば、プロジェクトが複数ある場合は、目的、所有者、場所、その他の要素に基づいて分類できます。

タグの使用例:

- プロジェクトを整理します。タグによる検索やフィルタリングができます。例えば、「test lab」や「paint shop」などのタグを追加して、それらのプロジェクトを簡単に見つけることができます。
- AWS リソースを特定して整理します。多くの AWS サービスはタグ付けをサポートしているため、異なる サービスのリソースに同じタグを割り当てて、リソースが関連していることを示すことができます。例えば、関連データを格納する Amazon Simple Storage Service (Amazon S3) バケットとプロジェクトをタグ付けできます。
- リソースへのアクセス制御。 Amazon Monitron プロジェクトへのアクセスを制御する AWS Identity and Access Management (IAM) ポリシーでタグを使用できます。これらのポリシーを IAM ロールまたはユーザーにアタッチして、タグベースのアクセスコントロールを有効にできます。詳細については、IAM ユーザーガイドの「タグを使用したアクセス制御」を参照してください。

各タグキーは、プロジェクト内で一意である必要があります。

Amazon Monitron プロジェクトタグには、次の制限も適用されます。

- 1 プロジェクトあたりのタグの最大数は 50 です。
- タグキーの最大長は 128 文字です。
- タグ値の最大長は 256 文字です。
- キーと値に使用できる文字は、a—z、A—Z、スペース、半角記号 (_ . : / = + - @) です。
- タグのキーと値では、大文字と小文字が区別されます。
- aws: プレフィックスは AWS 使用のために予約されています。
- 複数のサービス間およびリソース間でタグ付けスキーマを使用する場合、他のサービスでは有効な文字の制限が異なることがあるのでご注意ください。該当するサービスのドキュメントを参照してください。

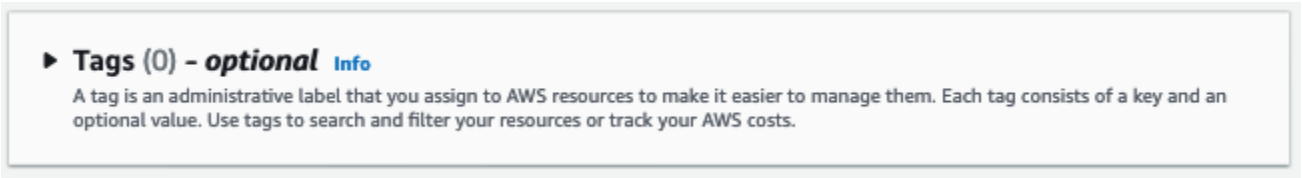
トピック

- プロジェクト作成時のタグの追加
- プロジェクト作成後のタグの追加
- タグの変更または削除

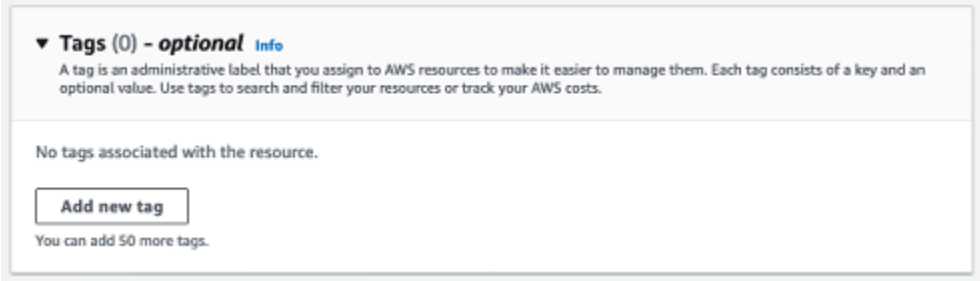
プロジェクト作成時のタグの追加

プロジェクトの作成時にタグを追加するには

1. Amazon Monitron コンソールを https://console.aws.amazon.com/monitron://https://https://https://https://https://https
2. [プロジェクトを作成] を選択します。
3. ナビゲーションペインで目的のプロジェクトを選択します。
4. [タグ] セクションを展開します。

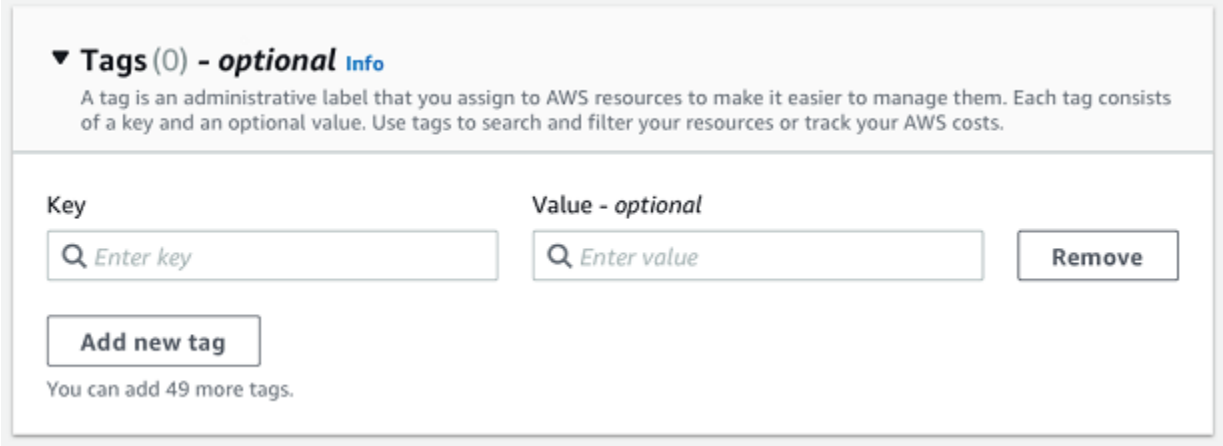


5. [新しいタグを追加] をクリックします。

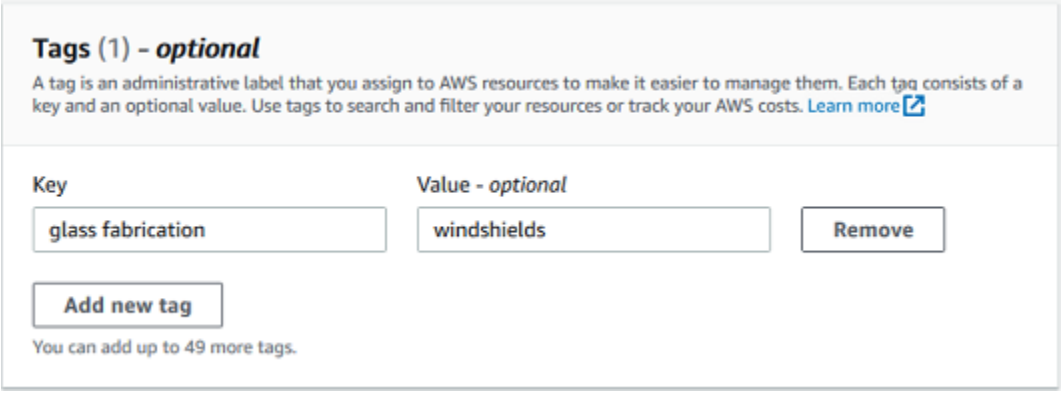


6. タグのキーと値のペアを入力します。

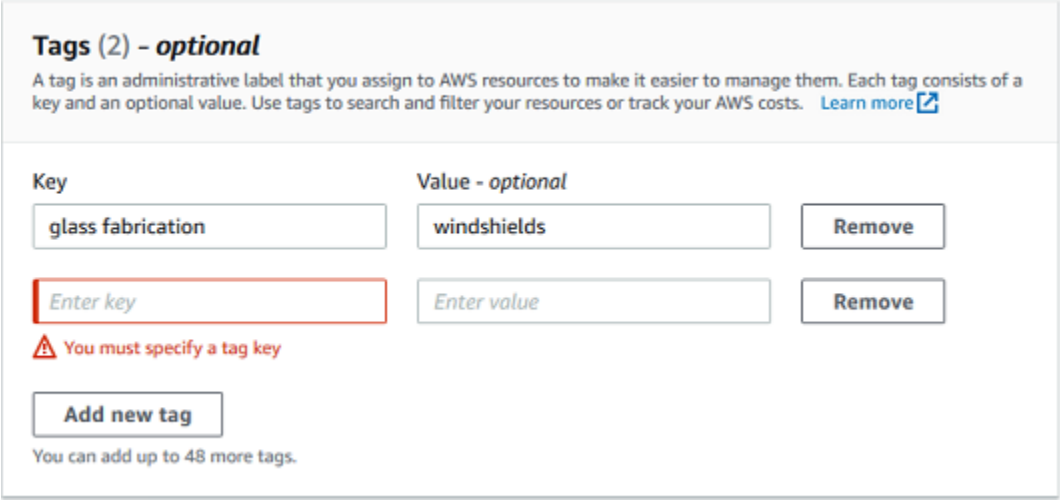
   キーはプロジェクト内で一意である必要があります。値はオプションです。



7. [新しいタグを追加] をクリックします。
8. さらにタグを追加するには、手順 2 ~ 3 を繰り返します。
9. タグを削除するには、[削除] を選択します。



10. 空白のタグエントリを削除し、[次へ] を選択します。

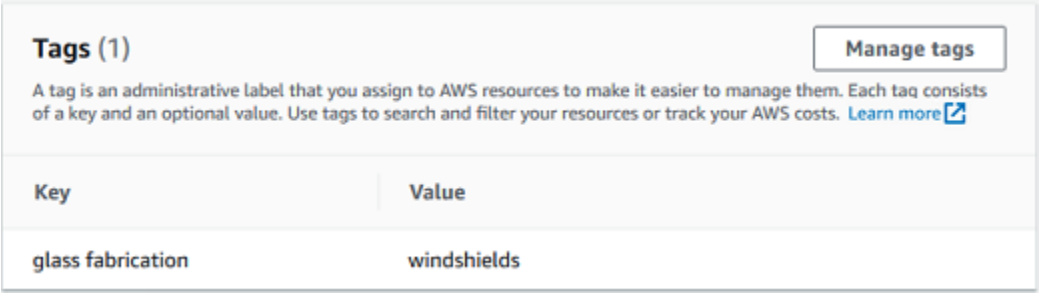


プロジェクト作成後のタグの追加

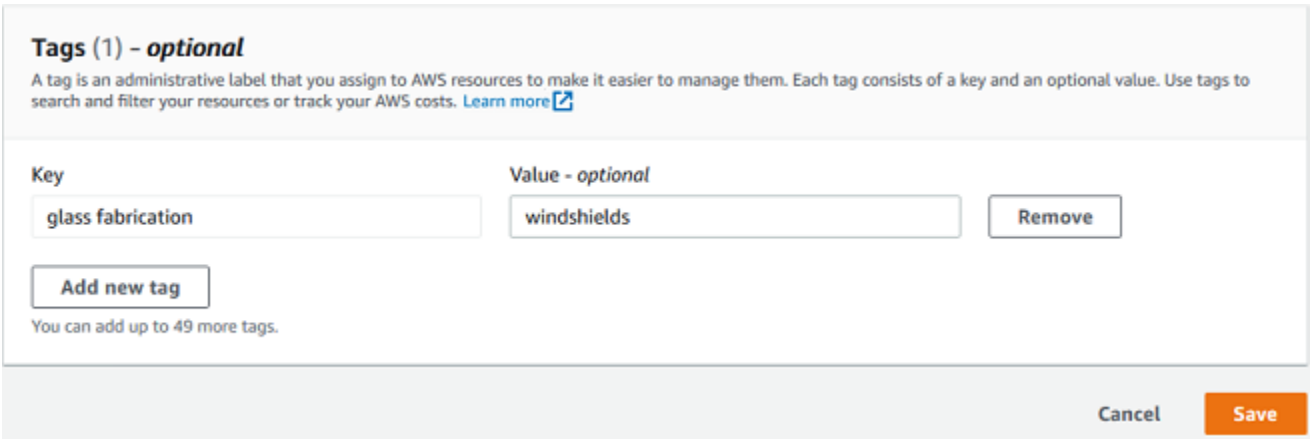
プロジェクトの詳細ページでプロジェクトにタグを追加できます。

既存のプロジェクトにタグを追加するには

1. Amazon Monitron コンソールを https://console.aws.amazon.com/monitron:///https://https://https://https://https://https
2. [プロジェクトの作成] を選択します。
3. ナビゲーションペインで [プロジェクト] を選択し、該当プロジェクトを選択します。
4. [タグ] の項目で、[タグの管理] を選択します。

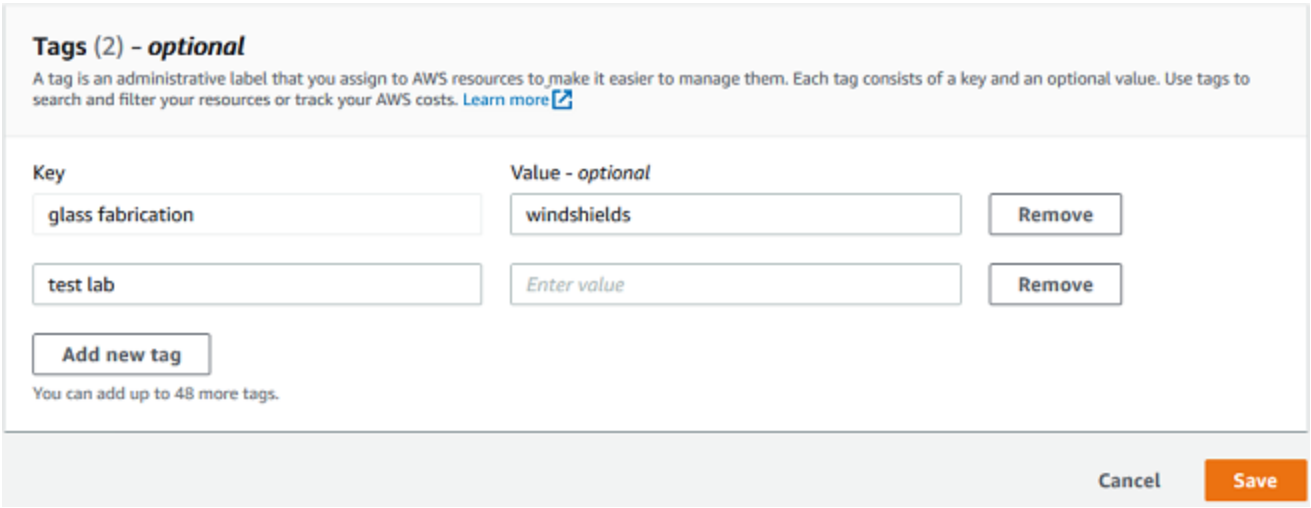


5. [新しいタグを追加] をクリックします。



6. タグのキーと値のペアを入力します。

> **Note**
>
> キーはプロジェクト内で一意である必要があります。値はオプションです。



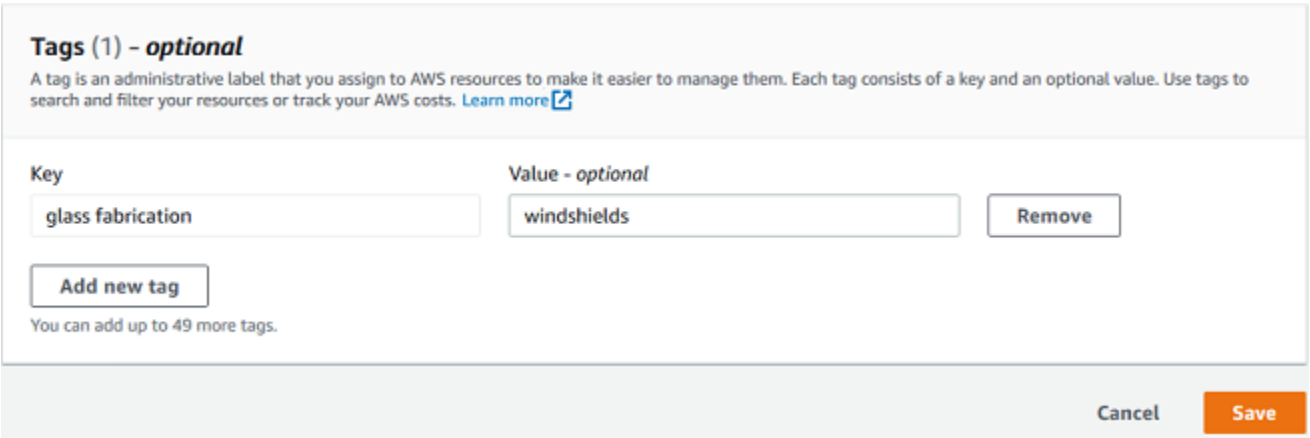
7. [Save] を選択します。

タグの変更または削除

タグ値は変更できますが、タグキーは変更できません。タグキーを変更するには、一度タグを削除し、新しいタグを別のキーで作成します。また、すべてのタグは削除可能です。タグは、プロジェクトの詳細ページで変更または削除します。

タグを変更または削除するには

1. Amazon Monitron コンソールを https://console.aws.amazon.com/monitron://https://https://https://https://https://https
2. [プロジェクトの作成] を選択します。
3. ナビゲーションペインで [プロジェクト] を選択し、該当プロジェクトを選択します。
4. [タグ] の項目で、[タグの管理] を選択します。
5. タグ値を変更する場合は、変更を行います。タグを削除するには、横にある [削除] を選択します。



6. [Save] を選択します。

プロジェクトの更新

この手順ではプロジェクト名のみを編集できます。管理者ユーザーのリストも変更できますが、これはユーザーの編集プロセスを使用して行います。

プロジェクトを編集するには

1. Amazon Monitron コンソールを https://console.aws.amazon.com/monitron://https://https://https://https://https://https
2. [プロジェクトの作成] を選択します。
3. ナビゲーションペインで、変更するプロジェクトを選択します。
4. [プロジェクト] リストから、編集するプロジェクトを選択します。
5. [プロジェクトを編集] を選択します。
6. プロジェクト名を編集します。

7. [保存] を選択します。

プロジェクトの切り替え

モバイルアプリとウェブアプリの両方から Amazon Monitron プロジェクトを切り替えることで、 リソースを管理できます。

> **Note**
>
> 一度に 1 つのプロジェクトにしかサインインできません。プロジェクトを切り替えると、アクティブに使用中のプロジェクトから自動的にログアウトされます。

アカウント認証情報を使用してプロジェクトにログインすると、 Amazon Monitron によってプロジェクト Amazon Monitron ページに自動的に追加され、追跡が容易になります。 Amazon Monitron 招待メールのプロジェクト URL を使用して、プロジェクトページにプロジェクトを手動で追加することもできます。

プロジェクトを追加した場合、そのプロジェクトは追加したプラットフォームでのみ保存されます。Amazon Monitron ウェブアプリに追加または保存されたプロジェクトは、ウェブアプリにも追加しない限り、 Amazon Monitron モバイルアプリに自動的に保存されません。

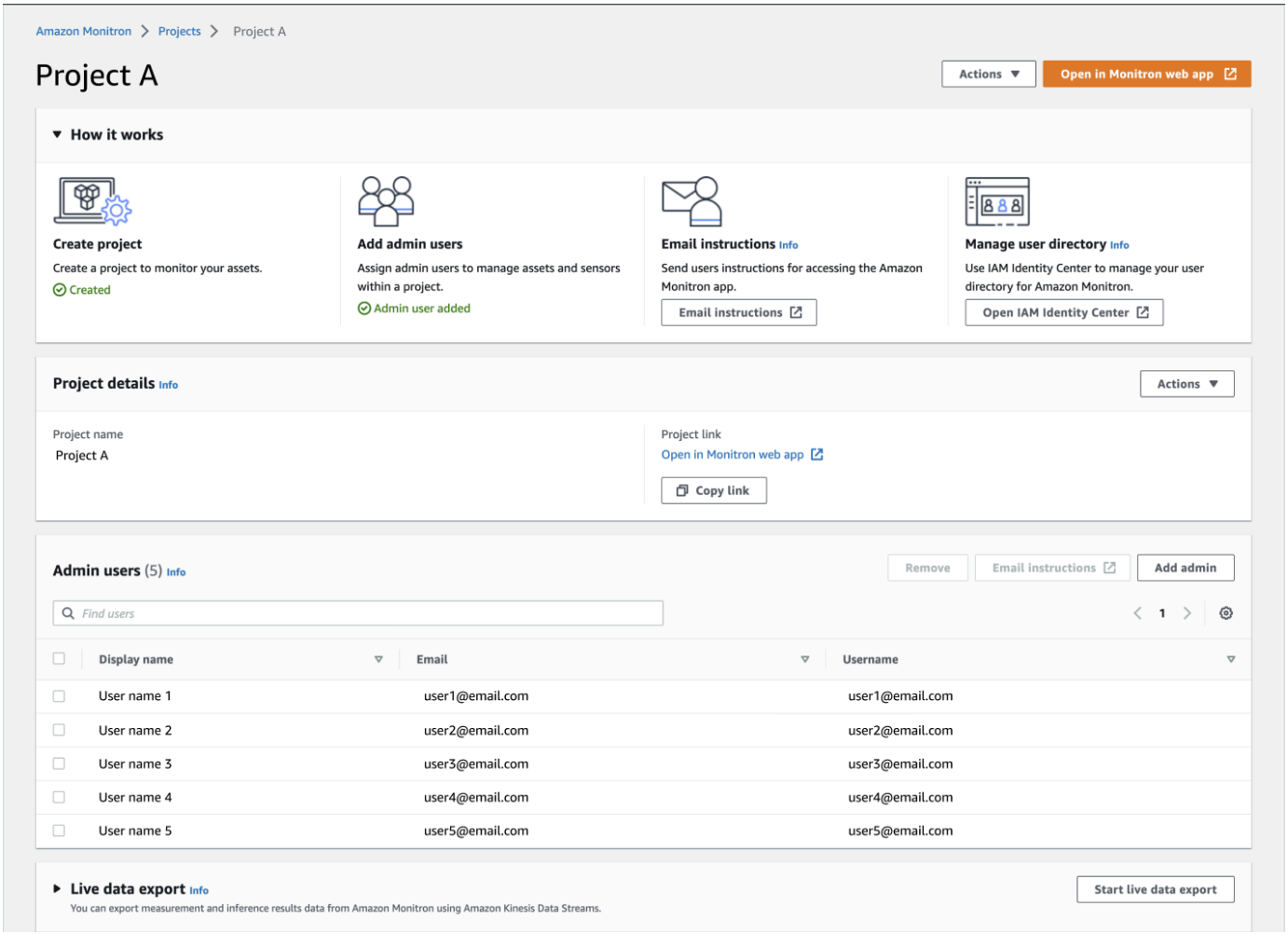
トピック

- ウェブアプリでのプロジェクトの切り替え
- モバイルアプリでのプロジェクトの切り替え

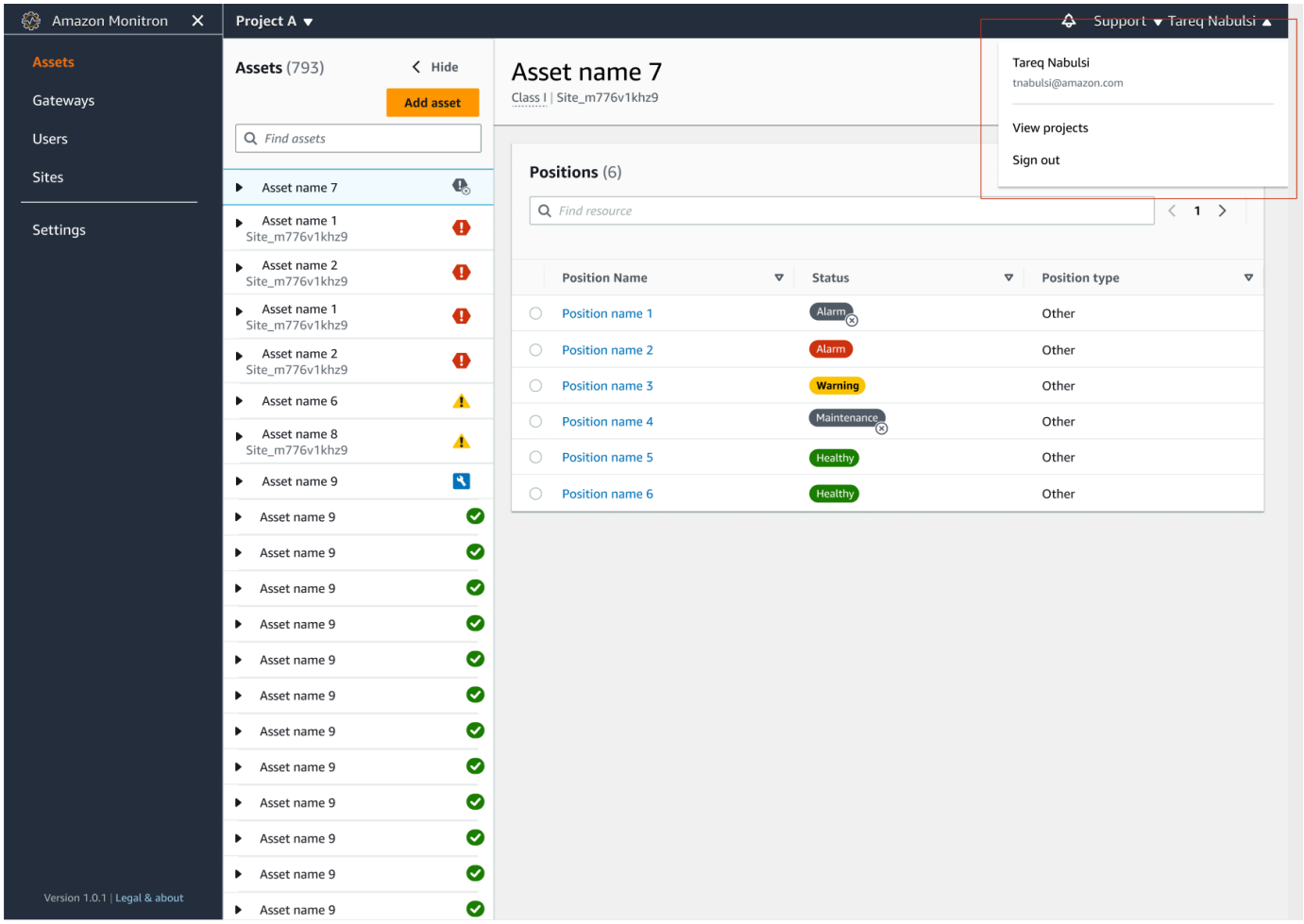
ウェブアプリでのプロジェクトの切り替え

ウェブアプリでプロジェクトを切り替えるには

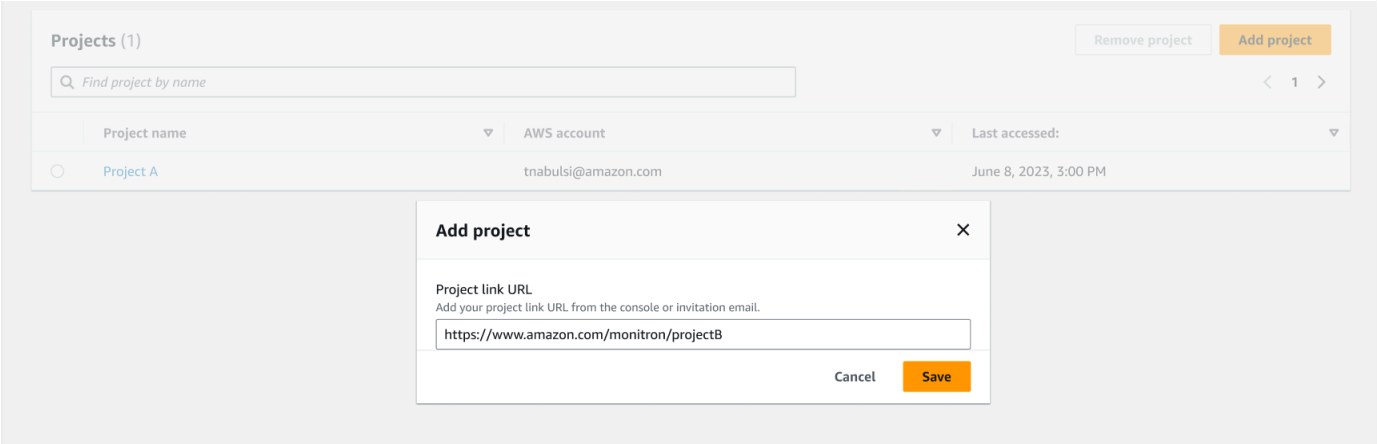
1. Amazon Monitron コンソールを https://console.aws.amazon.com/monitron://https://https://https://https://https://https
2. Amazon Monitron ウェブアプリケーションで開く を選択します。



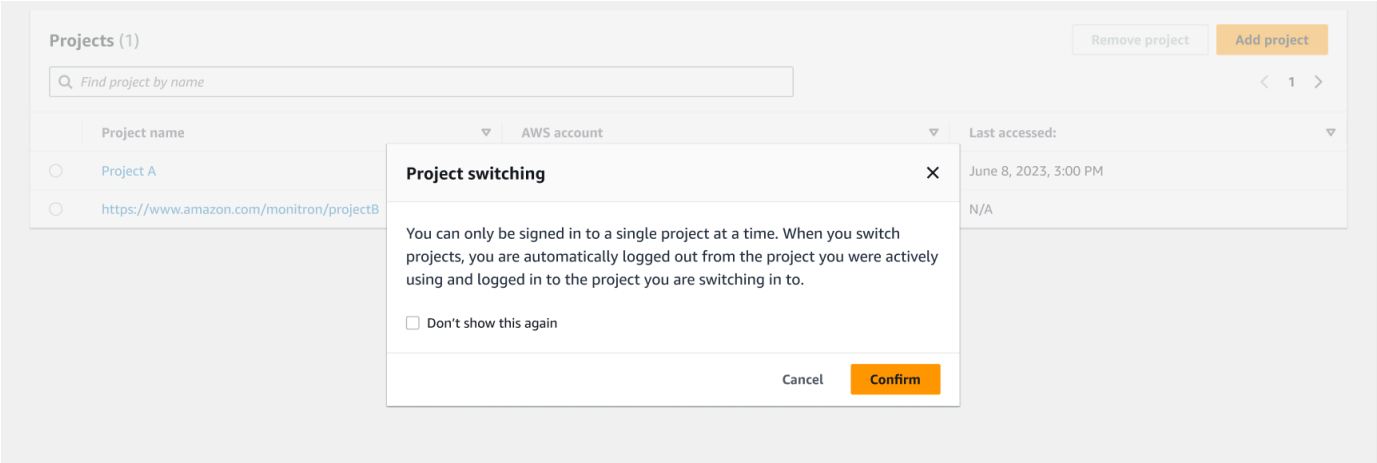
3. [サインイン] 画面で [ユーザー名] と [パスワード] を入力します。
4. [アセット] リストページで、アカウント詳細のドロップダウンメニューから [プロジェクトを表示] を選択します。



5. プロジェクトを追加する場合は、[プロジェクトを追加] を選択し、プロジェクトリンクの URL を入力します。



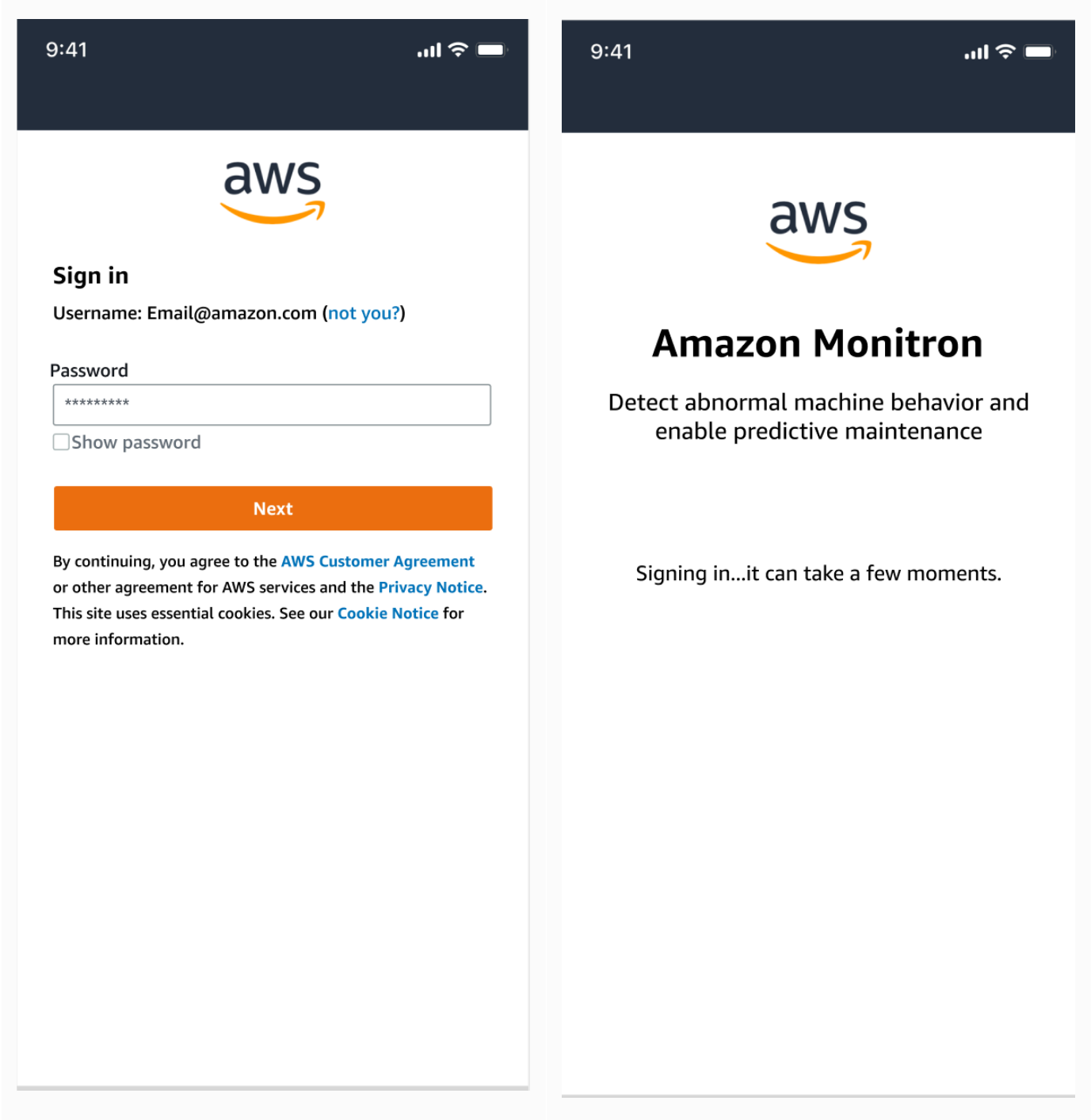
6. プロジェクトを切り替える場合は、プロジェクトリストから表示したいプロジェクトを選択します。切り替える際に次のメッセージが表示されます。



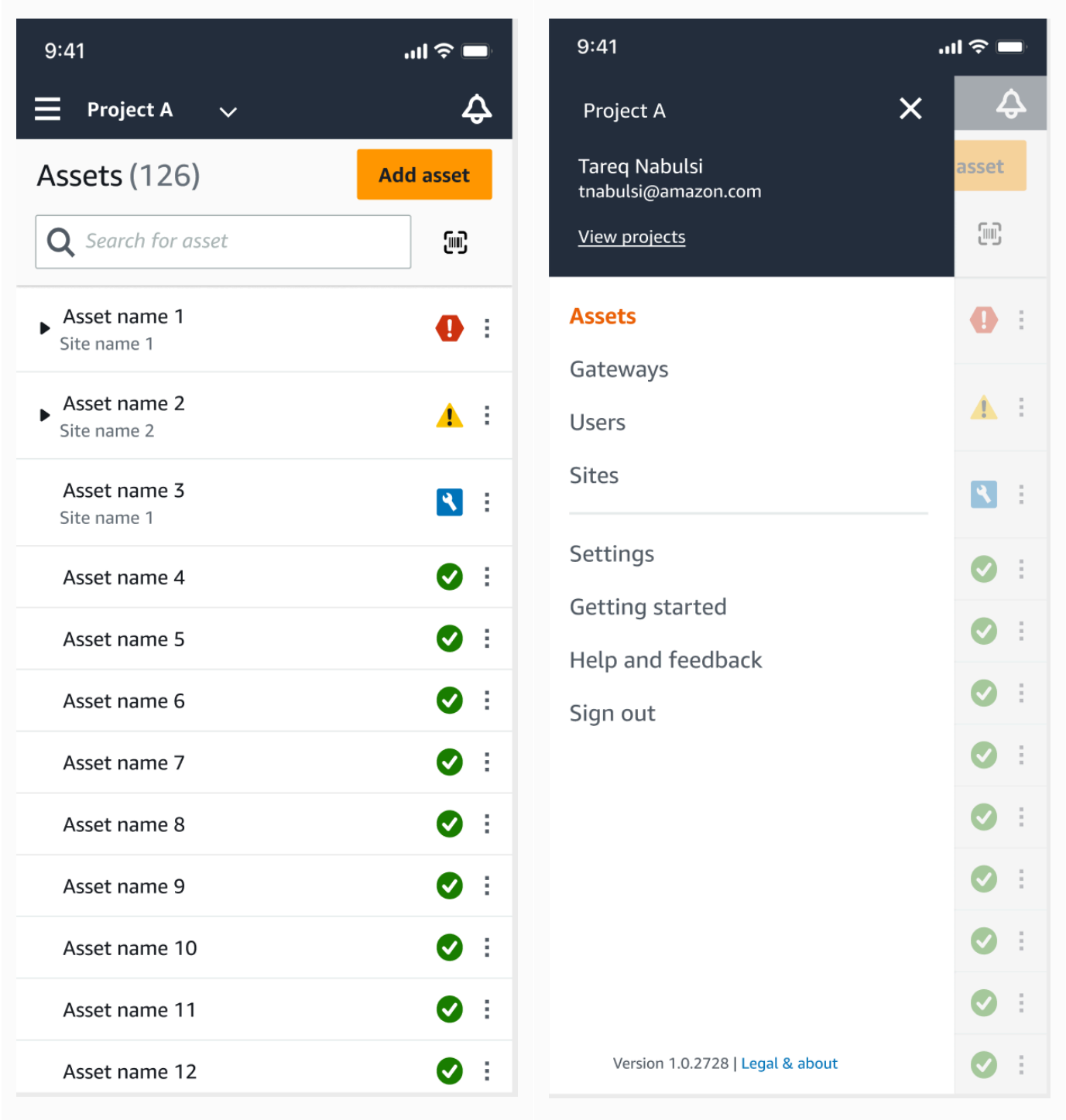
モバイルアプリでのプロジェクトの切り替え

モバイルアプリでプロジェクトを切り替えるには

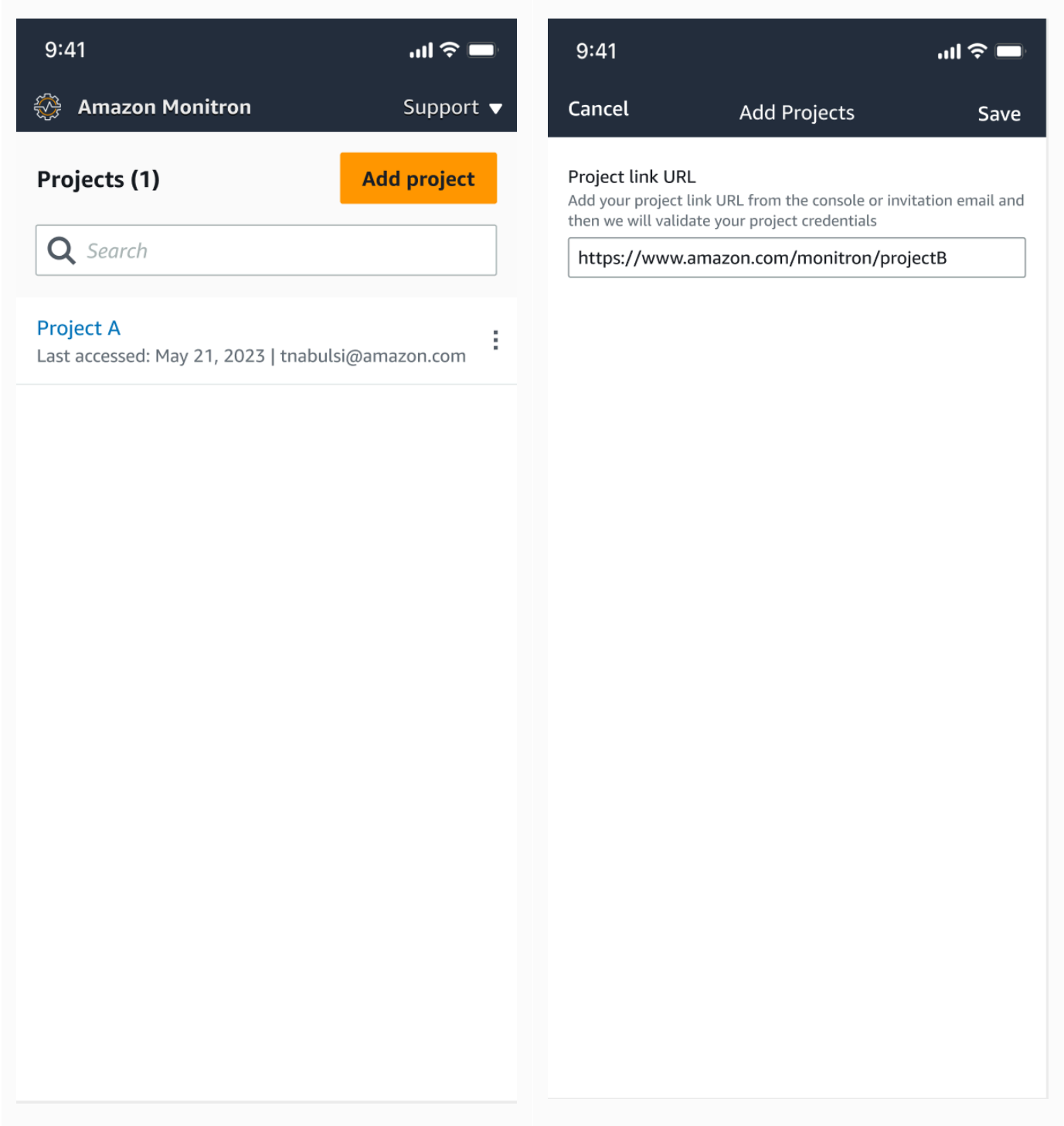
1. Amazon Monitron モバイルアプリを開き、ユーザー名とパスワードを使用してログインします。



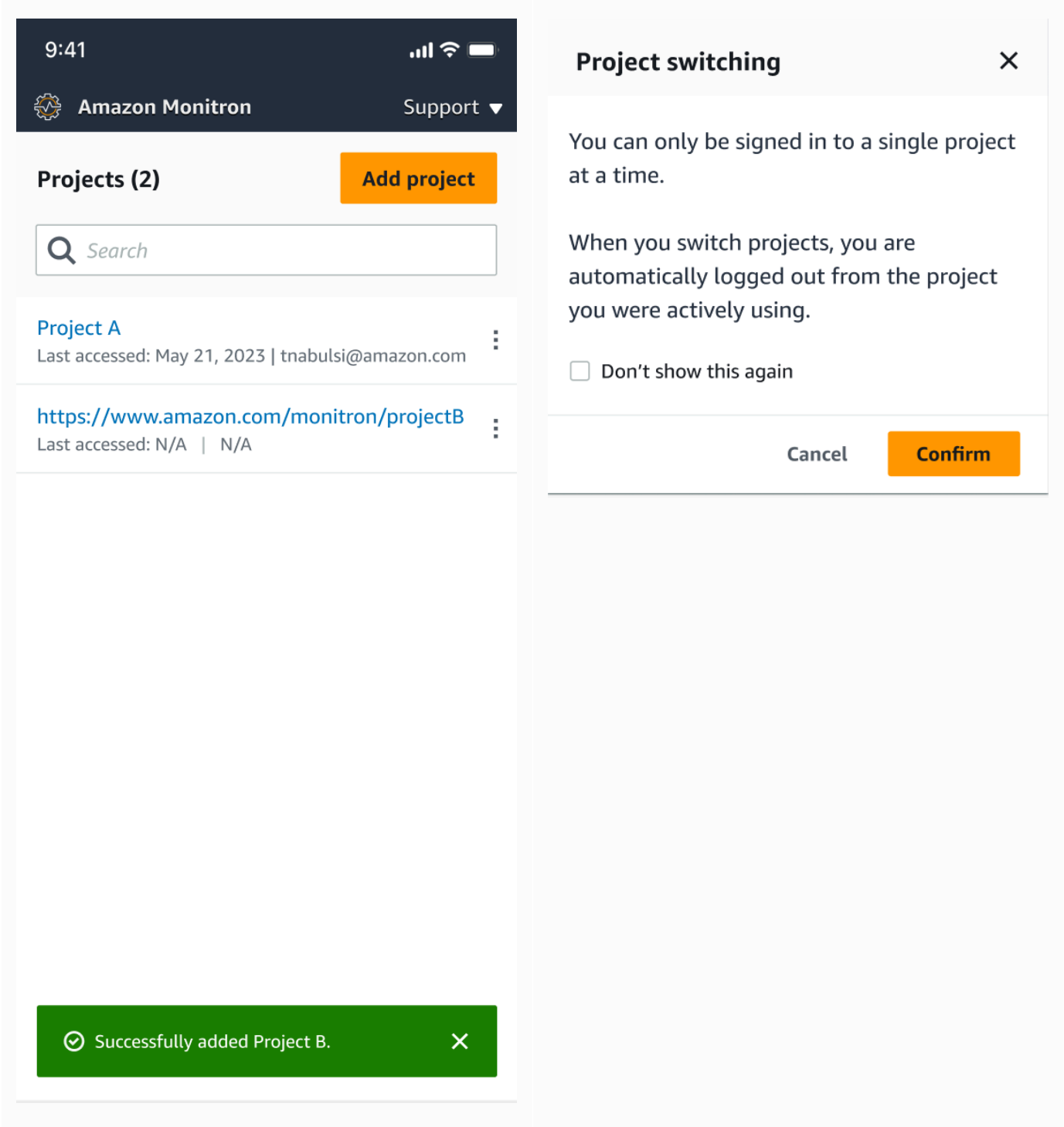
2. [アセット] リストページで、アカウント詳細のドロップダウンメニューから [プロジェクトを表示] を選択します。



3. プロジェクトを追加する場合は、[プロジェクトを追加] を選択し、プロジェクトリンクの URL を入力します。



4. プロジェクトを切り替える場合は、プロジェクトリストから表示したいプロジェクトを選択します。切り替える際に次のメッセージが表示されます。



プロジェクトの削除

`deleteProject` オペレーションでは、削除の AWS IAM Identity Center アクセス許可が必要です。この権限がない場合でも、コンソールのプロジェクト削除機能でプロジェクトは削除できます。ただ

し、IAM Identity Center からリソースは削除されないため、IAM Identity Center でダングリング参照が発生してしまう可能性があります。

プロジェクトを削除するには

1. Amazon Monitron コンソールを https://console.aws.amazon.com/monitron://https://https://https://https://https://https
2. [プロジェクトの作成] を選択します。
3. ナビゲーションペインで、[プロジェクト] を選択します。
4. [プロジェクト] ページで、削除するプロジェクトを選択します。
5. [プロジェクトを削除] を選択します。
6. 削除を確定するには、確認ボックスに [Delete] と入力します。

   プロジェクトにアクティブなアセット、センサー、ゲートウェイが含まれている場合は、プロジェクトを削除する前にそれらを削除する必要があります。この場合、確認ボックスや削除オプションは表示されません。

   このプロジェクトを削除するために削除する必要があるアクティブなアセットやセンサーがある場合は、管理者ユーザーに削除を依頼するか、Amazon Monitron モバイルアプリにログインして自分で削除してください。
7. [削除] をクリックします。

プロジェクトのその他のタスク

よくある一般的なプロジェクト関連のタスクとして、すべてのプロジェクトの一覧表示と、特定の 1 つのプロジェクトの詳細取得の 2 つがあります。 Amazon Monitron コンソールを使用して、これらのタスクの両方を実行します。

すべてのプロジェクトを一覧表示するには

1. Amazon Monitron コンソールを https://console.aws.amazon.com/monitron://https://https://https://https://https://https
2. [プロジェクトの作成] を選択します。
3. ナビゲーションペインで、[プロジェクト] を選択します。

   プロジェクトのリストが [プロジェクト] の下に表示されます。

プロジェクトの詳細を取得するには

1. Amazon Monitron コンソールを https://console.aws.amazon.com/monitron://https://https://https://https://https://https
2. [プロジェクトの作成] を選択します。
3. ナビゲーションペインで、[プロジェクト] を選択します。

   プロジェクトのリストが [プロジェクト] の下に表示されます。
4. 詳細を取得するプロジェクトを選択します。

サイト

プロジェクトを設定したら、そのプロジェクトをサイトに整理して、管理を容易にすることができます。サイトとは、目的を共有するアセット、ゲートウェイ、センサーの集まりです。プロジェクトに大量のアセット、ゲートウェイ、センサーがある場合は、プロジェクトをサイトに整理すると便利です。サイトを使用すると、そのプールの特定の部分に対するアクセスおよびアクセス許可を制御できます。

1 つのプロジェクトには、最大 50 のサイトを作成できます。また、各サイトには、最大 100 のアセットと 200 のゲートウェイを追加できます。

トピック

- プロジェクトのサイトへの整理
- プロジェクトやサイトへのアクセスの制御
- サイトの作成
- サイト名の変更
- サイトの削除
- モバイルアプリを使用したプロジェクトとサイト間の移動

プロジェクトのサイトへの整理

プロジェクトは、ビジネスニーズに基づいてサイトに整理できます。例えば、プロジェクトを以下のいずれかの方法で整理できます。

- サイトが一切ない: サイトは一切なく、すべてがプロジェクトに含まれます。このオプションは非常にシンプルなため、アセットやユーザーが少なく、簡単に追跡できるプロジェクトに最適です。
- 地域に基づくサイト: 都市、建物、建物内のエリアなど、ロケールごとにリソースとユーザーをグループ化します。例えば、工場のテストラボ内に機器のサイトをセットアップできます。
- 機能に基づくサイト: リソースとユーザーを機能別、つまり機械の機能ごと、または工場での使用方法ごとにグループ化します。例えば、ある品目を工場の一方からもう一方に移動させる際に使用するすべてのコンベアベルトのサイトをセットアップできます。
- 組織に基づくサイト: 会社または工場内の特定の組織構造をサイトで表します。例えば、出荷部門に割り当てられたリソースとユーザーを含む、単一のサイトが必要になる場合があります。

プロジェクトやサイトへのアクセスの制御

プロジェクト内のすべてのサイトにあるリソースを含む、プロジェクト内のすべてのリソースにユーザーがアクセスできるようにするには、ユーザーをプロジェクトに追加します。サイト内のリソースにのみユーザーがアクセスできるようにするには、ユーザーをサイトに追加します。同様に、プロジェクト全体にアクセスできるすべてのユーザーが、アセットまたはセンサーを利用できるようにするには、そのアセットまたはセンサーをプロジェクトに追加します。アセットまたはセンサーを特定のサイトでのみ使用できるようにするには、そのサイトにのみ追加します。ゲートウェイには、プロジェクト内の誰でも、どのセンサーからもいつでもアクセスできます。

例: Olga は、プロジェクト全体に関連付けられた管理者ユーザーです。プロジェクトレベルの管理者ユーザーとして、Olga はプロジェクト内のあらゆるユーザーとリソースを管理できます。これには、プロジェクト内のサイト A、B、C 内のユーザーやリソースも含まれます。Sam は、サイト B に関連付けられた管理者ユーザーです。サイトレベルの管理者ユーザーとして、Sam はサイト B 内のユーザーとリソースを管理できますが、サイト A と C 内のユーザーとリソースは確認および管理できません。サイト B のセンサーは、プロジェクト内の任意のゲートウェイを使用できます。

同様に、Ed がプロジェクトレベルの技術者である場合、Ed はプロジェクト内のあらゆるセンサーをモニタリングできます。ただし、サイト C のサイトレベルの技術者である Tom は、サイト C のセンサーのみを確認およびモニタリングできます。

サイトの作成

サイトをプロジェクトに追加するには、プロジェクトレベルの管理者ユーザーである必要があります。1 つのプロジェクトには、最大 50 のサイトを作成できます。また、各サイトには、最大 100 のアセットと 200 のゲートウェイを追加できます。最大 20 人のユーザーをサイトの管理者ユーザーまたは技術者に設定できます。

トピック

- モバイルアプリを使用してサイトを追加するには
- ウェブアプリを使用して新しいサイトを追加するには

モバイルアプリを使用してサイトを追加するには

1. スマートフォンで Amazon Monitron モバイルアプリにログインします。

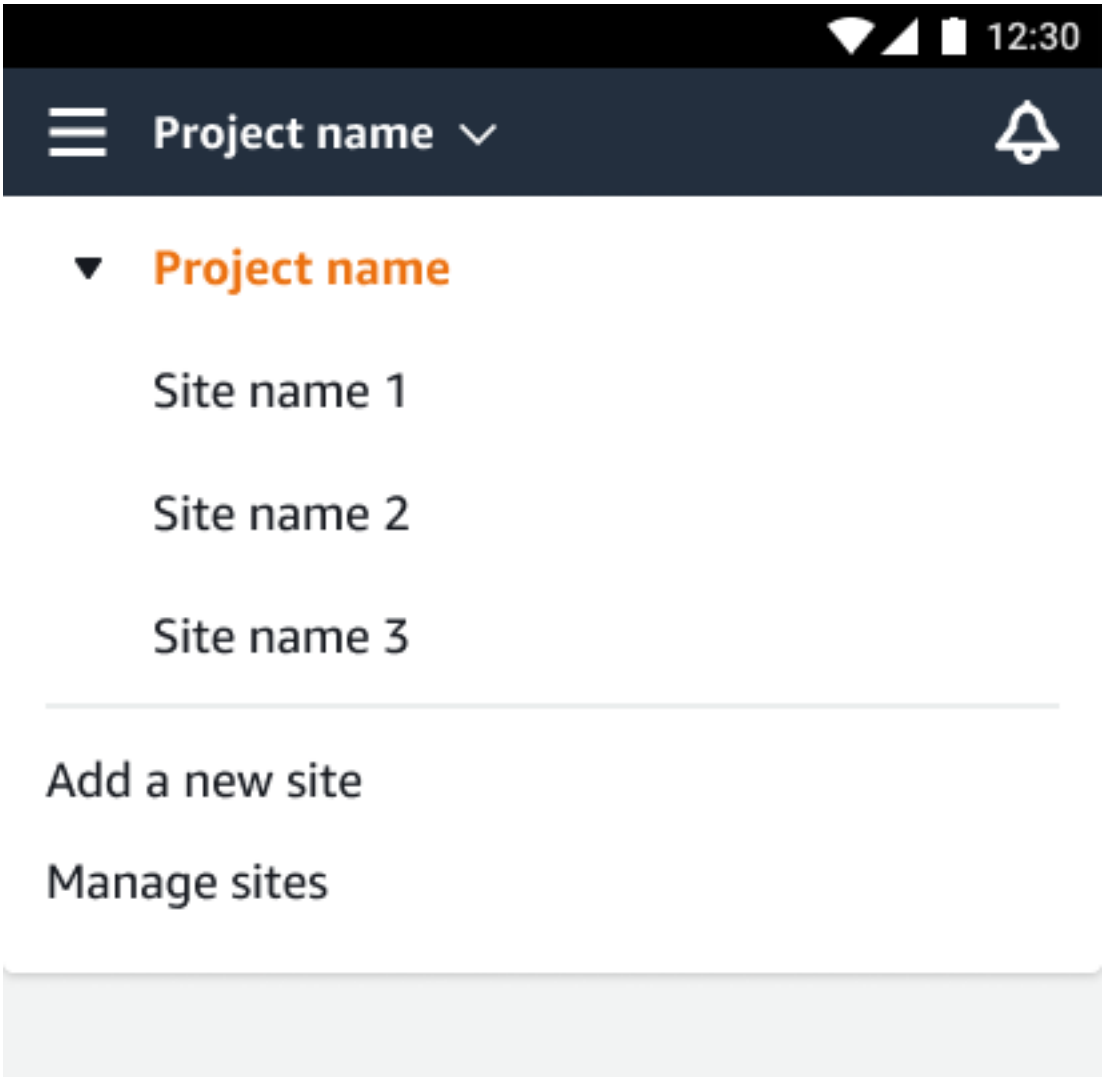
プロジェクト名が画面左上に表示されていることを確認します。これは、モバイルアプリのすべての画面に表示されます。

2. メニューアイコン (☰) をクリックします。
3. [サイト] を選択します。
4. [サイトを追加] をクリックします。
5. [ロール名] に名前を入力します。
6. [追加] をクリックします。

   [サイト] のリストに新しいサイトが表示されます。

ウェブアプリを使用して新しいサイトを追加するには

1. アプリウィンドウの左上にあるプロジェクトセレクタードロップダウンメニューを開きます。
2. [新しいサイトを追加] を選択します。



プロジェクトレベルの管理者ユーザーがサイトを作成する場合、自動的にそのサイトのサイトレベルの管理者ユーザーになります。ユーザーの追加の詳細については、「ユーザーの追加」を参照してください。

サイト名の変更

変更できるのはサイト名のみです。名前を変更しても、それ以外 (履歴データやユーザーのアクセス許可など) は変更されません。

トピック

- モバイルアプリを使用してサイト名を変更するには
- ウェブアプリを使用してサイト名を変更するには

モバイルアプリを使用してサイト名を変更するには

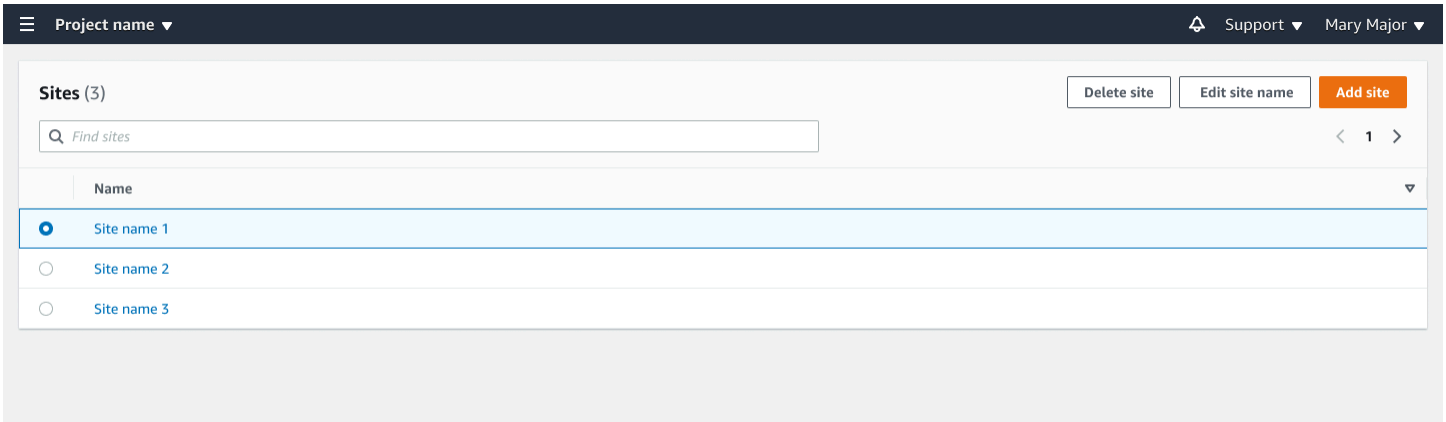
1. スマートフォンで Amazon Monitron モバイルアプリにログインします。

   プロジェクト名が画面左上に表示されていることを確認します。
2. メニューアイコン (☰) をクリックします。
3. [サイト] を選択します。
4. 名前を変更するサイトの横にある [アクション] をクリックします。
5. [サイト名を編集] を選択します。
6. サイト名を変更します。

   [サイト] のリストに新しい名前が表示されます。

ウェブアプリを使用してサイト名を変更するには

1. 左側のペインで [サイト] をクリックします。
2. 名前を変更するサイトを選択します。
3. [サイト名を編集] ボタンをクリックします。



サイトの削除

サイトを削除する前に、サイト内のすべてのアセットを削除する必要があります。[サイト] のリストには、サイトに関連付けられているすべてのデバイスとユーザーが表示されます。

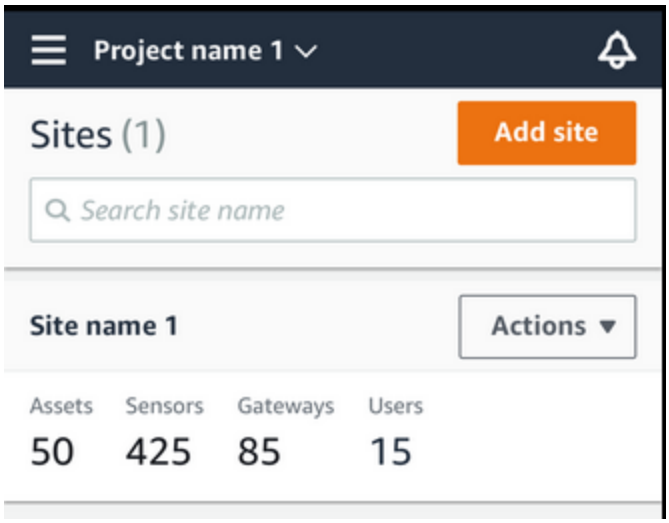
トピック

- モバイルアプリを使用してサイトを削除するには
- ウェブアプリを使用してサイトを削除するには

モバイルアプリを使用してサイトを削除するには

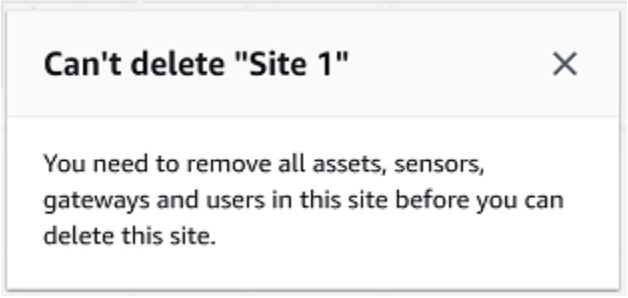
1. スマートフォンを使用して Amazon Monitron モバイルアプリにログインします。

   プロジェクト名が画面左上に表示されていることを確認します。



2. メニューアイコン (☰) をクリックします。
3. [サイト] を選択します。
4. 削除するサイトの横にある [アクション] をクリックします。
5. [サイトを削除] を選択します。
6. アセット、センサー、ゲートウェイ、ユーザーがサイトに関連付けられている場合は、[X] をクリックします。次に、先に進む前にそれらのリソースを削除します。

   サイトに関連付けられたリソースがない場合は、次のステップに進みます。

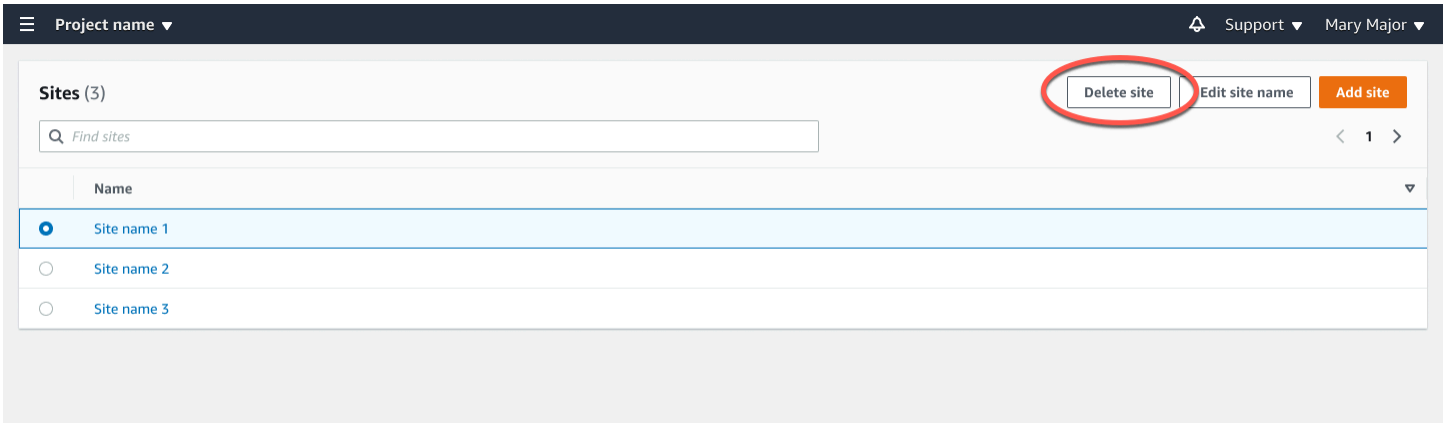


7. [削除] をクリックします。

このサイトが [サイト] のリストに表示されなくなります。

ウェブアプリを使用してサイトを削除するには

1. 左側のペインで [サイト] をクリックします。
2. 削除するサイトを選択します。
3. [サイトを削除] を選択します。



モバイルアプリを使用したプロジェクトとサイト間の移動

プロジェクトレベルの管理者ユーザーとプロジェクトレベルの技術者は、プロジェクトレベルまたはサイトレベルのリソースにアクセスして管理できます。プロジェクトレベルの管理者ユーザーは、プロジェクトレベルまたはサイトレベルでリソースとユーザーを追加できます。

サイト管理者とサイトレベルの技術者は、自分のサイトにのみアクセスできます。

自分がプロジェクトレベルにいるのか、特定のサイトにいるのかを確認するには、アプリ画面上部の名前に注目します。

or

プロジェクトレベルの管理者ユーザーと技術者は、プロジェクトレベルとサイトレベルを切り替えたり、個々のサイト間で切り替えたりできます。

トピック

- プロジェクトレベルからサイトレベルへの切り替え
- サイトレベルからプロジェクトレベルへの切り替え

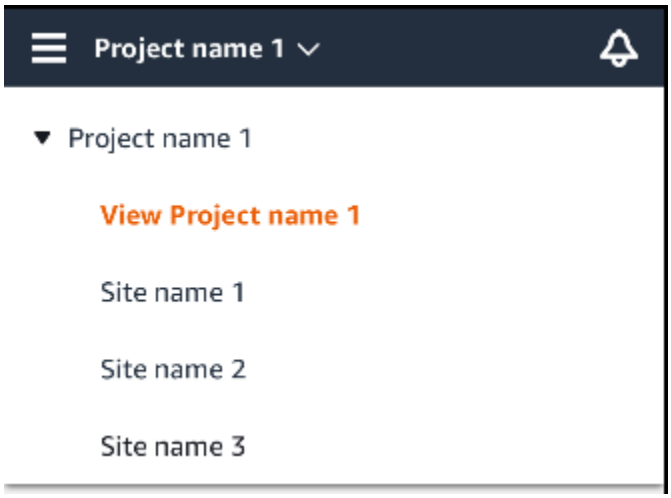
プロジェクトレベルからサイトレベルへの切り替え

プロジェクトレベルからサイトレベルに変更するには

1. スマートフォンで Amazon Monitron モバイルアプリにログインします。

   目的のプロジェクトに移動します。

2. プロジェクト名を選択します。



3. 表示するサイトを選択します。

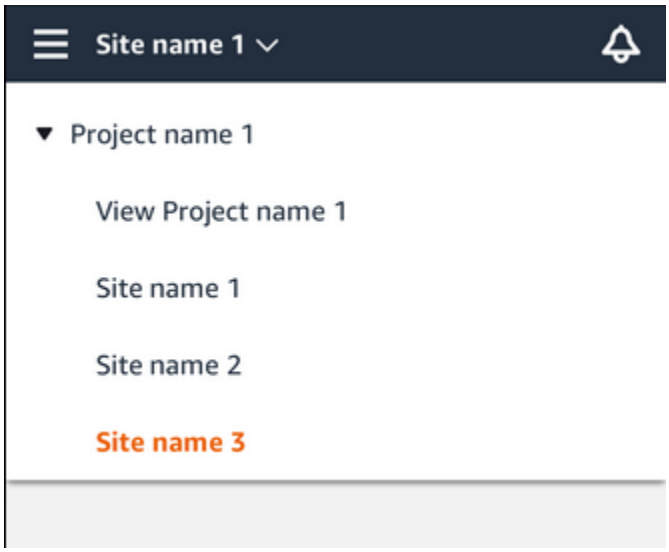
サイトレベルからプロジェクトレベルへの切り替え

サイトレベルからプロジェクトレベルに変更するには

1. スマートフォンで Amazon Monitron モバイルアプリにログインします。

   モバイルアプリに表示されているサイト名は、自分のサイトレベルです。

2. サイト名を選択します。



3. プロジェクト名を選択します。

   別のサイトに変更するには、変更先のサイト名を選択します。

ゲートウェイ

Amazon Monitron はゲートウェイを使用して、センサーによって Amazon Monitron 収集されたデータを AWS クラウドに転送します。ゲートウェイは、工場内のセンサーから 20～30 メートル以内に配置されます。Bluetooth Low Energy (BLE) 経由でセンサーと通信し、Wi-Fi またはイーサネットを使用して AWS クラウドと通信します。

このトピックでは、イーサネットゲートウェイと Wi-Fi ゲートウェイを設置する方法について説明します。また、不要なゲートウェイを削除する方法についても説明します。

> **Note**
>
> プロジェクトにゲートウェイを追加したら、すぐに見つけられるようにゲートウェイの名前を編集できます。

トピック

- イーサネットゲートウェイ
- Wi-Fi ゲートウェイ

イーサネットゲートウェイ

Amazon Monitron イーサネットゲートウェイには RJ-45 ソケットが装備されているため、Cat 5e または Cat 6 イーサネットケーブルを使用してイーサネットネットワークに接続できます。Power over Ethernet (POE) を使用して、イーサネットケーブルを介してゲートウェイに電力を供給します。そのため、POE をサポートするルーターか POE パワーインジェクターが必要です。

イーサネットケーブルをゲートウェイに挿入したら、[設定] ボタンを押してゲートウェイをコミッショニングモードにします。

Wi-Fi ゲートウェイ Amazon Monitron での の使用については、「」を参照してくださいWi-Fi ゲートウェイ。

トピック

- イーサネットゲートウェイの LED ライトの読み取り

- イーサネットゲートウェイの取り付けと設置
- イーサネットゲートウェイのコミッショニング
- イーサネットゲートウェイ検出のトラブルシューティング
- Bluetooth ペアリングのトラブルシューティング
- イーサネットゲートウェイの工場出荷時設定へのリセット
- ゲートウェイのリストの表示
- イーサネットゲートウェイの詳細の表示
- イーサネットゲートウェイの名前の編集
- インターネットゲートウェイの削除
- MAC アドレスの詳細の取得

イーサネットゲートウェイの LED ライトの読み取り

Amazon Monitron イーサネットゲートウェイの上部にある LED ライトは、ゲートウェイのステータスを示します。各ゲートウェイには、オレンジ色のライトが 1 つ、青色のライトが 1 つ、緑色のライトが 1 つあります。緑色のライトは電源がオンになっていることを示します。オレンジ色のライトは、ゲートウェイがイーサネットに接続されていることを示します。青色のライトは、ゲートウェイの Bluetooth がセンサーに接続されていることを示します。

以下の表に示すように、ライトが表示されるシーケンスはゲートウェイの状態を示します。

	LED シーケンス	説明
1	緑色のライトが点灯	イーサネットゲートウェイの電源がオンになっています。
2	オレンジ色のライトが点灯	ゲートウェイがイーサネットネットワークと Amazon Monitron バックエンドシステムに接続されています。
3	オレンジ色のライトが点滅 (低速)	ゲートウェイがイーサネットネットワークに接続を試みています。

	LED シーケンス	説明
4	オレンジ色のライトが点滅 (1 回高速、1 回低速)	ゲートウェイがイーサネットネットワークに接続されており、 Amazon Monitron バックエンドシステムへの接続を試みています。
5	青色のライトが点灯	少なくとも 1 つのセンサーがゲートウェイと通信しています。
6	青色のライトが点灯していない	現在、ゲートウェイと通信しているセンサーはありません。
7	オレンジ色と青色のライトが点滅 (低速)	ゲートウェイの電源がオンになっていますが、設定されていない (コミッショニングされていない) 状態で、コミッショニングモードになっていません (つまり、モバイルアプリで検出または設定できません)。
8	オレンジ色と青色のライトが点滅 (高速)	ゲートウェイの電源がオンで、コミッショニングモードになっていますが、まだどのセンサーにも接続されていません。コミッショニングモードでは、ゲートウェイは Amazon によって検出および設定可能ですが Amazon Monitron、まだ接続できるセンサーはありません。
9	ライトが点灯していない	ゲートウェイが電源に接続されていないか、ファームウェアの更新が進行中です。

	LED シーケンス	説明
10	オレンジ色と青色のライトが点灯	ゲートウェイが起動中です。

イーサネットゲートウェイの取り付けと設置

センサーとは異なり、イーサネットゲートウェイは監視対象の機械に取り付ける必要がありません。ただし、 が AWS クラウドに接続 Amazon Monitron できる利用可能なイーサネットネットワークが必要です。

トピック

- ゲートウェイの取り付け場所
- イーサネットゲートウェイを設置する
- ゲートウェイを差し込む

ゲートウェイの取り付け場所

ゲートウェイは、レイアウトにもよりますが、作業エリアのどこにでも設置できます。ゲートウェイの取り付け場所は壁になるのが通常ですが、天井、柱、その他の場所でも可能です。ゲートウェイは、対応するセンサーから 20～30 メートル以内に配置する必要があり、イーサネットゲートウェイは、接続できるイーサネットケーブルに十分近い位置にある必要があります。イーサネットゲートウェイはイーサネットケーブルから電力を供給することに注意してください。

ゲートウェイを取り付ける際には、他にも以下のような要素を考慮してください。

- ゲートウェイをセンサーよりも高い位置 (2 メートル以上) に取り付けると、カバレッジが向上する可能性があります。
- ゲートウェイとセンサーの間に障害物がないほど、カバレッジが向上します。
- むき出しの鉄骨梁などの建築構造物にゲートウェイを取り付けることは避けてください。信号に干渉する可能性があります。
- 信号に電子的干渉を引き起こす可能性のある機器は、すべて回避するようにしてください。
- 可能であれば、センサーの伝送距離内に複数のゲートウェイを設置してください。1 つのゲートウェイが使用できなくなった場合、センサーは別のゲートウェイに切り替えてデータ送信を行います。複数のゲートウェイがあると、データ損失を防ぐのに役立ちます。2 つのゲートウェイ間に最低限必要な距離はありません。

イーサネットゲートウェイを設置する

ゲートウェイを作業エリアに設置するのに必要なものはほとんど、ゲートウェイが梱包されているボックスに含まれています。

- ゲートウェイ
- 壁面取り付け用ブラケット
- 両面テープ
- 取り付けネジ (4 本)

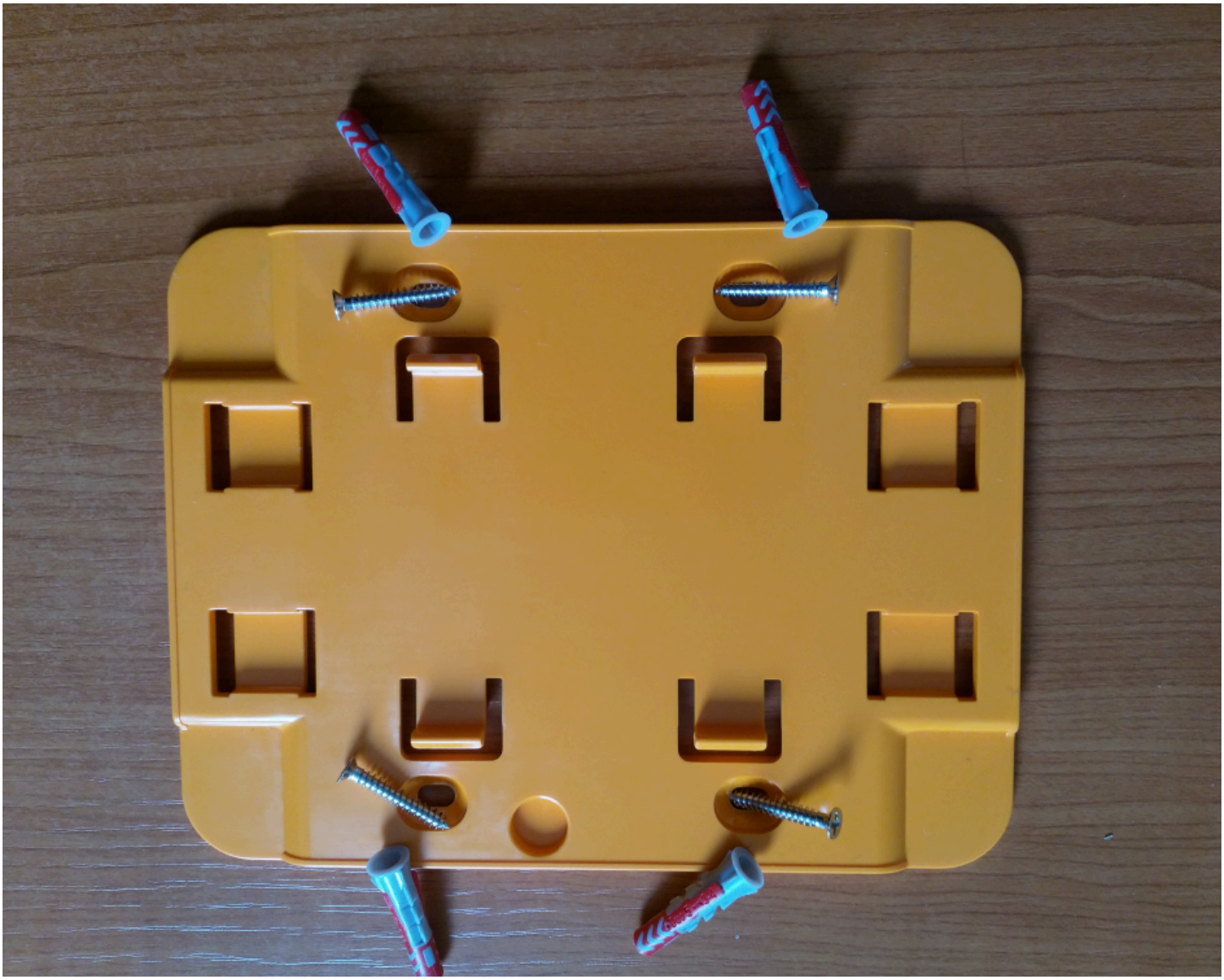
ゲートウェイを設置するには、壁面取り付け用ブラケットを壁面または別の場所に取り付けます。そのブラケットに対して、イーサネットケーブルを下向きにしてゲートウェイを取り付けます。

壁面取り付け用ブラケットを取り付けるには、ネジ取り付け、テープ取り付け、プラスチックタイ取り付けの 3 つの方法があります。使用する方法は、ゲートウェイの取り付け場所 (壁またはそれ以外) と取り付け面の材質によって異なります。

ブラケットの取り付けには、以下のいずれかの方法が利用できます。

ネジ取り付け

通常、ゲートウェイボックスに同梱されている取り付けネジを使用して、ブラケットを壁に直接取り付けます。ブラケットは正面から取り付けます。ネジを壁に固定するには、拡張プラグまたはトグルボルト (付属していません) が必要になる場合があります。



テープ取り付け

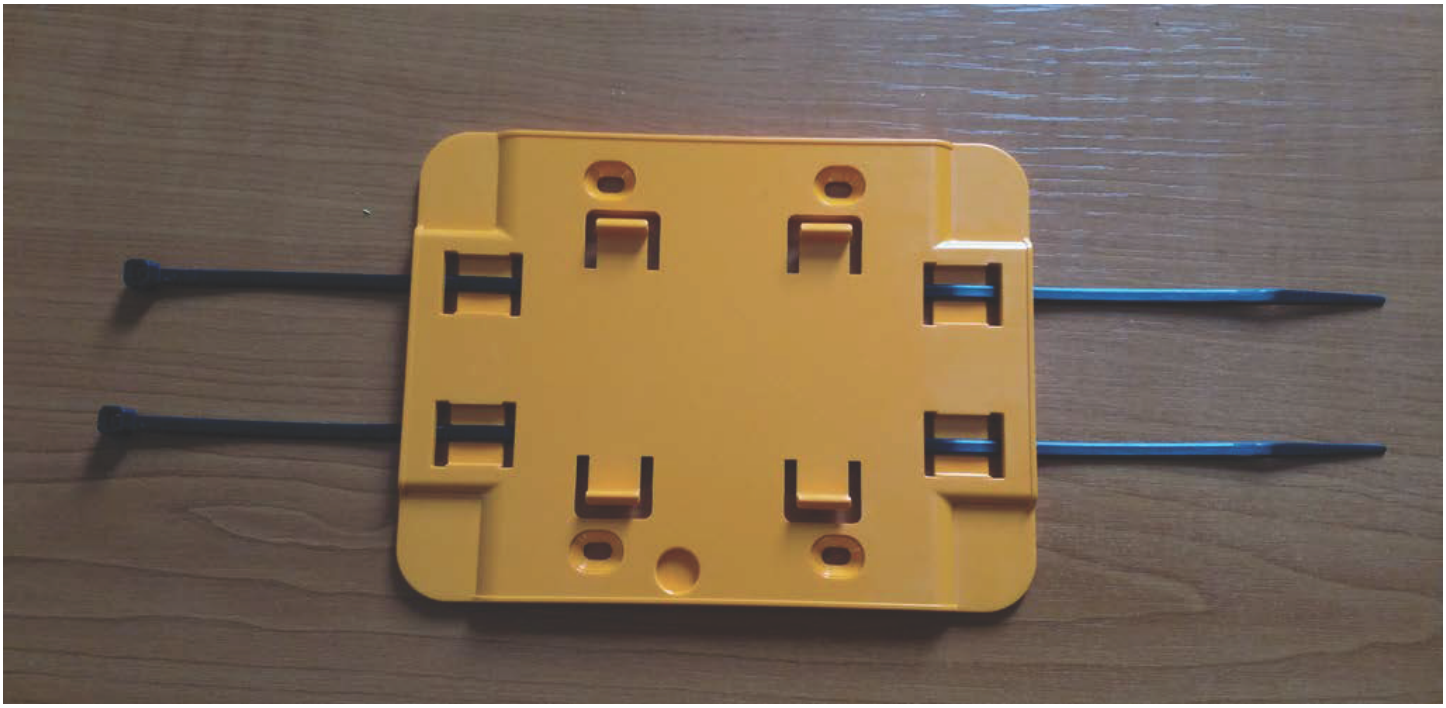
ゲートウェイボックスには、成形された両面テープが付属しています。取り付け面にネジを使用できない場合にお使いください。他の取り付け方法と組み合わせて使用すると、より安全に設置できます。

テープの片側の裏紙を剥がし、壁面取り付け用ブラケットの背面にある 4 つの隆起部分の間にテープを貼り付けます。

反対側の裏紙を剥がし、ブラケットを取り付け位置に貼り付けます。ブラケットを強く押して、テープが取り付け面にしっかりと付着していることを確認します。

プラスチックタイ取り付け

柱やフェンスなど、壁以外の小さな場所にゲートウェイを取り付ける場合は、ケーブルタイ (ジップタイとも呼ばれる) を使用して壁面取り付け用ブラケットを固定します。ブラケットの背面にある隆起した 4 つの穴にタイを通し、取り付け位置に巻き付けてからしっかりとタイを引っ張ります。



ブラケットを取り付けたら、そのブラケットにゲートウェイを取り付けます。

ゲートウェイを差し込む

1. 設置された壁面取り付け用ブラケットに対して、ゲートウェイを取り付けます。ゲートウェイの背面にある 2 つのプラスチックフックをブラケット下部のスロットに差し込みます。
2. ゲートウェイの上部をブラケットに押し当て、ゲートウェイの背面にあるプラスチックフックがブラケットの上部に引っかかるようにします。

> **Note**
>
> イーサネットケーブルを下向きにしてゲートウェイを設置します。

ゲートウェイへの接続に問題がある場合は、「イーサネットゲートウェイ検出のトラブルシューティング」を参照してください。

イーサネットゲートウェイのコミッショニング

ゲートウェイをファクトリーにマウントする場合、モバイルアプリにアクセスしてコ Amazon Monitron ミッショニングする必要があります。 は、近距離通信 (NFC) と Bluetooth を備えた

Android 8.0 以降または iOS 14 以降を使用するスマートフォンのみ Amazon Monitron をサポートします。

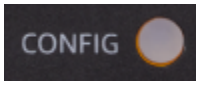
トピック

- ゲートウェイをコミッショニングするには

ゲートウェイをコミッショニングするには

1. スマートフォンの Bluetooth がまだオンになっていない場合は、オンにしてください。
2. ゲートウェイは、センサーとの通信に最適な場所に配置してください。

   ゲートウェイを取り付ける最適な場所は、センサーよりも高く、20 ~ 30 メートル以内の距離です。ゲートウェイの位置決めの詳細については、「イーサネットゲートウェイの取り付けと設置」を参照してください。
3. ゲートウェイを接続し、ゲートウェイの正面にあるネットワークライト (黄色) と Bluetooth ライト (青色) が交互に点滅していることを確認します。
4. ゲートウェイの [設定] ボタンを押して、コミッショニングモードにします。Bluetooth とネットワークの LED ライトがすばやく点滅し始めます。

5. スマートフォンでモバイルアプリを開きます。
6. [開始方法] ページまたは [ゲートウェイ] ページで、[ゲートウェイを追加] を選選択します。

   Amazon Monitron はゲートウェイをスキャンします。これには少し時間がかかることがあります。がゲートウェイ Amazon Monitron を検出すると、ゲートウェイリストに表示されます。
7. 表示されたゲートウェイを選択します。

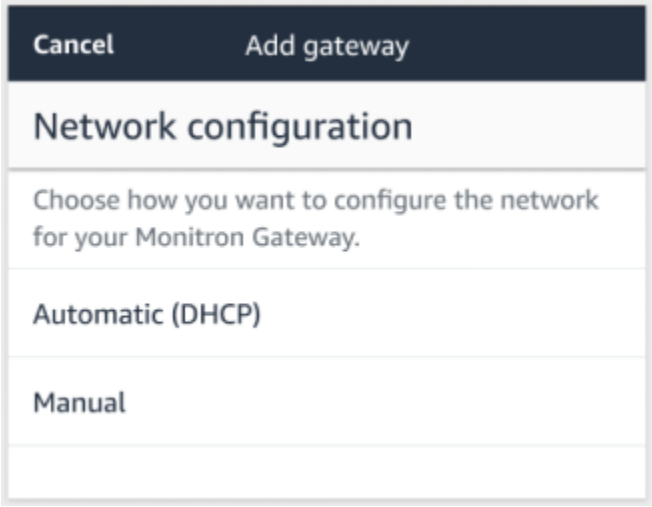
   > **Note**
   >
   > iOS モバイルデバイスを使用していて、以前にこの特定のゲートウェイとペアリングしたことがある場合は、再度ペアリングする前にデバイスにゲートウェイを「削除」させることが必要になる場合があります。詳細については、「Bluetooth ペアリングのトラブルシューティング」を参照してください。

   が新しいゲートウェイに接続する Amazon Monitron までに少し時間がかかる場合があります。

モバイルアプリケーションがゲートウェイへの接続を引き続き試みても成功しない場合は、「イーサネットゲートウェイ検出のトラブルシューティング」を参照してください。

> **Note**
>
> ゲートウェイが正常に接続されると、Amazon Monitron はモバイルアプリにゲートウェイデバイス ID と MAC ID を表示します。

8. ゲートウェイに接続すると、 Amazon Monitron にはゲートウェイのネットワーク接続を設定する 2 つのオプションが用意されています。



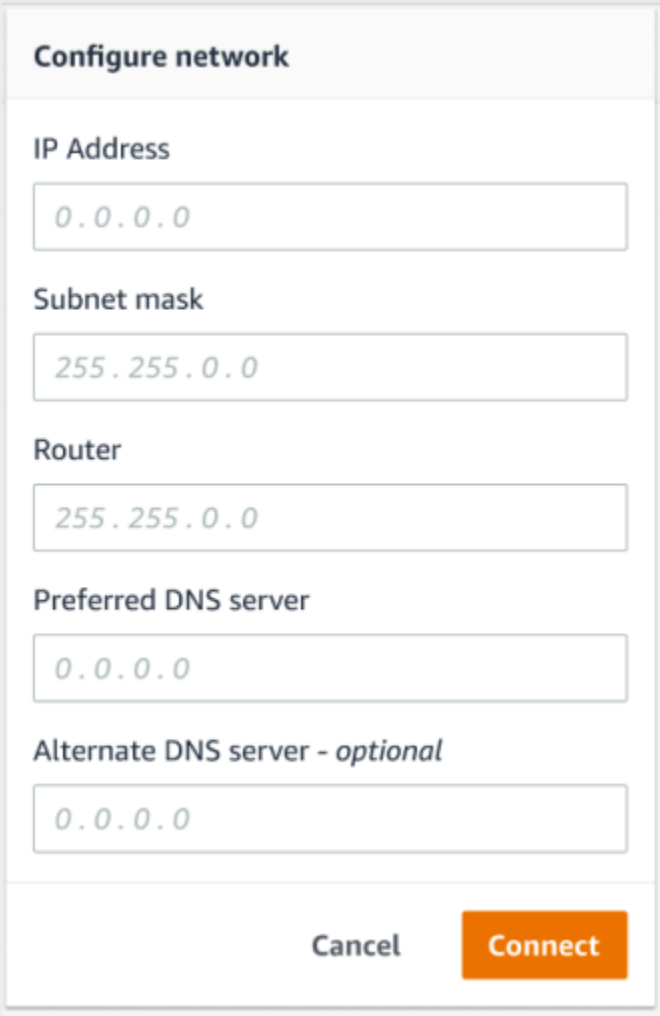
9. お使いのネットワーク設定を選択します。

ゲートウェイのコミッショニングが行われ、ネットワークに接続されるまでには、数分かかる場合があります。

ゲートウェイの動作に他の問題がある場合は、リセットすると役立つ場合があります。詳細については、「イーサネットゲートウェイの工場出荷時設定へのリセット」を参照してください。

a. 自動 (DHCP) を選択した場合、 Amazon Monitron はゲートウェイに接続するようにネットワークを自動的に設定します。

b. [手動] を選択した場合は、[IP アドレス]、[サブネットマスク]、[ルーター]、[優先 DNS サーバー]、[代替 DNS サーバー (オプション)] の情報を入力します。次に、[接続] を選択します。



イーサネットゲートウェイ検出のトラブルシューティング

プロジェクトまたはサイトにゲートウェイを追加すると、ゲートウェイの追加を選択するとすぐに、Amazon Monitron モバイルアプリはゲートウェイのスキャンを開始します。アプリでゲートウェイが検出されない場合は、以下のトラブルシューティングのヒントを試してください。

- ゲートウェイの電源がオンになっていることを確認します。ゲートウェイの右上隅の近くにある小さな緑色のライトを確認します。ライトが点灯している場合、ゲートウェイに電力が供給されています。

  ゲートウェイに電力が供給されていない場合は、以下の点を確認してください。

  - イーサネットケーブルが RJ-45 ソケットにしっかりと接続されていますか。
  - イーサネットケーブルの反対側にあるルーターは正しく機能していますか。
  - イーサネットケーブルは機能していますか。ケーブルを別のゲートウェイに接続すると、機能しているかどうかをテストできます。
  - RJ-45 ソケットは汚れていませんか。イーサネットケーブルの反対側にある終端のソケットも確認してください。
- ゲートウェイが設定モードになっていることを確認します。 Amazon Monitron モバイルアプリは、設定モードの場合にのみ新しいゲートウェイを見つけます。ゲートウェイの電源をオンにすると、Bluetooth と ネットワークの LED ライトがオレンジ色と青色に交互にゆっくり点滅します。[設定] ボタンを押してコミッショニングモードに移行すると、オレンジ色と青色が交互にすばやく点滅します。

- ボタンを押す前に LED がゆっくり点滅する以外のシーケンスを示している場合、ゲートウェイが設定モードに移行していない可能性があります。この場合は [リセット] ボタンを押してゲートウェイをリセットします。
- スマートフォンの Bluetooth が機能していることを確認します。ゲートウェイは Bluetooth を使用してスマートフォンに接続するため、Bluetooth 機能が中断の原因となる可能性があります。以下をチェックしてください:
  - スマートフォンの Bluetooth がオンになっていて、機能していますか。オフにしてからオンに切り替えてみてください。それでも解決しない場合は、スマートフォンを再起動してもう一度確認してください。
  - スマートフォンの Bluetooth 圏内にいますか。Bluetooth の通信範囲は比較的短く、通常は 10 メートル未満です。また、その信頼性は大きく異なる可能性があります。
  - Bluetooth 信号を電子的に妨害している可能性がある障害物はありますか。
- ゲートウェイがどのプロジェクトにもまだコミッショニングされていないことを確認します。デバイスは、コミッショニングを行う前にすべての既存プロジェクトから削除される必要があります。

これらのアクションを実行しても問題が解決しない場合は、以下の手順を実行します。

- ゲートウェイ MAC アドレスを表示およびコピーし、IT 管理者に連絡します。「MAC アドレスの詳細の取得」を参照してください。
- モバイルアプリからログアウトし、再起動します。
- [設定] を押したまま [リセット] を押して、ゲートウェイを工場出荷時設定にリセットします。

Bluetooth ペアリングのトラブルシューティング

iOS モバイルデバイスを、既にペアリングされているゲートウェイと再度ペアリングを試みる場合があります。これは、ゲートウェイが場所を変更したこと、または Amazon Monitron サイトの一般的な設定が変更されたことが原因である可能性があります。

その場合は、iOS デバイスでゲートウェイとの Bluetooth 接続を「削除」します。

トピック

- ゲートウェイとデバイスのペアリングを解除するには

ゲートウェイとデバイスのペアリングを解除するには

1. iOS デバイスで、[設定] を選択します。
2. [設定] 画面で [Bluetooth] を選択します。
3. Bluetooth 画面で、 Amazon Monitron ゲートウェイの名前の横にある情報アイコンを選択します。
4. 次に表示される画面で、[このデバイスを削除] を選択します。

イーサネットゲートウェイの工場出荷時設定へのリセット

削除されたゲートウェイを再利用する場合は Amazon Monitron、コミッショニングボタンを使用してゲートウェイを工場出荷時の設定にリセットします。これにより、ゲートウェイが再び使用される準備が整います Amazon Monitron。

トピック

- イーサネットゲートウェイを工場出荷時設定にリセットする (オプション 1)
- イーサネットゲートウェイを工場出荷時設定にリセットする (オプション 2)

イーサネットゲートウェイを工場出荷時設定にリセットする (オプション 1)

1. イーサネットケーブルをゲートウェイから取り外します。
2. [設定] ボタンを長押しします。
3. イーサネットケーブルをゲートウェイに再び接続します。

   LED ライトがオレンジ色と青色に交互にゆっくり点滅し始めたら、[設定] ボタンを放します。ゲートウェイがリセットされます。

イーサネットゲートウェイを工場出荷時設定にリセットする (オプション 2)

1. [設定] ボタンを長押しします。
2. [リセット] ボタンを押します。
3. LED ライトがオレンジ色と青色に交互にゆっくり点滅し始めたら、両方のボタンを放します。

ゲートウェイのリストの表示

このページでは、ゲートウェイを Amazon Monitron アプリに表示する方法について説明します。

トピック

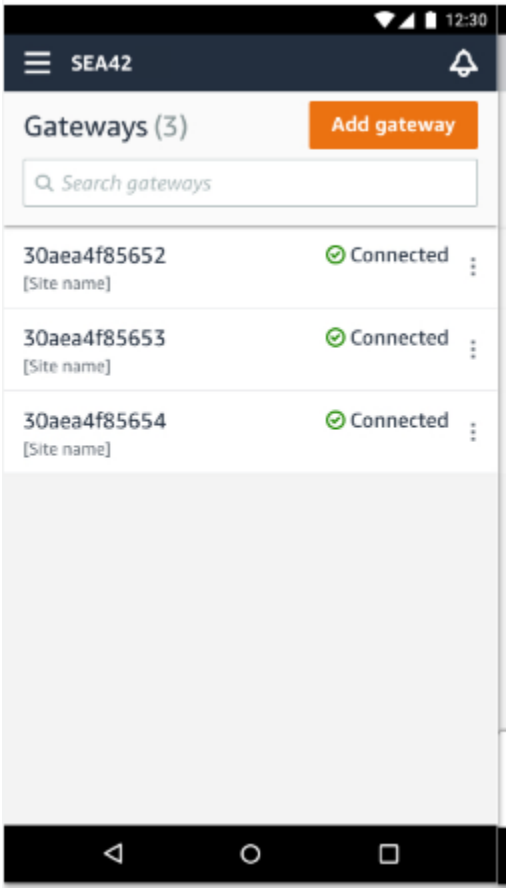
- モバイルアプリを使用してゲートウェイのリストを表示するには
- ウェブアプリを使用してゲートウェイのリストを表示するには

モバイルアプリを使用してゲートウェイのリストを表示するには

1. スマートフォンを使用して Amazon Monitron モバイルアプリにログインします。
2. 画面左上のメニューアイコンを選択します。

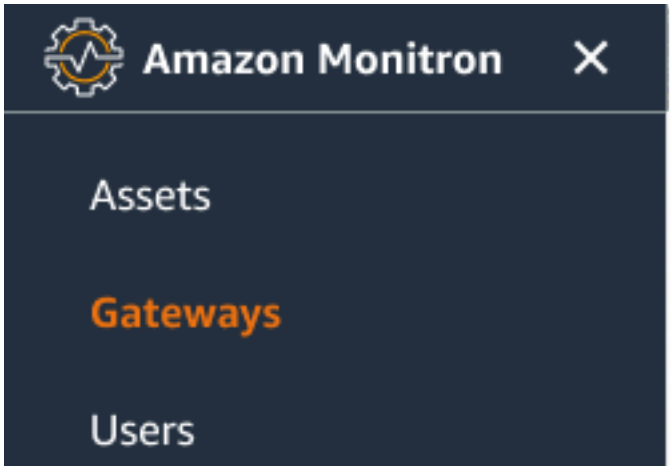
3. [ゲートウェイ] を選択します。

   プロジェクトに関連するすべてのゲートウェイのリストが表示されます。

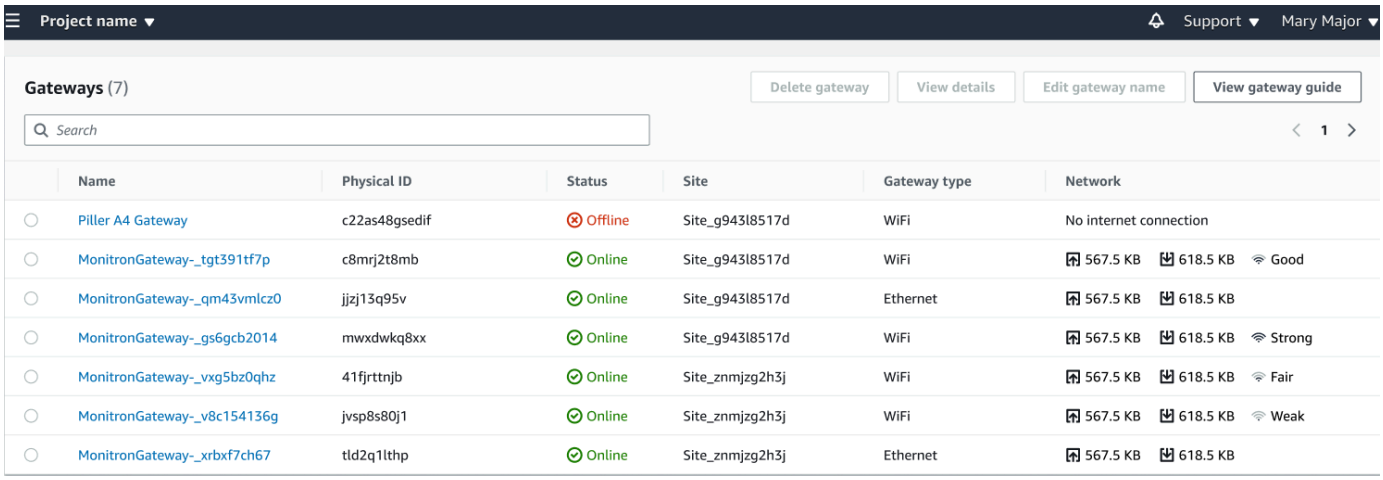


ウェブアプリを使用してゲートウェイのリストを表示するには

1. 左側のナビゲーションペインで [ゲートウェイ] をクリックします。



2. 右側のペインにゲートウェイのリストが表示されます。



イーサネットゲートウェイの詳細の表示

モバイルまたはウェブアプリケーションでゲートウェイの詳細を表示できます。以下のゲートウェイの詳細を表示できます。

- IP アドレス
- ファームウェアバージョン
- 最後のコミッショニング

> **Note**
>
> ゲートウェイ MAC アドレスを表示およびコピーすることもできます。「MAC アドレスの詳細の取得」を参照してください。

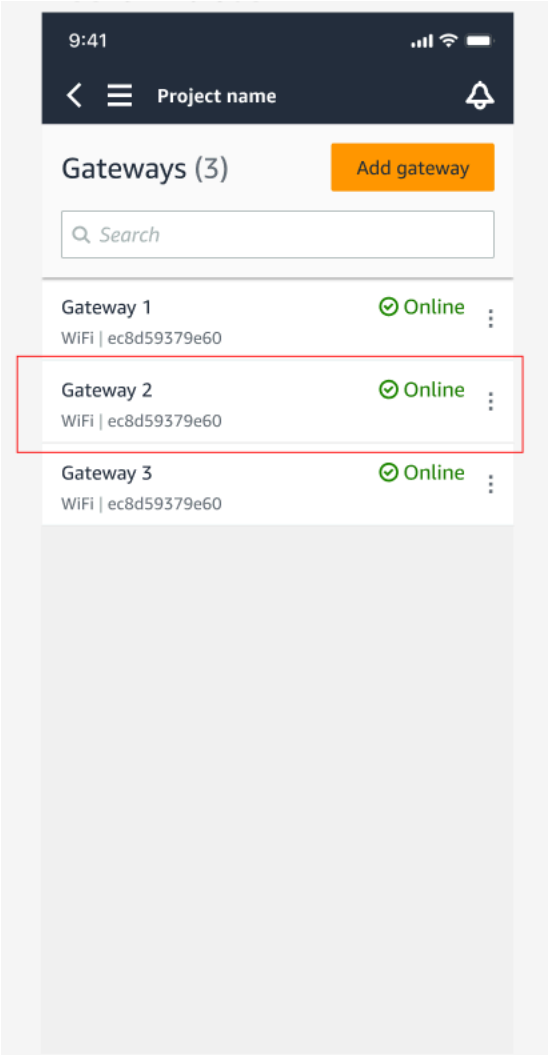
センサーの詳細は、モバイルアプリとウェブアプリの両方で確認できます。次のセクションでその確認方法について説明します。

トピック

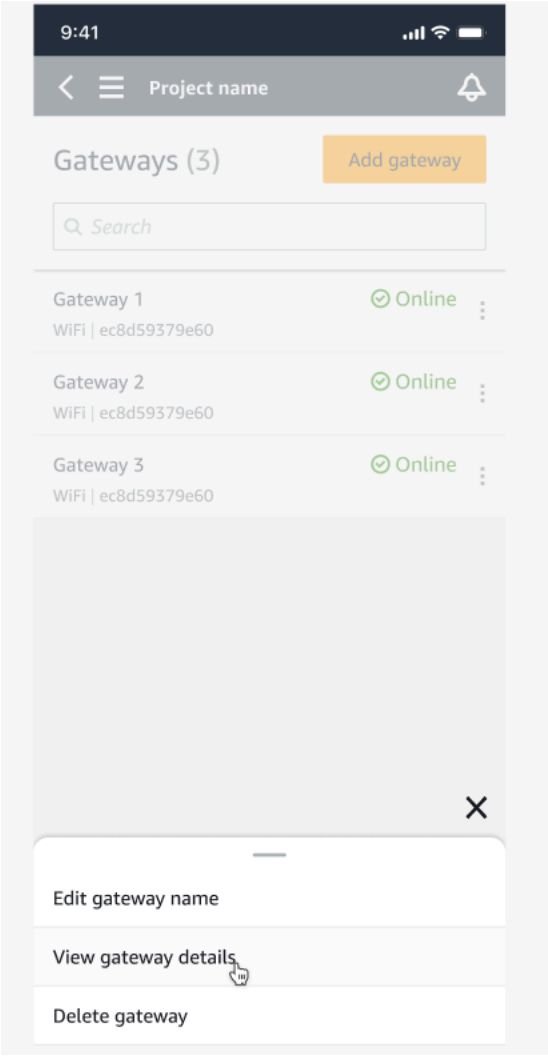
- モバイルアプリでイーサネットゲートウェイの詳細を表示するには
- ウェブアプリでイーサネットゲートウェイの詳細を表示するには

モバイルアプリでイーサネットゲートウェイの詳細を表示するには

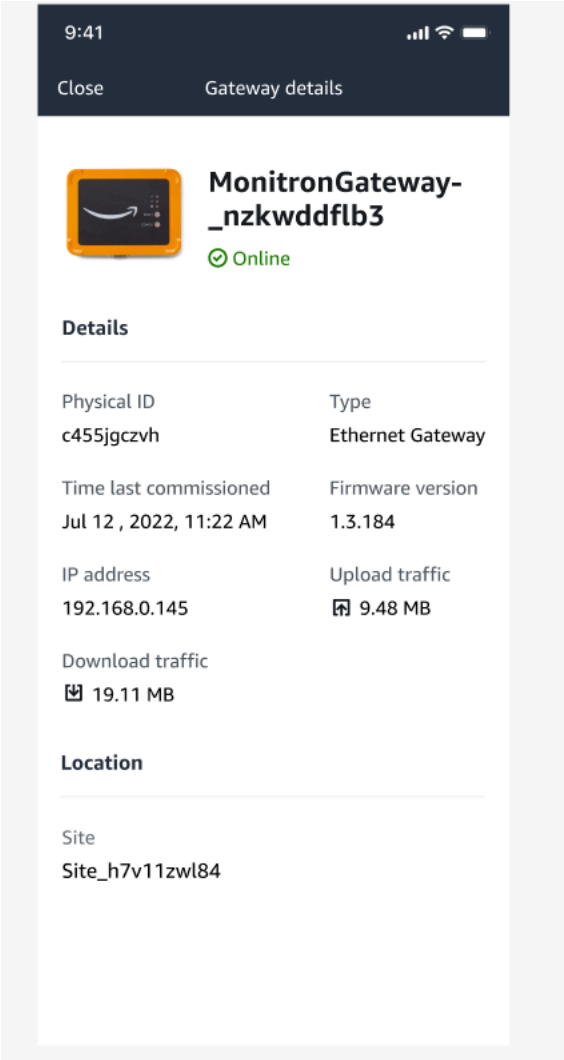
1. [ゲートウェイ] のリストから、詳細を表示するゲートウェイを選択します。



2. 表示されたオプションボックスから、[ゲートウェイの詳細を表示] を選択します。

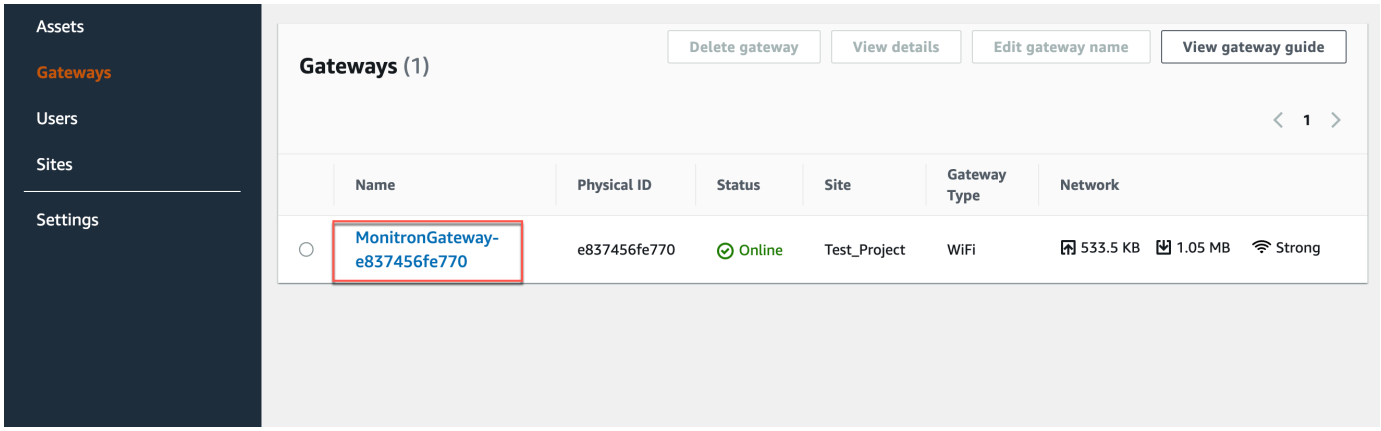


3. [ゲートウェイの詳細] ページが表示されます。

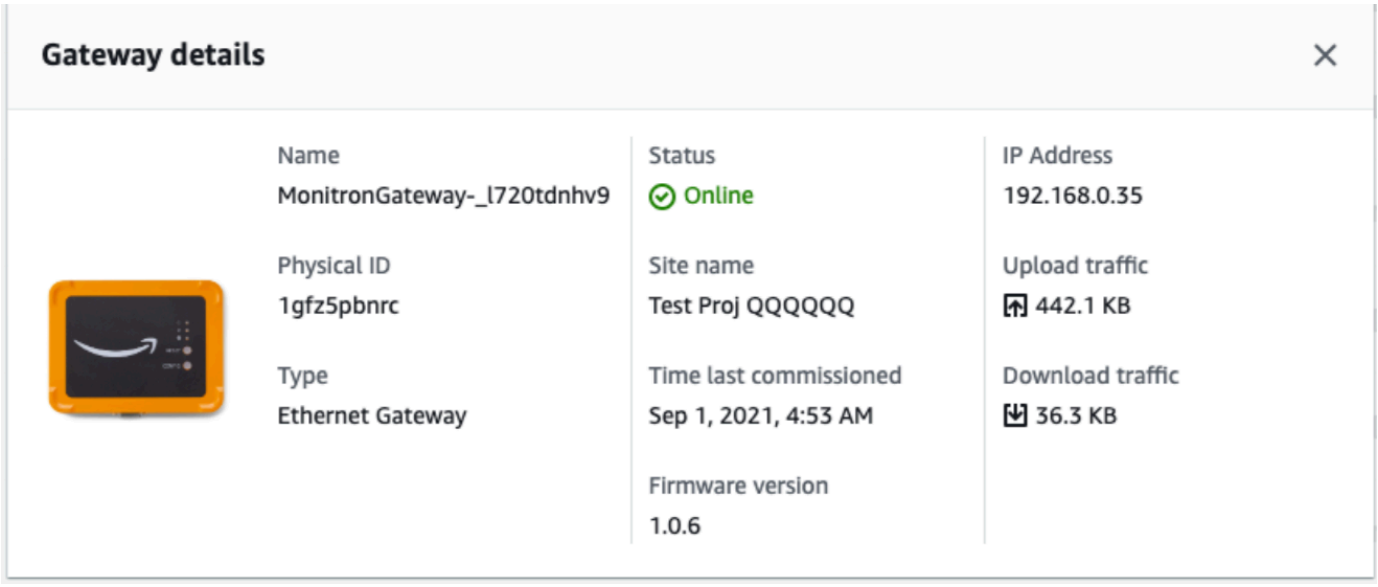


ウェブアプリでイーサネットゲートウェイの詳細を表示するには

1. [ゲートウェイ] のリストから、詳細を表示するゲートウェイを選択します。



2. [ゲートウェイの詳細] ページが表示されます。



イーサネットゲートウェイの名前の編集

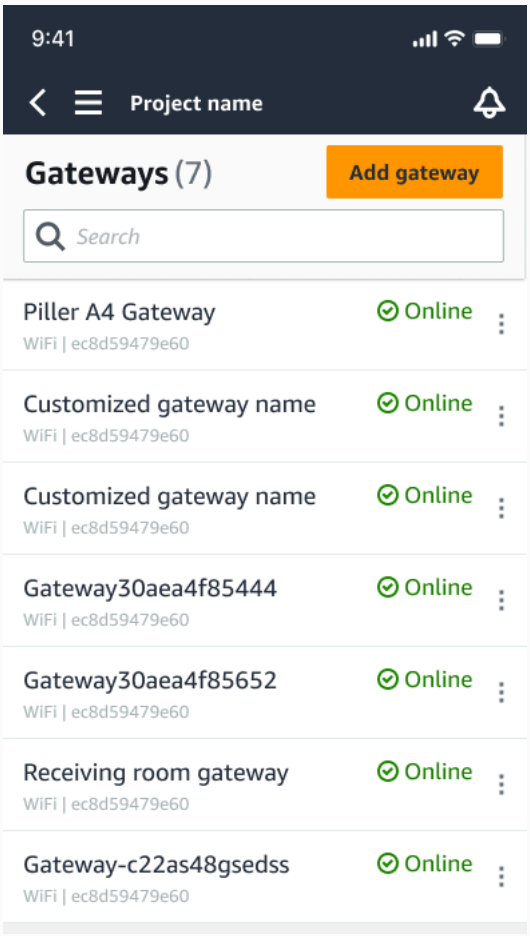
イーサネットゲートウェイの表示名を変更すると、すばやく見つけることができます。ゲートウェイの名前を編集するには、ウェブアプリまたはモバイルアプリを開いて以下の操作を行います。

トピック

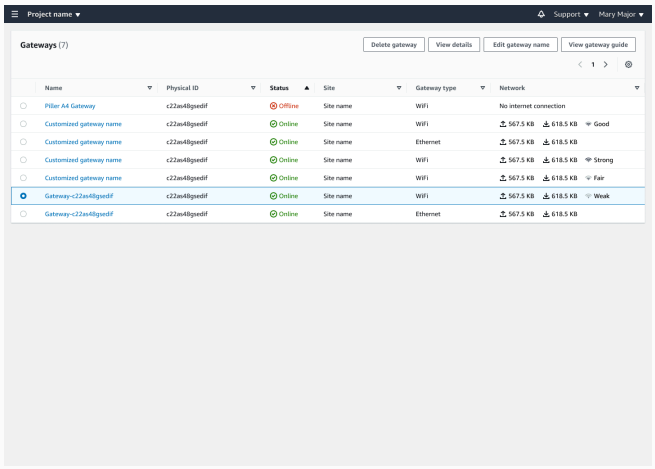
- イーサネットゲートウェイの名前を編集するには

イーサネットゲートウェイの名前を編集するには

1. [ゲートウェイ] ページから、編集するゲートウェイの名前を選択します。

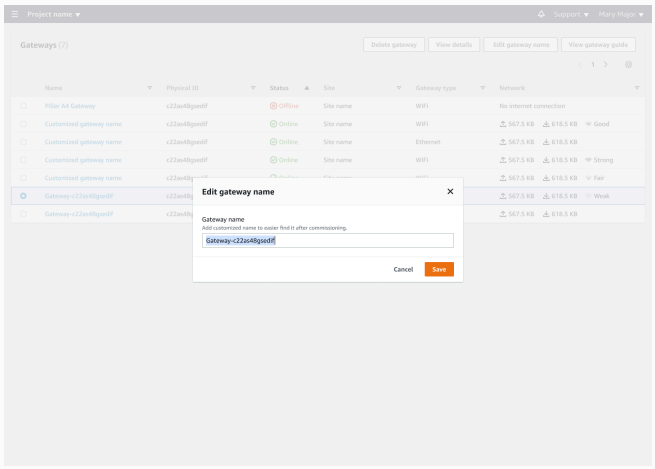


モバイルアプリの表示



ウェブアプリの表示

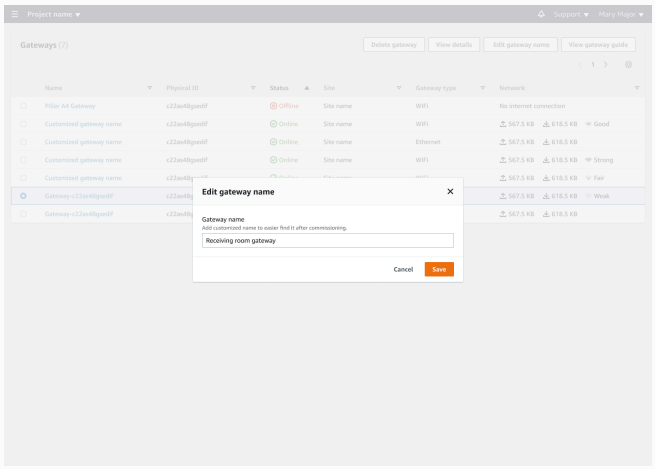
2. ゲートウェイにカスタマイズした名前を追加するように求めるポップアップが表示されます。



ウェブアプリの表示

モバイルアプリの表示

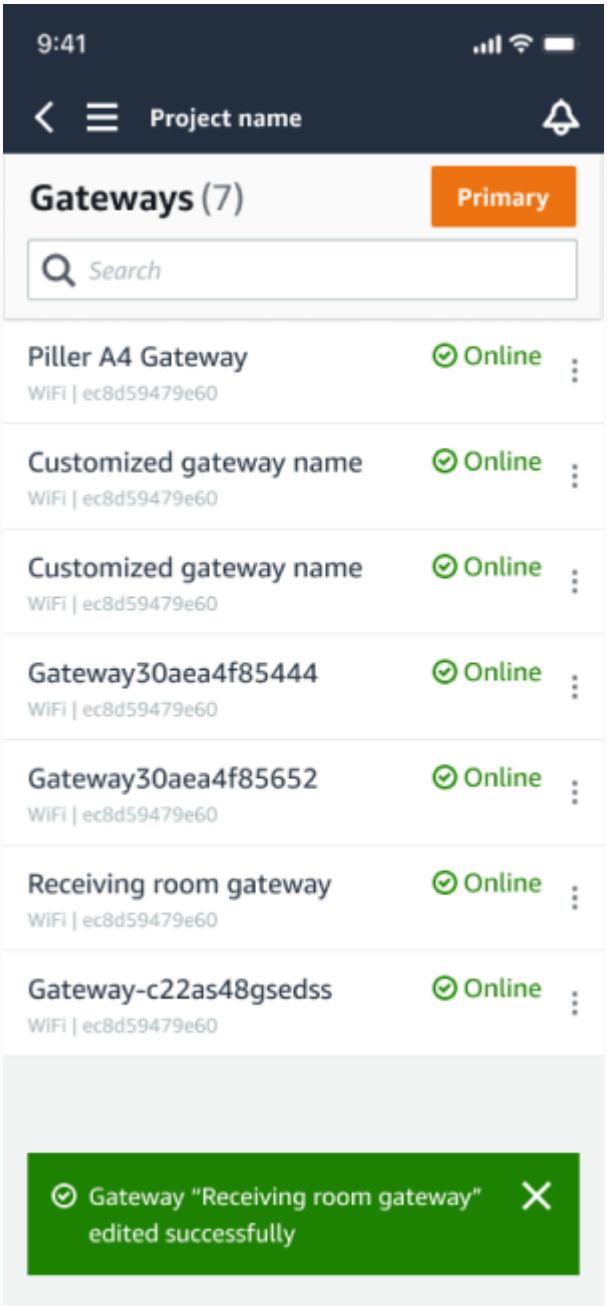
3. ゲートウェイの新しい名前を入力し、[保存] をクリックします。



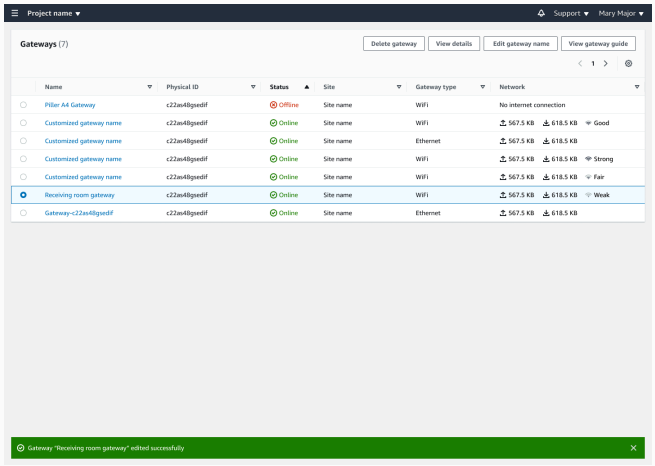
ウェブアプリの表示

モバイルアプリの表示

4. ゲートウェイの新しい名前を確認する成功メッセージが表示されます。



モバイルアプリの表示



ウェブアプリの表示

インターネットゲートウェイの削除

センサーには、データを AWS クラウドに中継するためのゲートウェイが必要です。ゲートウェイを削除すると、一部のセンサーが接続を失う可能性があります。ゲートウェイを削除する前には注意が必要です。

ゲートウェイを削除すると、センサーは範囲内にある別のゲートウェイ (存在する場合) に接続を切り替え、センサーからのデータ送信は中断されずに継続されます。範囲内にゲートウェイがない場合、データ送信は中断され、データが失われる可能性があります。

現在オフラインになっているゲートウェイを削除する場合は、デバイスを工場出荷時設定にリセットしてから再度コミッショニングする必要があります。

トピック

- モバイルアプリを使用してイーサネットゲートウェイを削除する
- ウェブアプリを使用してイーサネットゲートウェイを削除する

モバイルアプリを使用してイーサネットゲートウェイを削除する

1. モバイルアプリを使用して、[ゲートウェイ] ページに移動します。
2. 削除するゲートウェイの横にある縦 3 点アイコン

   ( )
   をクリックします。
3. [ゲートウェイを削除] を選択します。
4. [削除] をもう一度選択します。

ウェブアプリを使用してイーサネットゲートウェイを削除する

1. Wi-Fi ゲートウェイのリストに移動します。
2. テーブルから削除するゲートウェイを選択します。
3. [ゲートウェイを削除] を選択します。

MAC アドレスの詳細の取得

Amazon Monitron ゲートウェイの Media Access Control (MAC) アドレスを取得するには、携帯電話を使用してゲートウェイデバイスの QR コードをスキャンできます。Amazon Monitron は、QR コードをスキャンするときに MAC アドレスとゲートウェイ ID の両方を返します。

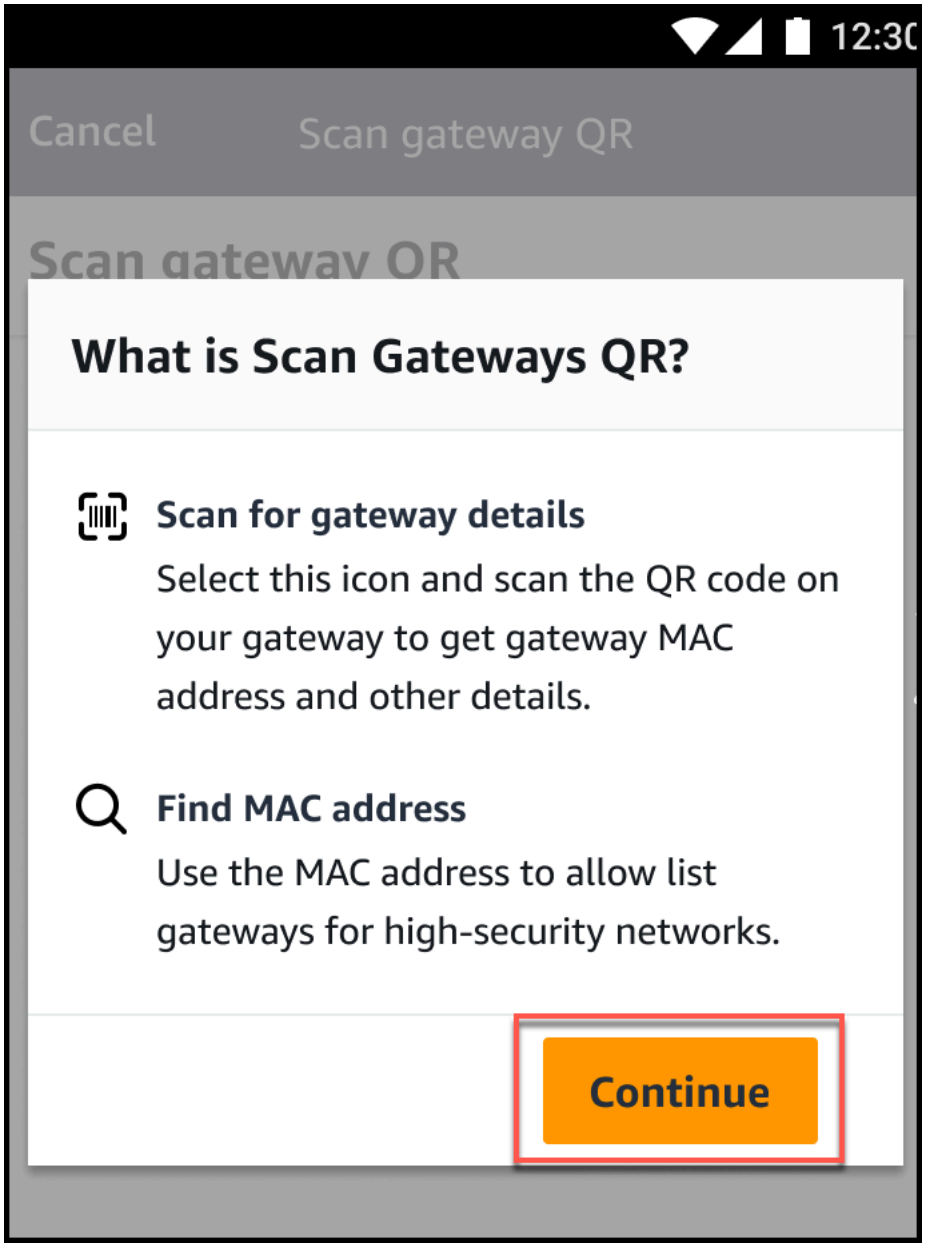
IT 管理者の場合は、スキャンされた MAC アドレスを使用して、ゲートウェイデバイスがコミッショニングされる前に正しいネットワーク設定で設定されていることを確認することができます。ゲートウェイをコミッショニングする技術者は、スキャンした MAC アドレスを使用して、IT 管理者のネットワーク問題のトラブルシューティングを行うことができます。

> **Note**
>
> QR コードをスキャンして MAC アドレスを取得することは、Amazon Monitron モバイルアプリでのみサポートされます。

次の手順では、ゲートウェイデバイスの MAC アドレスを取得する方法を示します。

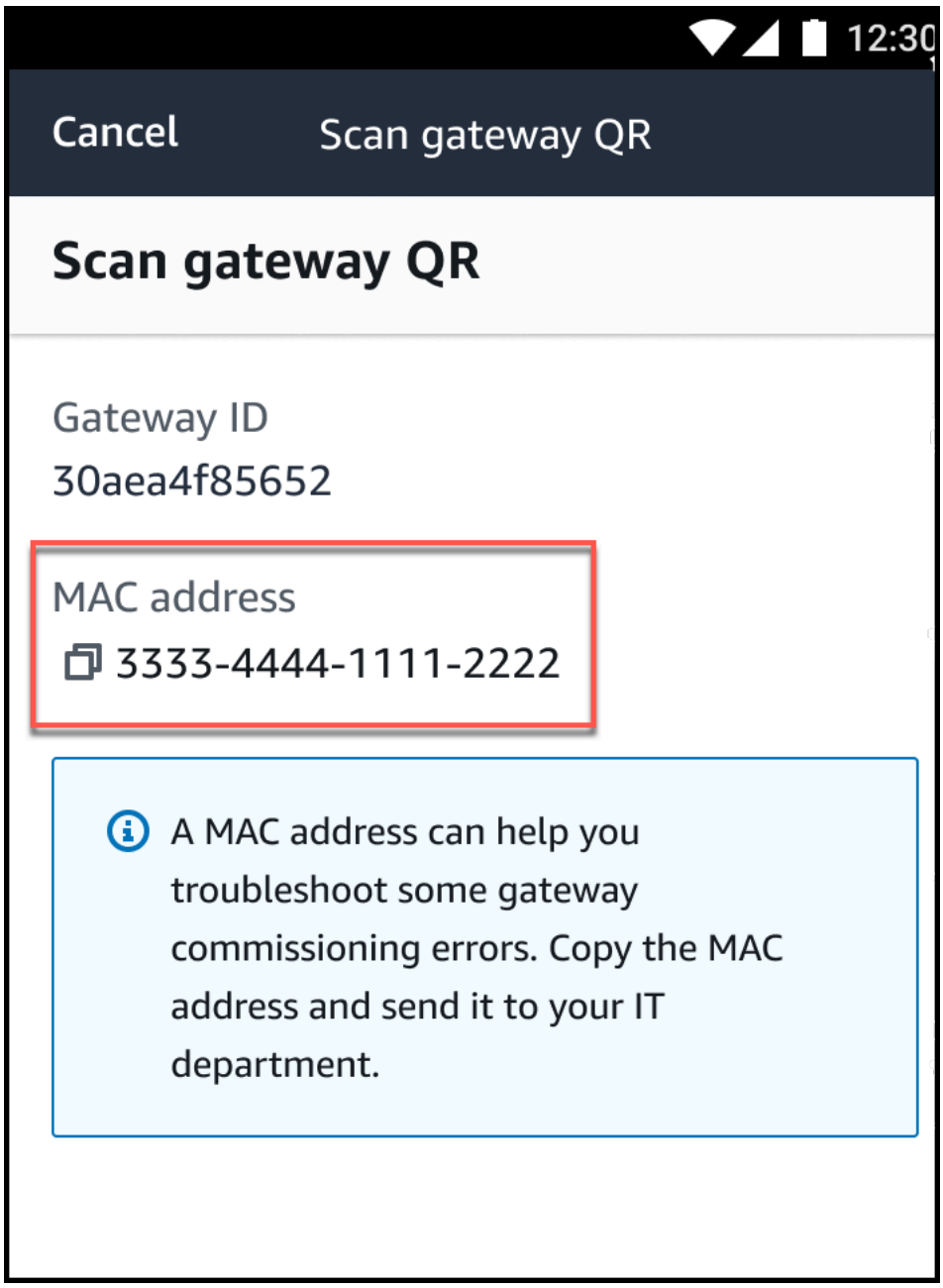
1. [ゲートウェイ] ページに移動します。
2. スキャンアイコンを選択します。

3. Amazon Monitron は、QR コードのスキャン内容を説明するメッセージを表示します。[Continue] (続行) をクリックします。



4. QR コードのスキャンページで、携帯電話のカメラを使用してゲートウェイの QR コードをスキャンします。

   スキャンが正常に完了すると、Amazon Monitron はモバイルアプリの QR コードのスキャンページにゲートウェイ ID と MAC アドレスを表示します。



コピーアイコン

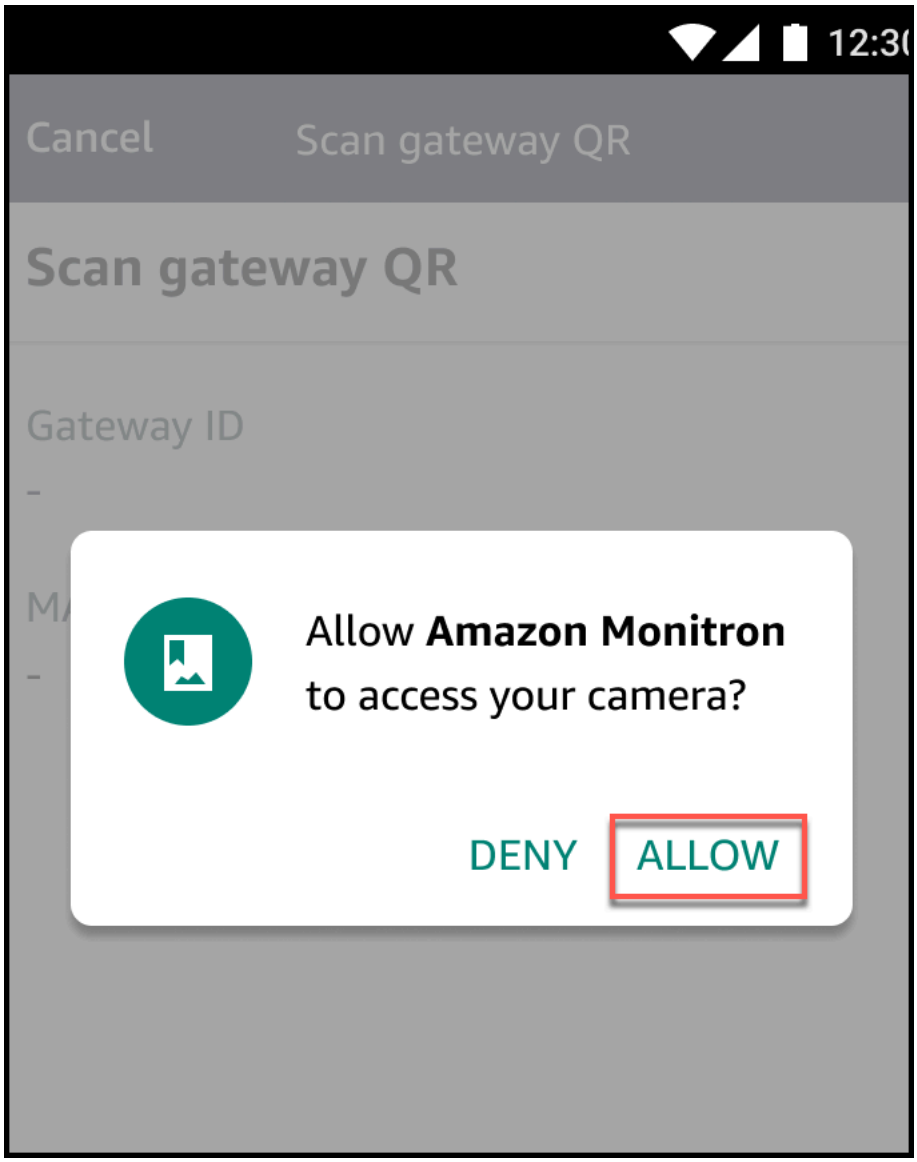
( )

を選択して MAC アドレスをコピーすることもできます。

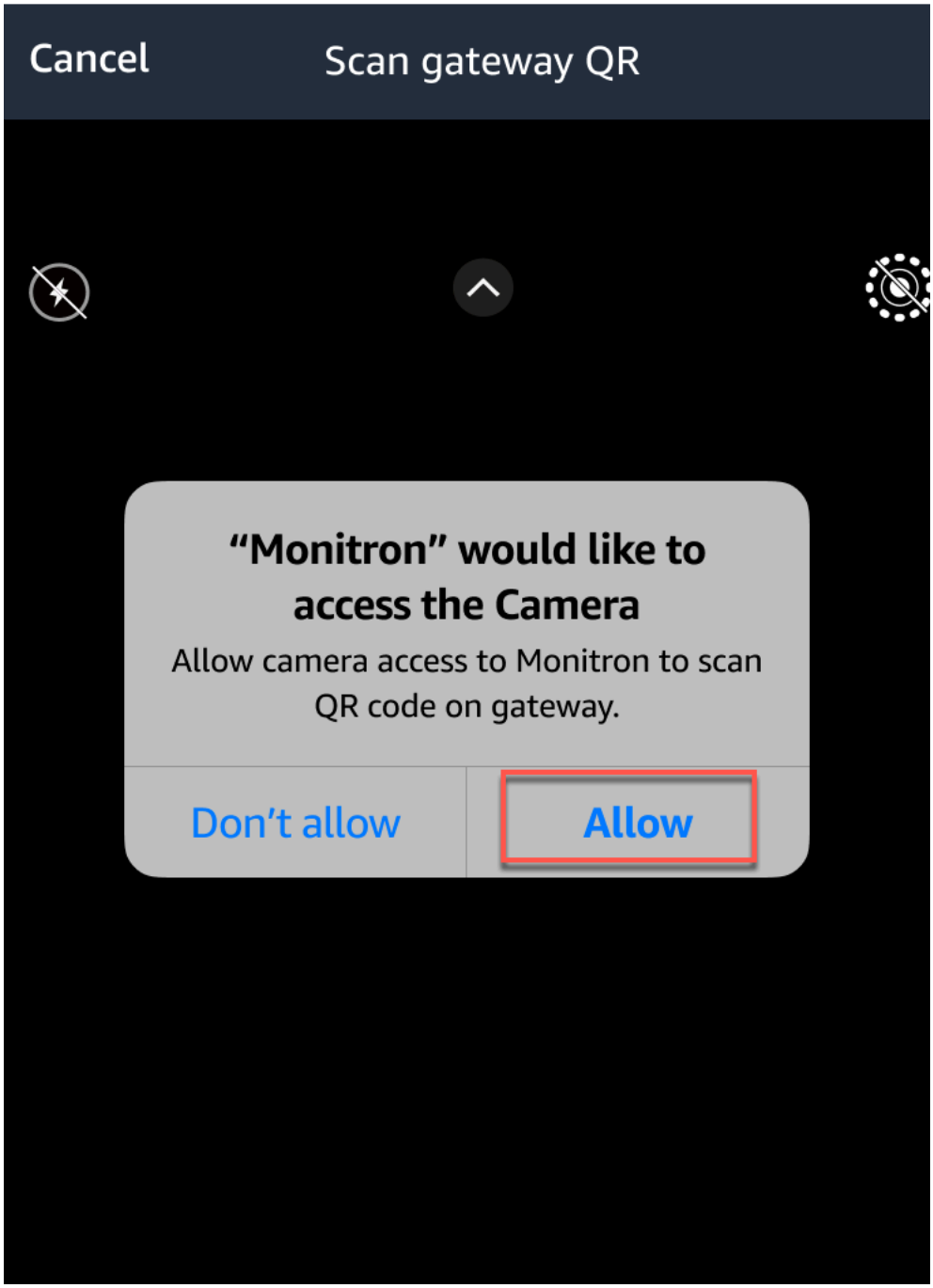
> **Note**
>
> まだ有効になっていない場合、Amazon Monitron はカメラにアクセスして QR コードをスキャンするためのアクセス許可が必要になる場合があります。これらのアクセス許可

は、デバイスの QR コードを正常にスキャンする前に、モバイルデバイスの設定ページから有効にする必要があります。アクセス許可がまだ付与されていない場合、Amazon Monitron はスキャンプロセス中にカメラアクセスを有効にするように求めます。

Android デバイスの場合



iOS デバイスの場合

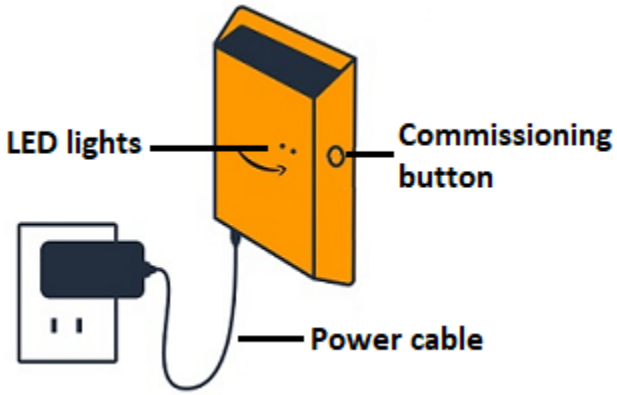


Wi-Fi ゲートウェイ

このトピックでは Wi-Fi ゲートウェイを設置する方法について説明します。また、不要なゲートウェイを削除する方法についても説明します。

イーサネットゲートウェイ Amazon Monitron で を使用する方法については、「」を参照してくださいイーサネットゲートウェイ。

Amazon Monitron ゲートウェイはインストールと運用が容易です。電源ケーブルを差し込んだ後、[コミッショニング] ボタンを押すと、ゲートウェイをコミッショニングモードに切り替えることができます。

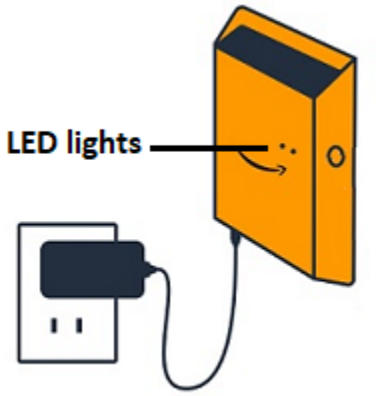


トピック

- Wi-Fi ゲートウェイの LED ライトの読み取り
- Wi-Fi ゲートウェイの取り付けと設置
- Wi-Fi ゲートウェイのコミッショニング
- Wi-Fi ゲートウェイ検出のトラブルシューティング
- Bluetooth ペアリングのトラブルシューティング
- Wi-Fi ゲートウェイの工場出荷時設定へのリセット
- ゲートウェイのリストの表示
- Wi-Fi ゲートウェイの詳細の表示
- Wi-Fi ゲートウェイの名前の編集
- Wi-Fi ゲートウェイの削除
- MAC アドレスの詳細の取得

Wi-Fi ゲートウェイの LED ライトの読み取り

Amazon Monitron ゲートウェイの上部にある LED ライトは、ゲートウェイのステータスを示します。LED ライトには、オレンジ色のライトが 1 つ、青色のライトが 1 つあります。オレンジ色のライトは、ゲートウェイが Wi-Fi ネットワークに接続されていることを示します。青色のライトは、ゲートウェイの Bluetooth がセンサーに接続されていることを示します。



以下の表に示すように、ライトが表示されるシーケンスはゲートウェイの状態を示します。

	LED シーケンス	説明
1	緑色のライトが点灯	Wi-Fi ゲートウェイの電源がオンになっています。
2	オレンジ色のライトが点灯	ゲートウェイは Wi-Fi ネットワークと Amazon Monitron バックエンドシステムに接続されています。
3	オレンジ色のライトが点滅 (低速)	ゲートウェイが Wi-Fi ネットワークに接続を試みています。
4	オレンジ色のライトが点滅 (1 回高速、1 回低速)	ゲートウェイが Wi-Fi ネットワークに接続されており、Amazon Monitron バックエンドシステムに接続しようとしています。
5	青色のライトが点灯	少なくとも 1 つのセンサーがゲートウェイと通信しています。

	LED シーケンス	説明
6	青色のライトが点灯していない	現在、ゲートウェイと通信しているセンサーはありません。
7	オレンジ色と青色のライトが点滅 (低速)	ゲートウェイの電源がオンになっていますが、設定されていない (コミッショニングされていない) 状態で、コミッショニングモードになっていません (つまり、モバイルアプリで検出または設定できません)。
8	オレンジ色と青色のライトが点滅 (高速)	ゲートウェイの電源がオンで、コミッショニングモードになっていますが、まだどのセンサーにも接続されていません。コミッショニングモードでは、ゲートウェイは Amazon によって検出および設定可能ですが Amazon Monitron、まだ接続できるセンサーはありません。
9	ライトが点灯していない	ゲートウェイが電源に接続されていないか、ファームウェアの更新が進行中です。
10	オレンジ色と青色のライトが点灯	ゲートウェイが起動中です。

Wi-Fi ゲートウェイの取り付けと設置

センサーとは異なり、Wi-Fi ゲートウェイは監視対象の機械に取り付ける必要がありません。ただし、 が AWS クラウドに接続 Amazon Monitron できる利用可能な Wi-Fi ネットワークが必要です。

トピック

- ゲートウェイの設置場所を決める
- ブラケットを取り付ける
- ゲートウェイをブラケットに取り付ける

ゲートウェイの設置場所を決める

ゲートウェイは、レイアウトにもよりますが、工場内のほぼどこにでも設置できます。通常、ゲートウェイは壁に取り付けられますが、天井、柱、その他ほとんどの場所でも可能です。ゲートウェイは、対応するセンサーから 20～30 メートル以内に配置する必要があります。また、接続できる電源コンセントに十分近い場所にある必要があります。

ゲートウェイを取り付ける際には、他にも以下のような要素を考慮してください。

- ゲートウェイをセンサーよりも高い位置 (2 メートル以上) に取り付けると、カバレッジが向上する可能性があります。
- ゲートウェイとセンサーの間に障害物がないほど、カバレッジが向上します。
- むき出しの鉄骨梁などの建築構造物にゲートウェイを取り付けることは避けてください。信号に干渉する可能性があります。
- 信号に電子的干渉を引き起こす可能性のある機器は、すべて回避するようにしてください。
- 可能であれば、センサーの伝送距離内に複数のゲートウェイを設置してください。1 つのゲートウェイが使用できなくなった場合、センサーは別のゲートウェイに切り替えてデータ送信を行います。複数のゲートウェイがあると、データ損失を減らすのに役立ちます。2 つのゲートウェイ間に最低限必要な距離はありません。

ブラケットを取り付ける

ゲートウェイを設置するには、壁面取り付け用ブラケットを壁面または別の場所に取り付け、そのブラケットに対してゲートウェイを取り付けます。

必要なものはほとんど、ゲートウェイが梱包されているボックスに含まれています。

- ゲートウェイ
- AC アダプター
- 欧州、英国、米国用の AC アダプタープラグ
- 壁面取り付けブラケット
- 両面テープ
- 取り付けネジ (2 本)
- ゲートウェイをブラケットに取り付けるための小さなネジ (1 本)

壁面取り付け用ブラケットを取り付けるには、ネジ取り付け、テープ取り付け、プラスチックタイ取り付けの 3 つの方法があります。使用する方法は、ゲートウェイの取り付け場所 (壁またはそれ以外) と取り付け面の材質によって異なります。ゲートウェイは、片方の短辺の中央にある小さなネジ穴を使用して壁面取り付け用ブラケットに取り付けます。

ブラケットの取り付けには、以下のいずれかの方法が利用できます。

ネジ取り付け

通常、ゲートウェイボックスに同梱されている取り付けネジを使用して、ブラケットを壁に直接取り付けます。ブラケットは正面から取り付けます。ネジを壁に固定するには、拡張プラグまたはトグルボルトが必要になる場合があります。拡張プラグやトグルボルトは付属していません。

テープ取り付け

ゲートウェイボックスには、成形された両面テープが付属しています。取り付け面にネジを使用できない場合にお使いください。他の取り付け方法と組み合わせて使用すると、より安全に設置できます。

テープの片側の裏紙を剥がし、壁面取り付け用ブラケットの背面にある 4 つの隆起部分の間にテープを貼り付けます。

反対側の裏紙を剥がし、ブラケットを取り付け位置に貼り付けます。ブラケットを強く押して、テープが取り付け面にしっかりと付着していることを確認します。

プラスチックタイ取り付け

柱やフェンスなど、壁以外の小さな場所にゲートウェイを取り付ける場合は、ケーブルタイ (ジップタイとも呼ばれる) を使用して壁面取り付け用ブラケットを固定します。ブラケットの背面にある隆起した 4 つの穴にタイを通し、取り付け位置に巻き付けてからしっかりとタイを引っ張ります。

ブラケットを取り付けたら、そのブラケットにゲートウェイを取り付けます。

ゲートウェイをブラケットに取り付ける

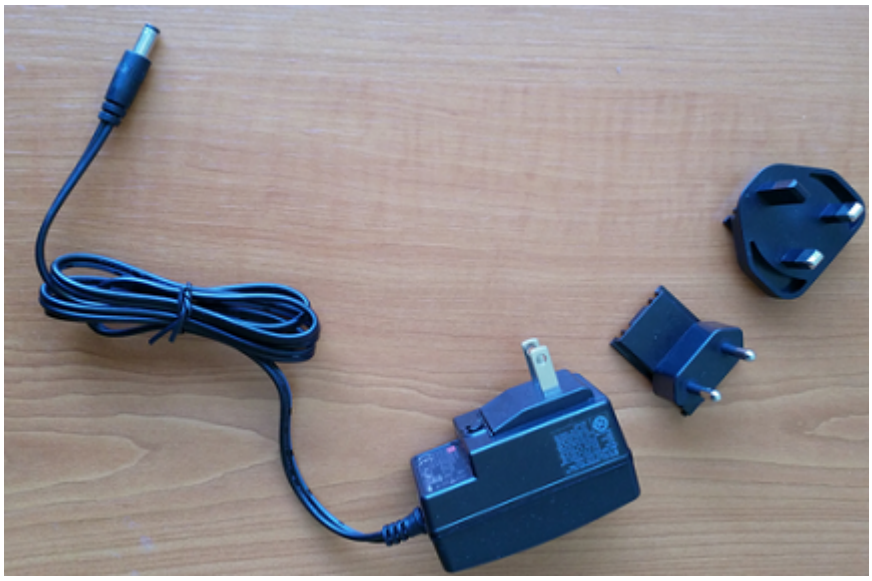
以下の手順では、ゲートウェイとブラケットの「上」と「下」について説明します。以下の 2 つの画像は、ゲートウェイの標準的な向きを示しています。デバイスは、以下に示すように直立していなくても機能します。この説明は、取り付け手順を理解するためのものです。

ゲートウェイが直立しているときは、デバイス正面の Amazon ロゴが正しい向きになります。LED が表示される 2 つの穴は、ロゴのすぐ上の右側にあります。ブラケットをゲートウェイに取り付ける小さなネジ用の穴は、上部の中央にあります。

デバイスの背面には、2 組のオレンジ色のプラスチックフックがあります。デバイスの下部にある大きなフックは下を向いています。デバイスの上部にある小さなフックは上を向いています。

1. 壁面取り付け用ブラケットを取り付けた状態で、ゲートウェイをブラケットに配置します。ゲートウェイの背面にある 2 つの大きなプラスチックフックは、ブラケット下部のスロットに差し込まれます。
2. ゲートウェイの上部をブラケットに押し付けて、ゲートウェイの背面にある 2 つの小さなプラスチックフックがブラケットの上部に引っかかるようにします。
3. ゲートウェイに付属している小さなネジを使用して、ゲートウェイ上部の穴からゲートウェイをブラケットに固定します。

4. 適切な AC プラグを AC アダプターに差し込みます。以下の画像は、アダプターに接続されている米国用プラグです。



5. AC アダプターをゲートウェイの下部と電源コンセントに差し込みます。

   ゲートウェイの LED ライトがオレンジ色と青色に交互にゆっくり点滅したら、ゲートウェイはオンになり、コミッショニングの準備が整います。

> **Note**
>
> ゲートウェイは、上部を小さなネジで固定して取り付けるように設計されています。ただし、逆さまに設置しても性能には影響しません。

ゲートウェイへの接続に問題がある場合は、「Wi-Fi ゲートウェイ検出のトラブルシューティング」を参照してください。

Wi-Fi ゲートウェイのコミッショニング

ゲートウェイをファクトリにマウントする場合、モバイルアプリにアクセスしてコ Amazon Monitron ミッショニングする必要があります。 は、近距離無線通信 (NFC) と Bluetooth を備えた Android 8.0 以降または iOS 14 以降を使用するスマートフォンのみ Amazon Monitron をサポートします。

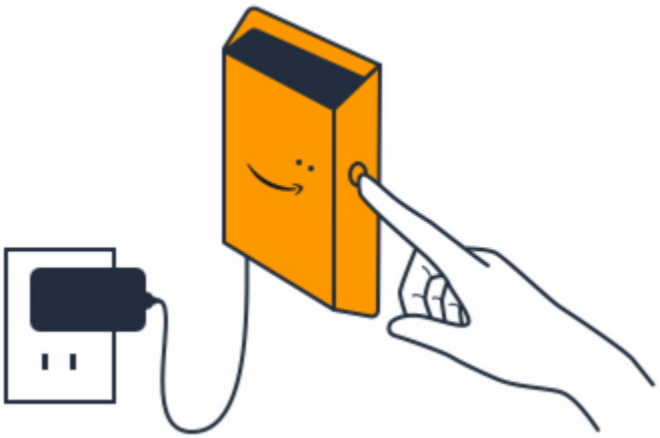
トピック

- ゲートウェイをコミッショニングするには

ゲートウェイをコミッショニングするには

1. スマートフォンの Bluetooth がまだオンになっていない場合は、オンにしてください。
2. ゲートウェイは、センサーとの通信に最適な場所に配置してください。

   ゲートウェイを取り付ける最適な場所は、センサーよりも高く、20～30 メートル以内の距離です。ゲートウェイの位置決めの詳細については、「Wi-Fi ゲートウェイの取り付けと設置」を参照してください。
3. ゲートウェイを接続し、上部の LED ライトが黄色と青色の交互に点滅していることを確認します。
4. ゲートウェイの側面にあるボタンを押して、コミッショニングモードにします。ライトがすばやく点滅し始めます。

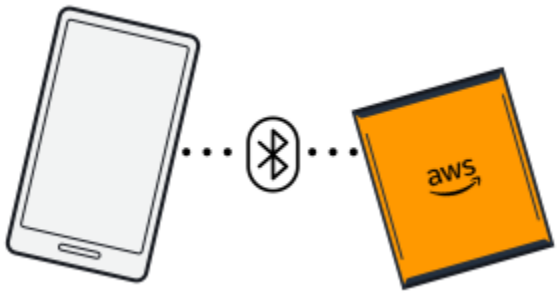


5. スマートフォンでモバイルアプリを開きます。
6. [開始方法] ページまたは [ゲートウェイ] ページで、[ゲートウェイを追加] を選択します。

   Amazon Monitron はゲートウェイをスキャンします。これには少し時間がかかることがあります。がゲートウェイ Amazon Monitron を検出すると、ゲートウェイリストに表示されます。
7. 表示されたゲートウェイを選択します。

> **Note**
>
> iOS モバイルデバイスを使用していて、以前にこの特定のゲートウェイとペアリングしたことがある場合は、再度ペアリングする前にデバイスにゲートウェイを「削除」させることが必要になる場合があります。詳細については、「Bluetooth ペアリングのトラブルシューティング」を参照してください。

が新しいゲートウェイに接続する Amazon Monitron までに少し時間がかかる場合があります。



モバイルアプリケーションがゲートウェイへの接続を引き続き試みても成功しない場合は、「Wi-Fi ゲートウェイ検出のトラブルシューティング」を参照してください。

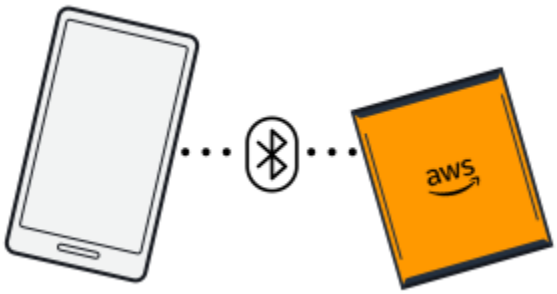
8. ゲートウェイに接続すると、 Amazon Monitron は Wi-Fi ネットワークをスキャンします。使用する Wi-Fi ネットワークを選択します。
9. Wi-Fi パスワードを入力して [接続] をクリックします。

   ゲートウェイのコミッショニングが行われ、Wi-Fi ネットワークに接続されるまでには、数分かかる場合があります。

   その他の問題がある場合は、「Wi-Fi ゲートウェイの工場出荷時設定へのリセット」を参照してください。

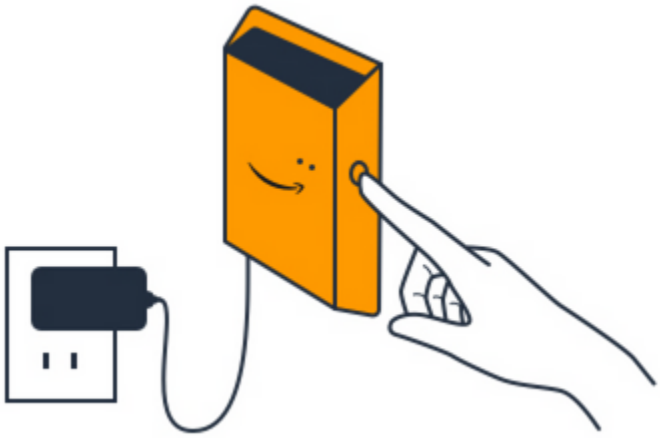
Wi-Fi ゲートウェイ検出のトラブルシューティング

プロジェクトまたはサイトにゲートウェイを追加するとき、[ゲートウェイを追加] を選択するとすぐに、Amazon Monitron モバイルアプリはゲートウェイを検索するためのスキャンを開始します。モバイルアプリでゲートウェイが検出されない場合は、以下のトラブルシューティングのヒントを試してください。



- ゲートウェイの電源がオンになっていることを確認します。LED ライト (ゲートウェイ上部の Amazon シンボルの横にある 2 つの小さなオレンジ色と青色のライト) を確認します。ライトが点灯している場合、ゲートウェイに電力が供給されています。ゲートウェイに電力が供給されていない場合は、以下の点を確認してください。
  - 電源コードはゲートウェイの背面と電源コンセントの両方にしっかりと接続されていますか。
  - 電源コンセントは正しく機能していますか。
  - ゲートウェイの電源ケーブルは機能していますか。ケーブルを別のゲートウェイに接続すると、機能しているかどうかをテストできます。
  - ケーブルをゲートウェイに差し込むコンセントは清潔で、内部にゴミが詰まっていませんか。ゲートウェイのコンセントとケーブルの接続端の両方を必ず確認してください。

- ゲートウェイがコミッショニングモードになっていることを確認してください。Amazon Monitron モバイルアプリは、コミッショニングモードの場合にのみ新しいゲートウェイを検出します。ゲートウェイをオンにすると、LED ライトがオレンジ色と青色に交互にゆっくり点滅します。ゲートウェイの側面にあるボタンを押してコミッショニングモードに移行すると、オレンジ色と青色が交互にすばやく点滅します。ボタンを押す前に LED がゆっくり点滅する以外のシーケンスを示している場合、ゲートウェイがコミッショニングモードに移行していない可能性があります。この場合は、電源をオフにしてから、[コミッショニング] ボタン (側面にある) を長押ししたままにして電源を再度オンにし、ゲートウェイを工場出荷時設定にリセットします。



- スマートフォンの Bluetooth が機能していることを確認します。ゲートウェイは Bluetooth を使用してスマートフォンに接続します。
  - スマートフォンの Bluetooth がオンになっていて、機能していますか。オフにしてからオンに切り替えてみてください。それでも解決しない場合は、スマートフォンを再起動してもう一度確認してください。
  - スマートフォンの Bluetooth 圏内にいますか。Bluetooth の通信範囲は比較的短く、通常は 10 メートル未満です。また、その信頼性は大きく異なる可能性があります。
  - Bluetooth 信号を電子的に妨害している可能性がある障害物はありますか。
- ゲートウェイがどのプロジェクトにもまだコミッショニングされていないことを確認します。デバイスは、コミッショニングを行う前にすべての既存プロジェクトから削除される必要があります。

これらのアクションを実行しても問題が解決しない場合は、以下の手順を実行します。

- ゲートウェイ MAC アドレスを表示およびコピーし、IT 管理者に連絡します。「MAC アドレスの詳細の取得」を参照してください。
- モバイルアプリからログアウトし、再起動します。

- ゲートウェイを工場出荷時設定にリセットするには、電源をオフにしてから、側面にある[コミッショニング] ボタンを長押ししたままにして電源を再度オンにします。

Bluetooth ペアリングのトラブルシューティング

iOS モバイルデバイスを、既にペアリングされているゲートウェイと再度ペアリングを試みる場合があります。これは、ゲートウェイの場所が変更されたか、Monitron サイトの一般設定が変更されたことが原因である可能性があります。

その場合は、iOS デバイスでゲートウェイとの Bluetooth 接続を「削除」します。

トピック

- ゲートウェイとデバイスのペアリングを解除するには

ゲートウェイとデバイスのペアリングを解除するには

1. iOS デバイスで、[設定] を選択します。
2. [設定] 画面で [Bluetooth] を選択します。
3. [Bluetooth] 画面で、Monitron ゲートウェイの名前の横にある情報アイコンをクリックします。
4. 次に表示される画面で、[このデバイスを削除] を選択します。

Wi-Fi ゲートウェイの工場出荷時設定へのリセット

削除されたゲートウェイを再利用する場合は Amazon Monitron、コミッショニングボタンを使用してゲートウェイを工場出荷時の設定にリセットします。これにより、ゲートウェイが再び使用される準備が整います Amazon Monitron。

現在オフラインになっているゲートウェイを削除する場合は、デバイスを工場出荷時設定にリセットしてから再度コミッショニングする必要があります。

トピック

- ゲートウェイを工場出荷時設定にリセットするには

ゲートウェイを工場出荷時設定にリセットするには

1. ゲートウェイのプラグを抜きます。

2. [コミッショニング] ボタンを長押しします。
3. ゲートウェイを再び接続します。
4. LED ライトがオレンジ色と青色に交互にゆっくり点滅し始めたら、[コミッショニング] ボタンを放します。
5. ゲートウェイのプラグを抜き、10 秒待ってからもう一度差し込みます。ゲートウェイがリセットされます。

ゲートウェイのリストの表示

このページでは、ゲートウェイをウェブアプリまたはモバイルアプリに表示する方法について説明します。

トピック

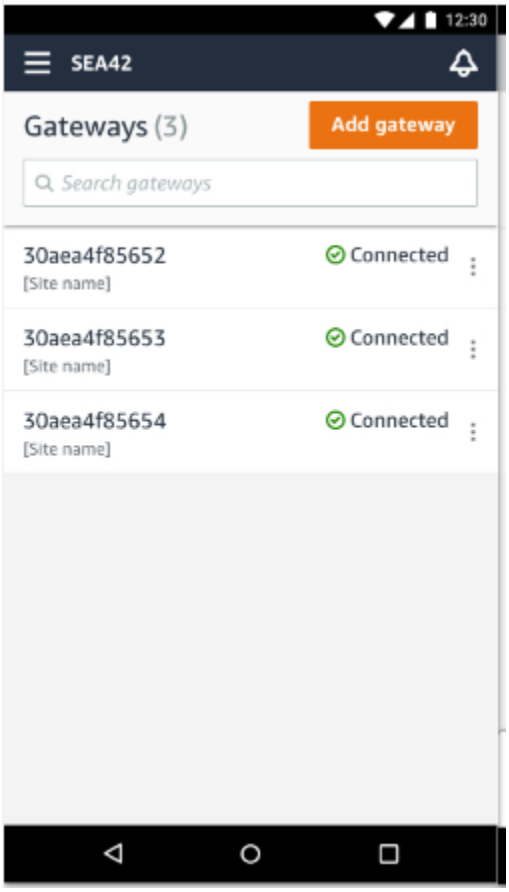
- モバイルアプリを使用してゲートウェイのリストを表示するには
- ウェブアプリを使用してゲートウェイのリストを表示するには

モバイルアプリを使用してゲートウェイのリストを表示するには

1. スマートフォンを使用して Amazon Monitron モバイルアプリにログインします。
2. 画面左上のメニューアイコンを選択します。

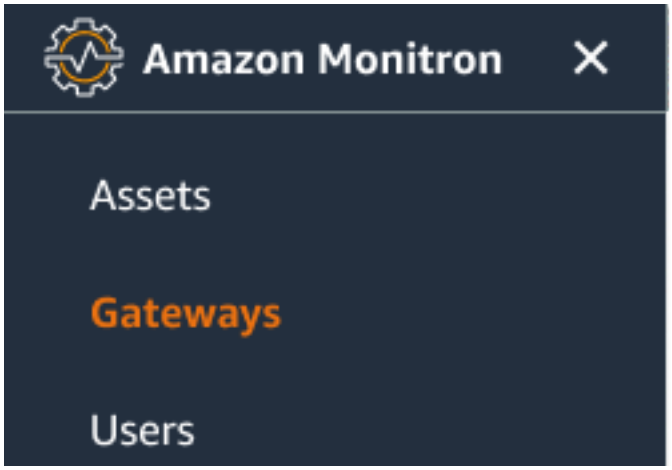
3. [ゲートウェイ] を選択します。

   プロジェクトに関連するすべてのゲートウェイのリストが表示されます。

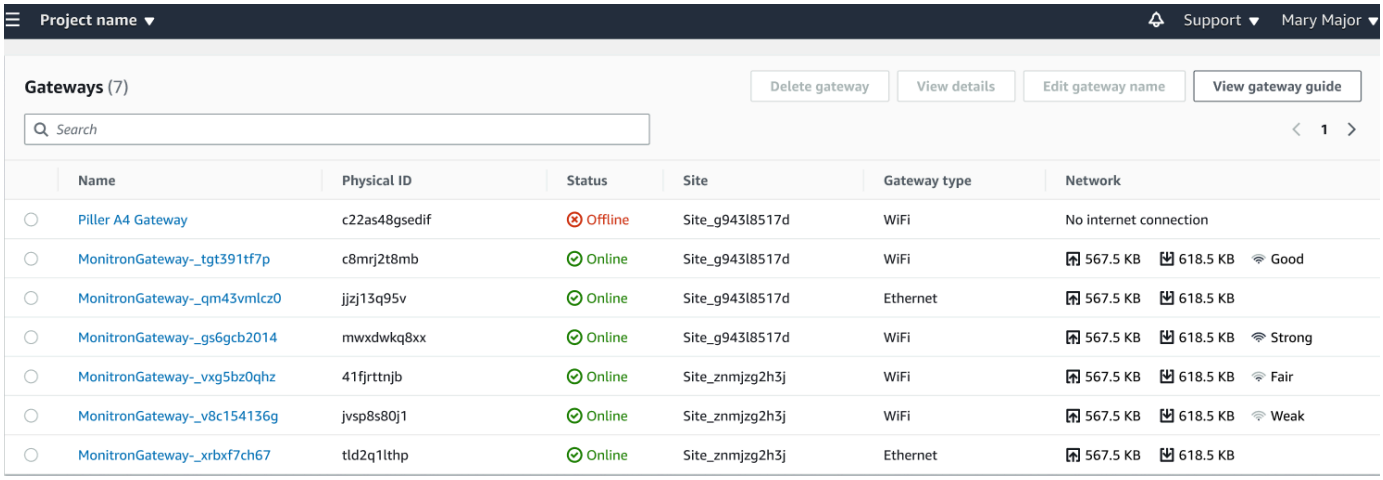


ウェブアプリを使用してゲートウェイのリストを表示するには

1. 左側のナビゲーションペインで [ゲートウェイ] をクリックします。



2. 右側のペインにゲートウェイのリストが表示されます。



Wi-Fi ゲートウェイの詳細の表示

モバイルまたはウェブアプリケーションでゲートウェイの詳細を表示できます。以下のゲートウェイの詳細を表示できます。

- IP アドレス
- ファームウェアバージョン
- 最後のコミッショニング

> **Note**
>
> ゲートウェイ MAC アドレスを表示およびコピーすることもできます。「MAC アドレスの詳細の取得」を参照してください。

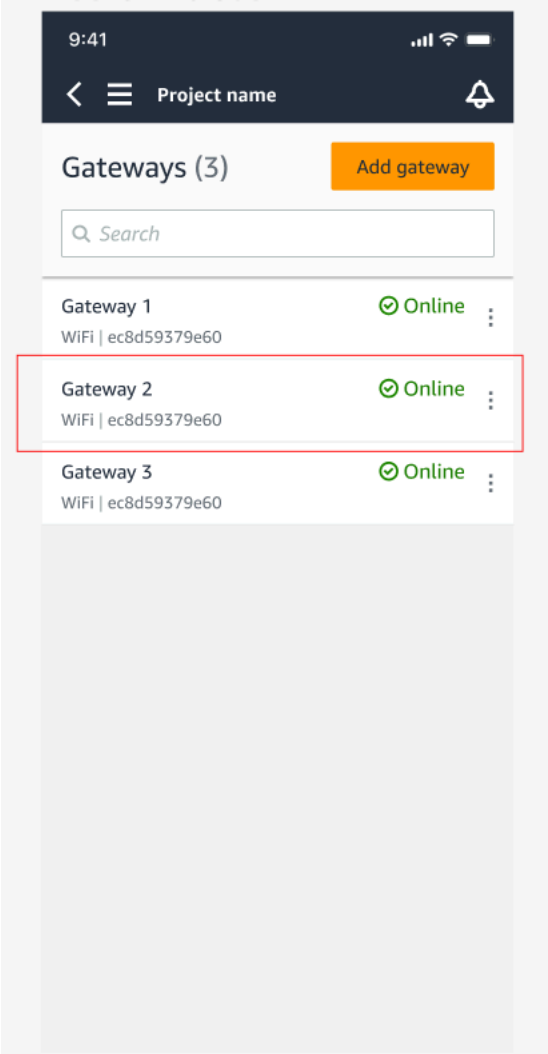
センサーの詳細は、モバイルアプリとウェブアプリの両方で確認できます。次のセクションでその確認方法について説明します。

トピック

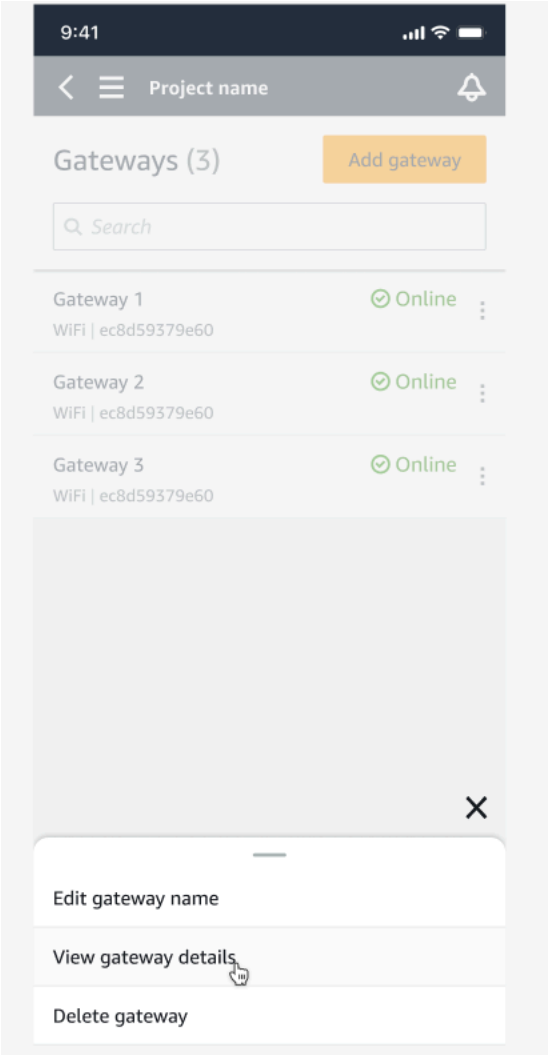
- モバイルアプリで Wi-Fi ゲートウェイの詳細を表示するには
- ウェブアプリで Wi-Fi ゲートウェイの詳細を表示するには

モバイルアプリで Wi-Fi ゲートウェイの詳細を表示するには

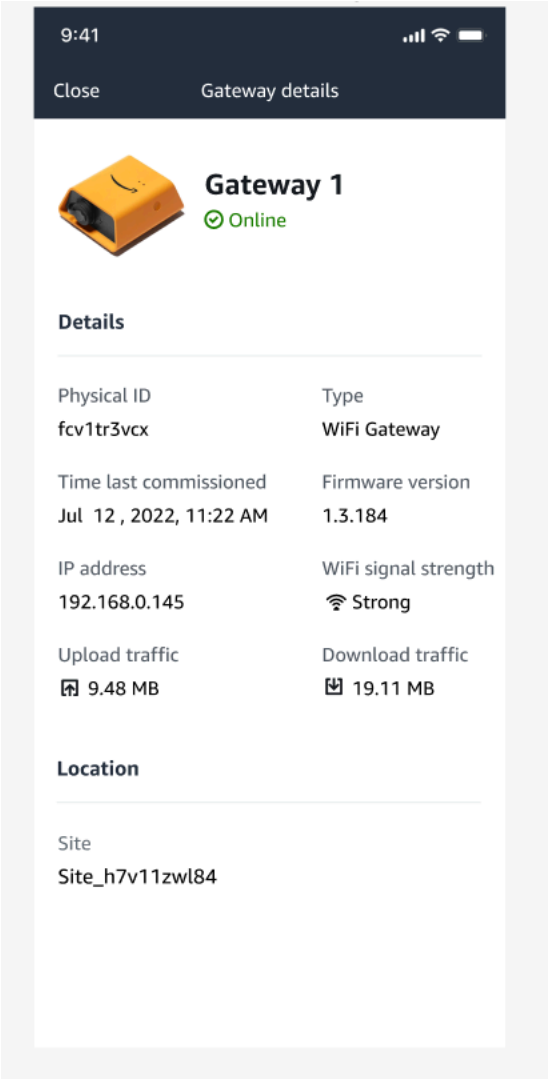
1. [ゲートウェイ] のリストから、詳細を表示するゲートウェイを選択します。



2. 表示されたオプションボックスから、[ゲートウェイの詳細を表示] を選択します。

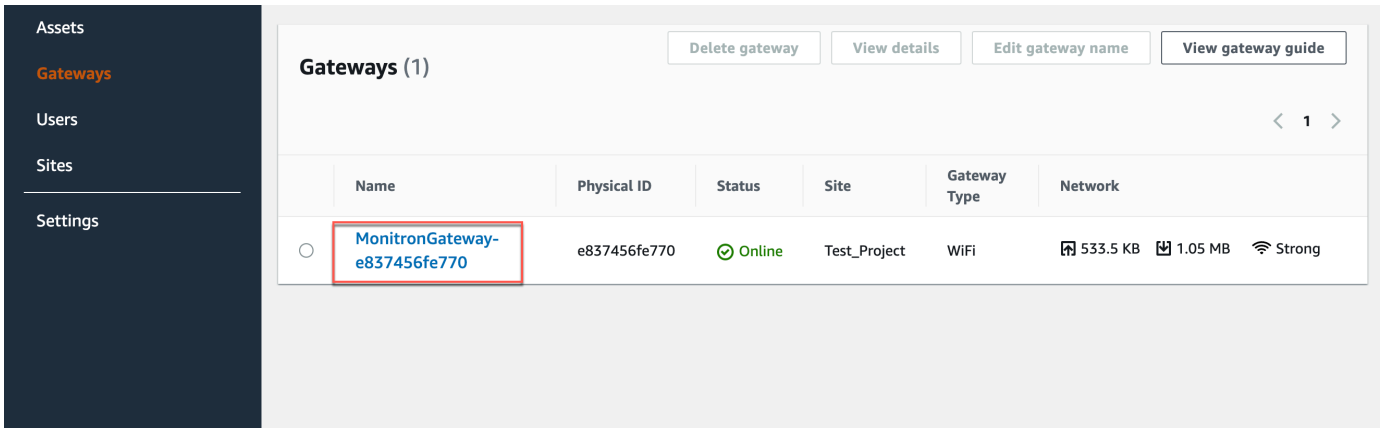


3. [ゲートウェイの詳細] ページが表示されます。

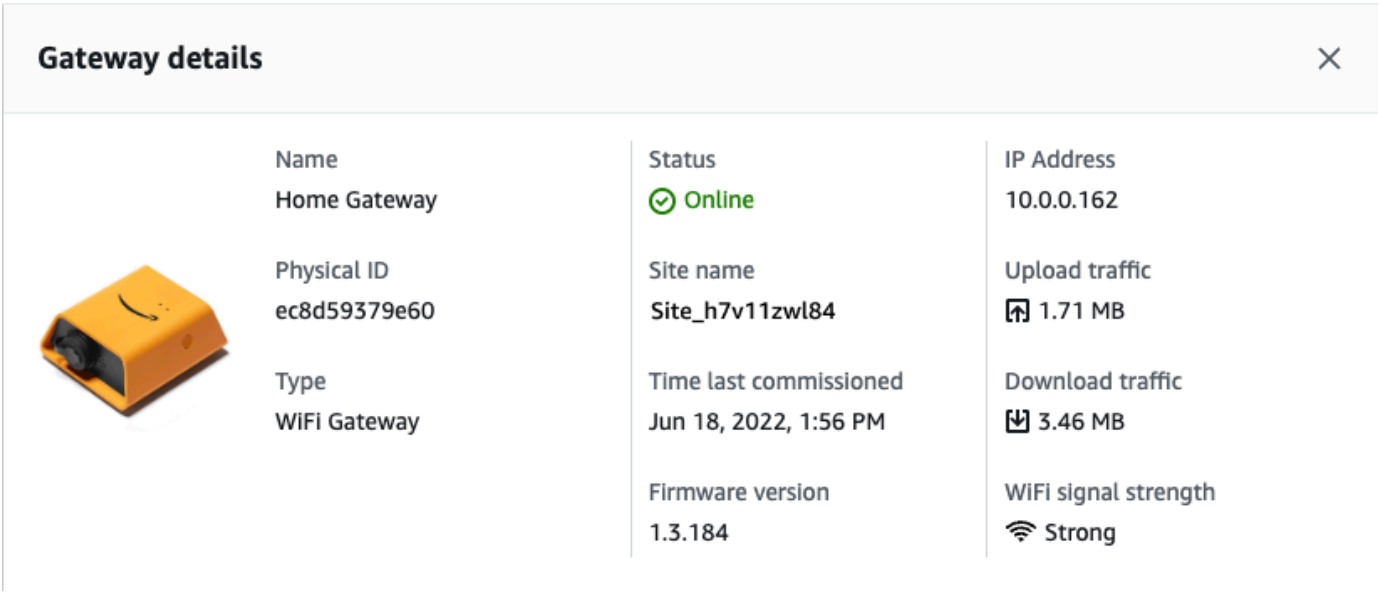


ウェブアプリで Wi-Fi ゲートウェイの詳細を表示するには

1. [ゲートウェイ] のリストから、詳細を表示するゲートウェイを選択します。



2. [ゲートウェイの詳細] ページが表示されます。



Wi-Fi ゲートウェイの名前の編集

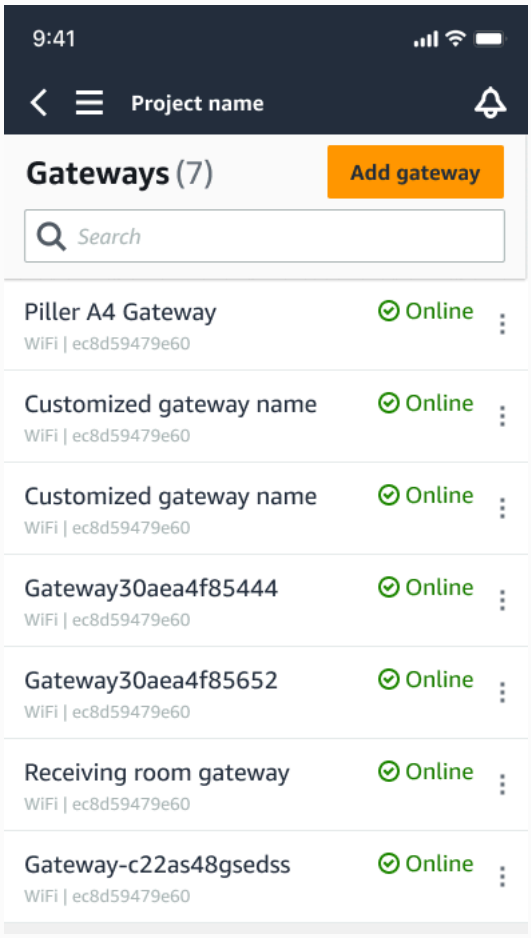
Wi-Fi ゲートウェイの表示名を変更すると、すばやく見つけることができます。ゲートウェイの名前を編集するには、ウェブアプリまたはモバイルアプリを開いて以下の操作を行います。

トピック

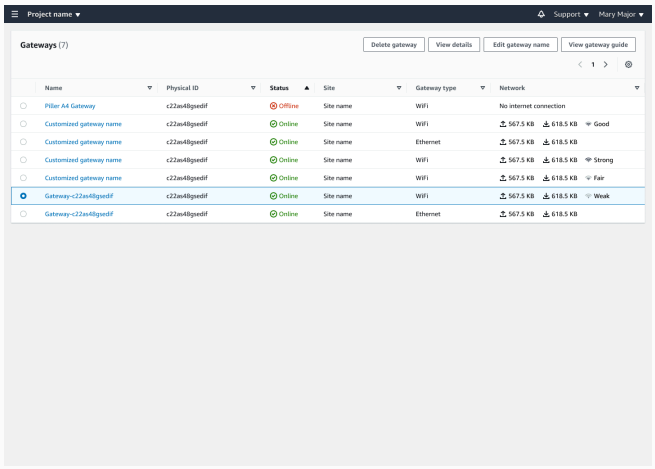
- Wi-Fi ゲートウェイの名前を編集するには

Wi-Fi ゲートウェイの名前を編集するには

1. [ゲートウェイ] ページから、編集するゲートウェイの名前を選択します。



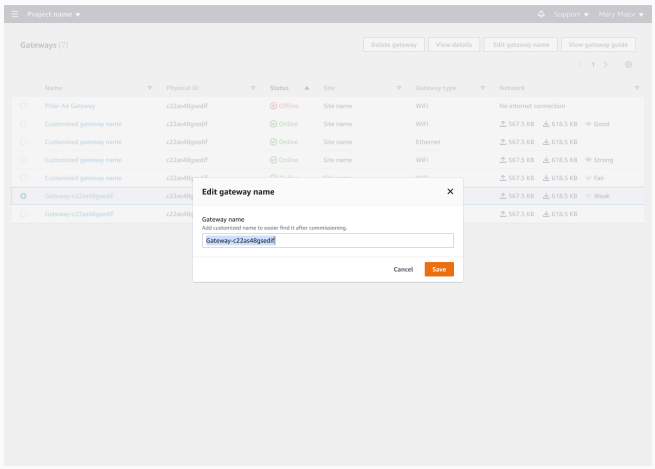
モバイルアプリの表示



ウェブアプリの表示

2. ゲートウェイにカスタマイズした名前を追加するように求めるポップアップが表示されます。

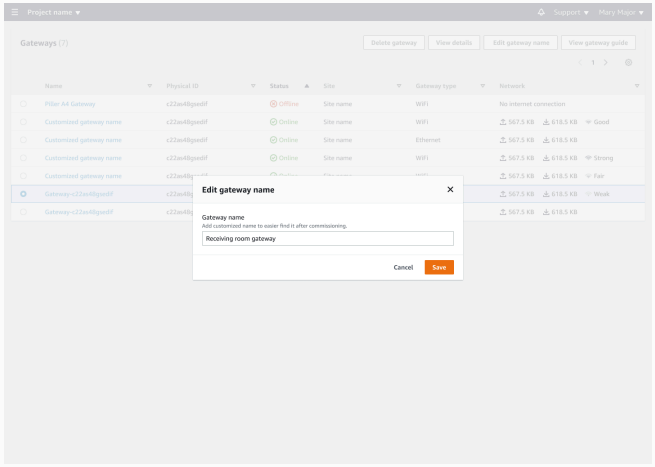
モバイルアプリの表示



ウェブアプリの表示

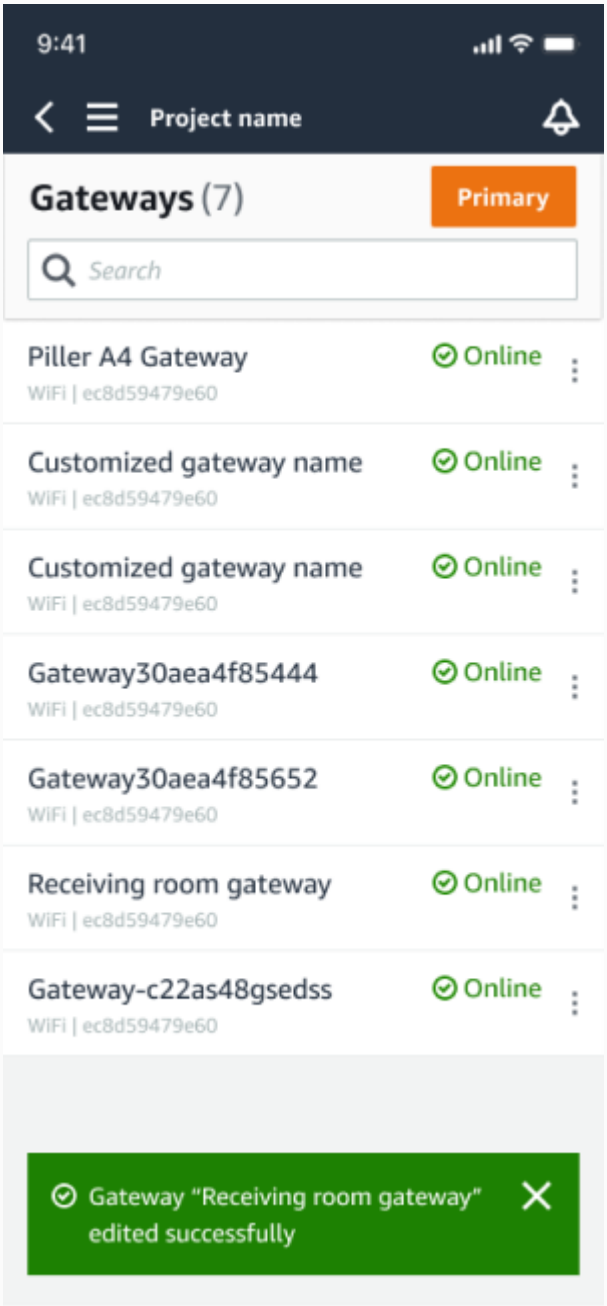
3. ゲートウェイの新しい名前を入力し、[保存] をクリックします。

モバイルアプリの表示

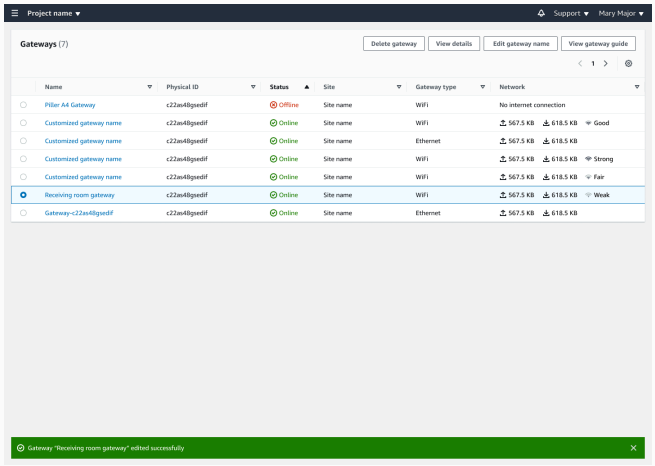


ウェブアプリの表示

4. ゲートウェイの新しい名前を確認する成功メッセージが表示されます。



モバイルアプリの表示



ウェブアプリの表示

Wi-Fi ゲートウェイの削除

センサーには、データを AWS クラウドに中継するためのゲートウェイが必要です。ゲートウェイを削除すると、一部のセンサーが接続を失う可能性があります。ゲートウェイを削除する前には注意が必要です。

ゲートウェイを削除すると、センサーは範囲内にある別のゲートウェイ (存在する場合) に接続を切り替えます。センサーからのデータ送信は中断されずに継続されます。範囲内にゲートウェイがない場合、データ送信は中断され、データが失われる可能性があります。

トピック

- モバイルアプリを使用してゲートウェイを削除するには
- ウェブアプリを使用してゲートウェイを削除するには

モバイルアプリを使用してゲートウェイを削除するには

1. [ゲートウェイ] ページに移動します。
2. 削除するゲートウェイの横にある縦 3 点アイコン

   ( )
   をクリックします。
3. [ゲートウェイを削除] を選択します。
4. [削除] をもう一度選択します。

ウェブアプリを使用してゲートウェイを削除するには

1. the section called “ゲートウェイのリストの表示” に移動します。
2. テーブルから削除するゲートウェイを選択します。
3. [ゲートウェイを削除] を選択します。

MAC アドレスの詳細の取得

Amazon Monitron ゲートウェイの Media Access Control (MAC) アドレスを取得するには、携帯電話を使用してゲートウェイデバイスの QR コードをスキャンできます。Amazon Monitron は、QR コードをスキャンするときに MAC アドレスとゲートウェイ ID の両方を返します。

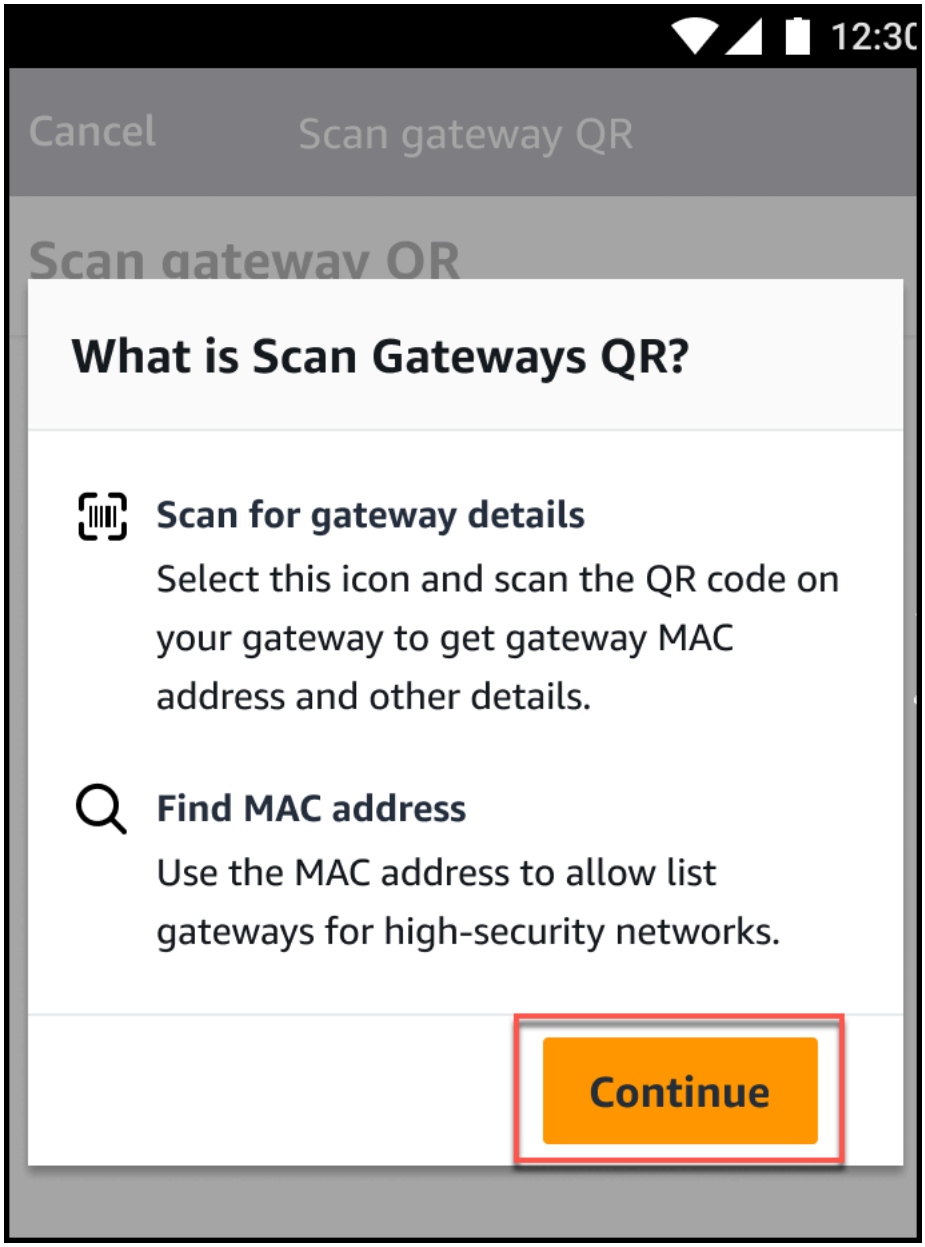
IT 管理者の場合は、スキャンされた MAC アドレスを使用して、ゲートウェイデバイスがコミッショニングされる前に正しいネットワーク設定で設定されていることを確認することができます。ゲートウェイをコミッショニングする技術者は、スキャンした MAC アドレスを使用して、IT 管理者のネットワーク問題のトラブルシューティングを行うことができます。

> **Note**
>
> QR コードをスキャンして MAC アドレスを取得することは、Amazon Monitron モバイルアプリでのみサポートされます。

次の手順では、ゲートウェイデバイスの MAC アドレスを取得する方法を示します。

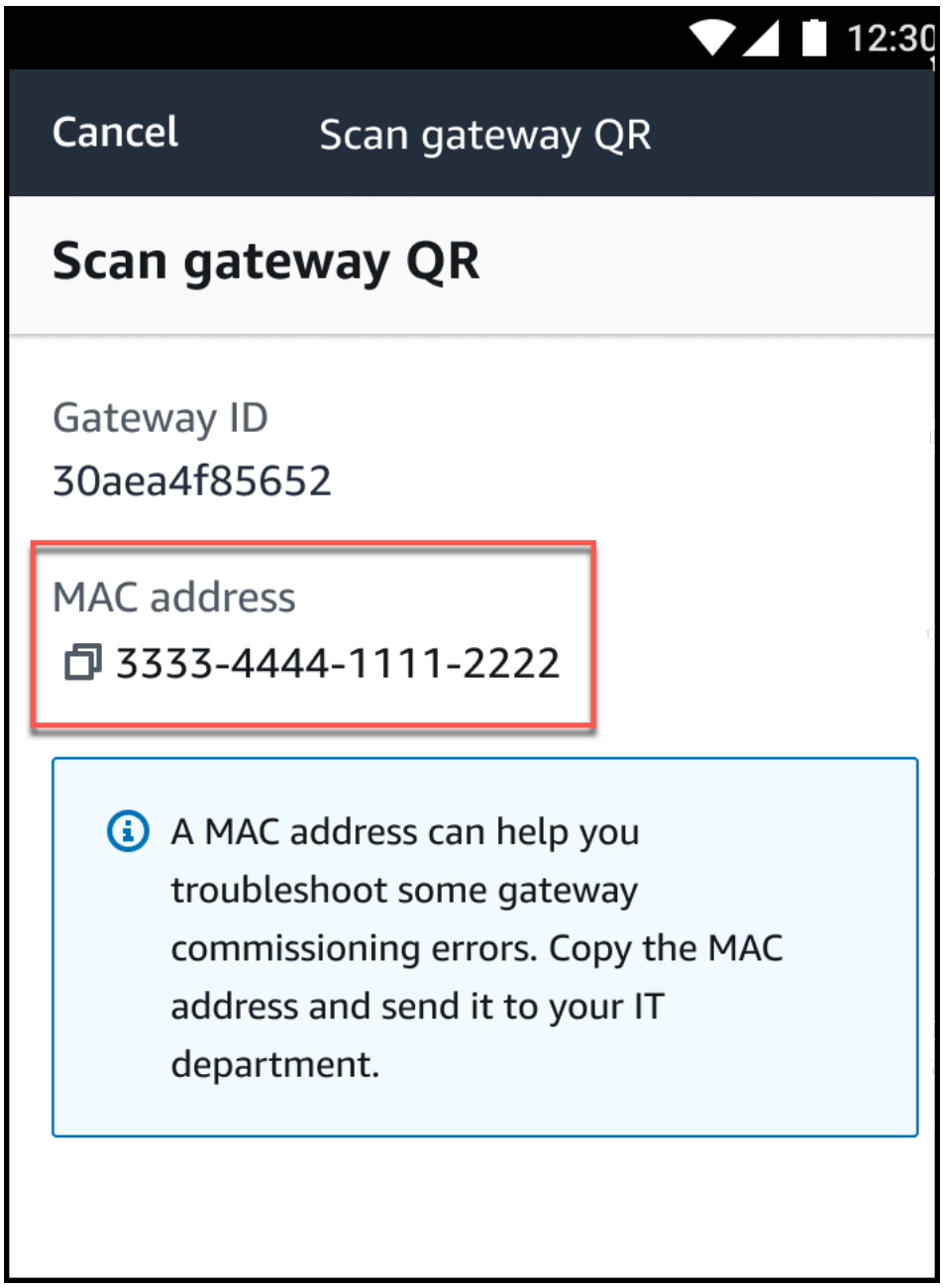
1. [ゲートウェイ] ページに移動します。
2. スキャンアイコンを選択します。

3. Amazon Monitron は、QR コードのスキャン内容を説明するメッセージを表示します。[Continue] (続行) をクリックします。



4. QR コードのスキャンページで、携帯電話のカメラを使用してゲートウェイの QR コードをスキャンします。

   スキャンが正常に完了すると、Amazon Monitron はモバイルアプリの QR コードのスキャンページにゲートウェイ ID と MAC アドレスを表示します。

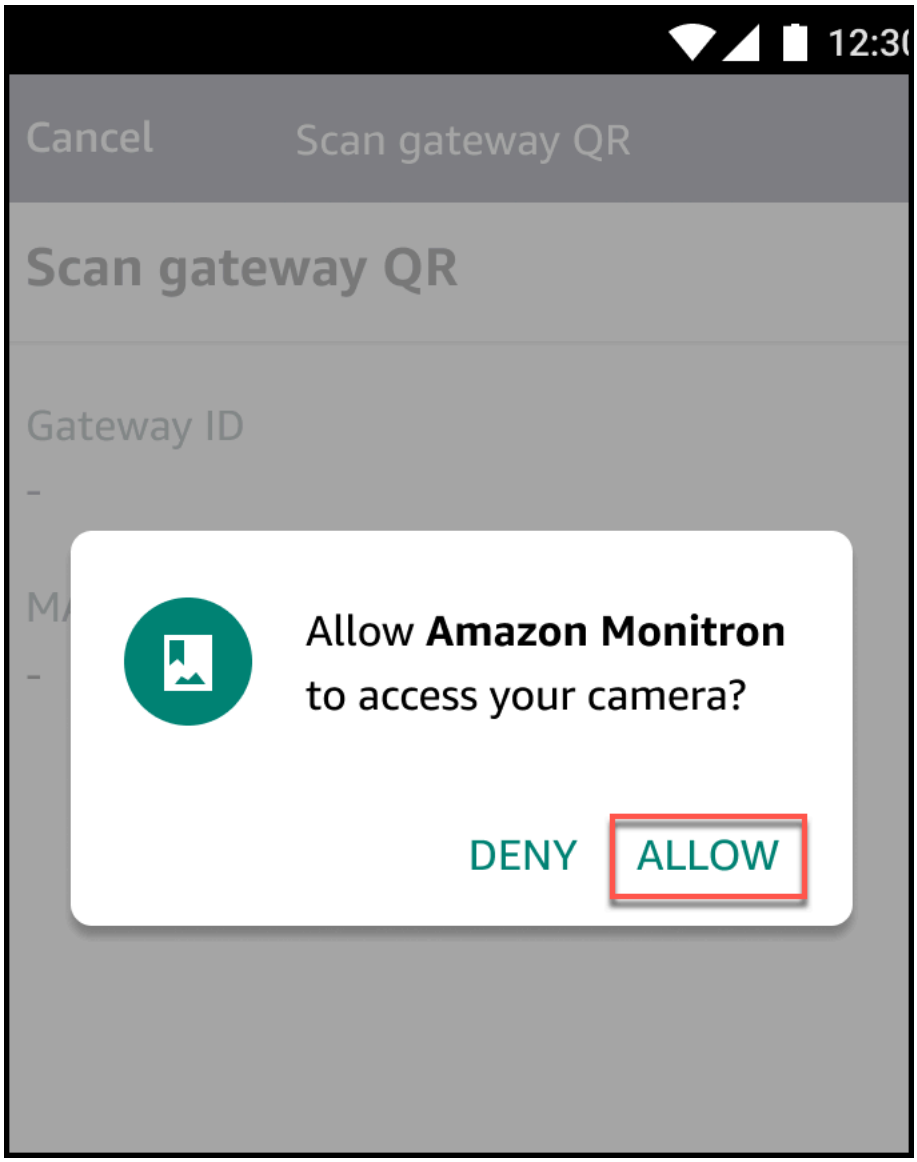


コピーアイコン
( )
を選択して MAC アドレスをコピーすることもできます。

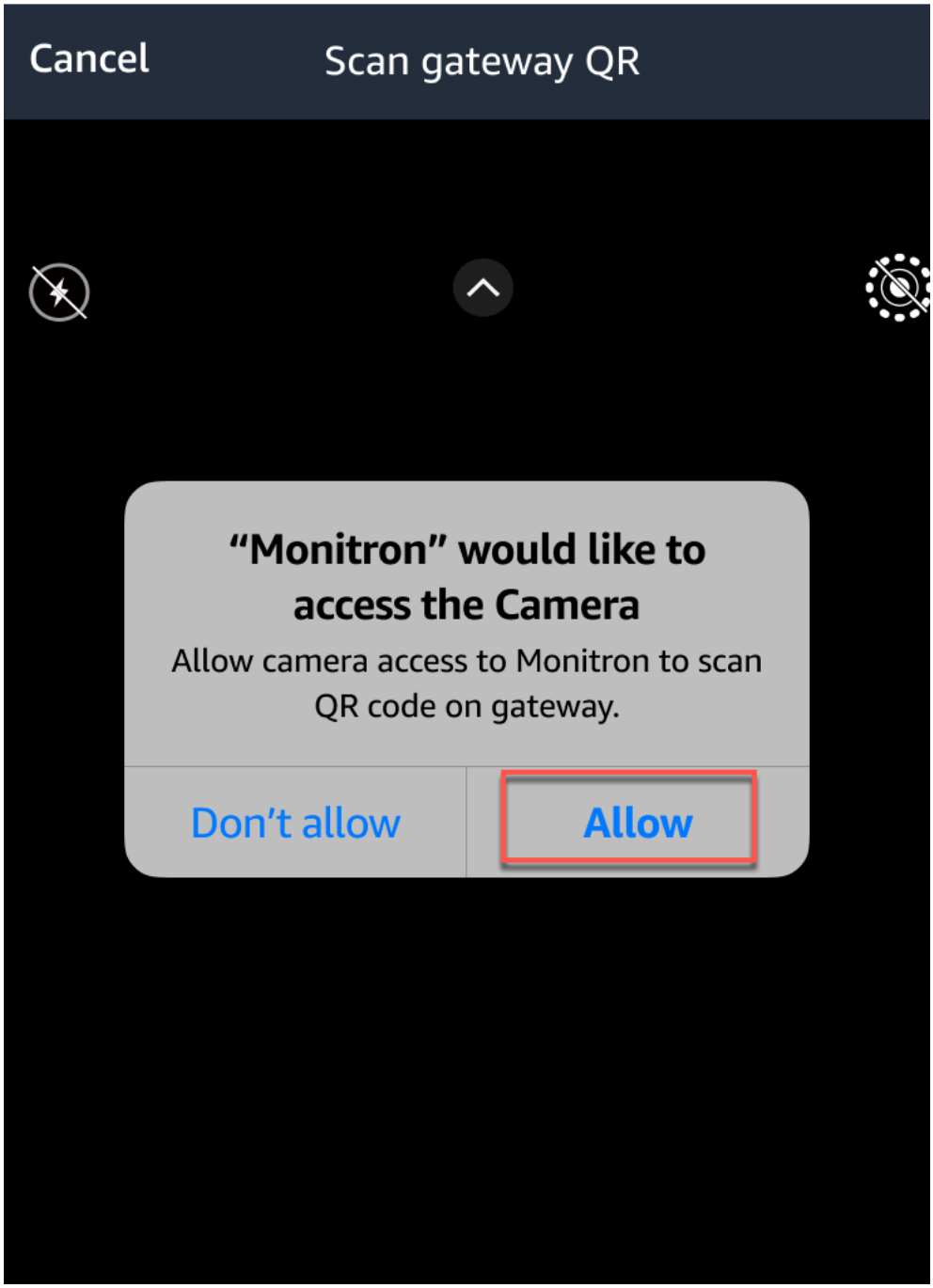
> **Note**
>
> まだ有効になっていない場合、Amazon Monitron はカメラにアクセスして QR コードをスキャンするためのアクセス許可が必要になる場合があります。これらのアクセス許可

は、デバイスの QR コードを正常にスキャンする前に、モバイルデバイスの設定ページから有効にする必要があります。アクセス許可がまだ付与されていない場合、Amazon Monitron はスキャンプロセス中にカメラアクセスを有効にするように求めます。

Android デバイスの場合



iOS デバイスの場合


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

アセット

のアセットは Amazon Monitron、工場のフロアにある機器です。通常、アセットは個別のマシンですが、大規模な機器の一部、工業プロセスの一部、または製造モデルの要素であってもかまいません。

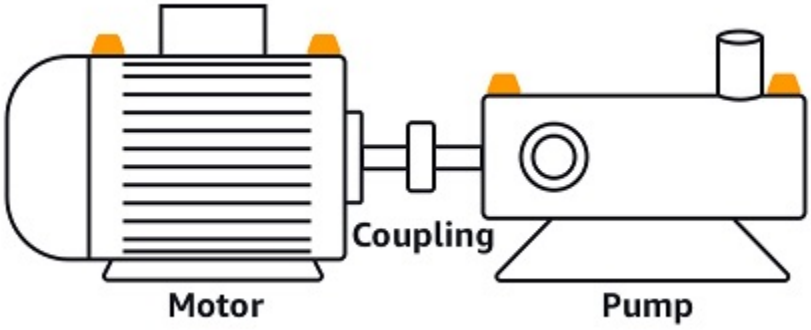
Amazon Monitron は現在、次のデフォルトの ISO 20186 標準ベースのマシンクラスをサポートしています。

- クラス I – エンジンとマシンの個々の部分。通常の動作状態でマシン全体と統合的に接続されます。例えば、最大 15 kW の本番稼働用電気モーターなどです。
- クラス II – 特別な基盤のない中型マシン (通常は 15 kW ~ 75 kW 出力の電気モーター) 、特別な基盤にエンジンまたはマシン (最大 300 kW) をリジッドにマウントします。
- クラス III – 振動方向に比較的硬い硬い基礎と重い基礎に回転する質量を持つ、大きなプライムムーバーやその他の大きな機械。
- クラス IV – 振動測定の方向に比較的ソフトである、剛性および重量の基盤に回転質量がマウントされた大規模なプライムムーバーやその他の大規模な機械。例えば、ターボジェネレーターセットや 10 MW を超える出力を持つガスタービンなどです。

ユースケースに合わせてアセットのカスタムクラスを作成することもできます。詳細については、「カスタムクラスの作成」を参照してください。

アセットはマシンの状態を確認するための基礎にもなります。マシンのアクティビティをモニタリングするには、モニタリング対象のアセットに 1 つ以上のセンサーをペアリングします。各センサーは、アセットのその部分がどのように機能しているかの情報を提供し、それらを組み合わせてアセット全体の概要を把握します。アセットに配置された各センサーには独自のマシンクラスを割り当てることができます。

以下の図では、1 つのアセットとして、電動モーターポンプセットを示しています。4 つのポジションがあり、それぞれにセンサーが 1 つずつ (モーターに 2 つ、ポンプに 2 つ) 付いています。各センサーは、ポンプの特定のポジションの温度と振動レベルのデータを収集します。 Amazon Monitron は次に、そのデータをそのポジションのベースラインとなる温度や振動レベルと比較して分析し、変化や異常がいつ発生したかを判断します。この場合、 Amazon Monitron アプリに通知が送信されます。



この章では、 でアセットを管理する方法と Amazon Monitron、それらのヘルスをモニタリングするセンサーとアセットをペアリングする方法について説明します。

トピック

- アセットクラスの作成
- アセットの管理
- アセットのリストの表示
- アセットの追加
- アセット名の変更
- アセットの移動
- アセットの削除

アセットクラスの作成

Amazon Monitron は、ISO 20816 標準に基づく 4 つのデフォルトのマシンクラスを提供しています。アセット位置を追加すると、これら 4 つのデフォルトクラスのいずれかを、アセットの異常を検出するために使用するマシンクラスとして選択できます。次に、Amazon Monitron は割り当てられたアセットクラスを使用して、アセット条件に関する警告とアラームを生成します。

アセットタイプが Amazon Monitron が提供するデフォルトのマシンクラスと一致しない場合は、アセットのカスタムマシンクラスを作成できます。作成後、これらのカスタムクラスをプロジェクト内のすべてのアセットポジションに割り当てることができます。

> **Important**
>
> カスタムクラスは、Amazon Monitron ウェブアプリを使用してのみ作成できます。Amazon Monitron プロジェクト管理者のみがカスタムアセットクラスを作成、更新、削除できます。

トピック

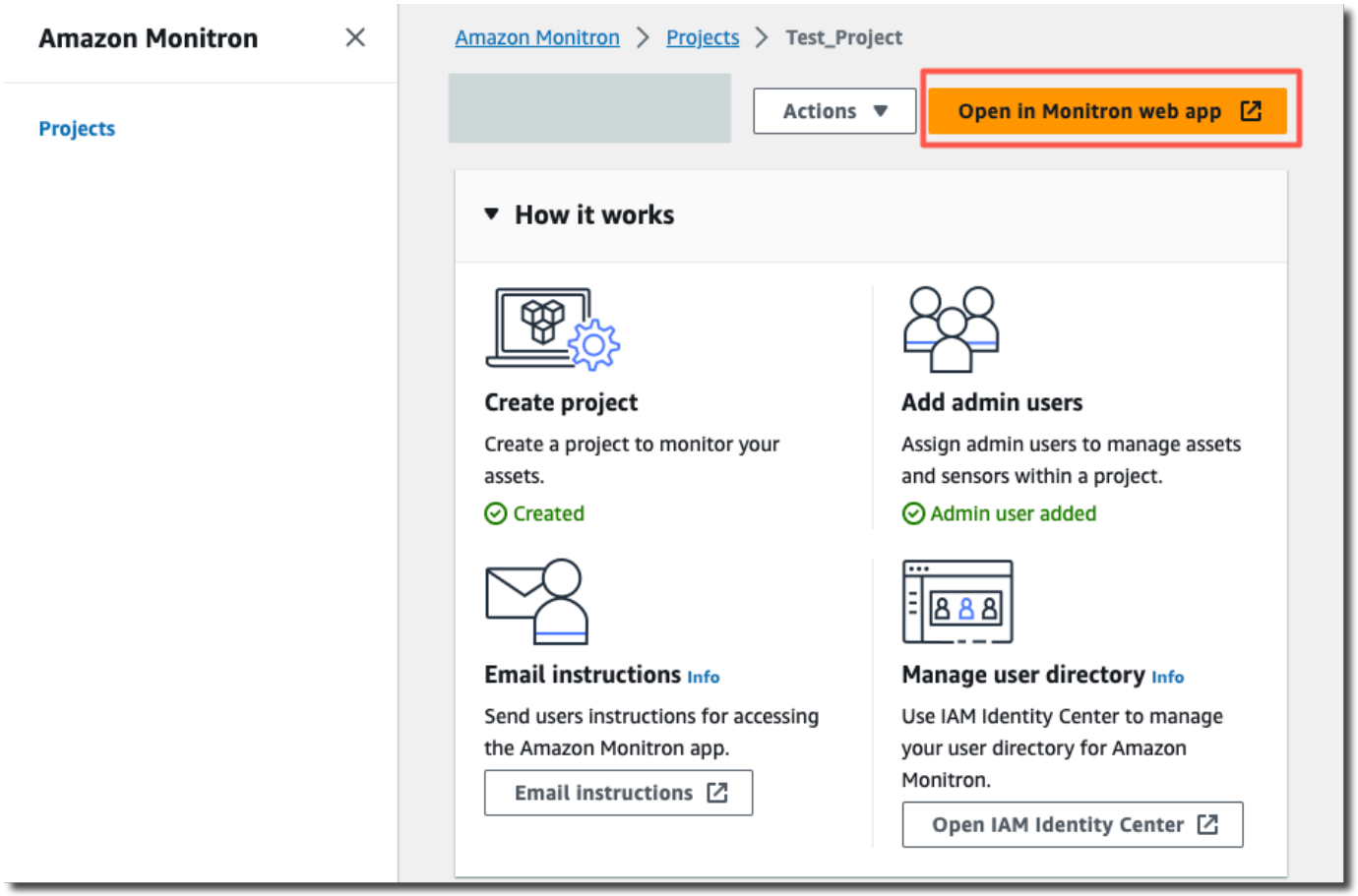
- カスタムクラスの作成
- カスタムクラスの更新
- カスタムクラスの削除

カスタムクラスの作成

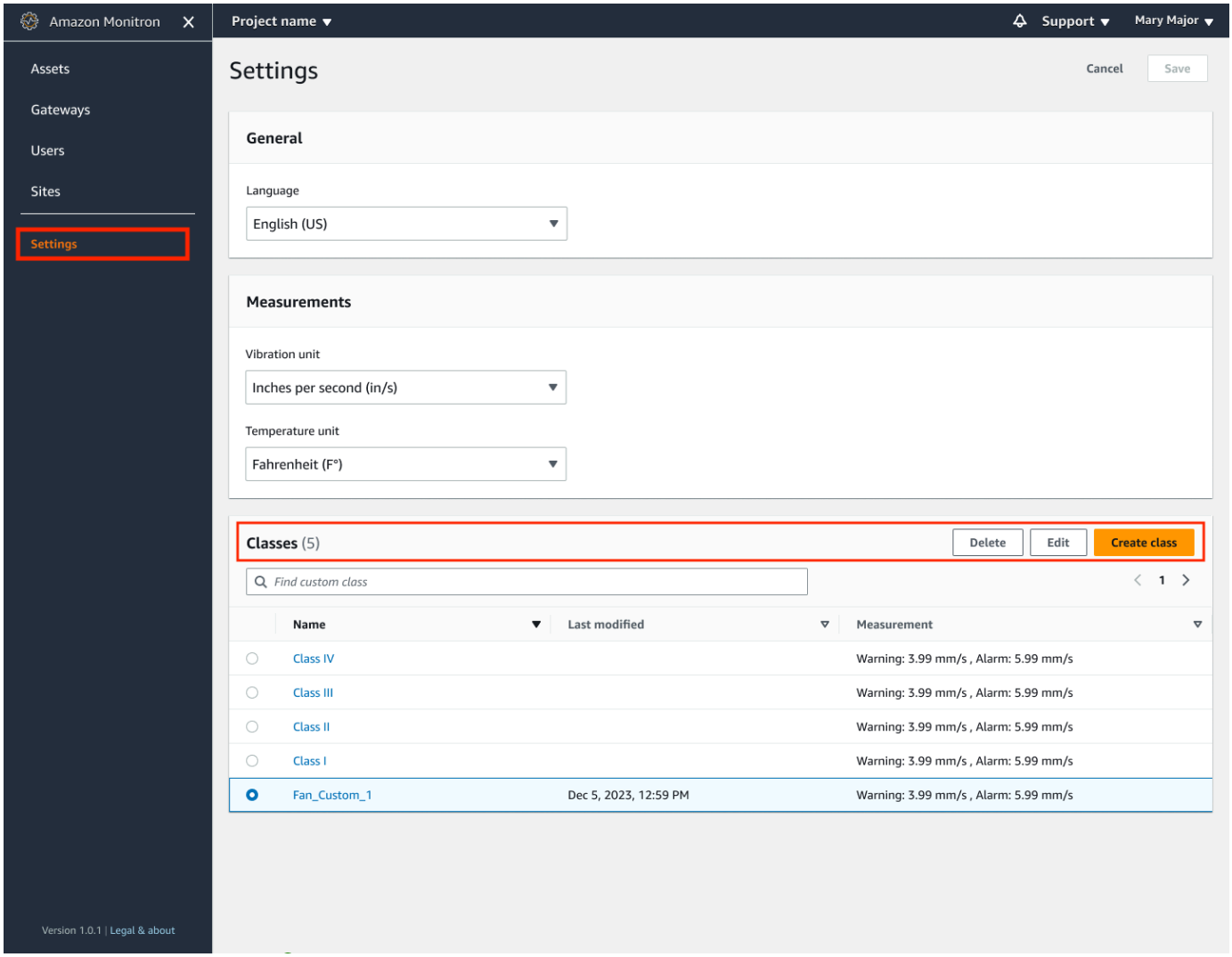
カスタムクラスを作成するには

1. Amazon Monitron コンソール (https://console.aws.amazon.com/monitron) を開きます。
2. [プロジェクトを作成] を選択します。
3. プロジェクトを初めて作成する場合は、「プロジェクトの作成」で説明されているステップに従います。

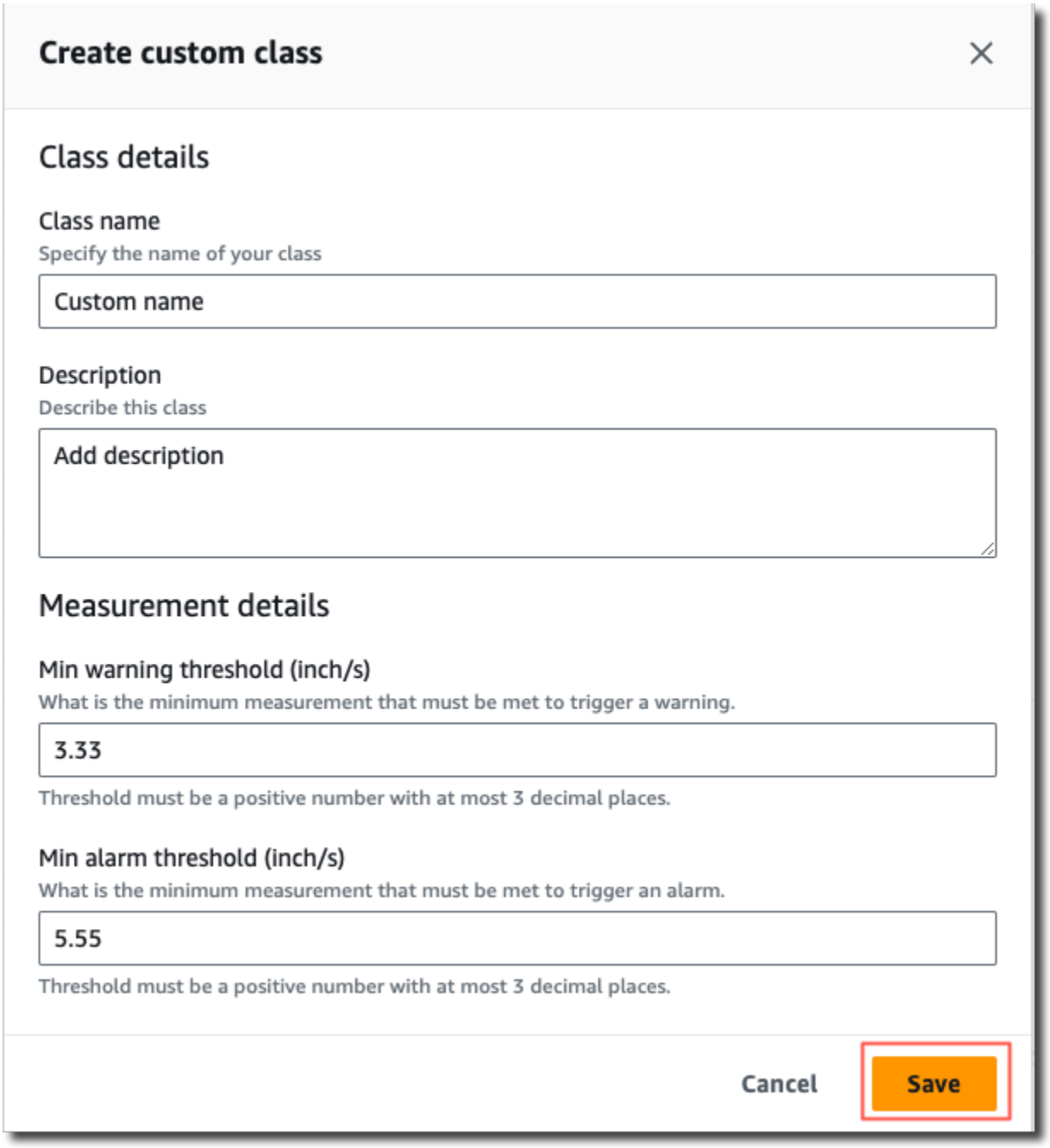
   既存のプロジェクトを選択する場合は、左側のナビゲーションメニューからプロジェクトを選択し、カスタムクラスを作成するプロジェクトを選択します。
4. プロジェクトの詳細ページから、Amazon Monitron ウェブアプリケーションで開くを選択します。



5. Amazon Monitron ウェブアプリページで、左側のナビゲーションペインから設定を選択します。



6. 次に、Classes から選択し、Create class を選択します。



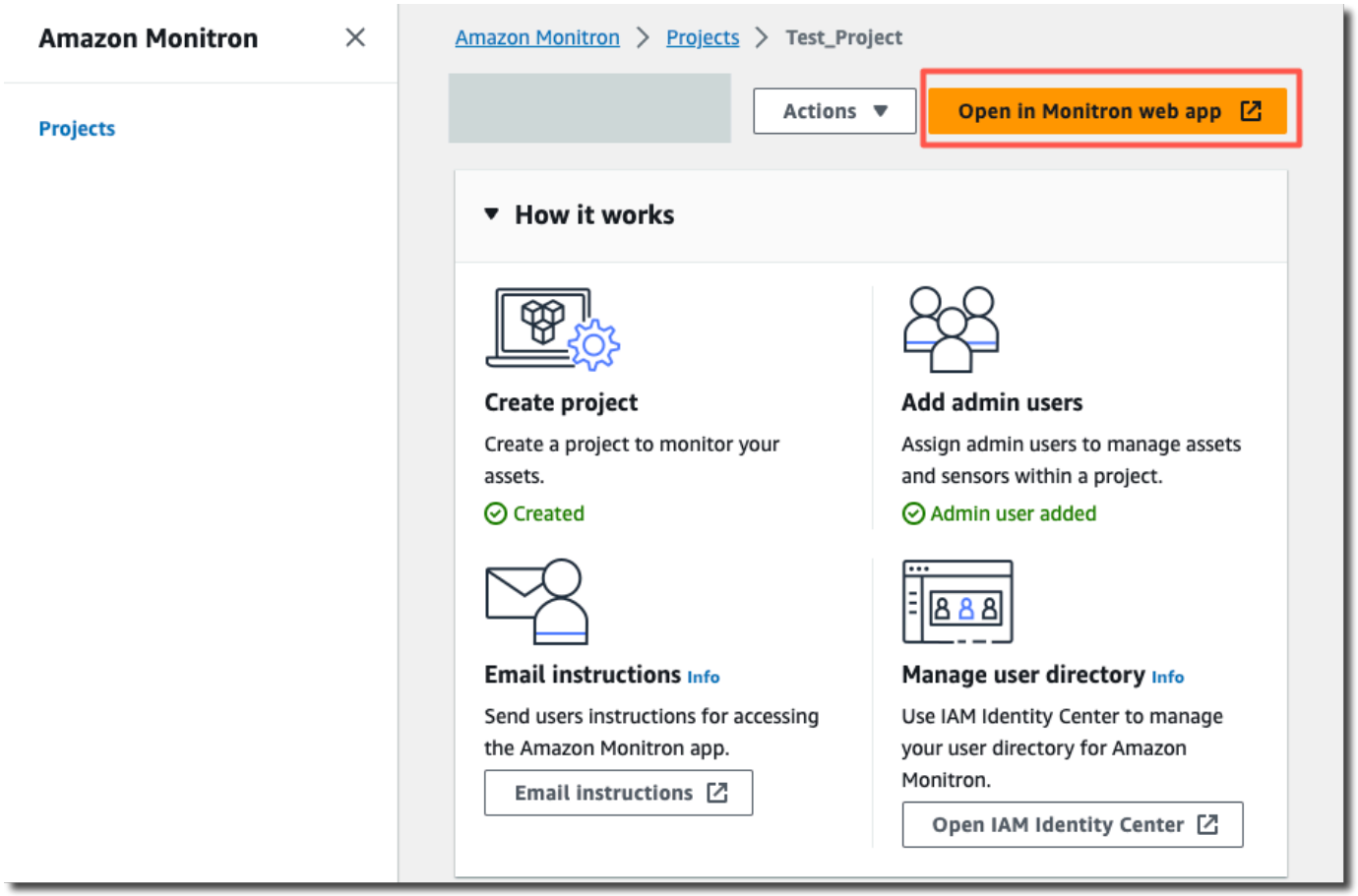
7. カスタムクラスの作成ページで、次の操作を行います。
   - クラスの詳細で、クラス名 - カスタムクラスの名前。
   - 説明 – カスタムマシンクラスの説明。
   - 測定の詳細の「測定しきい値」 – アセットのカスタム測定しきい値。
8. [Save] を選択します。

カスタムクラスの更新

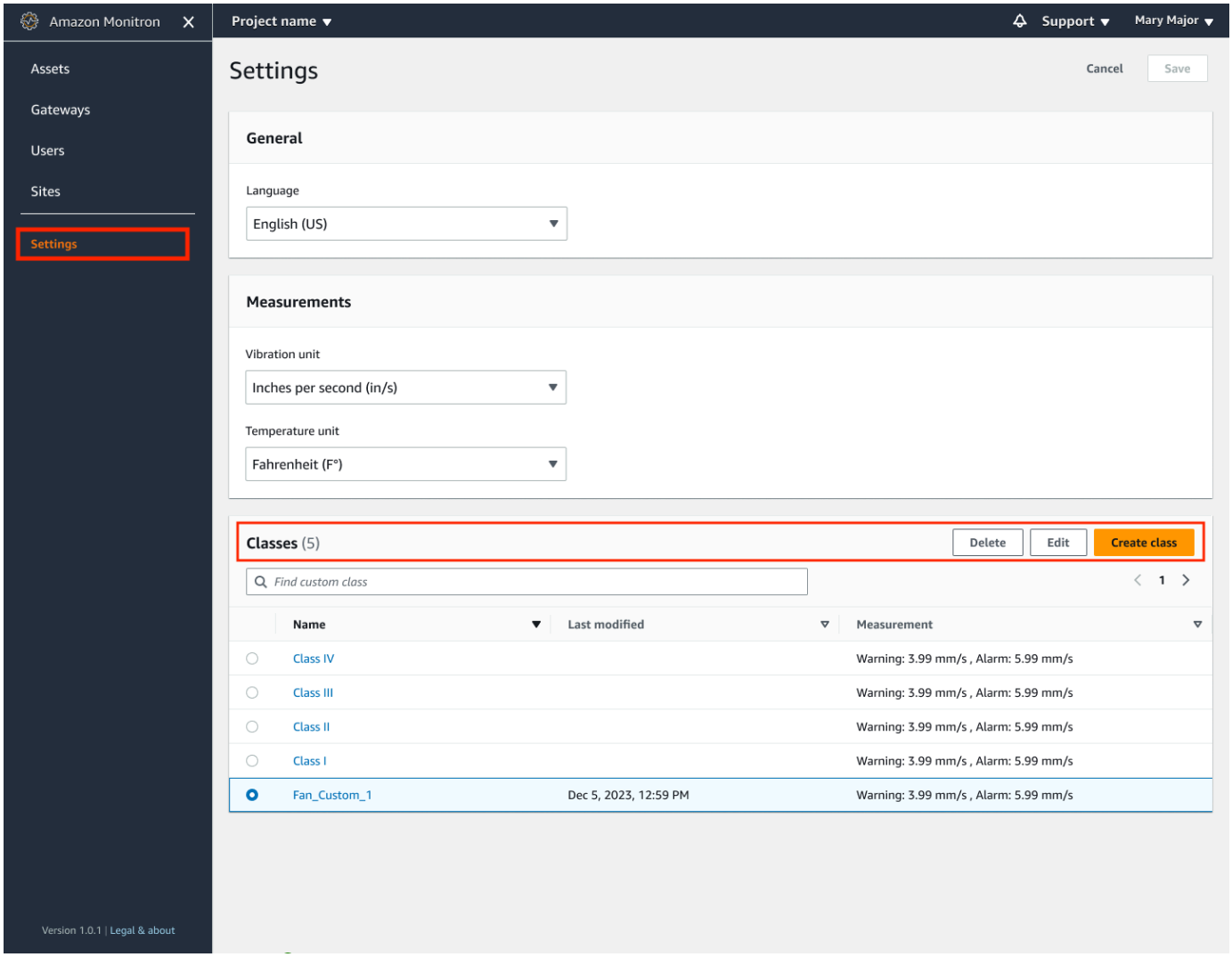
カスタムクラスを更新するには

1. Amazon Monitron コンソール (https://console.aws.amazon.com/monitron) を開きます。
2. [プロジェクトを作成] を選択します。
3. プロジェクトを初めて作成する場合は、「プロジェクトの作成」で説明されているステップに従います。

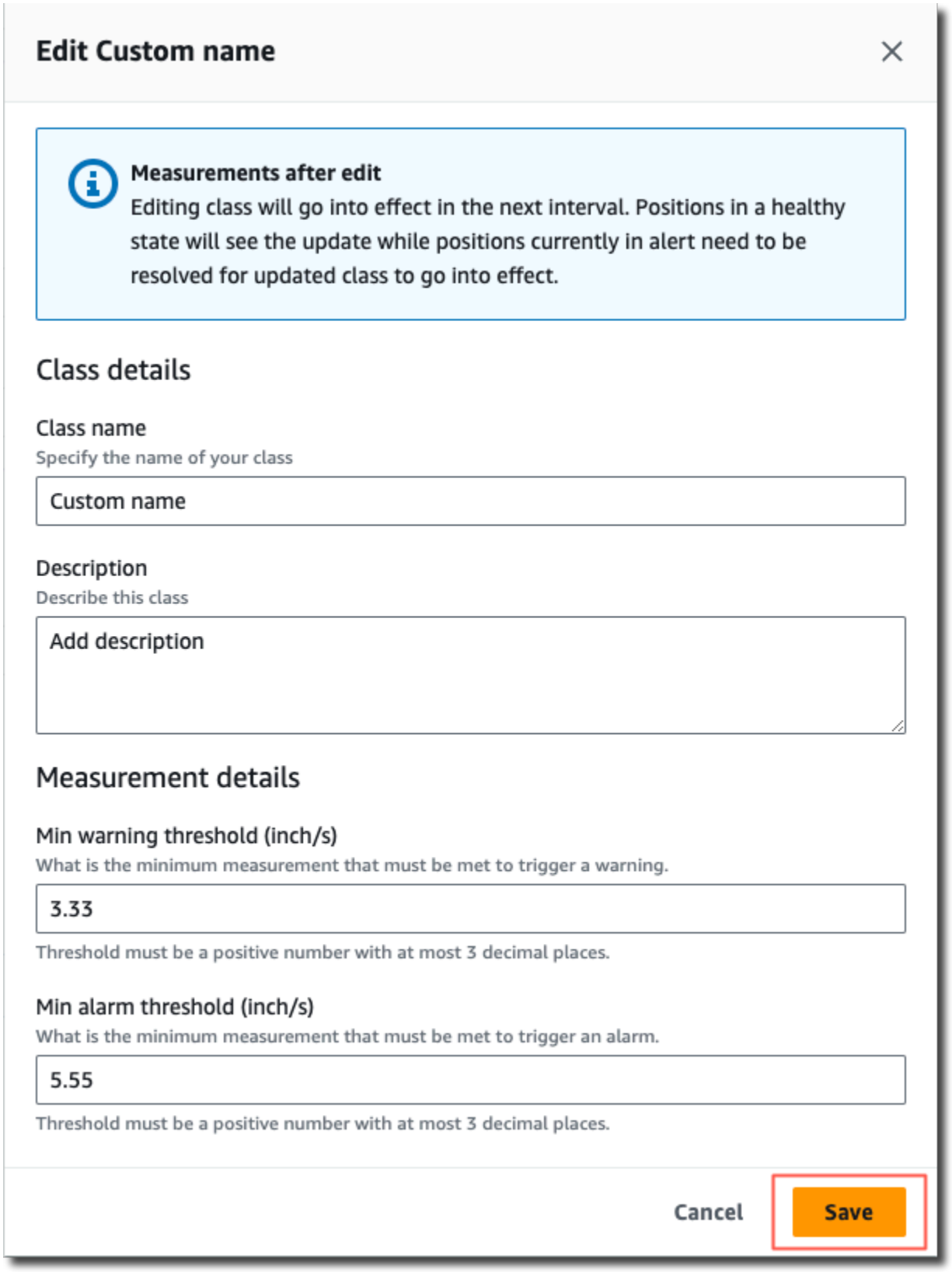
   既存のプロジェクトを選択する場合は、左側のナビゲーションメニューからプロジェクトを選択し、カスタムクラスを作成するプロジェクトを選択します。
4. プロジェクトの詳細ページから、Amazon Monitron ウェブアプリケーションで開くを選択します。



5. Amazon Monitron ウェブアプリページで、左側のナビゲーションペインから設定を選択します。



6. 次に、Classes から、更新するクラスを選択し、Edit を選択します。



7. クラスの編集ページで、次の操作を行います。

- クラスの詳細で、クラス名 - カスタムクラスの名前。
- 説明 – カスタムマシンクラスの説明。
- 測定の詳細の「測定しきい値」 – アセットのカスタム測定しきい値。

8. [Save] を選択します。

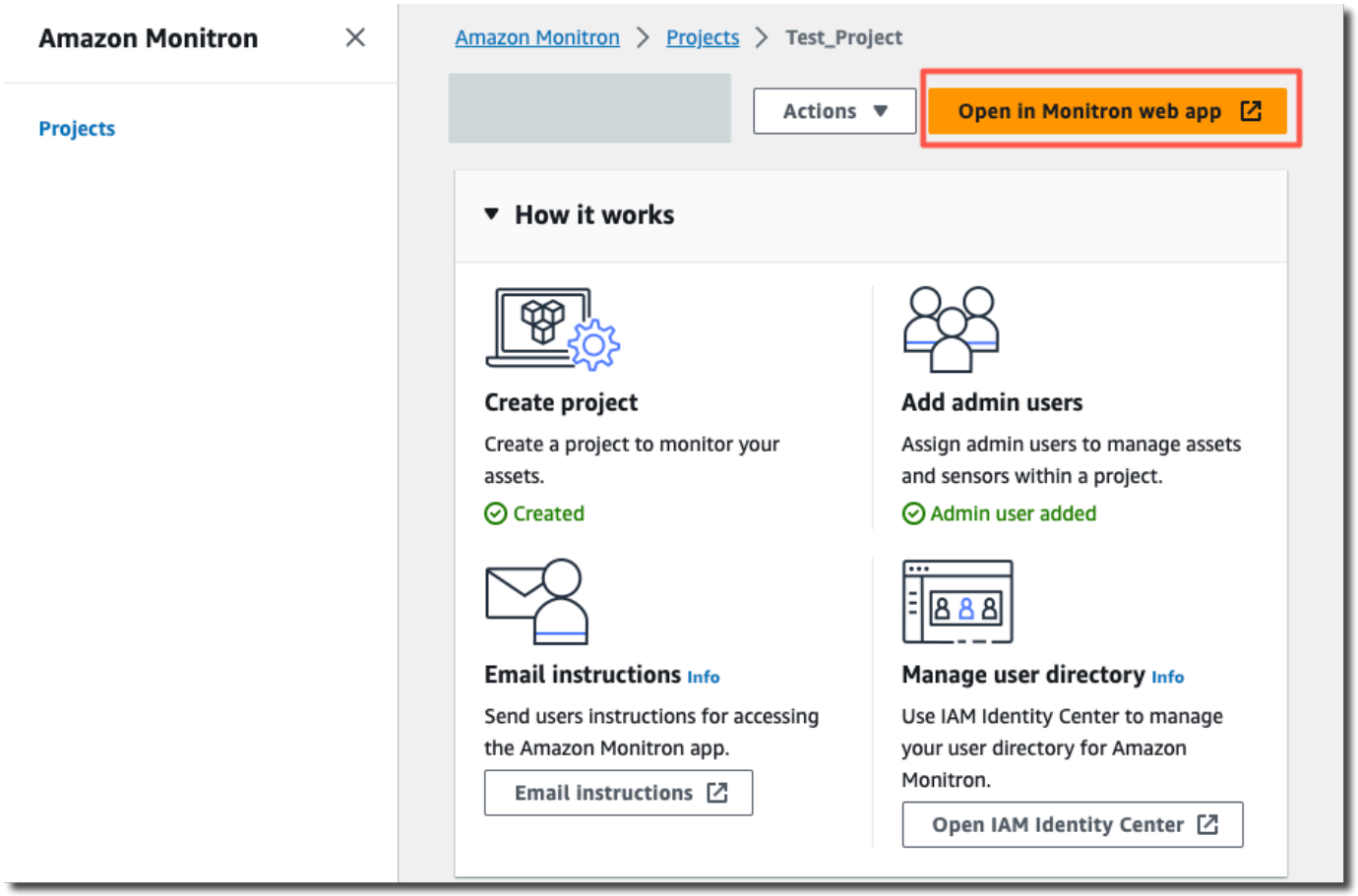
> **Note**
>
> 編集されたマシンクラスは、次の Amazon Monitron 測定間隔中に有効になります。

カスタムクラスの削除

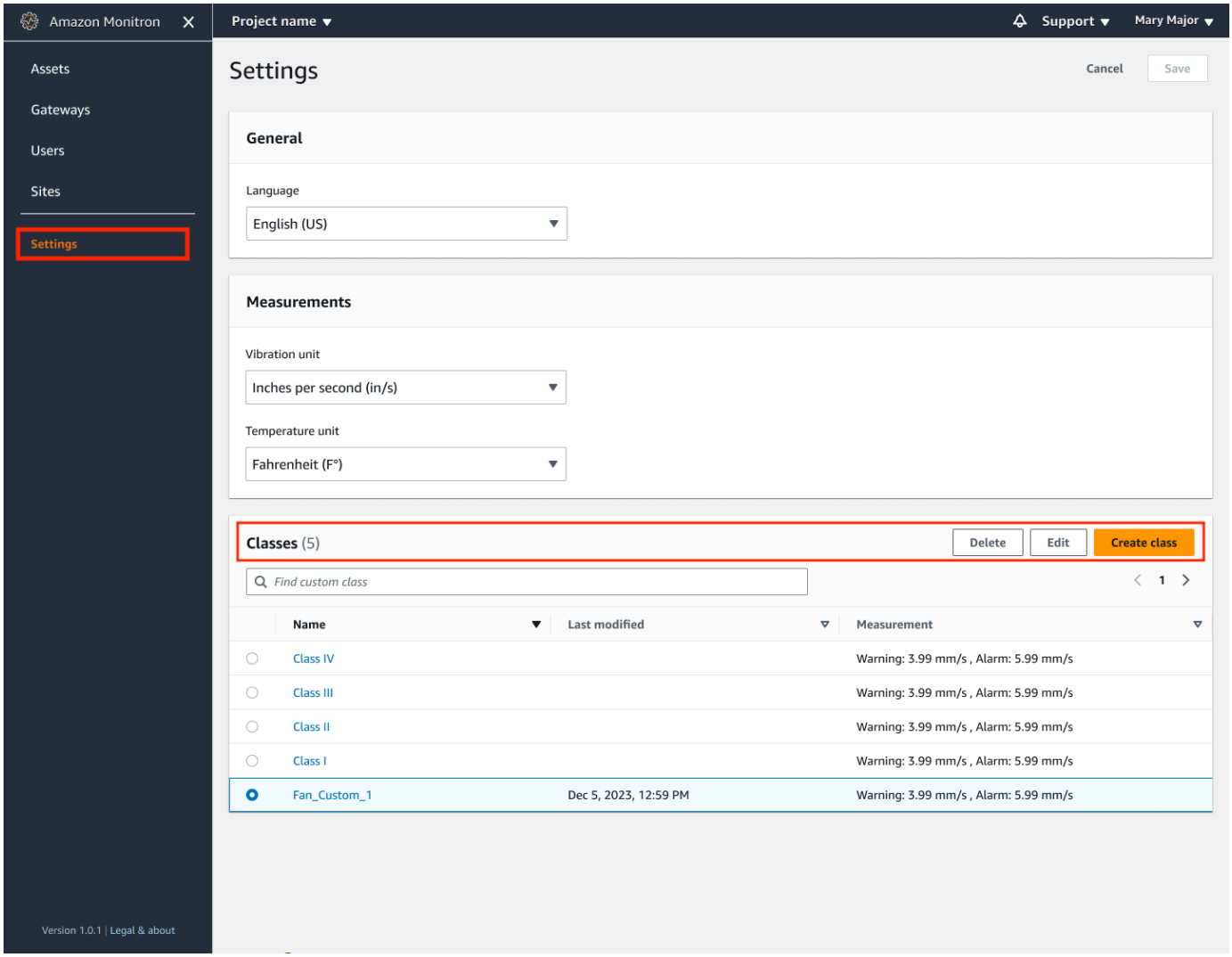
カスタムクラスを削除するには

1. Amazon Monitron コンソール (https://console.aws.amazon.com/monitron) を開きます。
2. [プロジェクトを作成] を選択します。
3. プロジェクトを初めて作成する場合は、「プロジェクトの作成」で説明されているステップに従います。

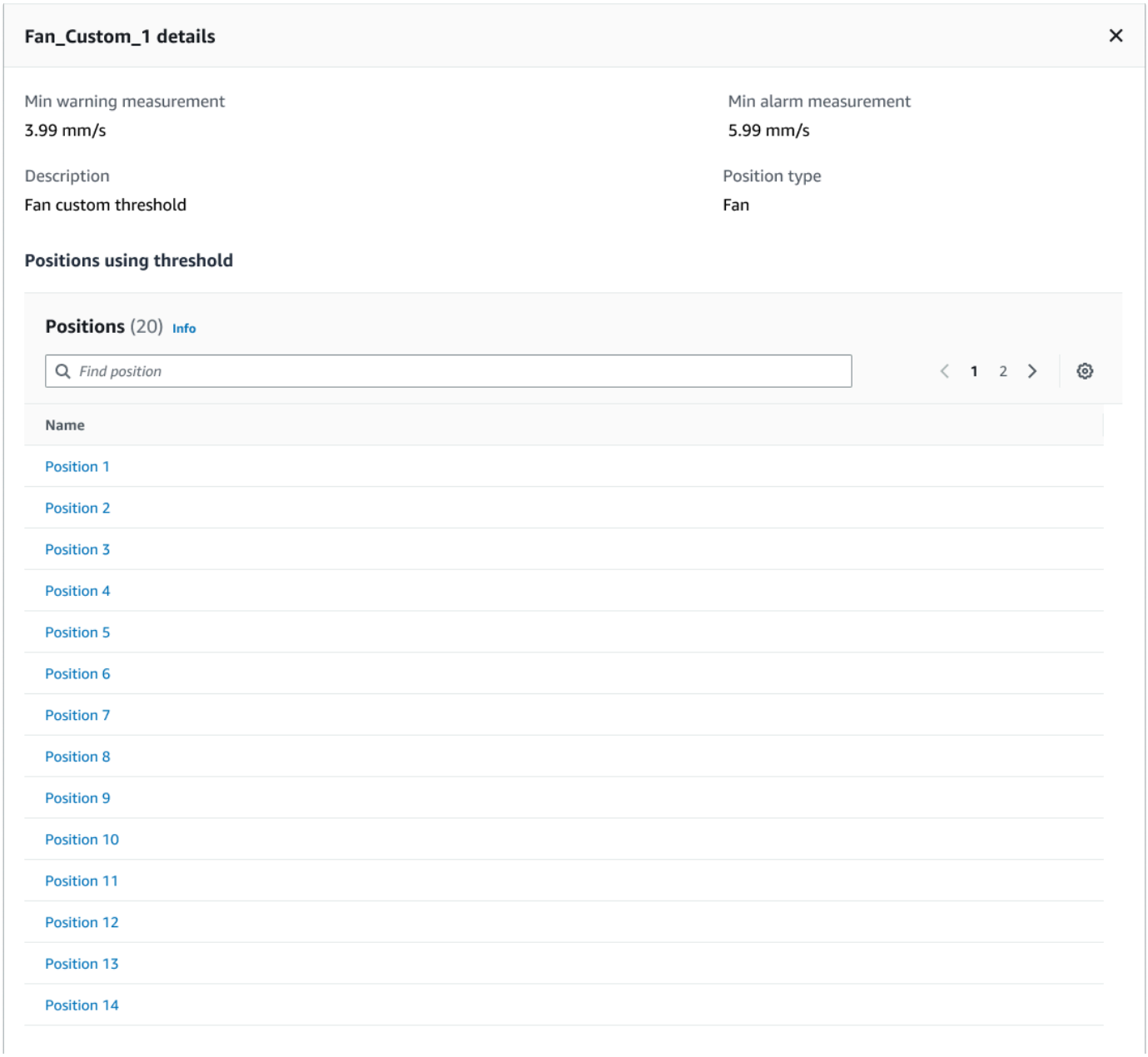
   既存のプロジェクトを選択する場合は、左側のナビゲーションメニューからプロジェクトを選択し、カスタムクラスを作成するプロジェクトを選択します。
4. プロジェクトの詳細ページから、Amazon Monitron ウェブアプリケーションで開くを選択します。



5. Amazon Monitron ウェブアプリページで、左側のナビゲーションペインから設定を選択します。



6. 次に、クラスから、削除するマシンクラスを選択し、削除を選択します。



> **Important**
>
> 1 つ以上のポジションで現在使用されているカスタムマシンクラスは削除できません。現在マシンクラスを使用しているポジションのリストが表示され、これらのポジションにアタッチされているマシンクラスを削除する前に、これらのポジションを別のマシンクラスに更新する必要があります。

7. 削除を確認するには、「」と入力し**delete**、保存を選択します。

アセットの管理

Amazon Monitron アプリを使用して、サイトまたはプロジェクト内のすべてのアセットを一覧表示します。

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

アセットのリストの表示

[アセット] ページにはアセットのリストが表示されます。[アセット] ページはアプリのメインページです。メインページは、アプリを開いたときに表示されるページです。アプリ内の別のページから [アセット] ページに戻るには、次の手順に従います。

トピック

- アセットリストを開くには。

アセットリストを開くには。

1. メニューアイコン (☰) をクリックします。

2. [アセット] を選択します。

アセットの追加

サイトまたはプロジェクトを設定したら、センサーがモニタリングするアセットを追加します。

> **Note**
>
> アセットを作成した後は、名前だけを変更できます。

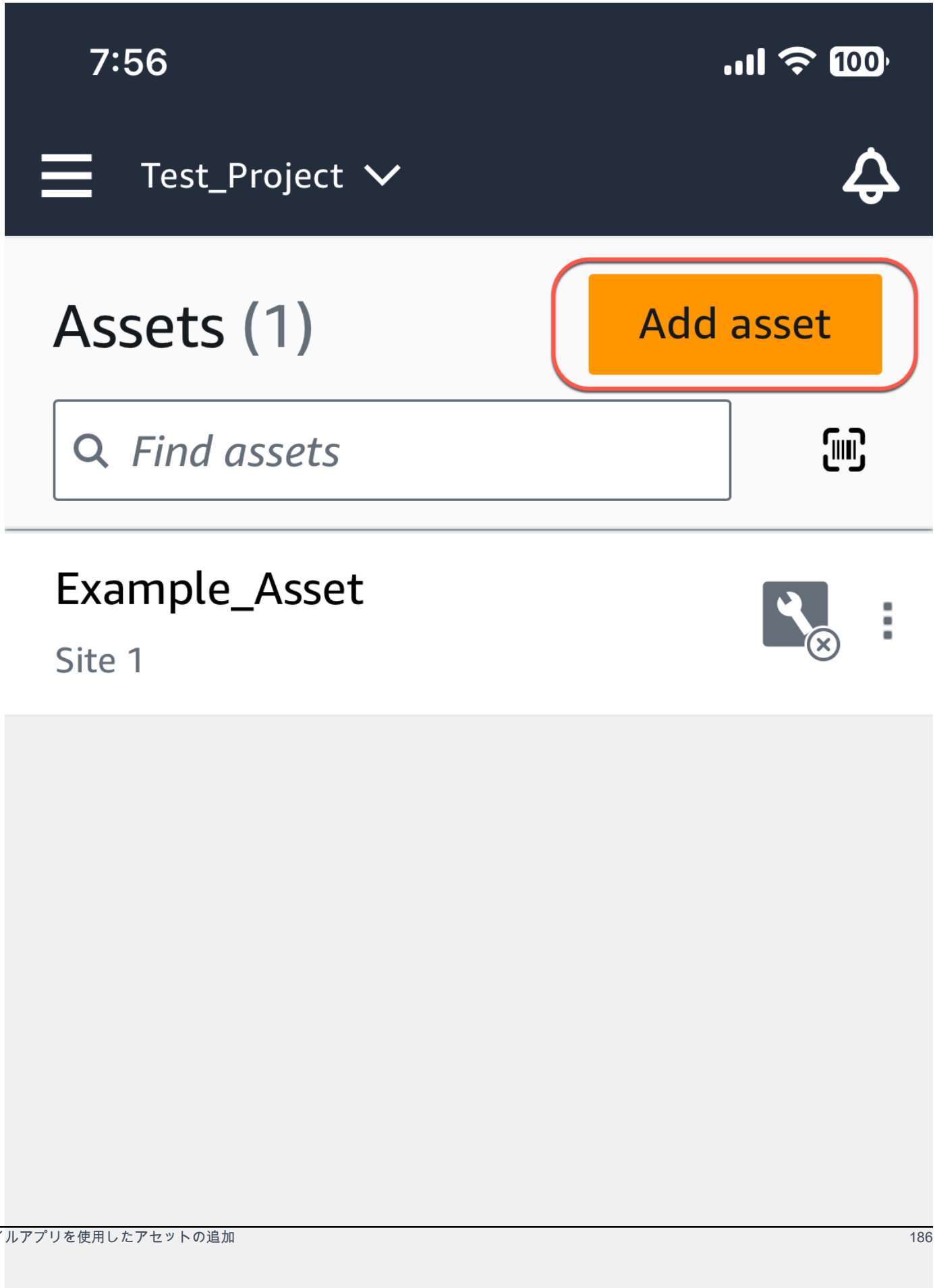
トピック

- モバイルアプリを使用したアセットの追加
- ウェブアプリを使用したアセットの追加

モバイルアプリを使用したアセットの追加

モバイルアプリを使用してアセットを追加するには

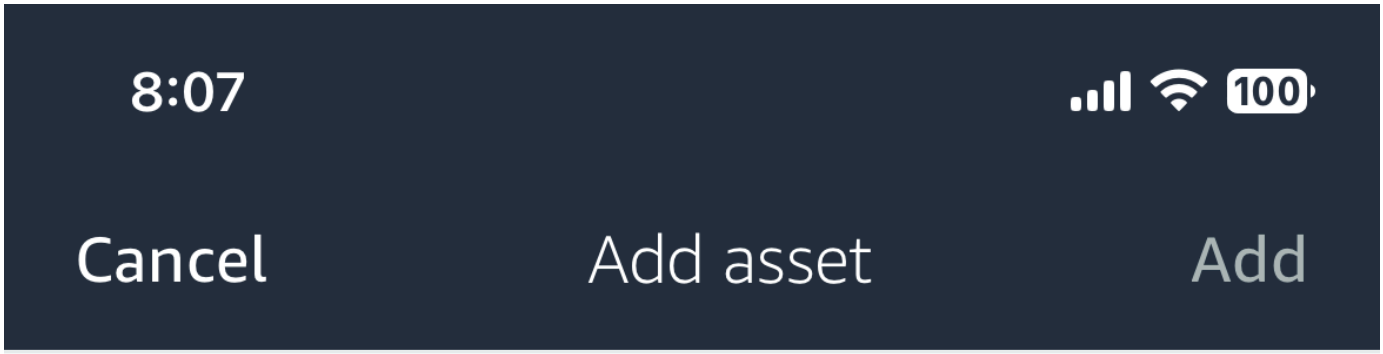
1. モバイルアプリにサインインし、アセットを追加するプロジェクトを選択します。


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

2. アセットを追加するプロジェクトが正しいサイトにいることを確認します。プロジェクト名またはサイト名は、アプリ内でそのレベルにいることを示しています。

サイトレベルからプロジェクトレベルへの変更、またはその逆の変更の詳細については、「モバイルアプリを使用したプロジェクトとサイト間の移動」を参照してください。

3. アセット ページから、アセットの追加 を選択します。
4. アセットの追加ページで、アセット名に、作成するアセットの名前を追加し、追加を選択します。



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.

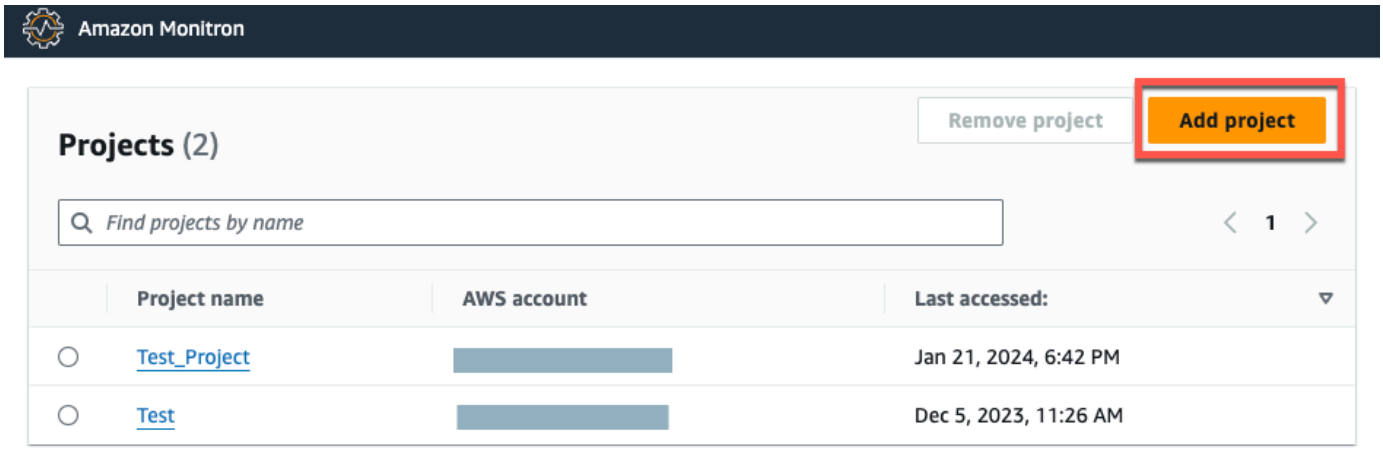
> **Note**
>
> アセット名を特定する QR コードがある場合は、その QR コードを選択してスキャンできます。

最初のアセットを追加すると、[アセット] ページのリストにそのアセットが表示されます。

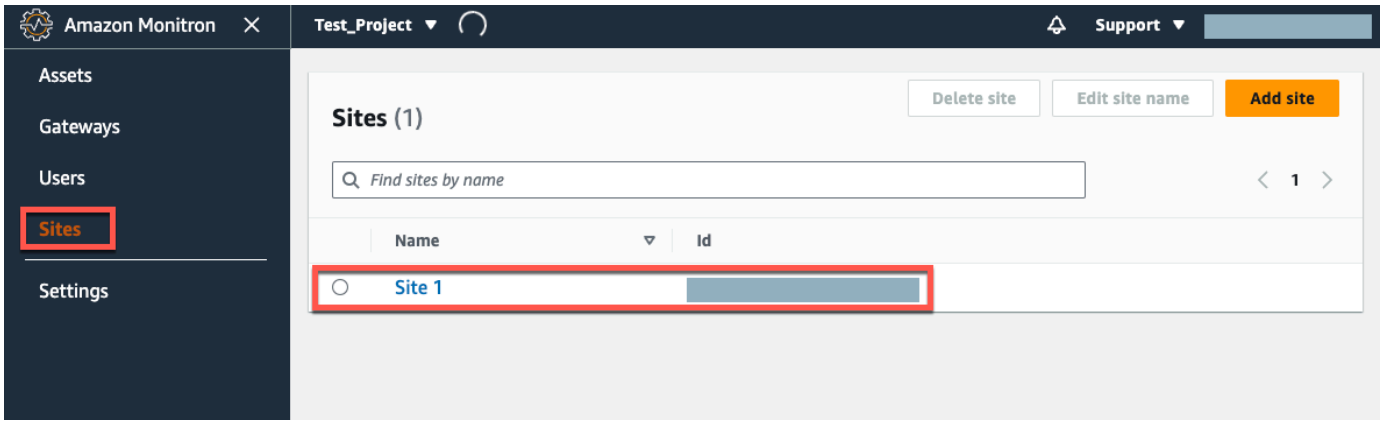
ウェブアプリを使用したアセットの追加

ウェブアプリを使用してアセットを追加するには

1. ウェブアプリにサインインし、アセットを追加するプロジェクトを選択します。

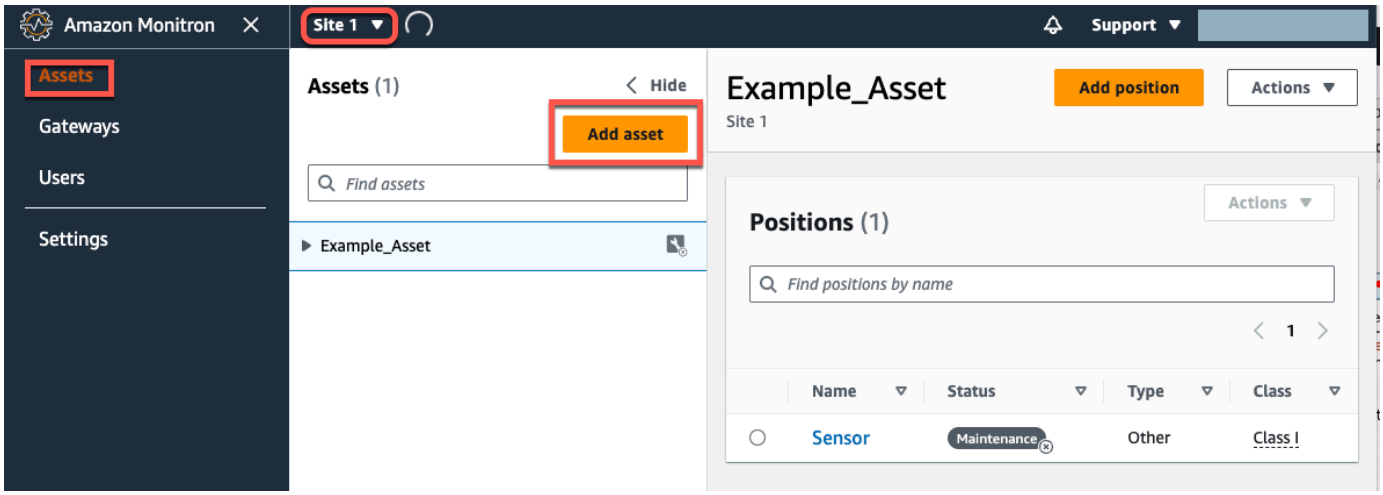


2. 左側のナビゲーションメニューから、サイトを選択し、アセットの対象となるサイトを選択します。

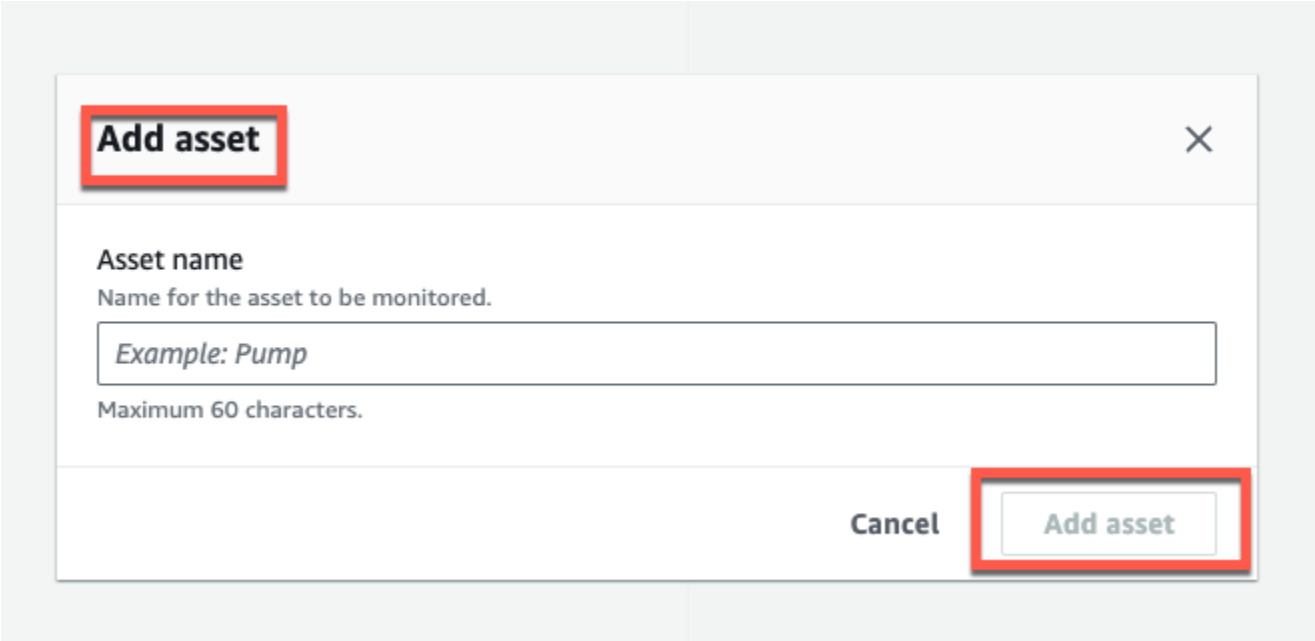


> **Note**
>
> アセットをプロジェクトに直接追加することもできます。

3. アセットページから、アセットの追加を選択します。



4. アセットの追加ページで、アセット名に、作成するアセットの名前を追加し、アセットの追加を選択します。



最初のアセットを追加すると、[アセット] ページのリストにそのアセットが表示されます。

アセット名の変更

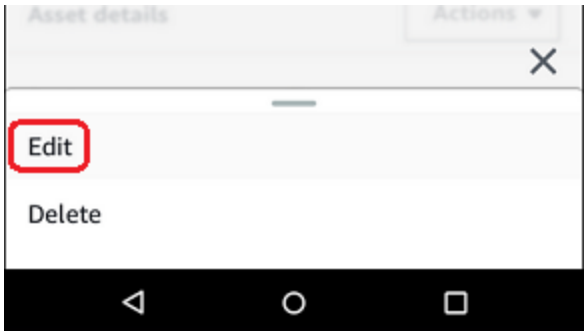
アセットを追加したら、名前とマシンクラスの両方を変更できます。

トピック

- モバイルアプリでアセット名を変更するには
- ウェブアプリでアセット名前を変更するには

モバイルアプリでアセット名を変更するには

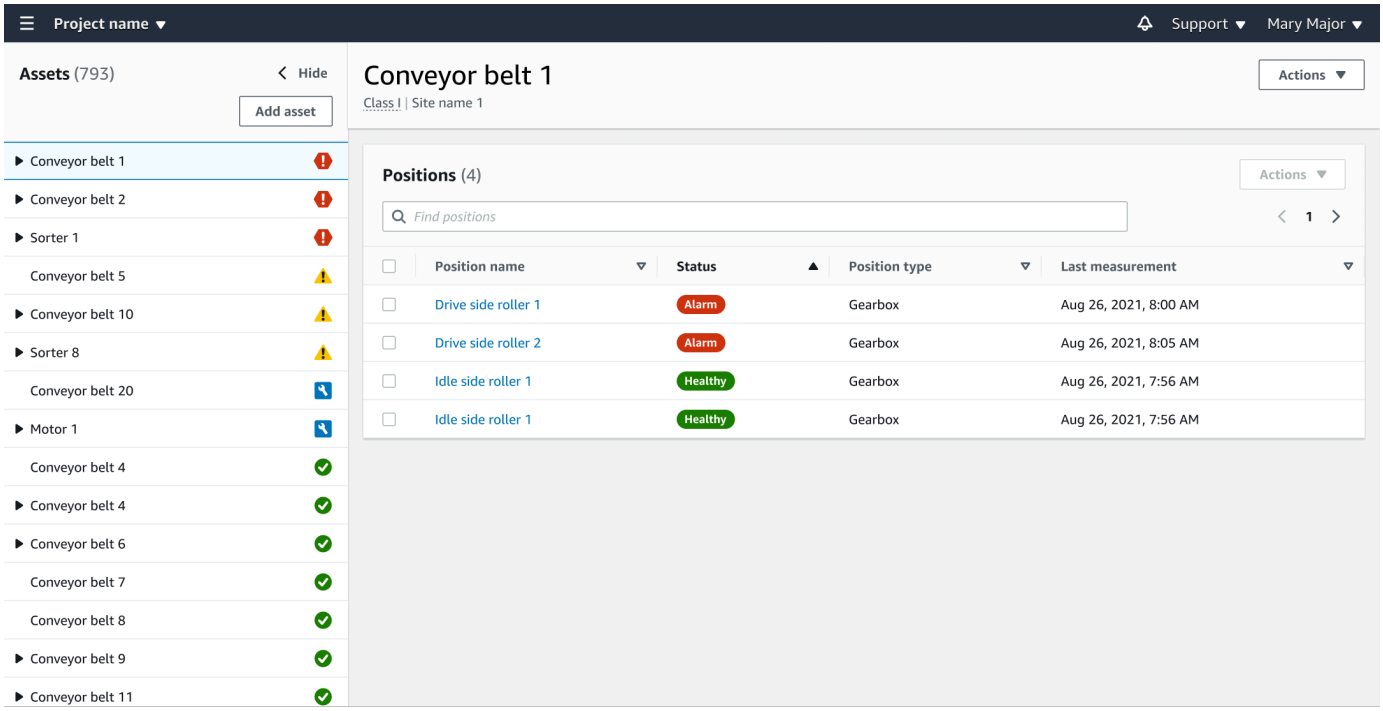
1. アプリのメインメニューから [アセット] を選択します。
2. [アセットの詳細] へは、[アクション] を選択します。
3. [アセットを編集] を選択します。



4. 新しい名前を入力します。
5. [保存] を選択します。

ウェブアプリでアセット名前を変更するには

1. アセットを選択します。
2. 大きいタブ内で、アセット名を含む行の右端にある [アクション] ボタンを選択します。



3. 新しい名前を入力します。
4. [Save] を選択します。

アセットの移動

プロジェクト内のアセットは、さまざまなサイトにグループ化できます。アセットとサイトを再編成する必要がある場合は、各アセットを再作成することなく、あるサイトから別のサイトにアセットを移動できます。

> **Note**
>
> アセットをプロジェクトレベルからサイトレベルに移動できます。ただし、アセットをサイトレベルからプロジェクトレベルに移動することはできません。

アセットを移動すると、新しい送信先サイトで通知の生成が続行されます。アセットに関連付けられたすべての位置が新しいサイトに移動します。ただし、通知の生成と、古いソースサイトのユーザーへの表示は停止します。

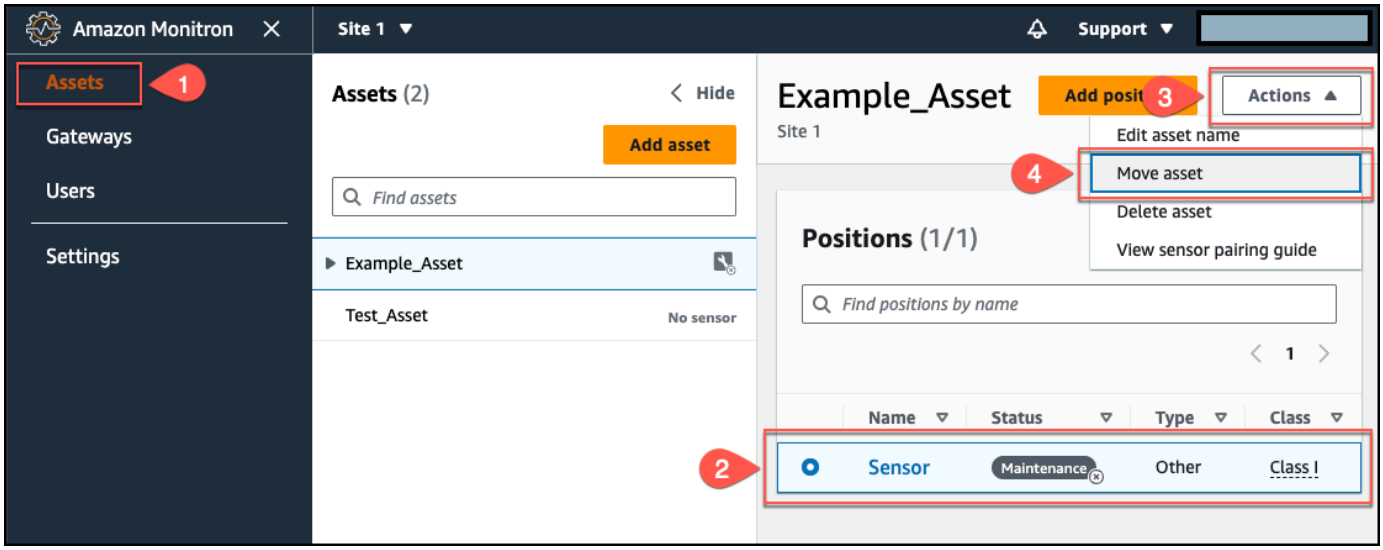
> **Important**
>
> アセットを移動できるのは、送信元サイトと送信先サイトの両方に管理者権限を持つユーザーのみです。

トピック

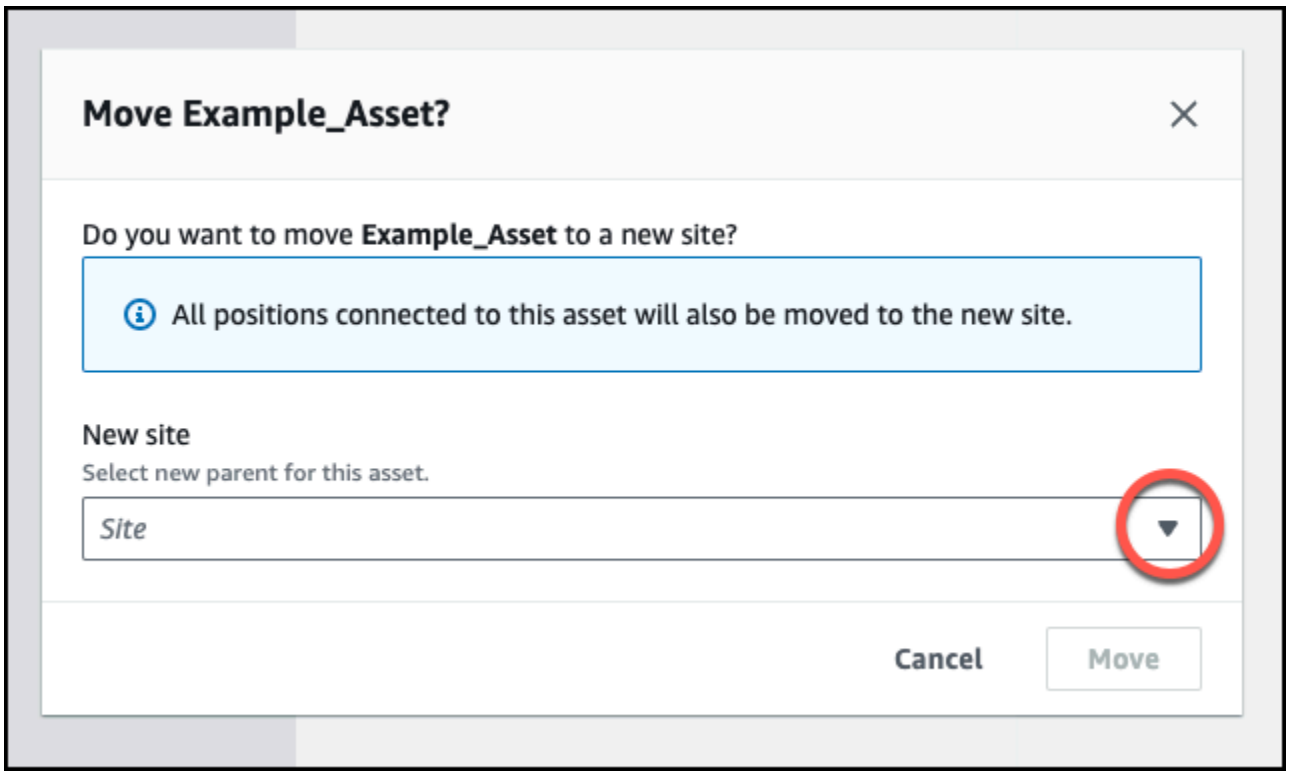
- ウェブアプリでアセットを移動するには
- モバイルアプリでアセットを移動するには

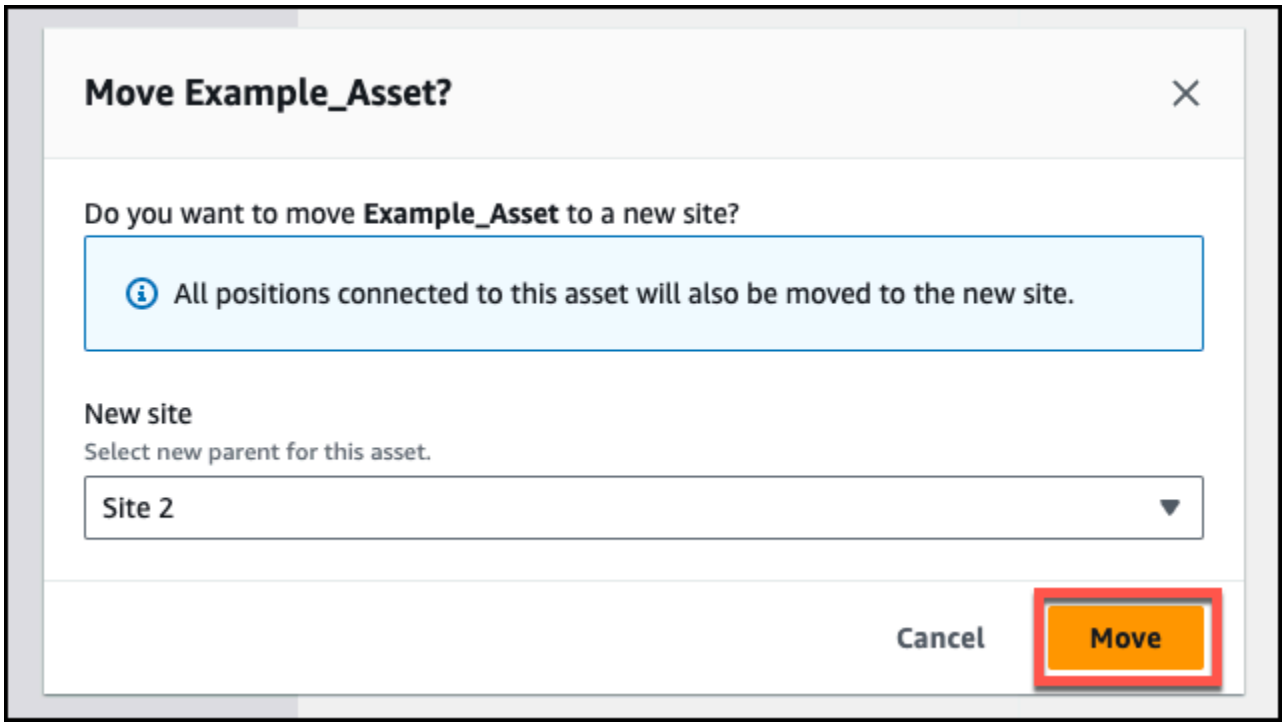
ウェブアプリでアセットを移動するには

1. ウェブアプリケーションのメインメニューから、アセットを選択します。
2. 移動するアセットを選択します。
3. アセットメニューからアクションを選択し、アセットの移動を選択します。



4. 開いたダイアログボックスで、新しいサイトのドロップダウンメニューからアセットを移動するサイトを選択し、移動を選択します。

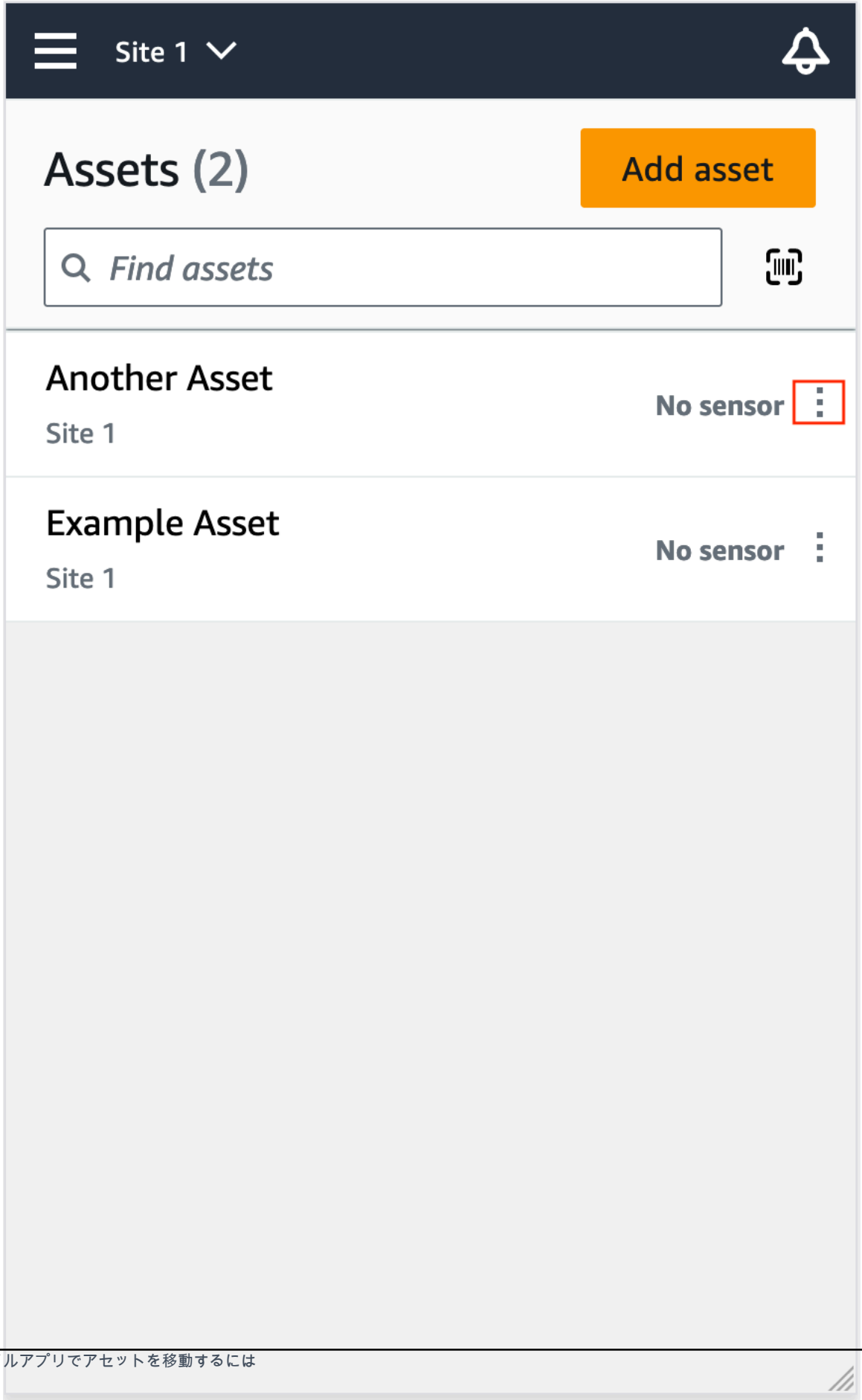




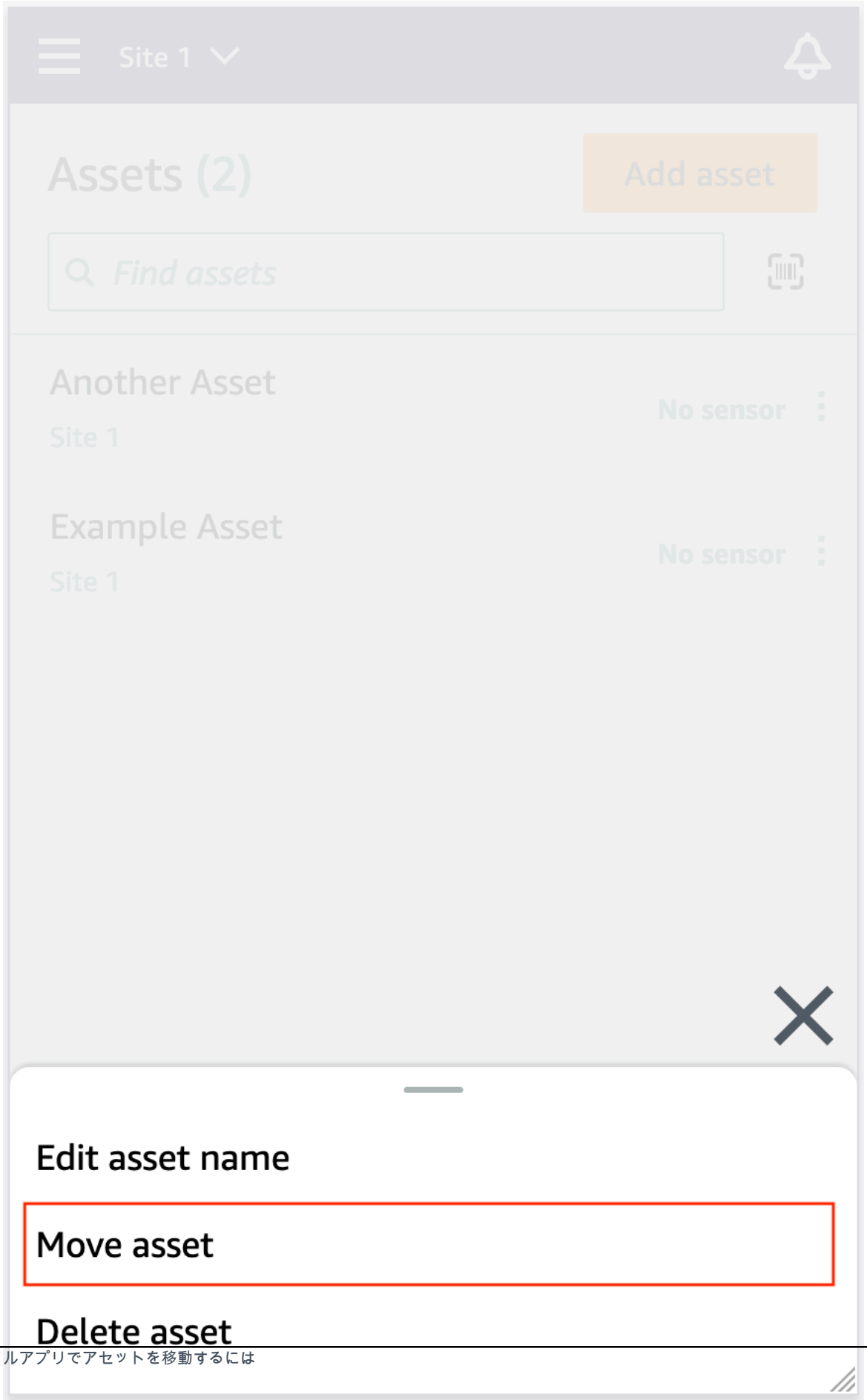
アセットが正常に移動されると、アプリに成功メッセージが表示されます。

モバイルアプリでアセットを移動するには

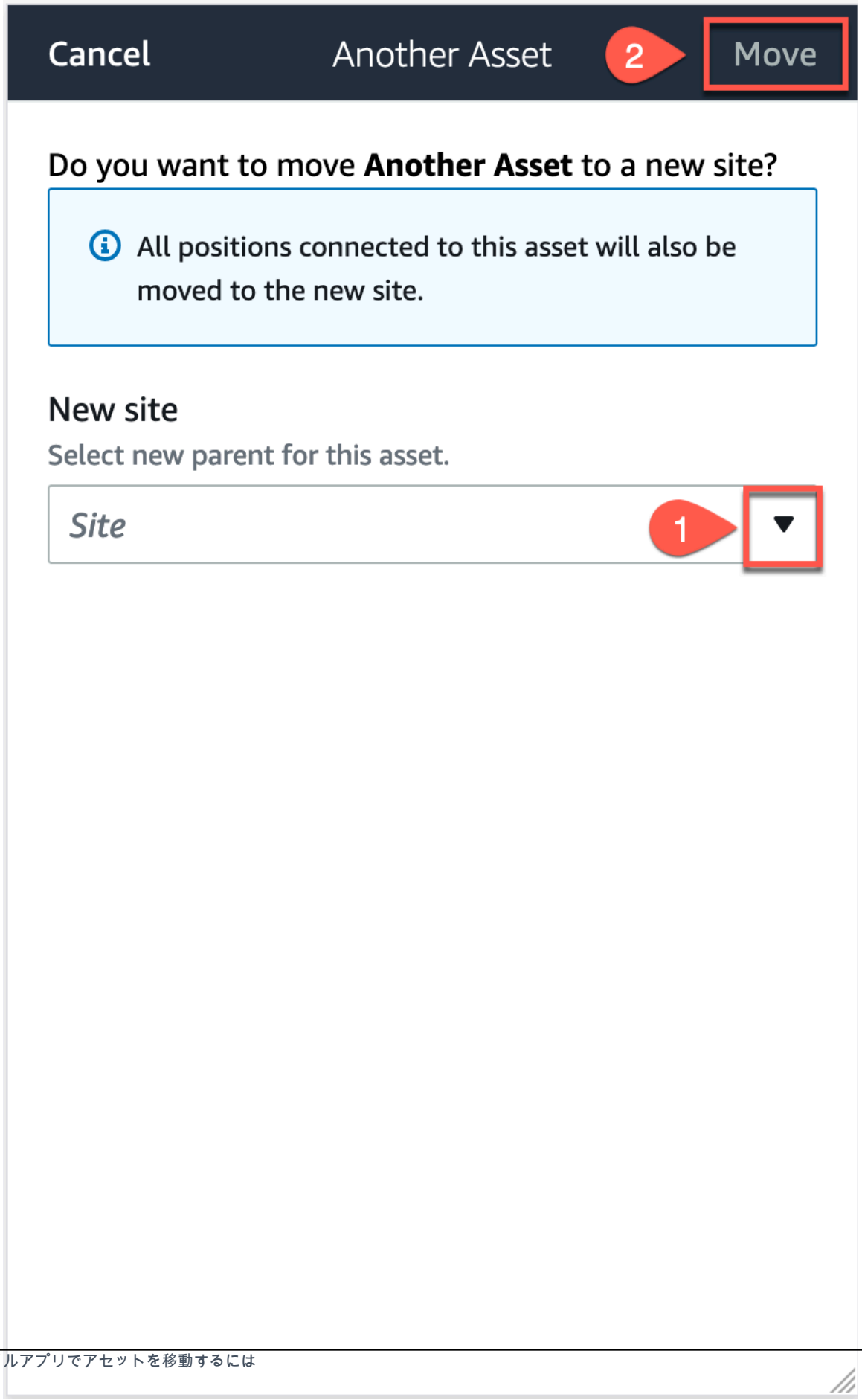
1. モバイルアプリのメインメニューから、アセットを選択します。
2. 新しいサイトに移動するアセットを選択します。次に、アセットの詳細メニューを開きます。


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

3. アセットの詳細メニューから、アセットの移動を選択します。


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. アセットページから、新しいサイトから、アセットを移動する新しいサイトを選択します。次に、移動を選択します。


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

アセットが正常に移動されると、アプリに成功メッセージが表示されます。

アセットの削除

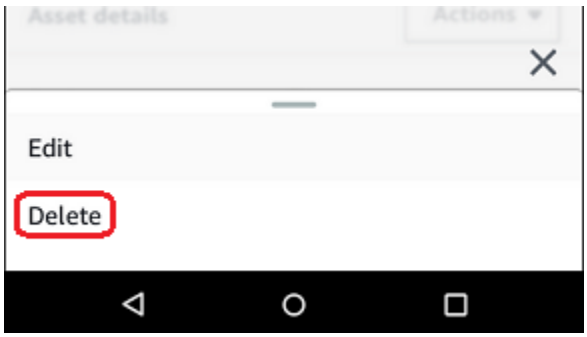
アセットを削除すると、関連するすべてのセンサーとそのポジション、およびそれらに関連する履歴データが削除されます。

トピック

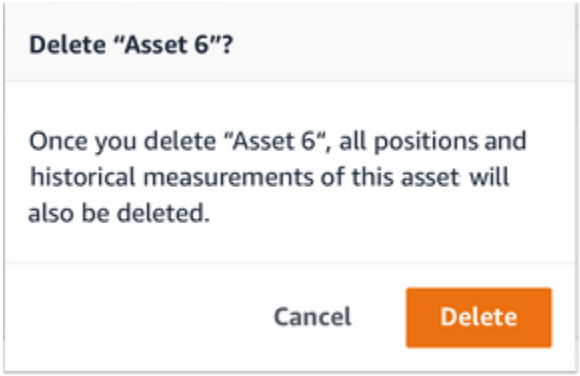
- アセットを削除するには

アセットを削除するには

1. アプリのメインメニューから [アセット] を選択します。
2. 削除するアセットを選択します。
3. [アセットの詳細] へは、[アクション] を選択します。
4. [アセットを削除] を選択します。

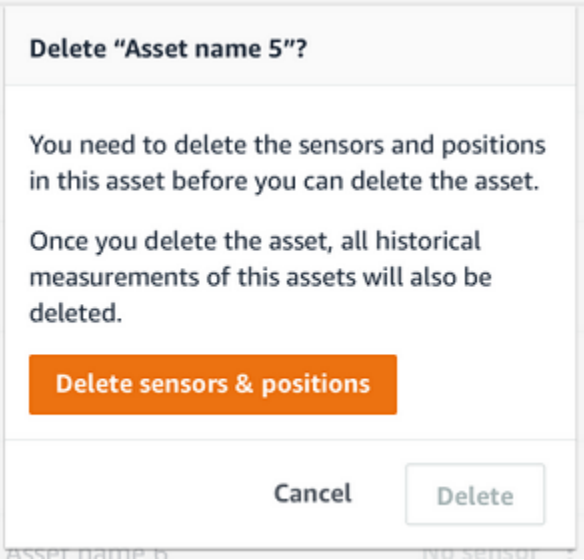


5. 次のいずれかのオプションを選択します。
   - アセットとペアリングされているセンサーがない場合は、[削除] を選択して次のステップに進みます。



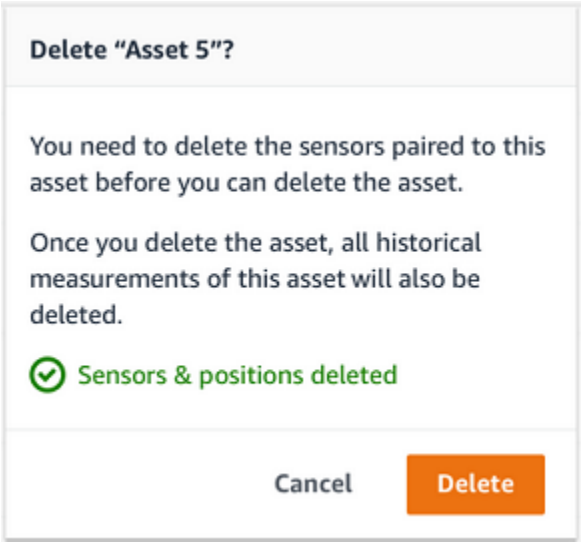
- アセットとペアリングされているセンサーがある場合は、それらを削除します。

  [センサーとポジションを削除] を選択します。センサーまたはポジションを削除すると、そのポジションで行われた過去の測定値もすべて削除されます。



  がペアリングされたすべてのセンサーと位置を削除する Amazon Monitron までに時間がかかる場合があります。

6. [削除] を選択します。



センサー

センサーは機器からデータを収集し、そのデータ Amazon Monitron を使用して異常の発生を検出します。データの収集と分析では、センサーを取り付ける場所 (位置) が非常に重要です。

アセットの状態をより詳細に把握するには、アセット上で複数の位置からデータを収集する必要があります。各アセットに対して最大 20 か所センサーを配置できます。各センサーの位置には、異なる機械クラスを割り当てることができます。複数の潜在的な障害点がある複雑な機械では、複数のポジションからデータを収集することを推奨します。

トピック

- センサーの配置
- センサーを取り付ける
- センサーのポジションを追加する
- センサーをアセットにペアリングする
- センサーのポジション名を変更する
- 機械のクラスを編集する
- センサーを削除する
- センサーポジションを削除する
- センサーの詳細を理解する
- センサーポジションを識別する
- 定格超過センサー

センサーの配置

マシンコンポーネントの異常を検出するには、温度と振動を効果的に測定できるすべての場所にセンサーを取り付けます。

精度を最大限に高めるには:

- センサーをターゲットコンポーネントのハウジングに直接取り付けます。
- 振動伝達経路 (振動源とセンサー間の距離) の長さを最小限にしてください。
- 板金のカバーなど、固有振動数によって測定値が変動する可能性のある場所にセンサーを取り付けることは避けてください。

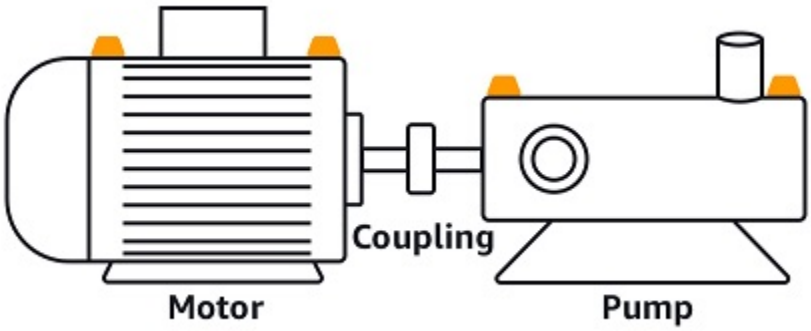
振動は、発生源から最大 30 ~ 36 インチ (75 ~ 90 cm) 離れた場所で減衰します。

伝達経路の長さを短くする振動伝達経路には、次のような特性があります。

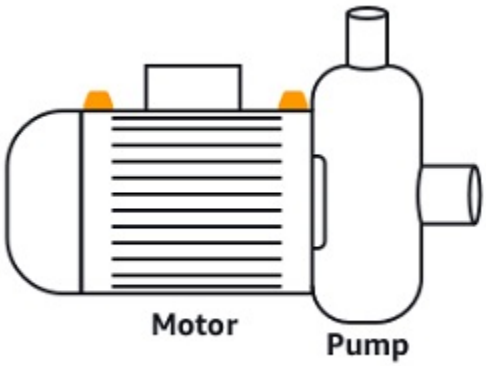
- 信号反射が発生する取り付け面の数
- ゴムやプラスチックなど、振動を吸収する素材

> **Note**
>
> Amazon Monitron センサーは 3 軸振動センサーです。X、Y、Z マークは 3 つの軸の方向を示しています。これらの軸はセンサー本体にマークされています。そのため、特定の軸をアセットの振動方向に合わせる必要はありません。

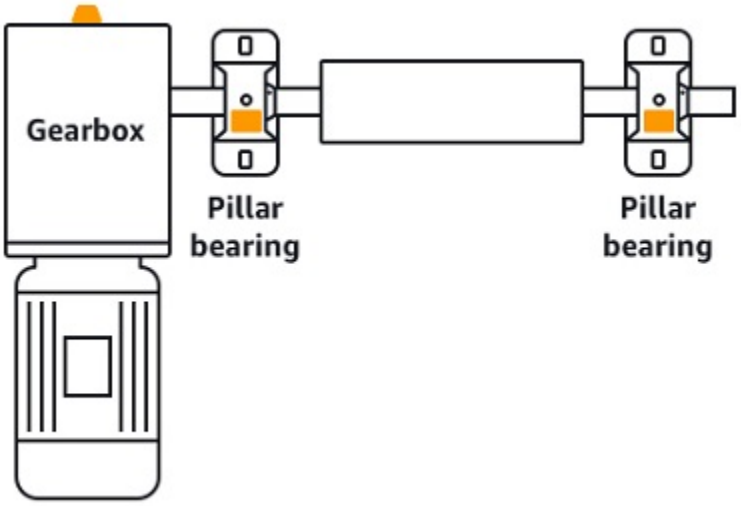
以下の電動モーターポンプセットの例は、4 つのセンサーの位置 (モーターに 2 つ、ポンプに 2 つ) を示しています。



次の例は、ポンプよりもモーターに重点を置く場合にセンサーを取り付ける場所を示しています。

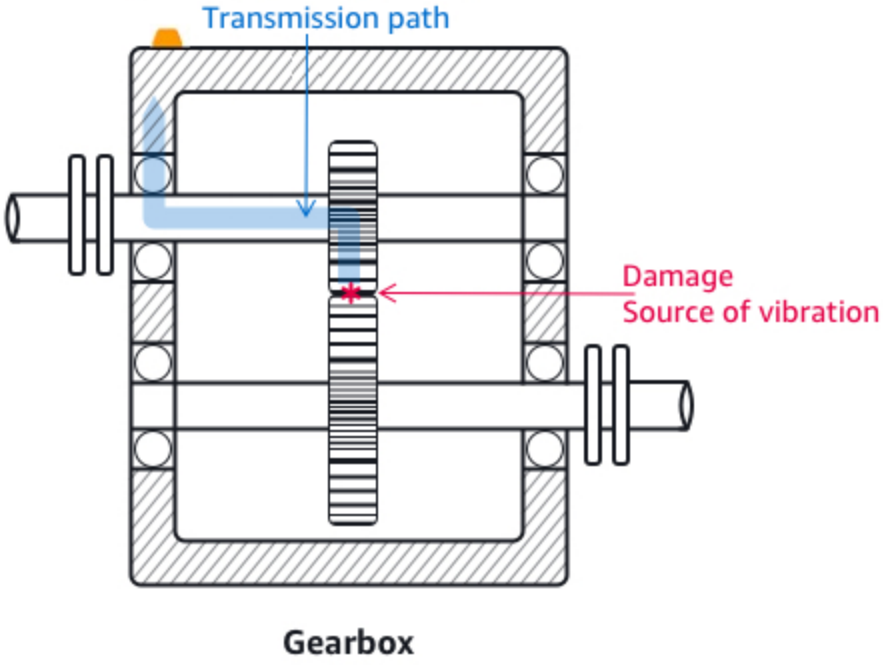


ギアボックスとベアリングも、センサーを設置する一般的な場所の例です。

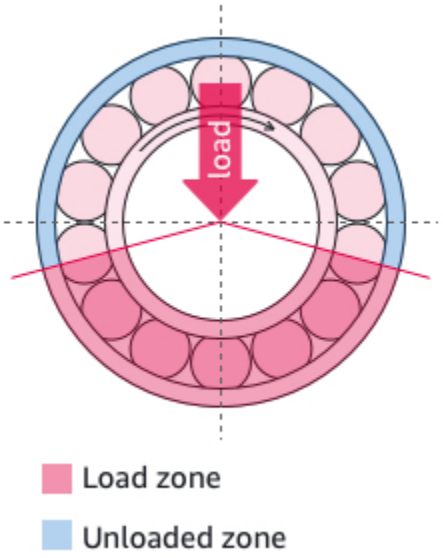


複数の可動部品がある複雑な機器 (ギアボックスなど) の場合は、主な振動源からの伝達経路の長さが最小になるように、センサーを配置します。しかし、機器の隣接する部品間で振動が伝わると振動が減少するため、センサーと振動源の間の距離を最短にすることがいつでも最適な方法であるとは限らないことに注意してください。

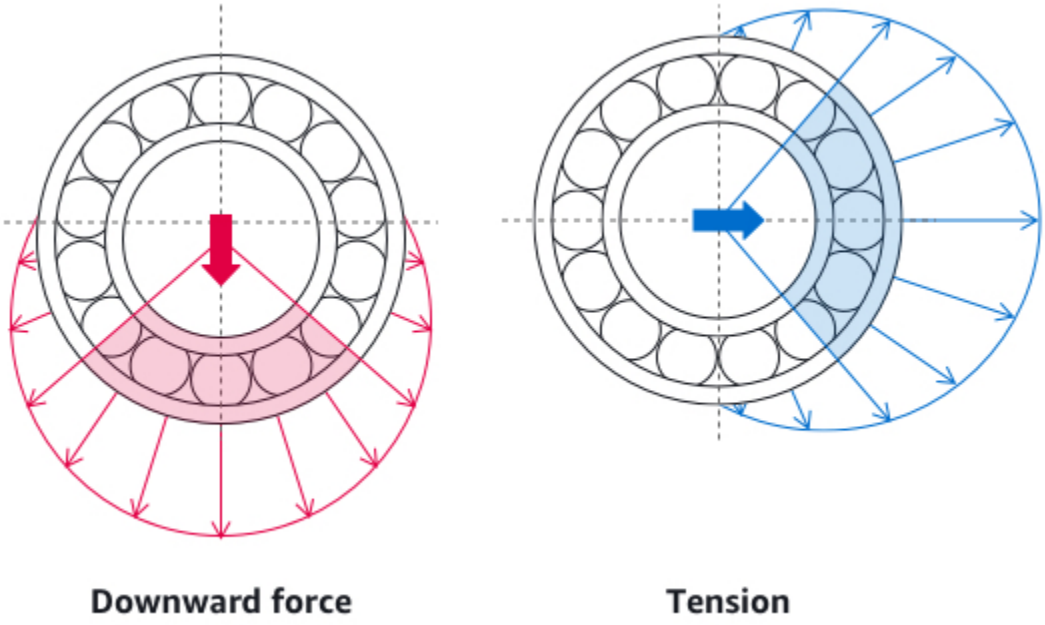
以下のギアボックスの例は、このように振動が機器に伝わる仕組みと、センサーが振動を検知する可能性のある位置を示しています。



他のタイプの機器は、最適な位置がわかりにくい場合があります。例えば、ベアリングを監視するセンサーを配置する場合、以下に示すようにベアリングにかかる荷重の方向に基づいて、ベアリングの荷重ゾーンの近くにセンサーを配置します。



ベアリングにかかる荷重の種類が異なれば、荷重ゾーンも異なります。センサーを荷重ゾーンの中心にできるだけ近づけると、最適なデータが取得できる可能性が高くなります。

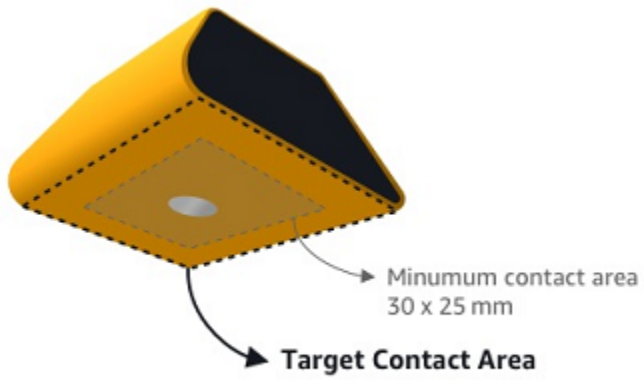


センサーを取り付ける方法については、「センサーを取り付ける」を参照してください。

センサーを取り付ける

> **Warning**
>
> センサーをインストールして使用する前に、「Amazon Monitron Sensor Device Safety and Compliance Guide」を参照してください。Ex-rated センサーをインストールして使用する前に、Ex Safety and Compliance Guide ですべての警告と手順を確認してください。

温度および振動ディテクターは、 Amazon Monitron センサーのベースにあります。底面はどの部分でもターゲットの接触領域として有効ですが、信頼性の高い検出には接触面積が 30 × 25 mm 以上必要です。最も信頼性の高い検出結果を得るには、取り付け位置の中央にターゲットの接触領域を配置してください。円形のアルミニウムセンサー (ターゲット接触領域の中央) は、アセットの表面から直接、 Amazon Monitron センサー内部の温度検知メカニズムに熱を伝導します。



アセットを最も効果的にモニタリングできる場所と方向を決め、その場所にセンサーを取り付けます。センサーを取り付けるには、工業用接着剤を購入する必要があります。Loctite 454 や Loctite 3090 や Loctite 4070 などのシアノアクリレート工ポキシを使用することをお勧めします。センサーを取り付ける表面が平らで比較的滑らかな場合は、Loctite 454 のような接着剤を薄く塗るだけで問題ありません。表面が丸くなったり、多少不均一になったりする場合は、Loctite 3090 や Loctite 4070 などの接着剤をわずかに厚く塗ります。

センサーを取り付ける場所がわからない場合は、「センサーの配置」を参照してください。

> **Warning**
>
> センサーを設置する際は、該当する安全規則を確認して従ってください。お客様は、あらゆる機器または機械部品にセンサーを安全に取り付ける責任があります。センサーを取り付け

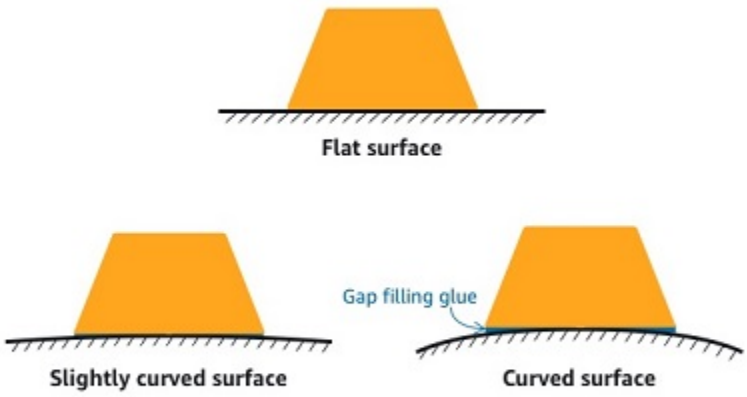
るには、工業用接着剤を使用してください。接着剤メーカーの安全性と取り扱いに関する指示を必ず確認して従ってください。
推奨される接着剤の詳細については、必要に応じて「Loctite 454 技術情報」、「Loctite 3090 技術情報」、または「Loctite 4070 技術情報」を参照してください。

センサーを取り付けるには

1. センサーを取り付けたいアセットの表面から油脂をすべて取り除きます。
2. センサーを取り付ける表面が平らで比較的滑らかな場合は、センサーの底面に Loctite 454 などの接着剤を薄く塗布して、アセットと接触する面積を広くします。

   表面が丸くなったり、多少不均一になったりする場合は、Loctite 3090 や Loctite 4070 などの接着剤のリベラル層をセンサーの下部に適用します。必要に応じて接着表面とセンサーの間のすき間を最大 5 mm まで接着剤の層で埋めることができます。
3. 機械部品の取り付け位置にセンサーを 30 秒間固定し、しっかりと押します。

   カーブした面にセンサーを取り付ける場合は、センサーと表面が接触しやすいように、両面に少量の接着剤を追加で塗ります。接着表面と使用する接着剤によって、以下のような結果となります。



センサーのポジションを追加する

センサーをアセットとペアリングすると、ポジションのタイプが記録されます。位置のタイプは、そのセンサーのデータを分析するときに位置を評価する Amazon Monitron 方法を に指示します。

Amazon Monitron ウェブアプリと Amazon Monitron モバイルアプリの両方からアセット位置を作成および更新できます。アプリを使用すると、次のことができるようになります。

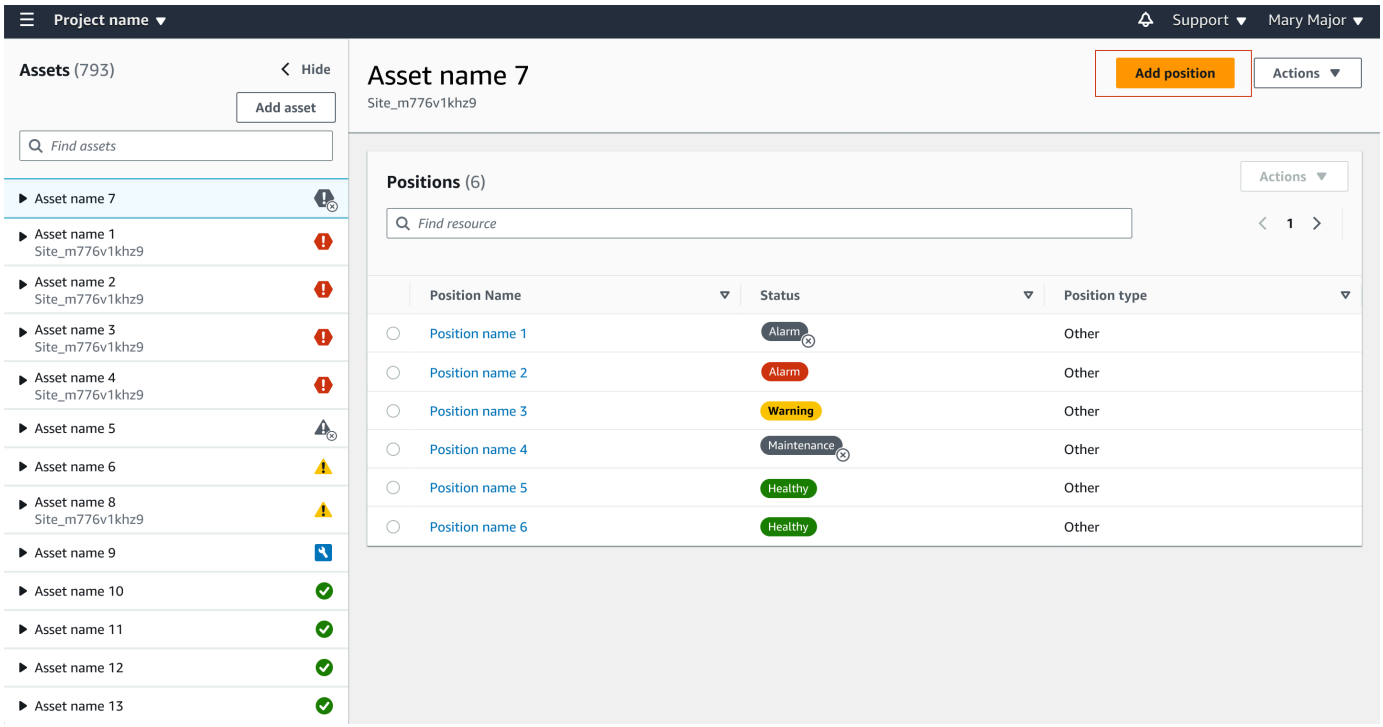
- 既存のアセットに新しいポジションを追加できます。
- 新しいアセットに新しいポジションを追加できます。
- 新しいセンサーを既存のポジションとペアリングできます。
- ポジションが割り当てられていない既存のアセットに新しいポジションを追加できます。

トピック

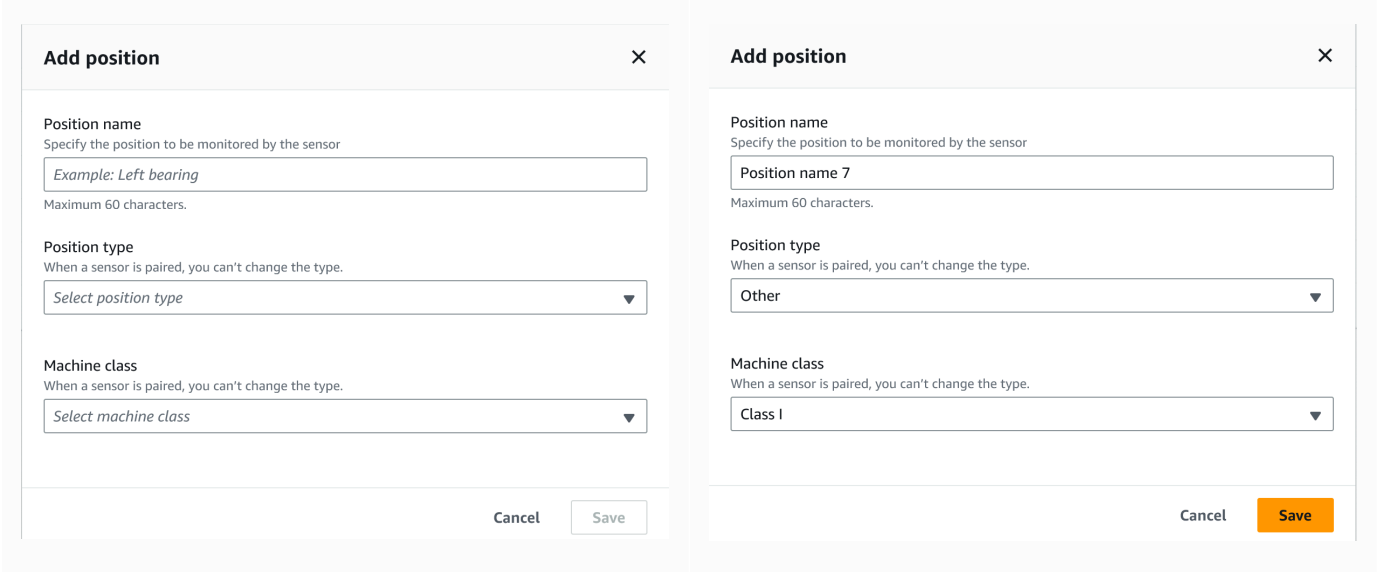
- ウェブアプリでセンサーのポジションを追加するには
- モバイルアプリでセンサーのポジションを追加するには

ウェブアプリでセンサーのポジションを追加するには

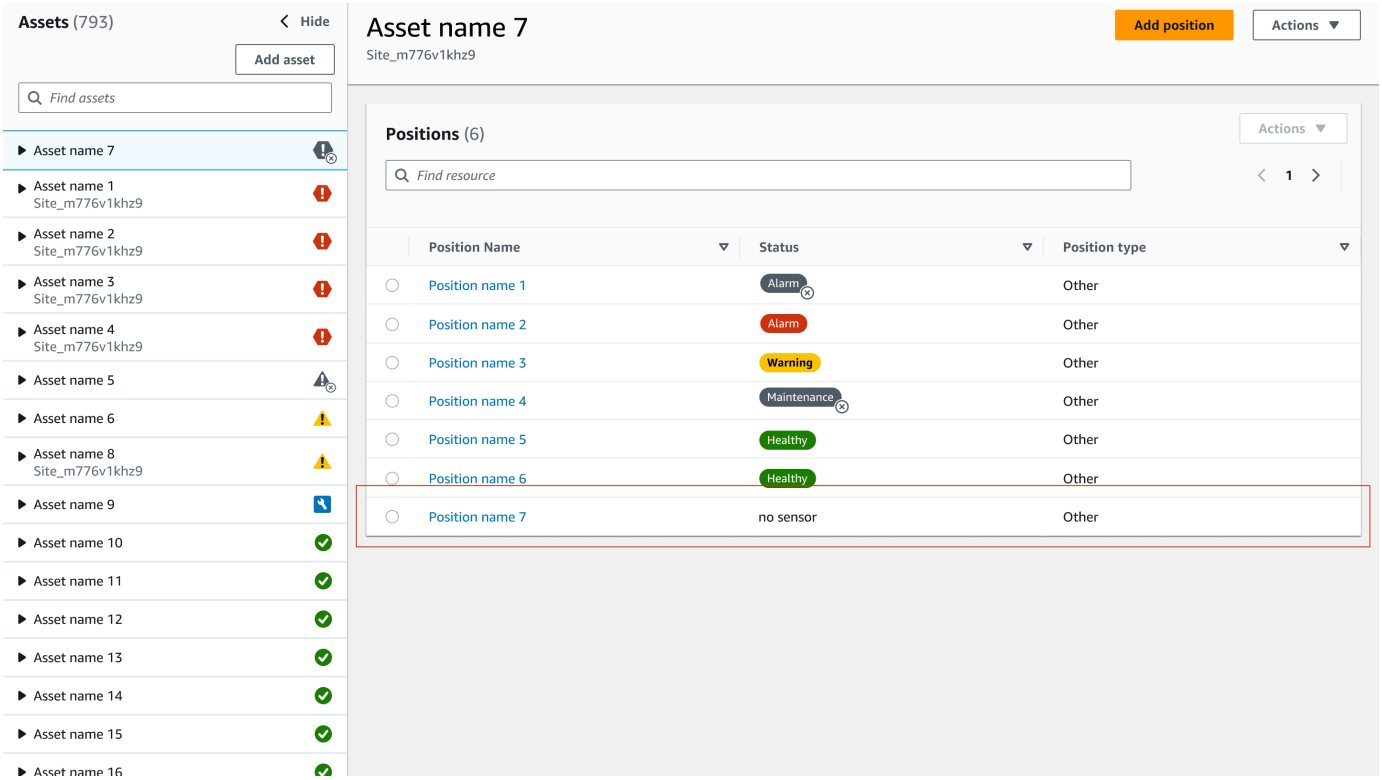
1. [アセット] リストから、ポジションを作成または編集したいセンサーを選択します。
2. [ポジションを追加] ボタンを選択します。



3. 表示されたダイアログボックスで、[ポジション名]、[ポジションのタイプ]、[機械のクラス] を入力します。



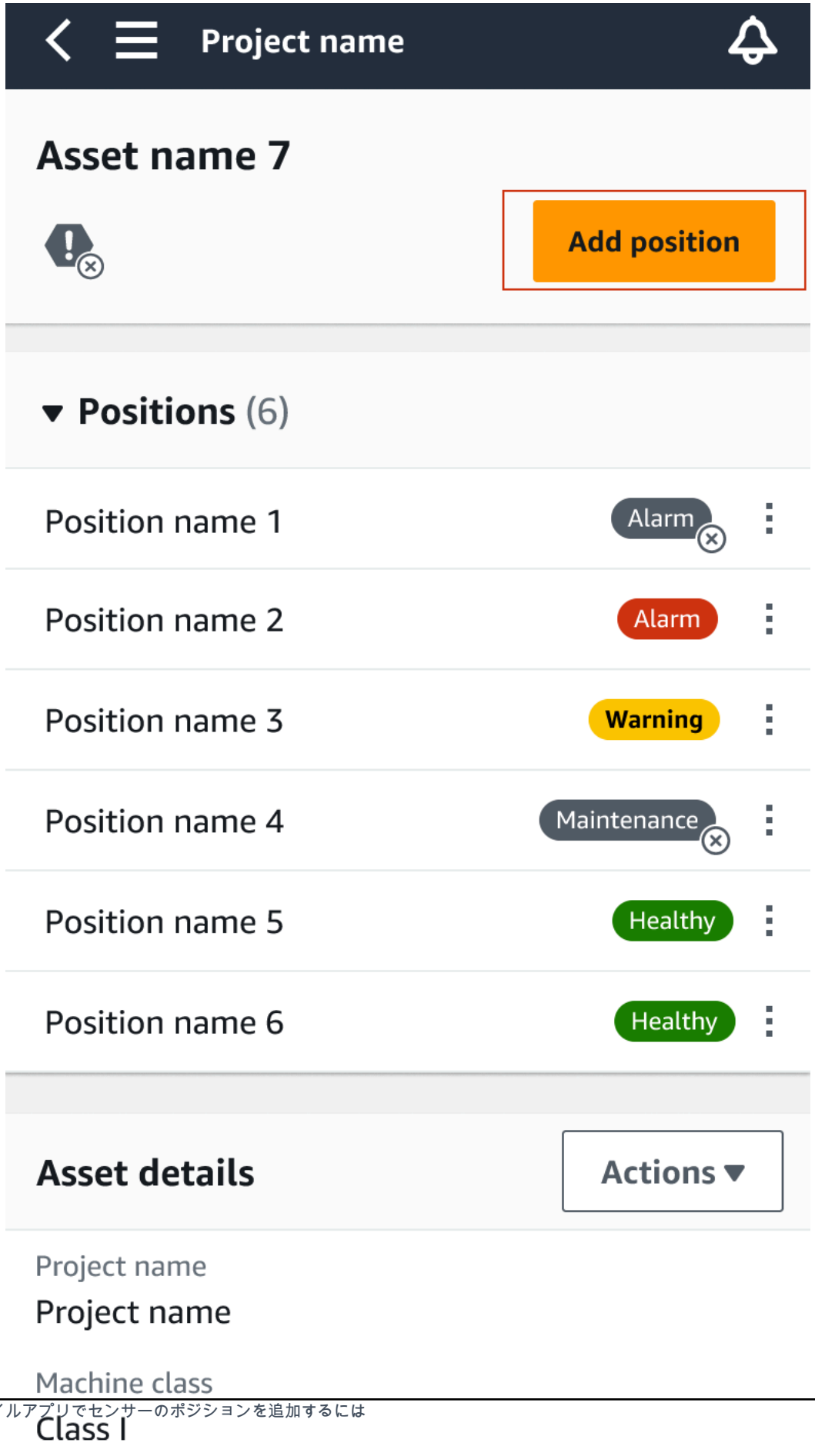
4. [Save] を選択します。
5. ポジションがアセットに追加されます。



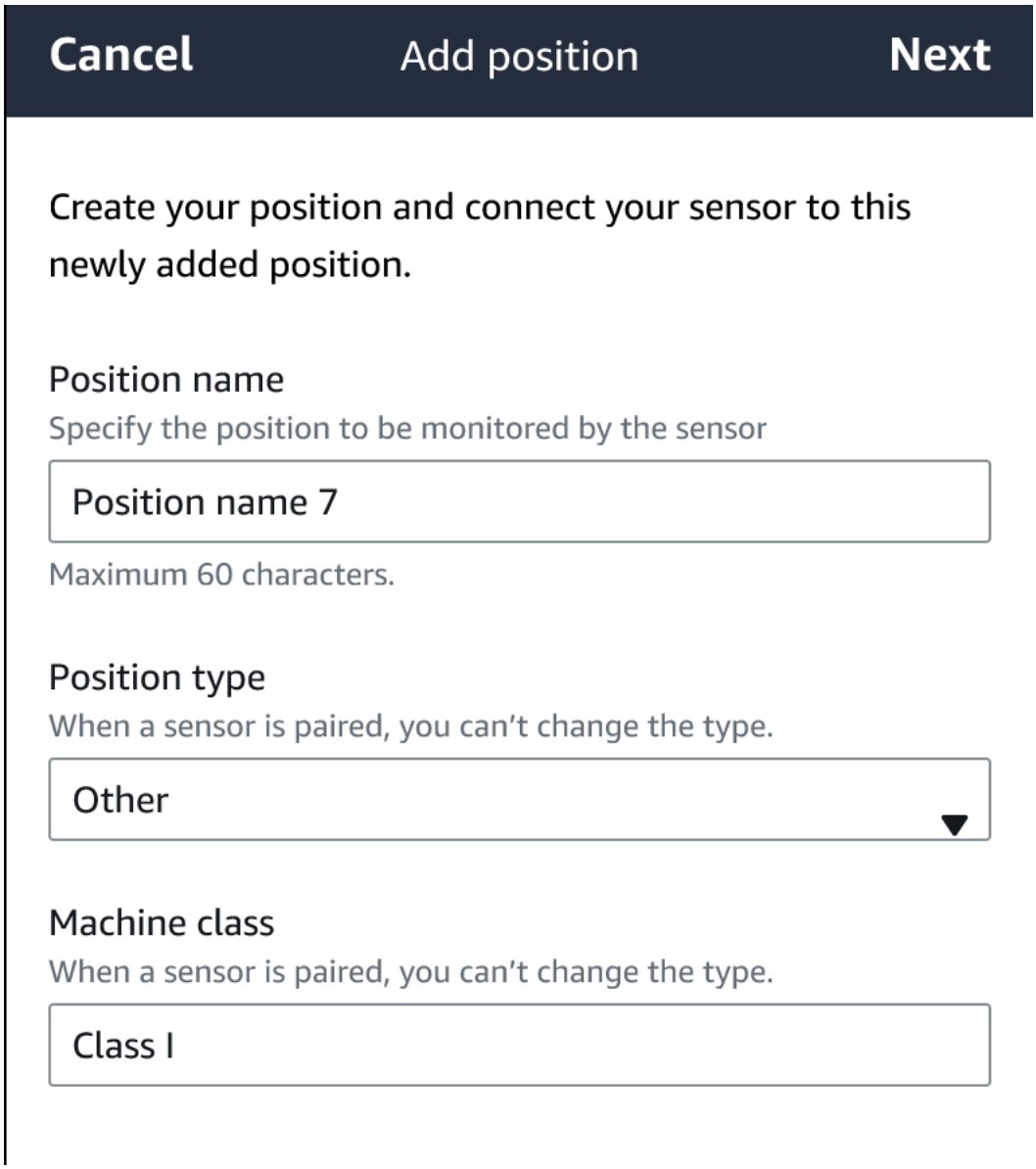
モバイルアプリでセンサーのポジションを追加するには

1. [アセット] リストから、ポジションを作成または編集したいセンサーを選択します。

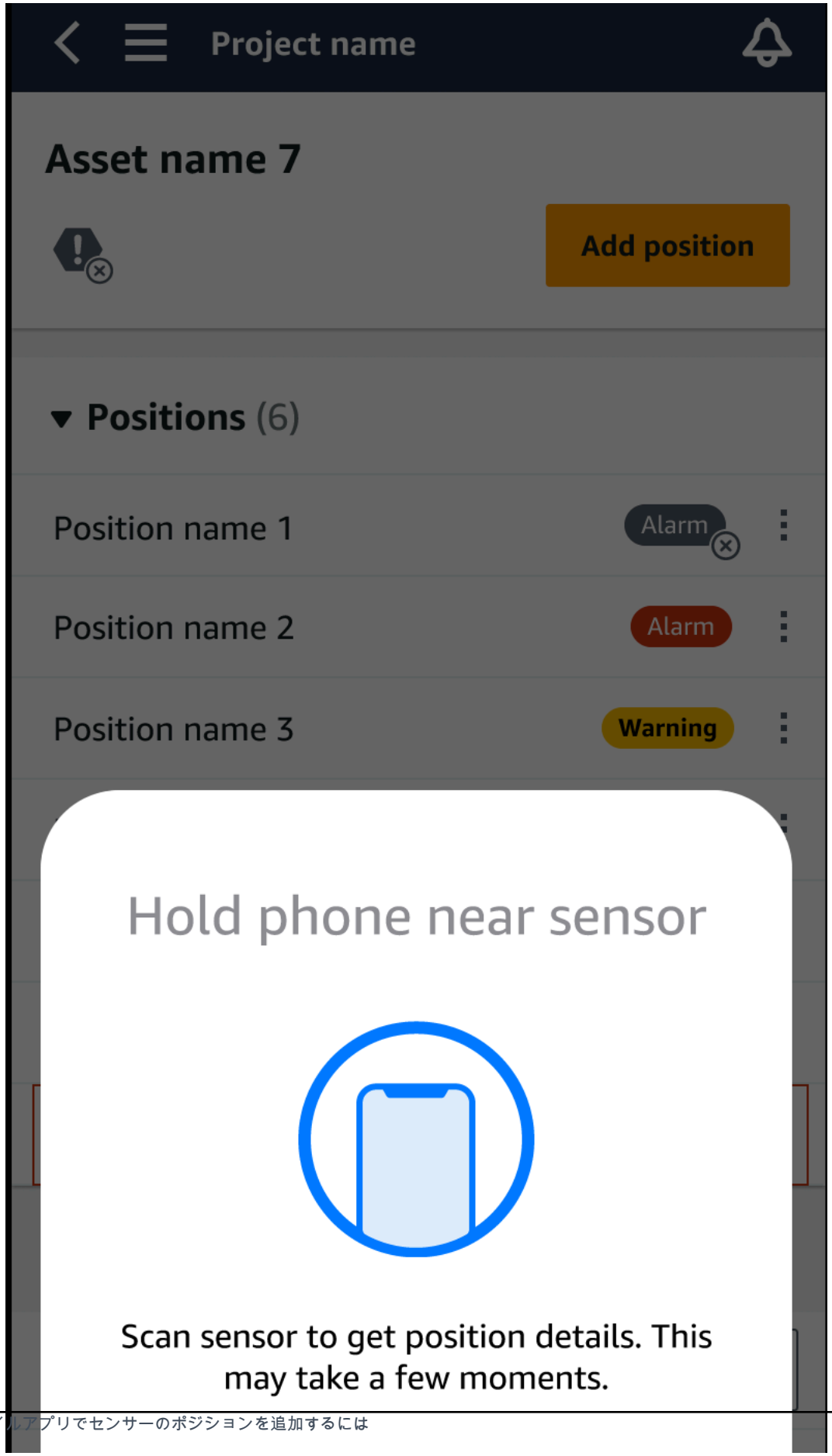
2. [ポジションを追加] ボタンを選択します。


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

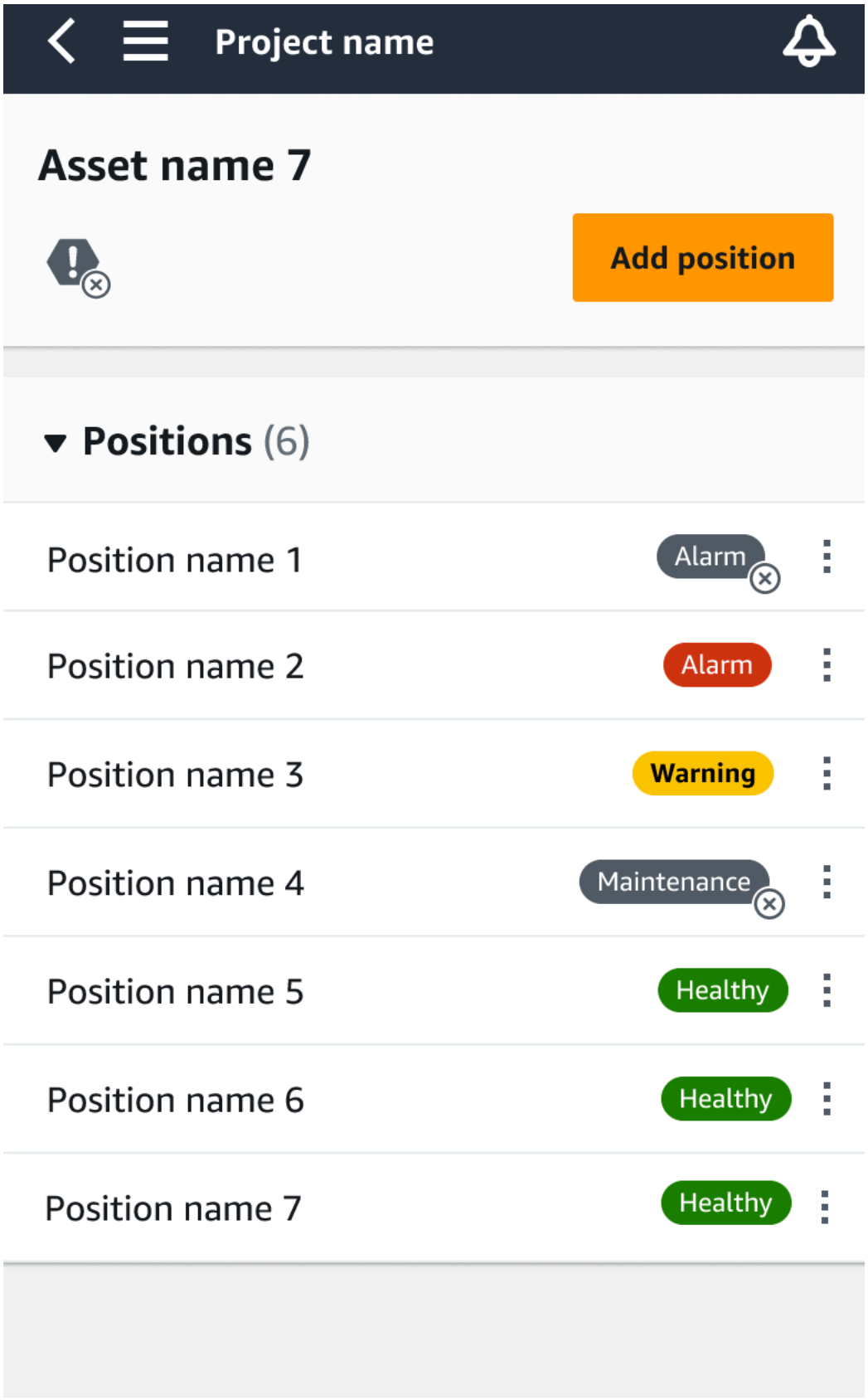
3. 表示されたダイアログボックスで、[ポジション名]、[ポジションのタイプ]、[機械のクラス] を入力します。



4. [Next (次へ)] を選択します。
5. モバイルデバイスでセンサーを再スキャンし、ポジションを保存します。


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. ポジションがアセットに追加されます。



センサーをアセットにペアリングする

アセットを追加したら、1 つ以上のセンサーとペアリングして状態をモニタリングします。各センサーはアセットのそれぞれの位置に取り付けられます。アセットに取り付けられた各センサーには、それぞれ機械クラスを割り当てることができます。

センサーをアセットとペアリングすると、ポジションのタイプが記録されます。位置のタイプは、そのセンサーのデータを分析するときに位置を評価する Amazon Monitron 方法を に指示します。各ポジションによって、アセットの見方が大きく異なる可能性があります。多くの場合、大規模なアセットの状態を明確に把握するには、複数の場所を監視する必要があります。1 つのアセットに最大 20 か所、センサーを配置できます。それほど複雑ではないアセットでは、1 つか 2 つのセンサーのみを必要とする場合もあります。

各センサーは、設置された場所で温度と振動を測定します。ポジションには任意の名前を付けることができ、必要に応じて後で名前を変更することもできます。例えば、前の例でポンプを監視するように設定されたセンサーでは、ポジションのタイプが「Pump」の「左ポジション」とすることができます。位置名は位置を識別し、位置タイプはモニタリングするアセットの Amazon Monitron どの部分を指示します。各センサーに割り当てられた機械のクラスを編集することもできます。

センサーの配置場所の詳細については、「センサーの配置」を参照してください。

> **Important**
>
> センサーをアセットにペアリングすると、 はその位置のベースライン Amazon Monitron を確立します。ベースラインは、アセットが通常の条件下でどのように動作 Amazon Monitron するかを示します。 はこの情報 Amazon Monitron を使用して異常な状態を特定します。この間、 は条件が正常であり、アラームを生成しないこと Amazon Monitron を前提としています。

トピック

- センサーをアセットにペアリングするには

センサーをアセットにペアリングするには

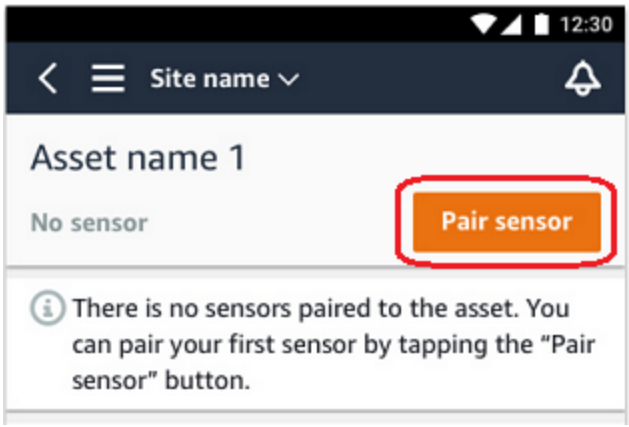
1. 近距離無線通信 (NFC) がスマートフォンでオンになっていることを確認します。

> **Tip**
>
> 多くのスマートフォンモデルでは、デフォルトで NFC がオンになっています。NFC をオンにする必要があるかどうか、またその方法については、次の資料を参考にしてください。
>
> - NFC (サムスン) とは
> - NFC タグリーダー (iPhone) をサポートしているモデル

2. [アセット] リストからアセットを選択します。

   - アセットを作成したばかりの場合:

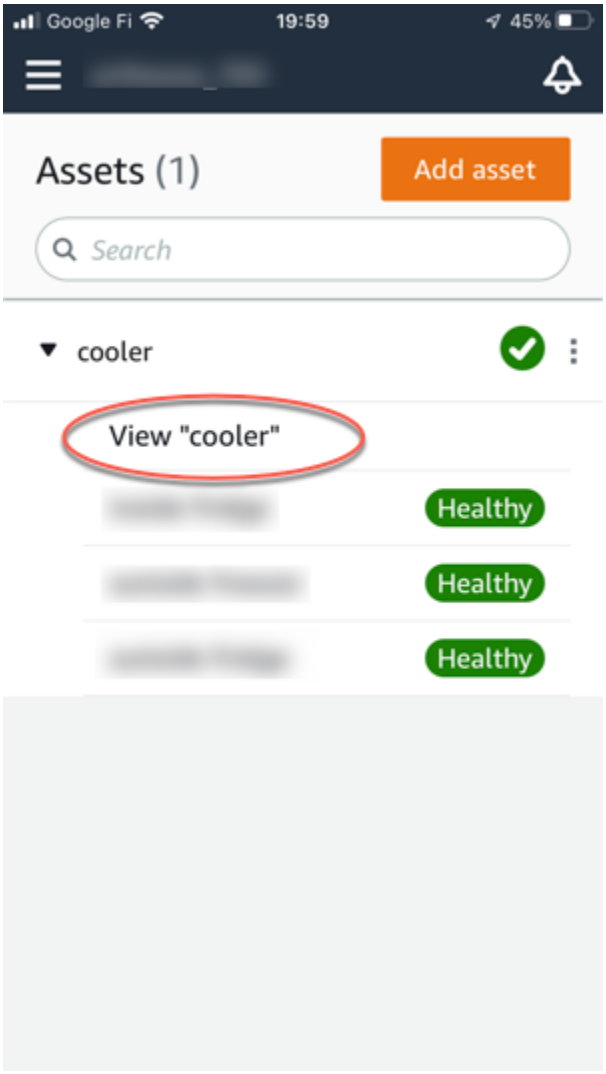
     [ポジションを追加] を選択します。

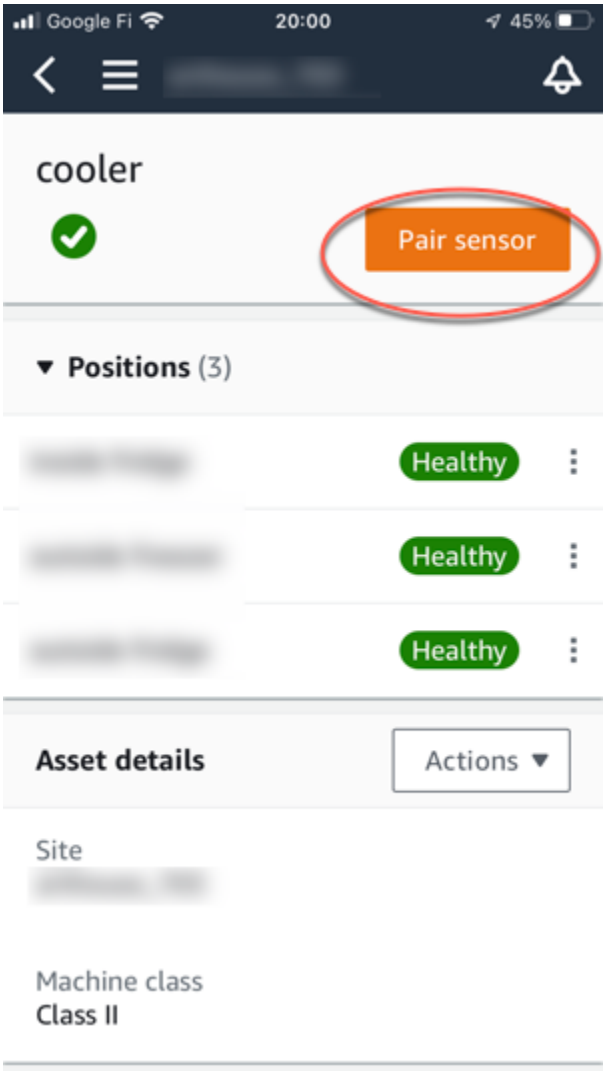
   - 以前にアセットを作成し、すでに複数のセンサーとペアリングしている場合:

     a. アセットを選択すると、そのアセットに関連するセンサーのドロップダウンリストが表示されます。

        リスト上部にある [表示] オプションを選択します。



b. [センサーをペアリング] をクリックします。



3. センサーを機械の正しい位置に配置します。センサーのペアリングに関する詳細については、「センサーの配置」および「センサーを取り付ける」を参照してください。
4. センサーが監視する位置に名前を付けます。

   わかりやすく、扱いやすい名前を使用することをお勧めします。
5. [ポジションのタイプ]では、ポジションの種類を選択します。

   有効な値:

   - ベアリング
   - コンプレッサー
   - ファン
   - ギアボックス

- モーター
- ポンプ
- その他

> **Note**
>
> センサーをアセットにペアリングした後は、ポジションのタイプを変更することはできません。タイプの変更が必要な場合は、センサーを削除して追加し直す必要があります。

6. [機械のクラス]では、センサーを配置するアセット部品の機械のクラスを選択します。有効なオプションは ISO 20816 規格に基づきます。

   クラス I

   エンジンや機械の個々の部品を、通常の運転状態で機械全体に一体的に接続します。例えば、最大 15 キロワット (kW) または 20 馬力 (hp) の生産用電気モーターなど。

   クラス II

   特別な基礎を持たない中型機械 (通常、出力が 15 ~ 75 kW (20 ~ 101 hp) の電気モーター)、特別な基礎の上に強固に取り付けられたエンジンまたは機械 (最大 300 kW または 402 hp)。

   クラス III

   振動方向において比較的堅い、強固で重い基礎に取り付けられた回転質量を持つ大型の原動機やその他の大型機械。

   クラス IV

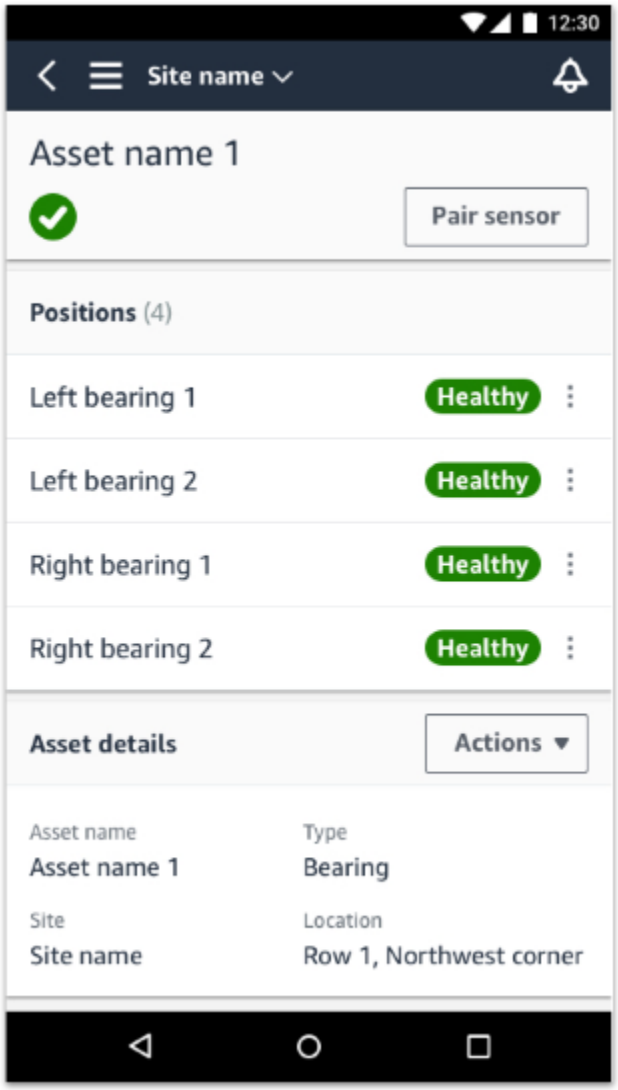
   振動測定の方向は比較的柔らかく、強固で重い基礎に取り付けられた、回転質量を持つ大型原動機やその他の大型機械。例えば、出力が 10 メガワット (MW) または 13,404 hp を超えるターボ発電機セットやガスタービンなど。

7. [Next (次へ)] を選択します。
8. スマートフォンをセンサーに近づけてコミッショニングします。センサーのコミッショニング中は、スマートフォンを動かさないでください。

がセンサーをコミッショニングし、ペアリング Amazon Monitron するまでに少し時間がかかる場合があります。接続中に、以下のメッセージが表示されます。

> **Note**
>
> ペアリング中にモバイルデバイスを適切に保つ方法は、お使いのモバイルデバイスの種類によって異なります。詳細については、「Amazon Monitron デバイスの問題のトラブルシューティング」を参照してください。

複数のセンサーが特定のアセットとペアリングされている場合、[アセット] ページには各センサーのポジションとその状態が表示されますが、各ポジションの詳細は表示されません。詳細を表示するには、リストからポジションを選択します。各アセットでモニタリングできるデータの詳細については、「センサーの測定値について」を参照してください。



ポジションはステータス順に表示されます。例えば、アラーム状態のポジションは、確認済みポジションの上に表示されます。健全な状態のポジションは、確認済みポジションのあとに表示されます。

センサーのポジション名を変更する

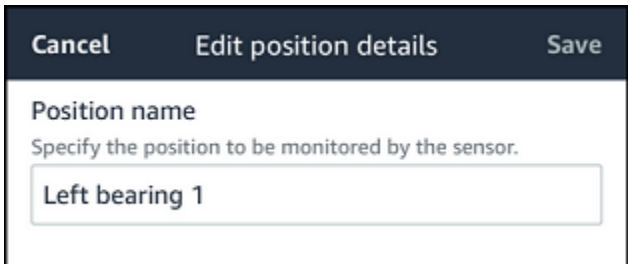
トピック

- モバイルアプリでセンサーのポジション名を変更する

- ウェブアプリでセンサーのポジション名を変更する

モバイルアプリでセンサーのポジション名を変更する

1. [アセット] リストから、名前を変更するセンサーポジションがあるアセットを選択します。
2. 名前を変更するポジションのセンサーを選択します。
3. [センサーの詳細] タブを選択します。
4. [ポジションの詳細] で [アクション] を選択します。
5. [ポジションの詳細を編集] を選択します。
6. [ポジション名] に新しい名前を入力します。

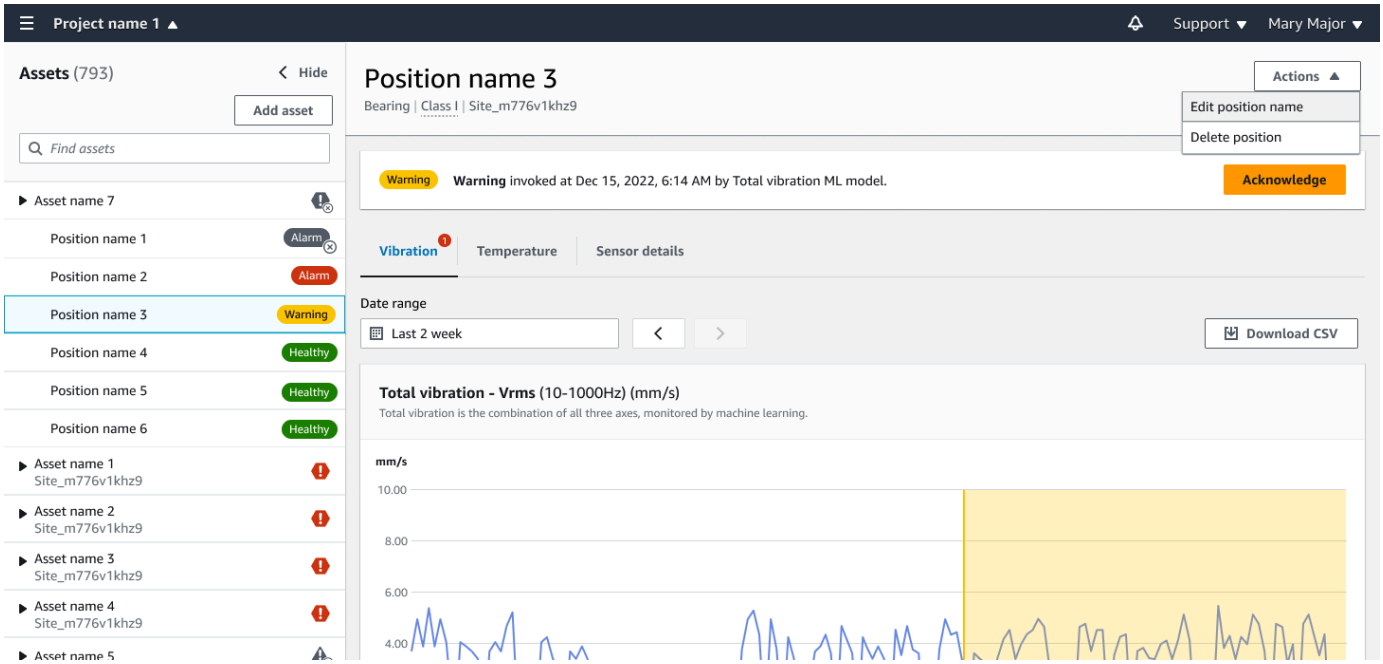


7. [Save] を選択します。

ウェブアプリでセンサーのポジション名を変更する

1. ポジションを選択します。

   [ポジション] テーブルの [アクション] ボタンを選択します。



2. [ポジション名を編集] を選択します。
3. [ポジション名] に新しい名前を入力します。
4. [Save] を選択します。

機械のクラスを編集する

センサーの機械クラスは、モバイルアプリとウェブアプリの両方で、[アセットの詳細] セクション、または [ポジションの詳細] セクションから編集できます。

センサーの機械クラスを編集すると、更新された機械クラスに基づくアセットの状態アラートは、更新後の次の測定から有効になります。

> **Important**
>
> センサーの機械クラスに未解決のアラートがある場合、そのセンサーの機械クラスは編集できません。機械のクラスを編集する前に、すべてのアラートを解決する必要があります。

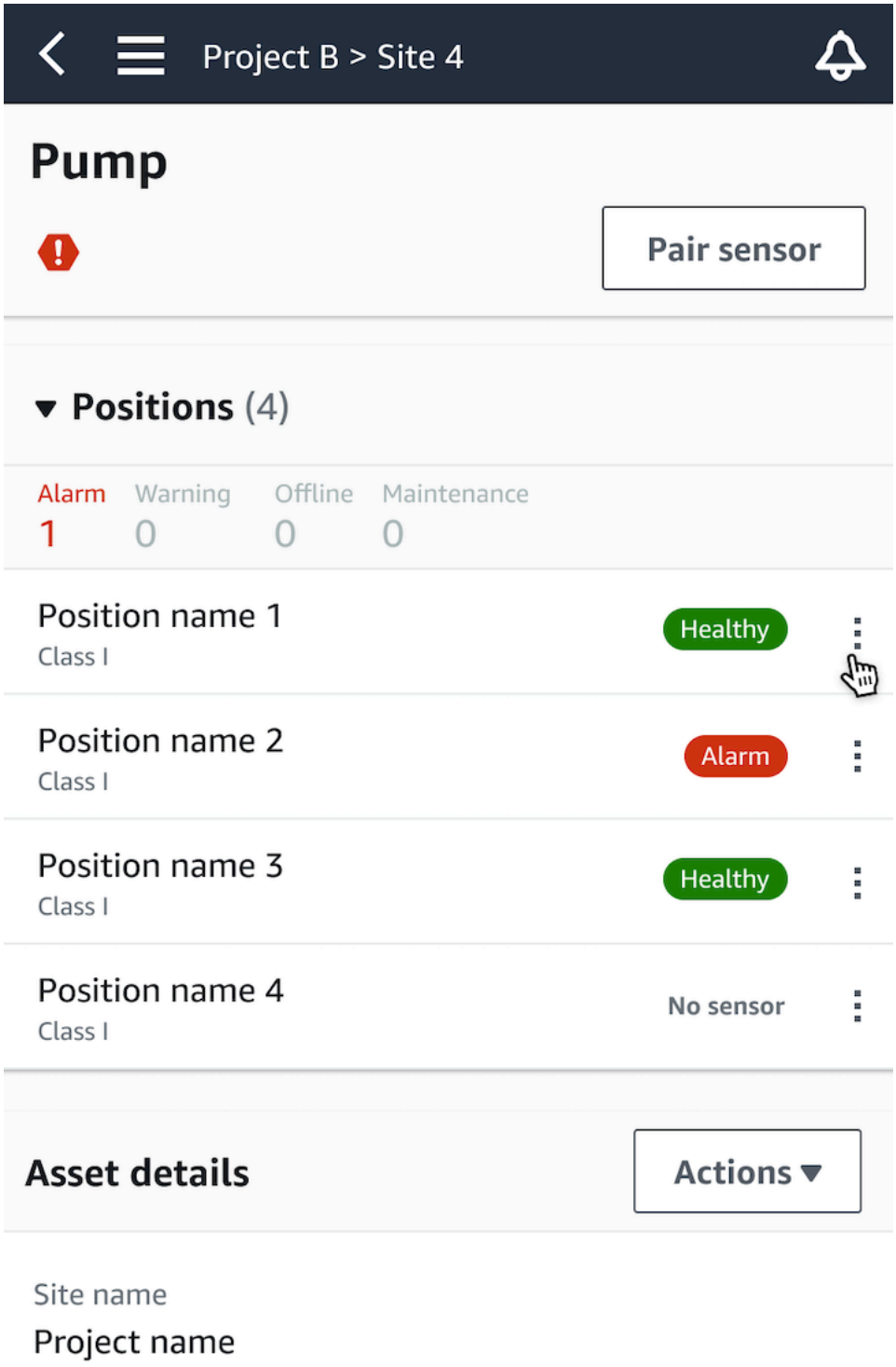
トピック

- モバイルアプリで機械のクラスを編集するには
- ウェブアプリで機械のクラスを編集するには

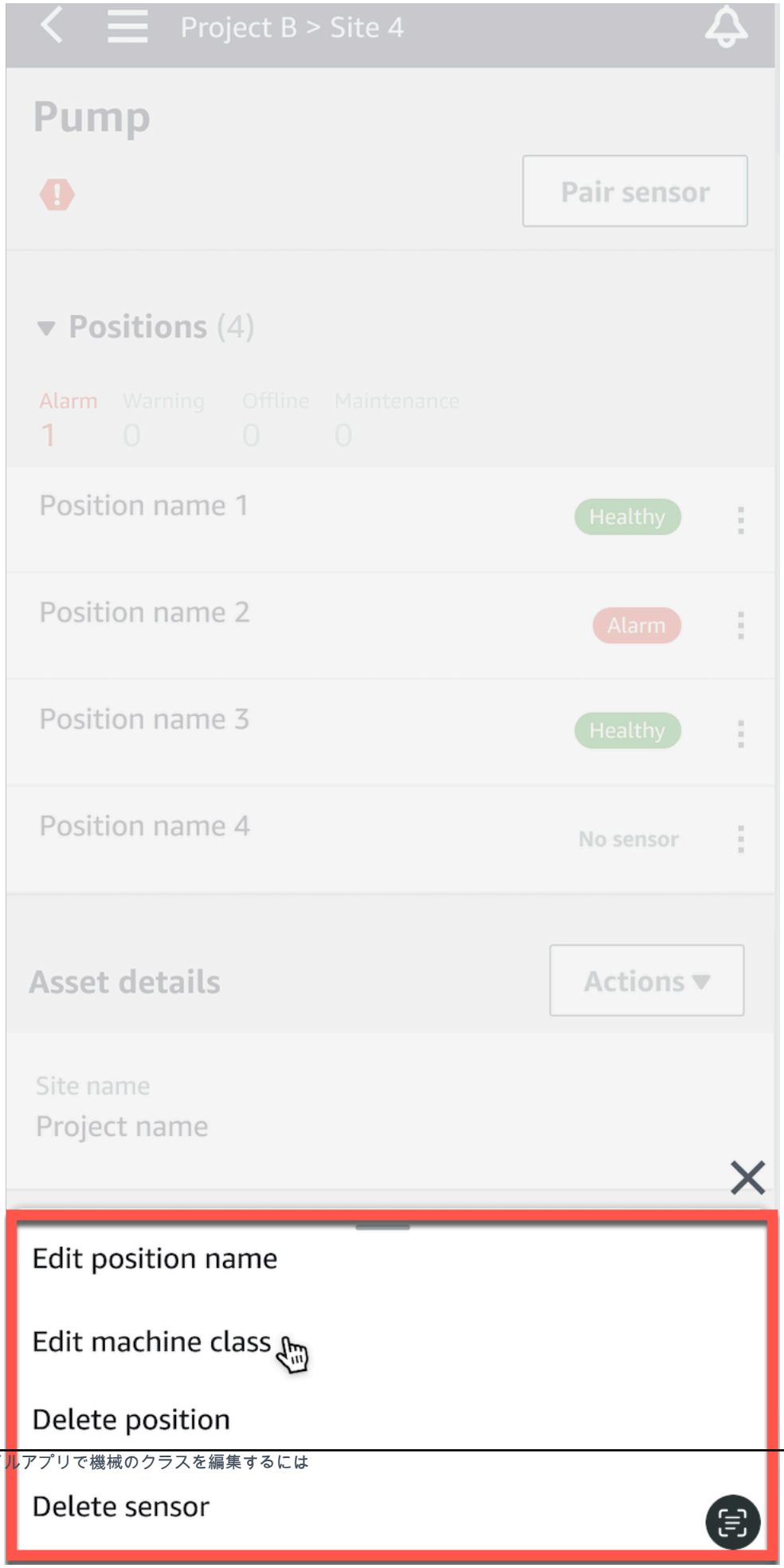
- ポジションの詳細ページから機械クラスを編集するには

モバイルアプリで機械のクラスを編集するには

1. [アセット] リストから、編集したいセンサーポジションのアセットを選択します。
2. [ポジション] リストから、機械クラスを変更するポジションのセンサーを選択します。
3. センサーの詳細を確認します。



4. 表示されるオプションから、[機械のクラスを編集] を選択します。

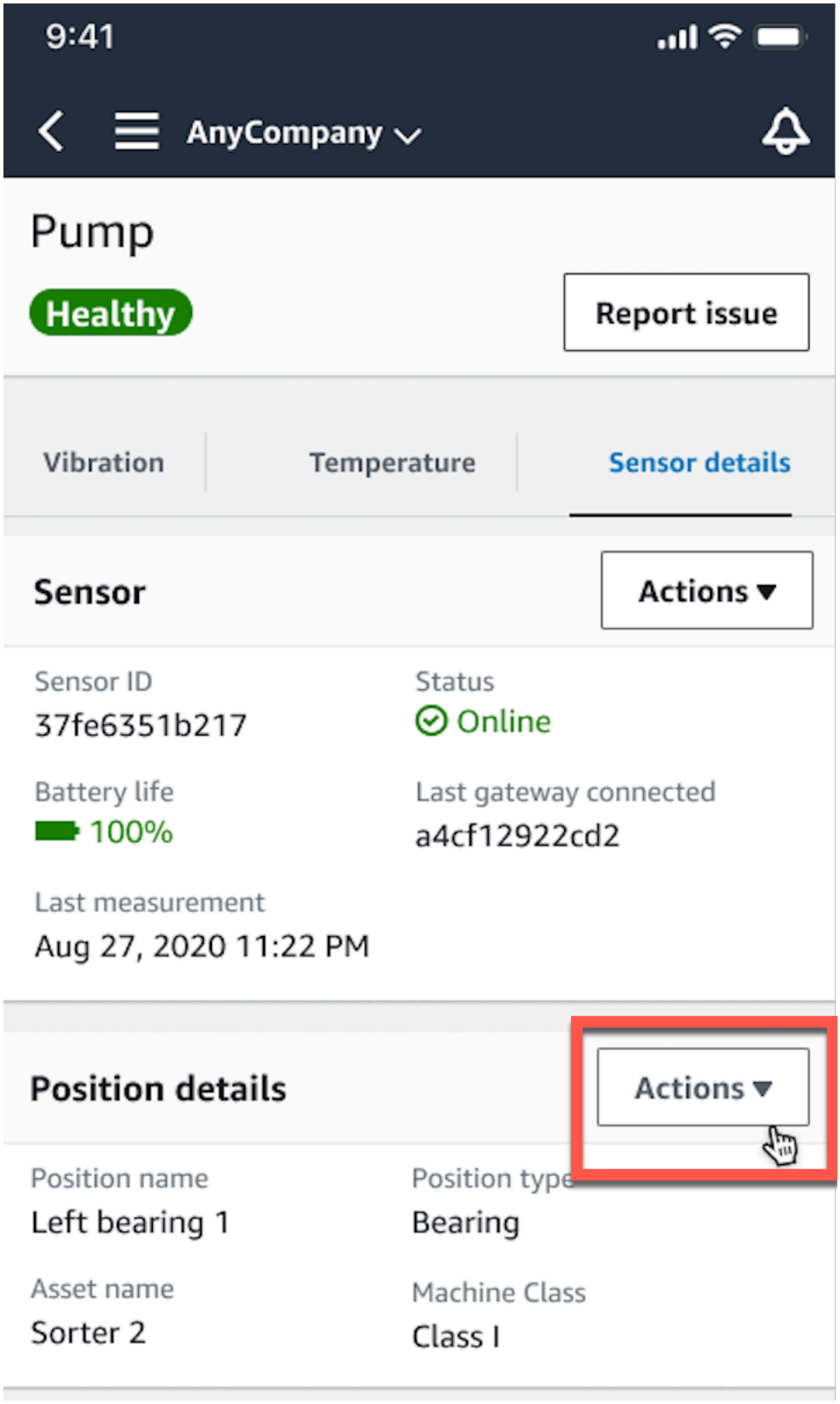

Project B > Site 4
Pump
Pair sensor
Positions (4)
Alarm
1
Warning
0
Offline
0
Maintenance
0
Position name 1
Healthy
Position name 2
Alarm
Position name 3
Healthy
Position name 4
No sensor
Asset details
Actions
Site name
Project name
Edit position name
Edit machine class
Delete position
Delete sensor

5. [機械のクラスを編集] から、センサーに割り当てる新しい機械のクラスを選択します。[保存] を選択します。

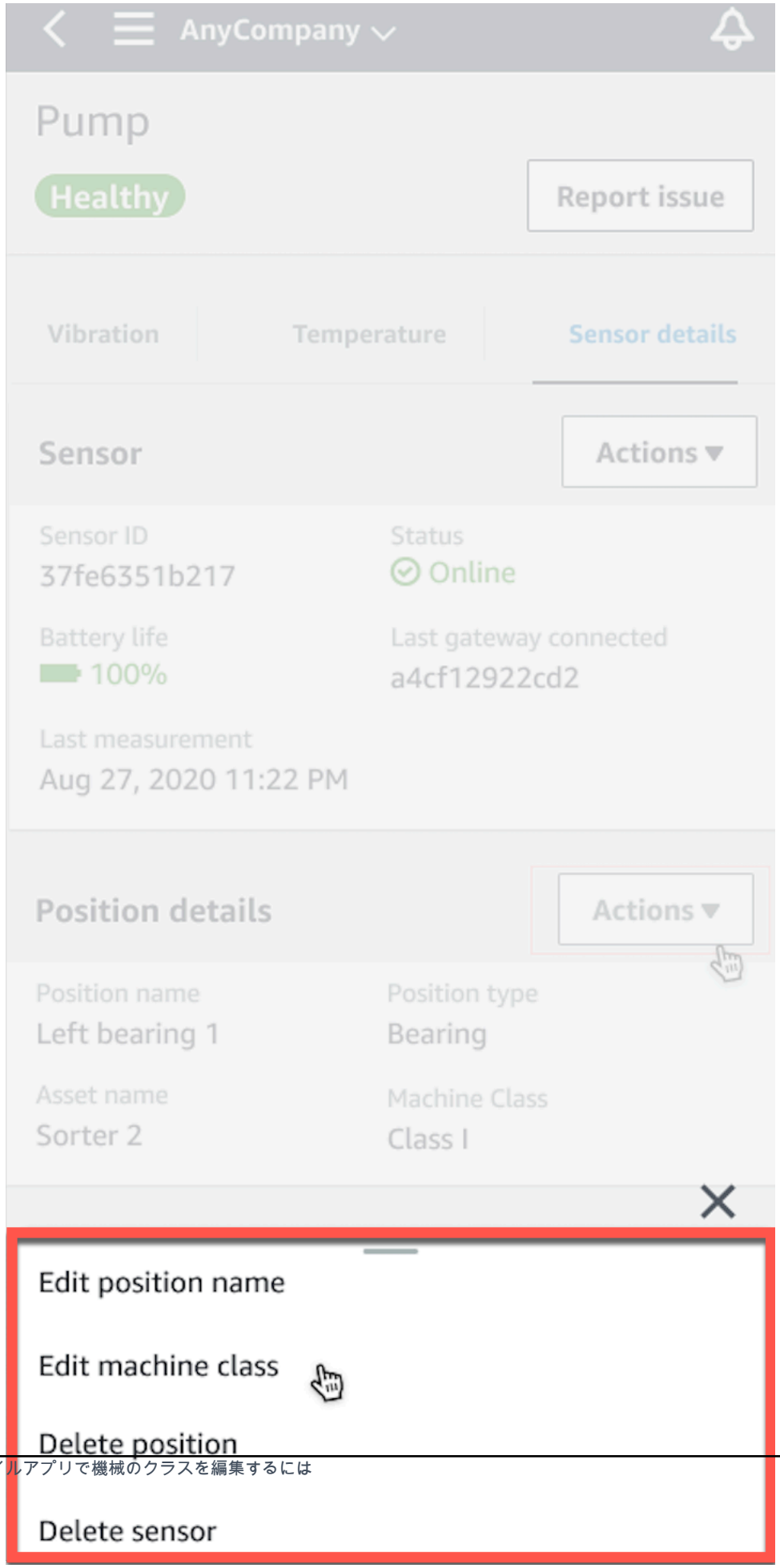
> **Note**
>
> 新しい機械クラスは、次の測定区間で有効になります。単軸チャートのしきい値が更新されます。

ポジションの詳細ページから機械クラスを編集するには

1. [ポジションの詳細] リストから [アクション] タブを選択します。



2. 表示されるオプションから、[機械のクラスを編集] を選択します。

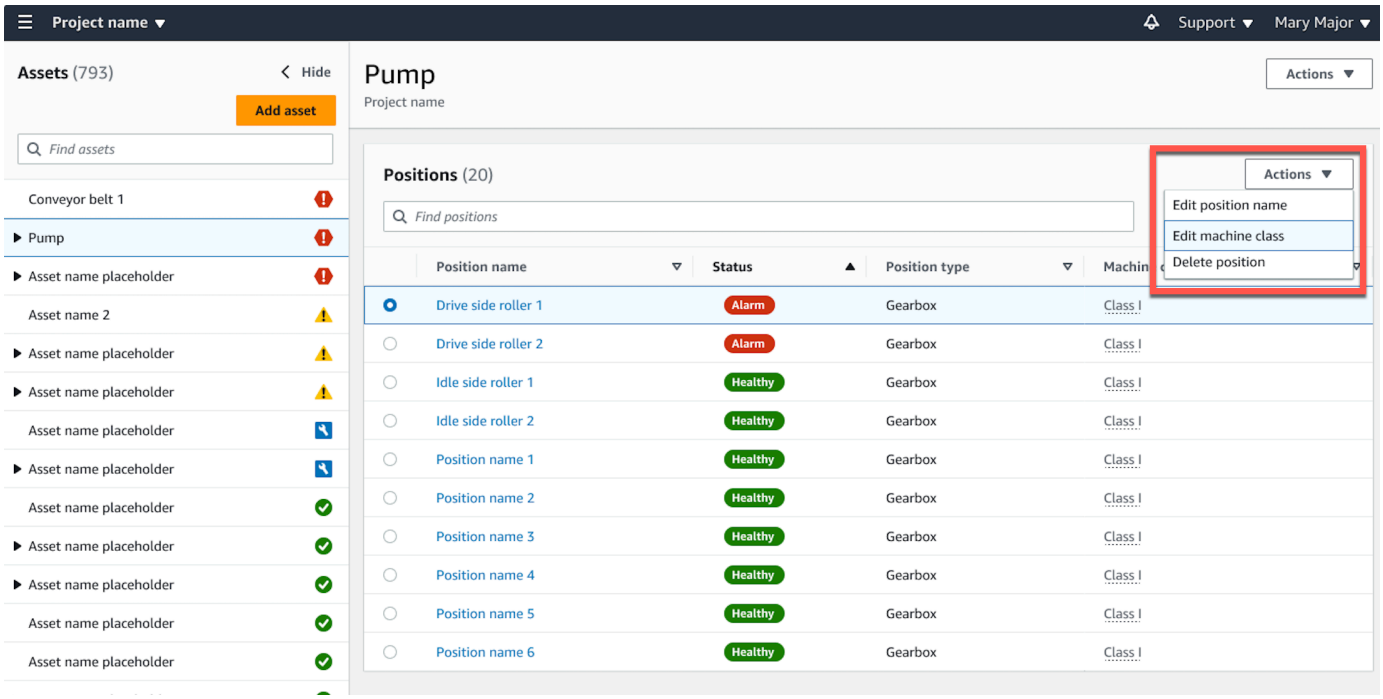

AnyCompany
Pump
Healthy
Report issue
Vibration
Temperature
Sensor details
Sensor
Actions
Sensor ID
37fe6351b217
Status
Online
Battery life
100%
Last gateway connected
a4cf12922cd2
Last measurement
Aug 27, 2020 11:22 PM
Position details
Actions
Position name
Left bearing 1
Position type
Bearing
Asset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

3. [機械のクラスを編集] メニューから、センサーに割り当てる新しい機械のクラスを選択します。[Next (次へ)] を選択します。

> **Note**
>
> 新しい機械クラスは、次の測定区間で有効になります。単軸チャートのしきい値が更新されます。

ウェブアプリで機械のクラスを編集するには

1. [アセット] テーブルから、[アクション] ボタンを選択します。
2. オプションから、[機械のクラスを編集] を選択します。

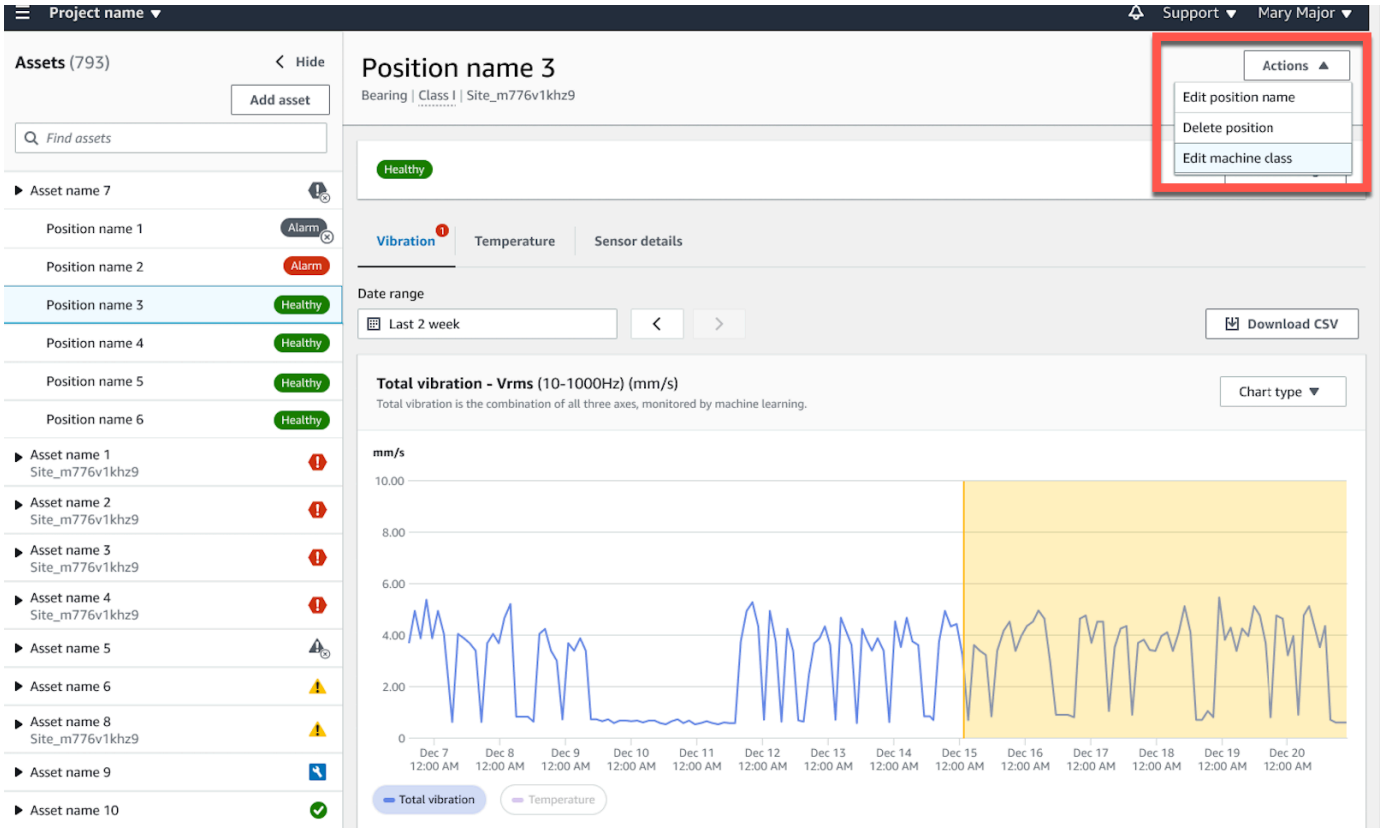


3. [機械のクラスを編集] メニューから、センサーに割り当てる新しい機械のクラスを選択して、[変更を保存] を選択します。

> **Note**
>
> 新しい機械クラスは次の測定区間から有効になり、ポジションの状態に反映されます。単軸チャートのしきい値が更新されます。

ポジションの詳細ページから機械クラスを編集するには

1. [ポジション] テーブルから、[アクション] ボタンを選択します。
2. オプションから、[機械のクラスを編集] を選択します。



3. [機械のクラスを編集] メニューから、センサーに割り当てる新しい機械のクラスを選択して、[変更を保存] を選択します。

> **Note**
>
> 新しい機械クラスは、次の測定区間で有効になります。単軸チャートのしきい値が更新されます。

センサーを削除する

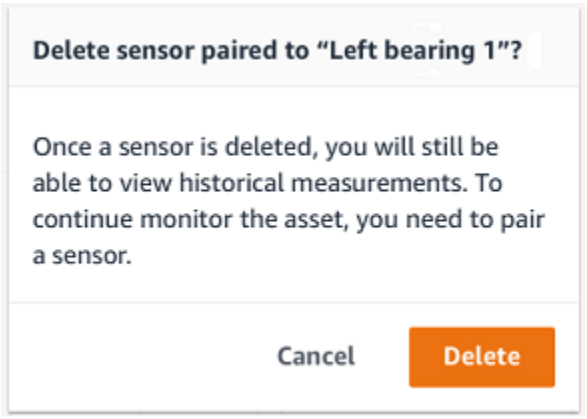
センサーを削除すると、 Amazon Monitron はそれを使用してより多くのデータを収集できなくなります。すでに収集されたデータは削除されません。

トピック

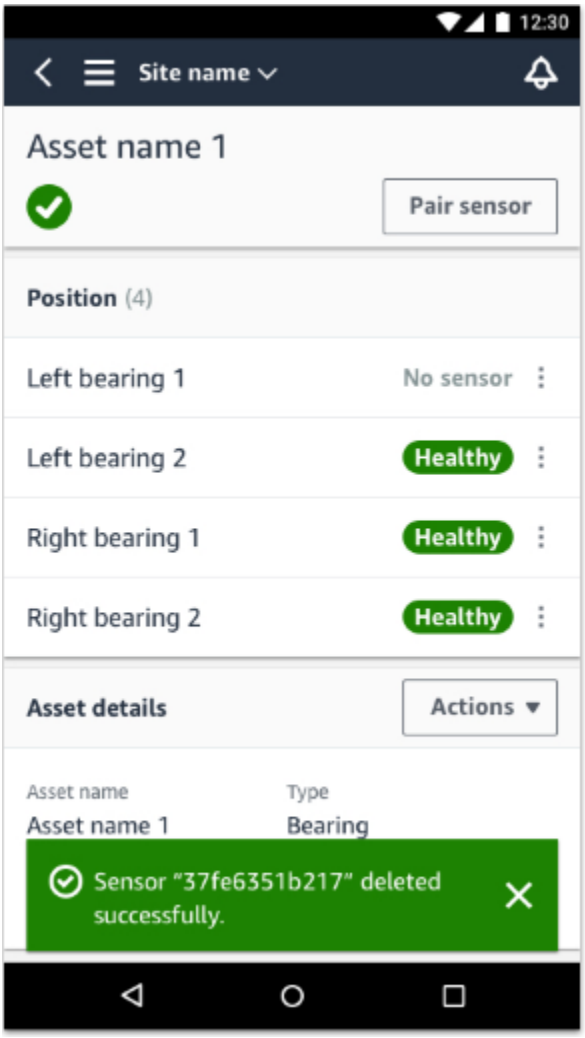
- モバイルアプリでセンサーを削除するには
- ウェブアプリでセンサーを削除するには

モバイルアプリでセンサーを削除するには

1. [アセット] リストから、削除するセンサーとペアリングされているアセットを選択します。
2. センサーを選択します。
3. [センサー] で [アクション] を選択します。
4. [センサーを削除] を選択します。
5. [削除] を選択します。

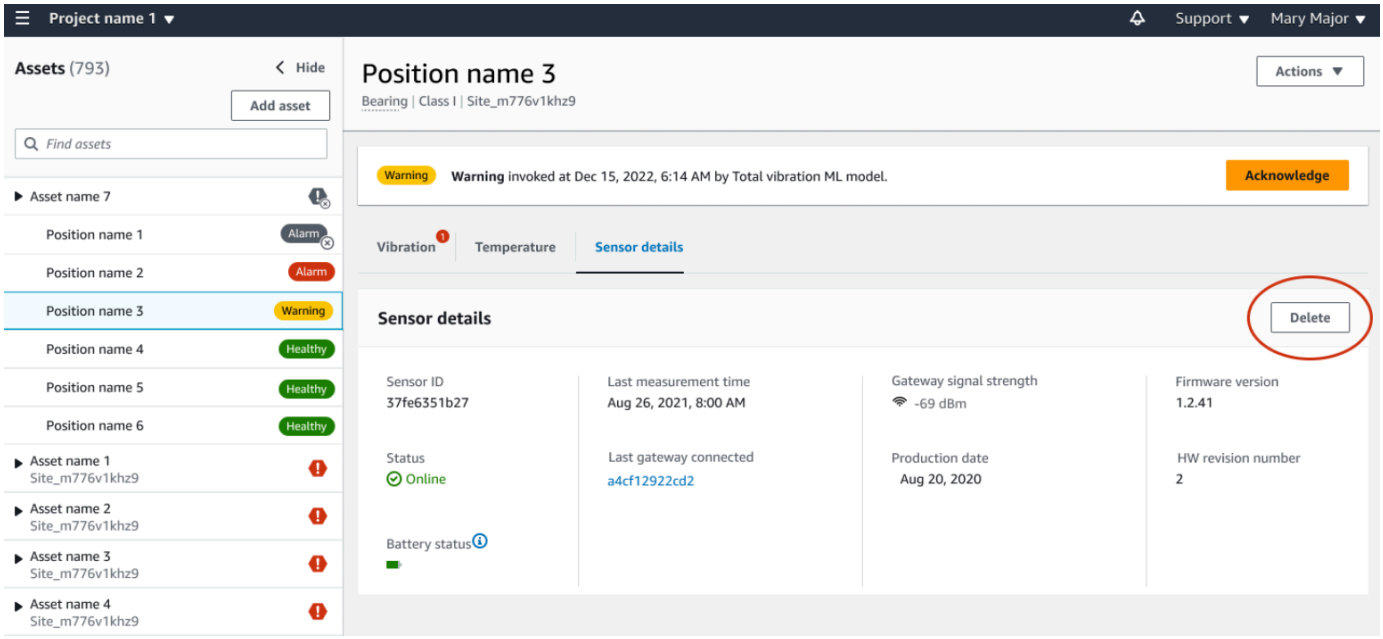


センサーが削除されると、そのポジションのステータスは[センサーなし]となります。



ウェブアプリでセンサーを削除するには

- [センサーの詳細] タブから [削除] を選択します。



センサーポジションを削除する

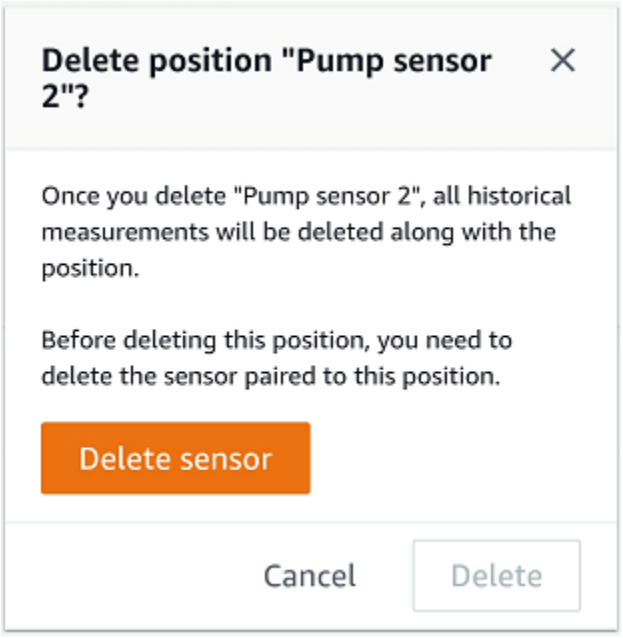
センサーポジションを削除すると、そのデータの収集ポイントがアセットから削除されます。このポジションにセンサーがまだペアリングされている場合は、ポジションを削除する前にセンサーを削除する必要があります。

トピック

- モバイルアプリでセンサーポジションを削除するには
- ウェブアプリでセンサーポジションを削除するには

モバイルアプリでセンサーポジションを削除するには

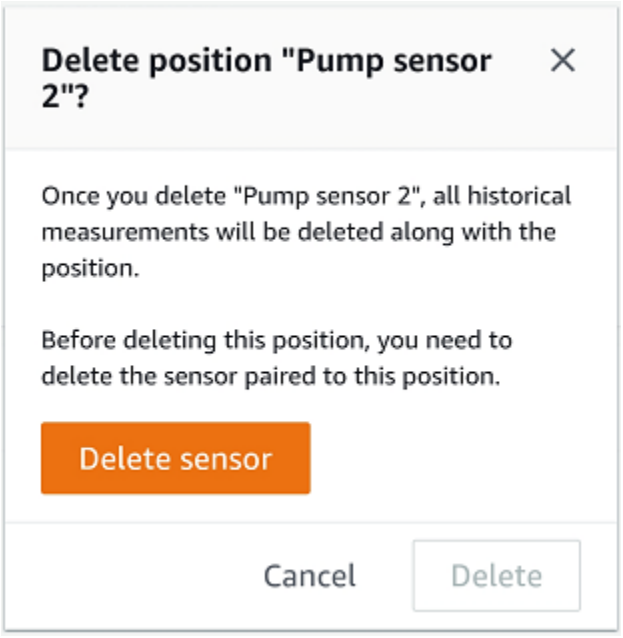
1. [アセット] リストから、削除するセンサーポジションを持つアセットを選択します。
2. [センサー] で [アクション] を選択します。
3. [ポジションを削除] を選択します。
4. ポジションにセンサーがペアリングされている場合は、[センサーを削除] を選択してセンサーを削除します。それ以外の場合は、次のステップに進みます。



5. [削除] を選択します。

ウェブアプリでセンサーポジションを削除するには

1. ポジションを選択します。
2. [ポジション] テーブルの [アクション] ボタンを選択します。
3. [ポジションを削除] を選択します。
4. ポジションにセンサーがペアリングされている場合は、[センサーを削除] を選択してセンサーを削除します。それ以外の場合は、次のステップに進みます。



5. [削除] を選択します。

センサーの詳細を理解する

センサーが期待どおりに動作していることを確認するには、センサーの詳細ページを確認してください。[センサーの詳細] ページでは、以下の情報が表示されます。

- センサー ID
- センサーのステータス
- センサーが最後にコミッショニングされた日付
- 最後に測定した日付
- 最後に接続したゲートウェイ
- 最後に接続したゲートウェイの現在の信号強度
- センサータイプ
- ファームウェアバージョン
- センサーのバッテリーステータス

トピック

- センサーの詳細を表示する
- センサーの接続ステータス

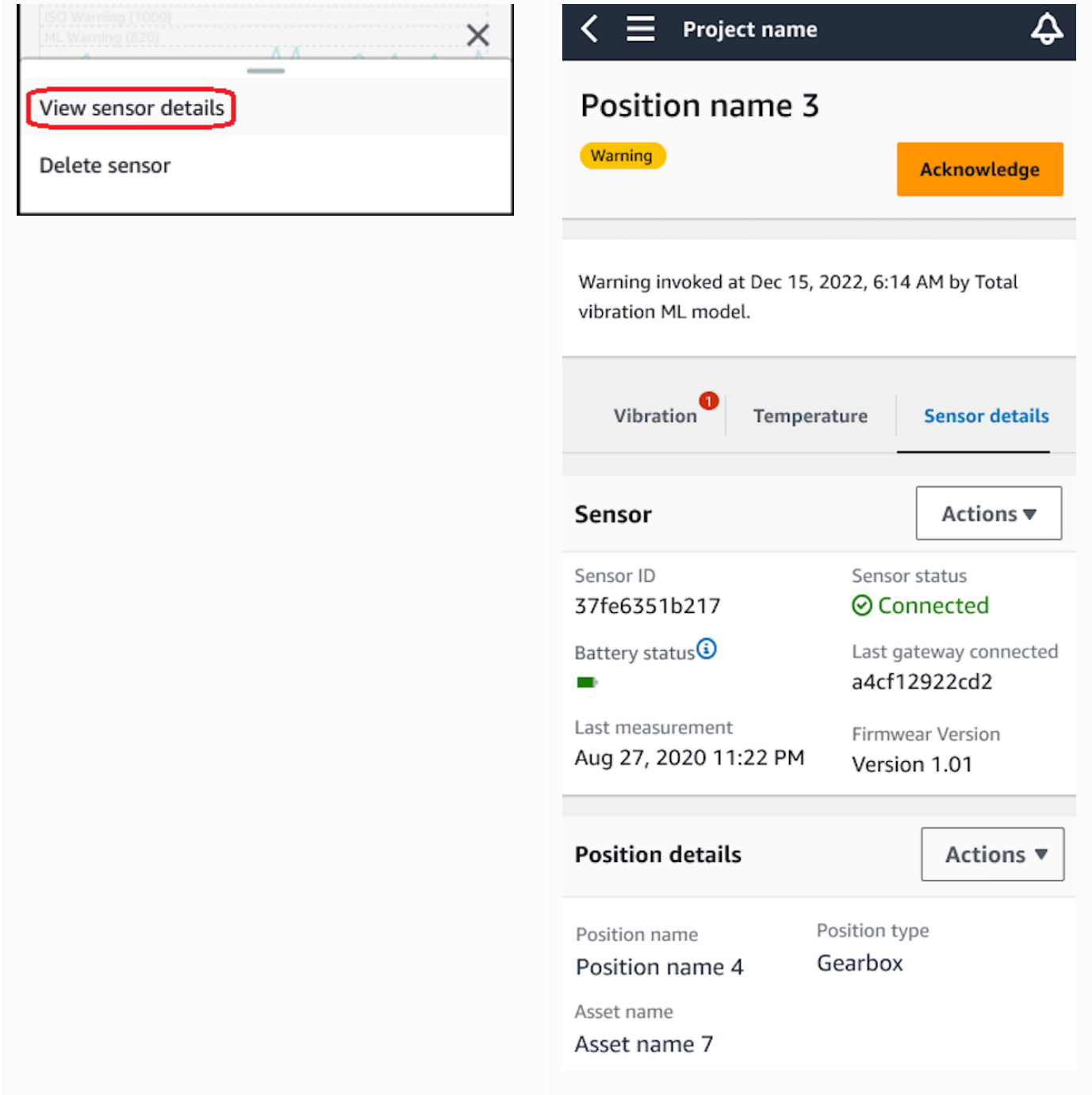
- センサーのバッテリーステータス

センサーの詳細を表示する

センサーの詳細は、モバイルアプリとウェブアプリの両方で確認できます。次のセクションでその確認方法について説明します。

モバイルアプリでセンサーの詳細を表示するには

1. [アセット] リストから、確認するセンサーとペアリングされているアセットを選択します。
2. センサーを選択します。
3. 確認するセンサーに接続されている[ポジション]を選択します。
4. [センサーの詳細] タブを選択します。
5. [センサーのアクション] ボタンを選択します。
6. [センサーの詳細を表示] を選択します。

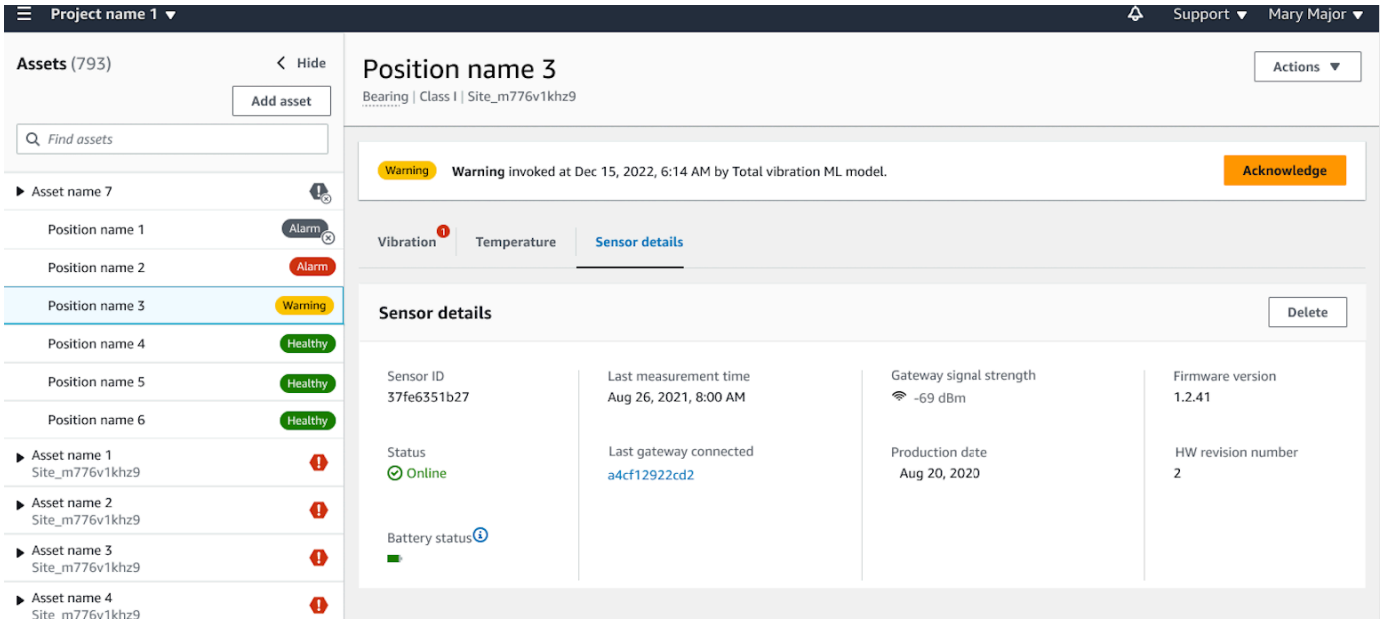


[センサーの詳細] ページが表示されます。

ウェブアプリでセンサーの詳細を表示するには

1. [アセット] リストから、確認するセンサーとペアリングされているアセットを選択します。

2. センサーに関する情報は、アプリウィンドウの右下にある [センサーの詳細] タブに自動的に表示されます。



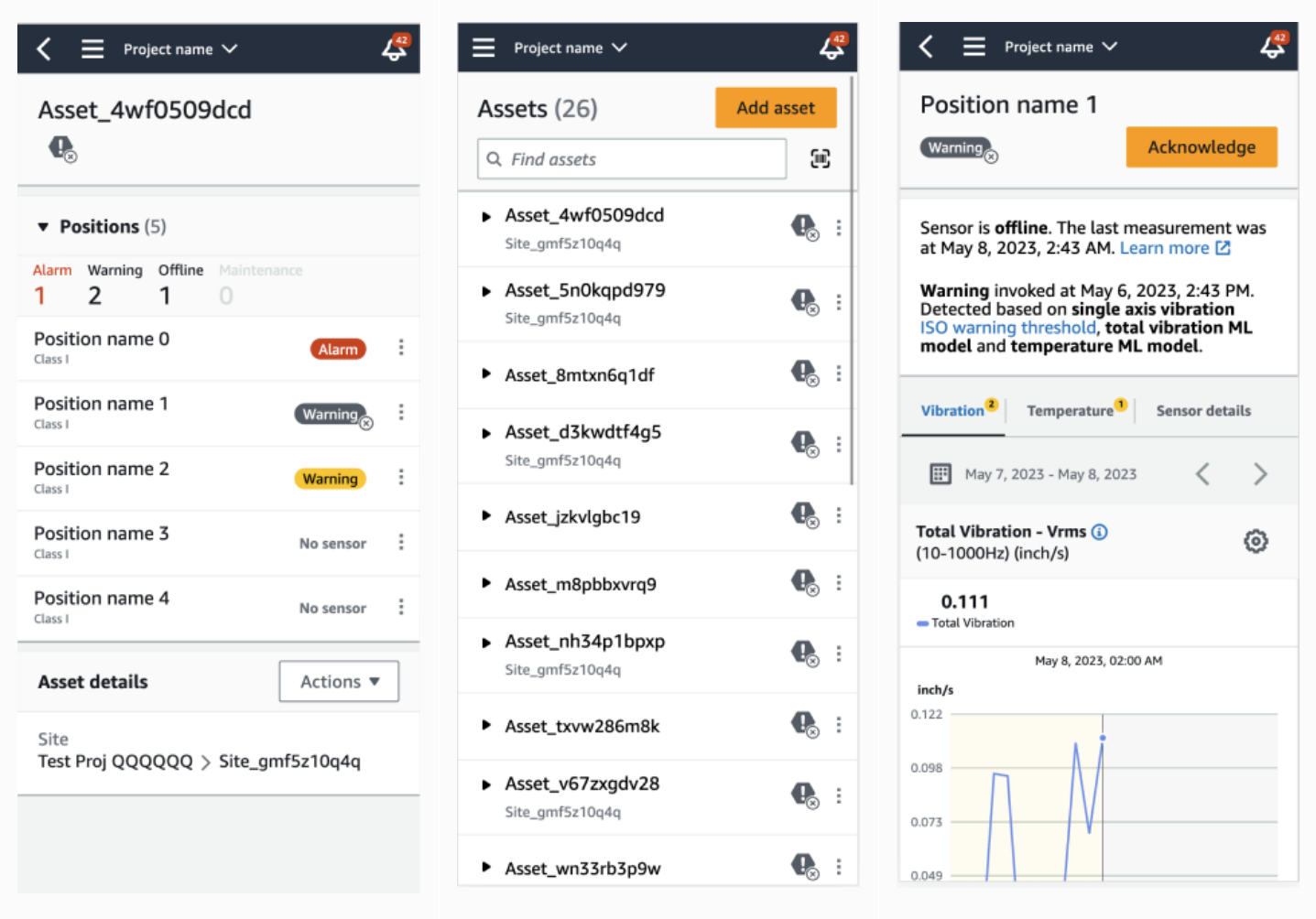
センサーの接続ステータス

センサーを作成すると、Amazon Monitron のアセットリストでセンサーのポジションとその接続状態をモニタリングできます。センサーポジションのステータスには、[正常/メンテナンス/警告/アラーム] があり、センサーの接続ステータスには、[オンライン/オフライン] があります。デフォルトのセンサーステータスは [オンライン] です。接続の問題でタイムアウトになると、ステータスは [オフライン] に変わります。接続が回復すると、センサーステータスは [オンライン] に戻ります。センサーはオフラインになっても最新の状態を維持します。

アセットリストにあるアセットのバッジには、重要度の高いポジションと接続状態が表示されます。そのポジションに [警告] と [正常] の両方のステータスが含まれている場合、アセットリストには [警告] ステータスが表示されます。少なくとも 1 つのアセットが [オフライン] の場合、そのアセットは、アセットリストで [オフライン] ステータスになります。

> **Note**
>
> センサーが [オフライン] の場合、そのステータスは Amazon Monitron アプリケーションのアセットリストで優先されます。アプリではセンサーがオフラインになった場合の通知はサポートされませんが、デバイスがオフラインになるとアプリで通知されます。

次の図は、オフライン状態のセンサーを示しています。



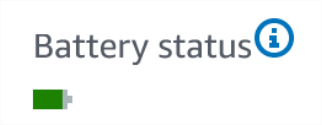
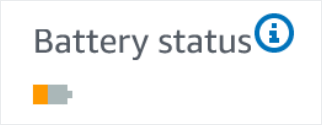
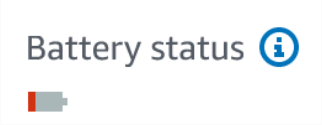
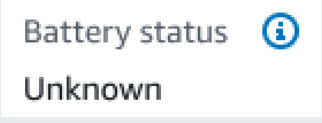
センサーのバッテリーステータス

センサーの状態を追跡しやすくするために、 にはセンサーのバッテリー残量ステータス Amazon Monitron が表示されます。センサーのバッテリー寿命は、モバイルアプリとウェブアプリの両方で確認できます。このバッテリーステータスを利用することで、新しいセンサーを購入する時期を検討することができます。

> **Note**
>
> 推定バッテリー残量は、1 時間ごとに測定を行うセンサーの 5 年間のセンサーバッテリー寿命に基づいて計算されます。

> **Important**
>
> バッテリー寿命ステータスは、ファームウェアバージョンが 1.6.0 以前のセンサーには表示されません。バッテリー寿命ステータスを確認するには、センサーが更新されるまで待つ必要があります。

次の表に、センサーの各バッテリーステータスを示します。

バッテリーステータス	条件	残り時間	アクション
	ノーマル	センサーのバッテリーは正常な状態です。	現在、センサーのバッテリー監視は不要です。
	低	バッテリーの寿命は残り 1 年未満です。	センサーバッテリーの監視を開始してください。
	緊急	バッテリーの寿命は残り 3 か月未満です。	できるだけ早くセンサーを交換してください。
	不明	バッテリー寿命の状態が不明です。	1. センサーを初めてコミッショニングする場合は、センサーが最初の測定値を送信するまで 1 分ほどお待ちください。

バッテリーステータス	条件	残り時間	アクション
			2. 次に、ゲートウェイを正しくコミッショニングしたことを確認し、モバイルアプリを使用して測定を行います。 詳細については、「Gateways」と「Taking a one-time measurement」を参照してください。

> **Note**
>
> バッテリーステータスが [緊急] になった後、センサーを交換しないと、センサーの接続状態は [オフライン] に変わります。

センサーポジションを識別する

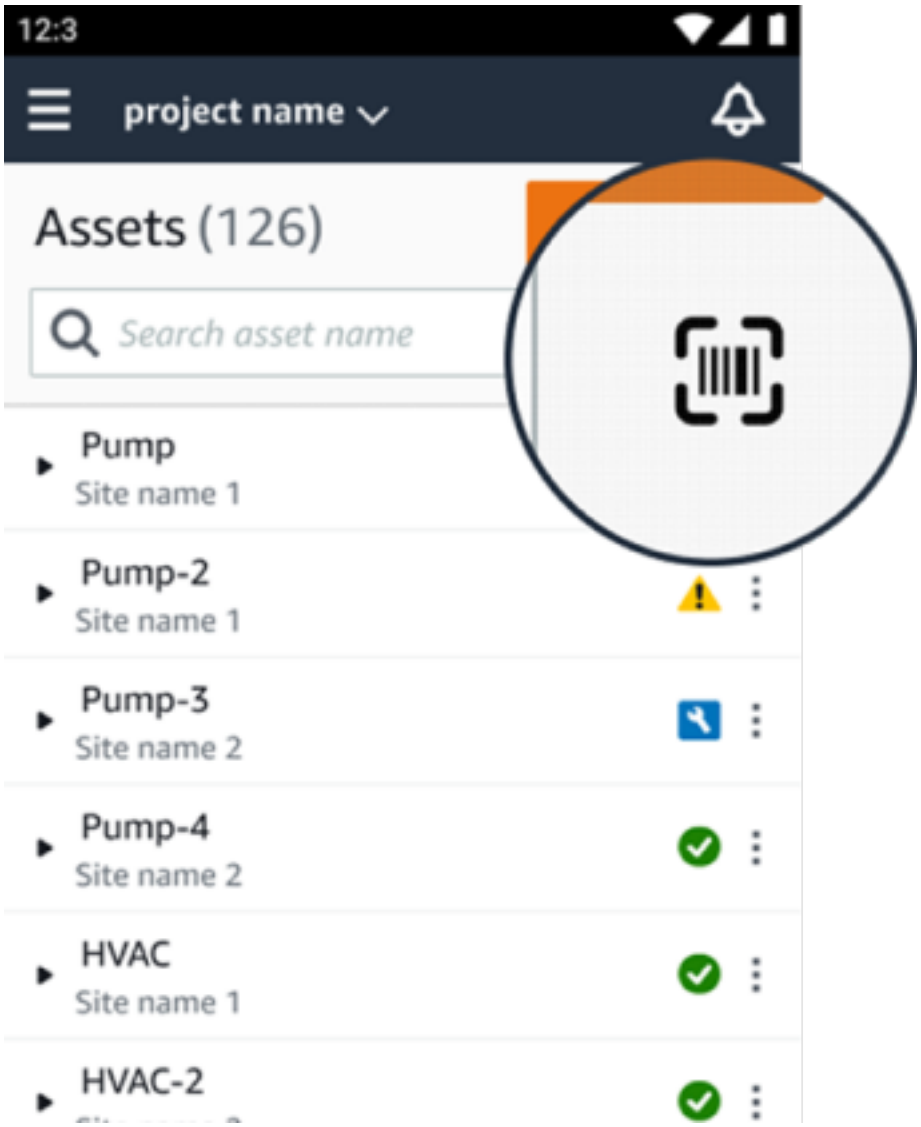
モバイルアプリを使えば、アセットリストを検索しなくても工場や現場のセンサーを検索することができます。

トピック

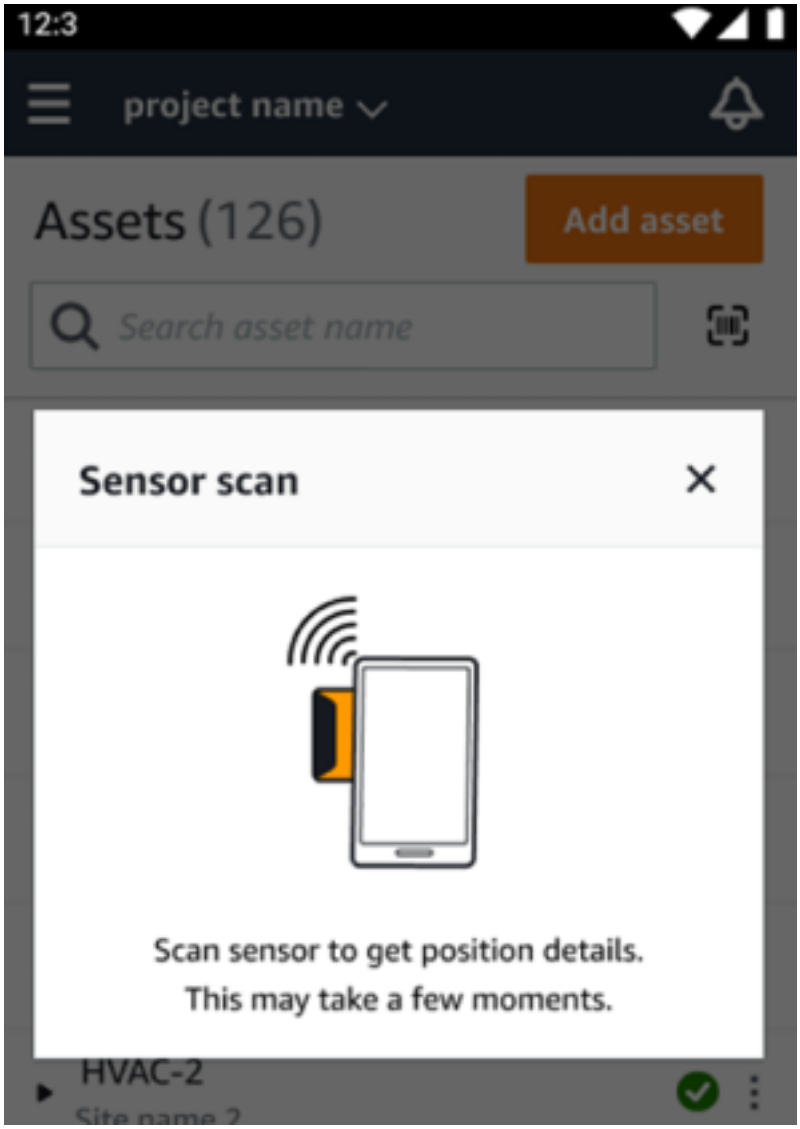
- ペアリングされたセンサーを識別する
- センサーが見当たらない、または読み取れない
- 権限とサイトコミッショニングの問題
- 別のサイトからセンサーをスキャンする

ペアリングされたセンサーを識別する

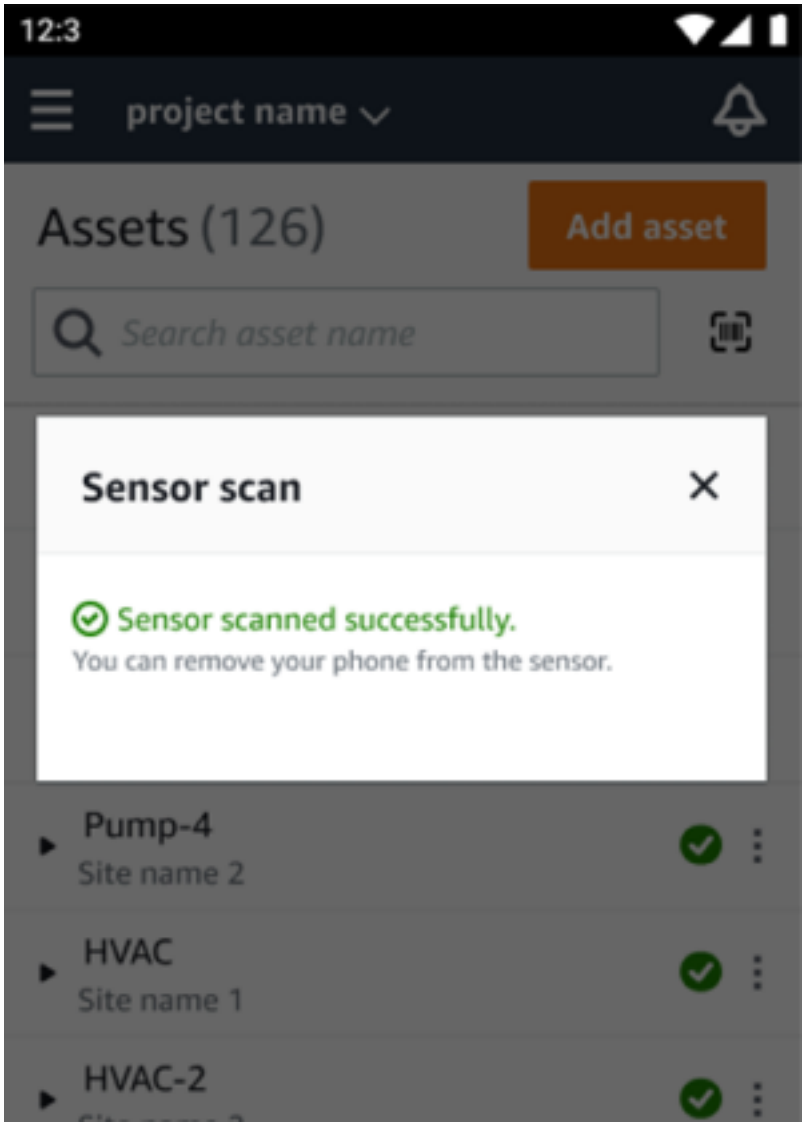
1. センサーがペアリングされている場合は、アセットページから [センサーのスキャン] アイコンを選択して、プロジェクトに関連するセンサーをスキャンします。



2. スキャンしたいアセットを選択します。
3. スマートフォンをセンサーに近づけてスキャンし、ポジションの詳細を読み取ります。モバイルアプリに結果が生成されるまでに、少し時間がかかる場合があります。

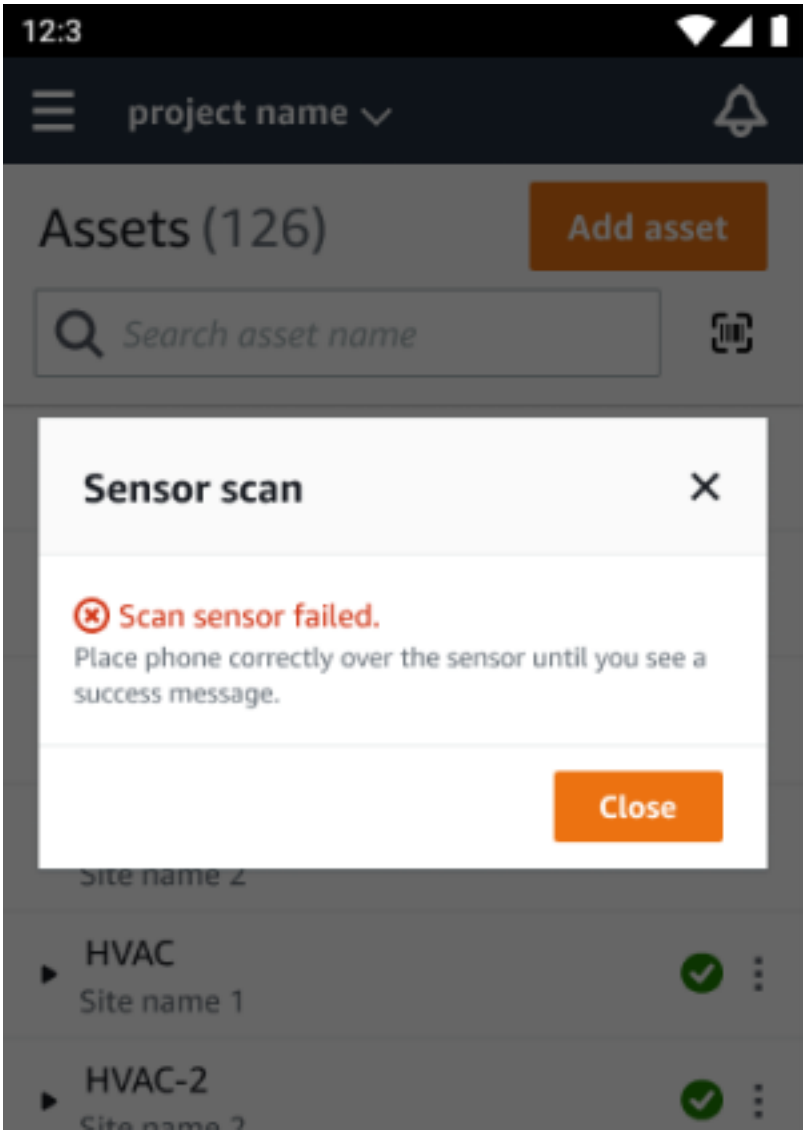


4. センサーのスキャンが完了すると、モバイルアプリにセンサーのポジションと詳細が表示されます。


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

センサーが見当たらない、または読み取れない

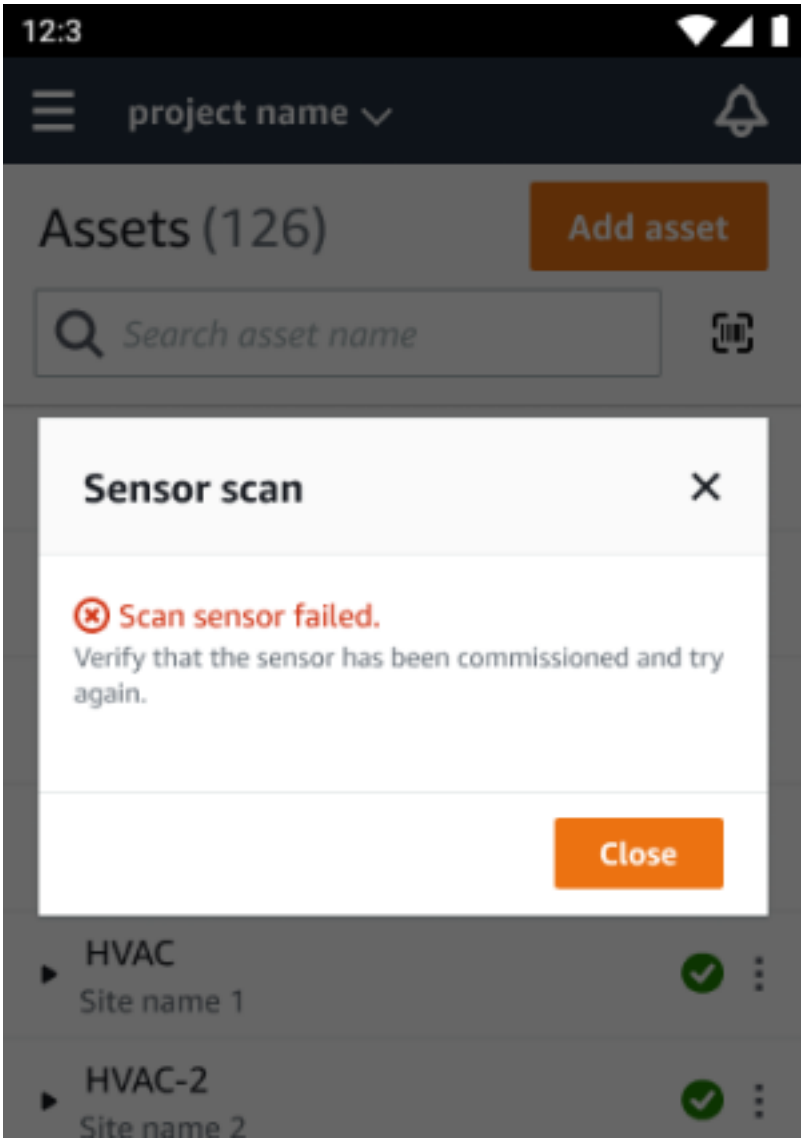
スキャン中にセンサーが読み取れない場合は、成功のメッセージが表示されるまでスマートフォンをセンサーの上に正しくかざしてください。



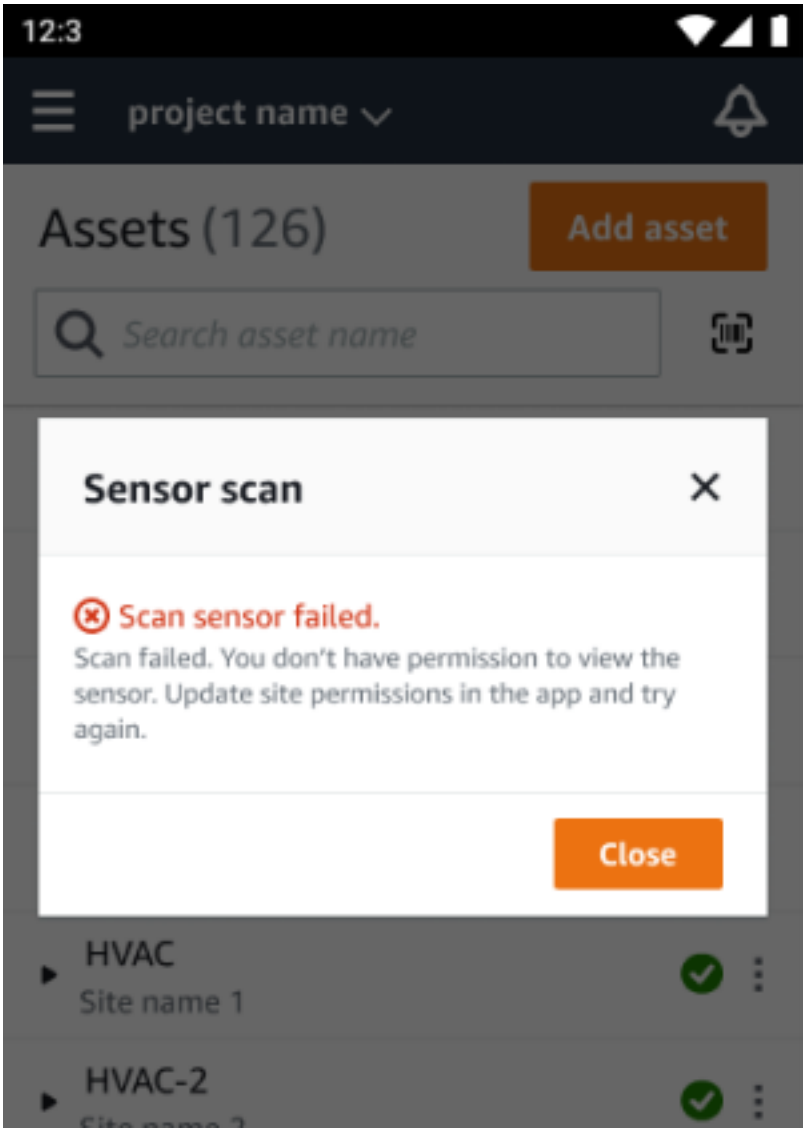
センサーが追加されなかった場合は、アセットを追加してやり直してください。

権限とサイトコミッショニングの問題

センサーがサイトにコミッショニングされていない場合は、センサーをコミッショニングしてからもう一度お試しください。

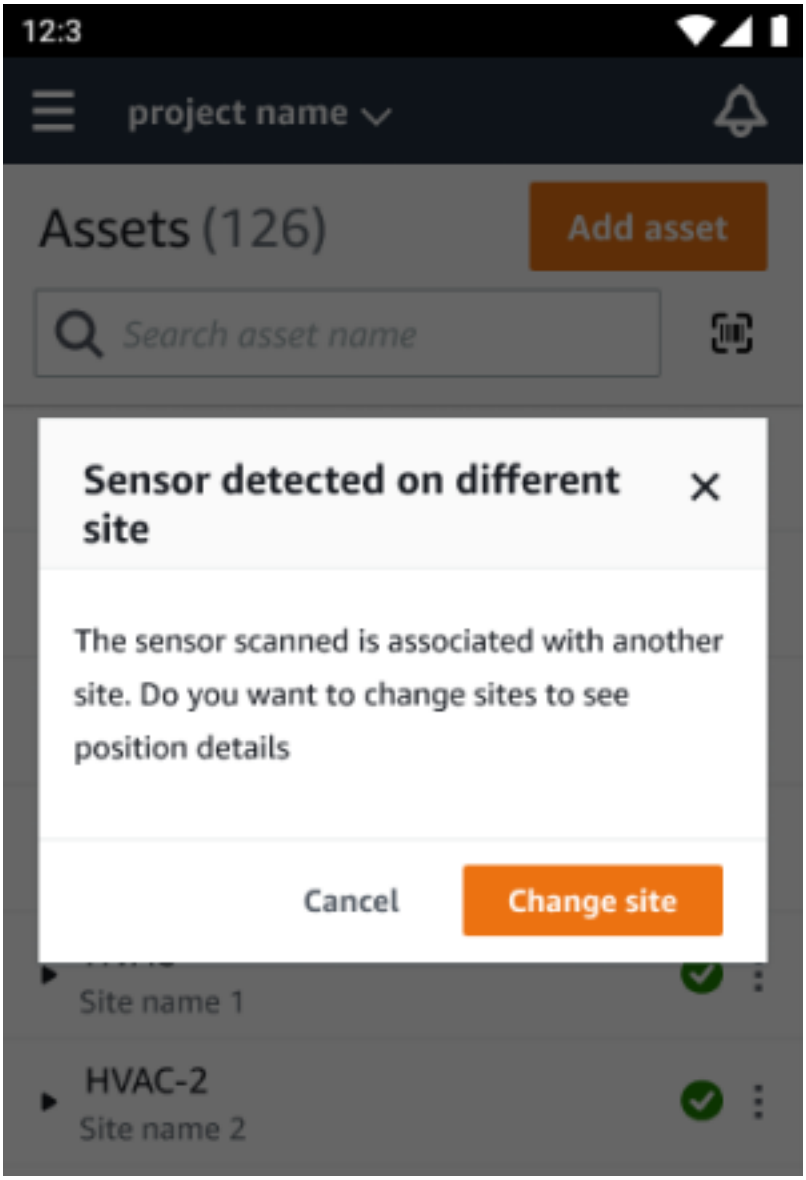


アクセスできないサイトにセンサーをコミッショニングした場合は、アプリのサイト権限を更新して、センサーポジションの詳細をもう一度読み取ってみてください。



別のサイトからセンサーをスキャンする

別のサイトにコミッショニングされたセンサーをスキャンし、そのサイトにリダイレクトされた場合は、そのサイトのセンサーをスキャンしてください。

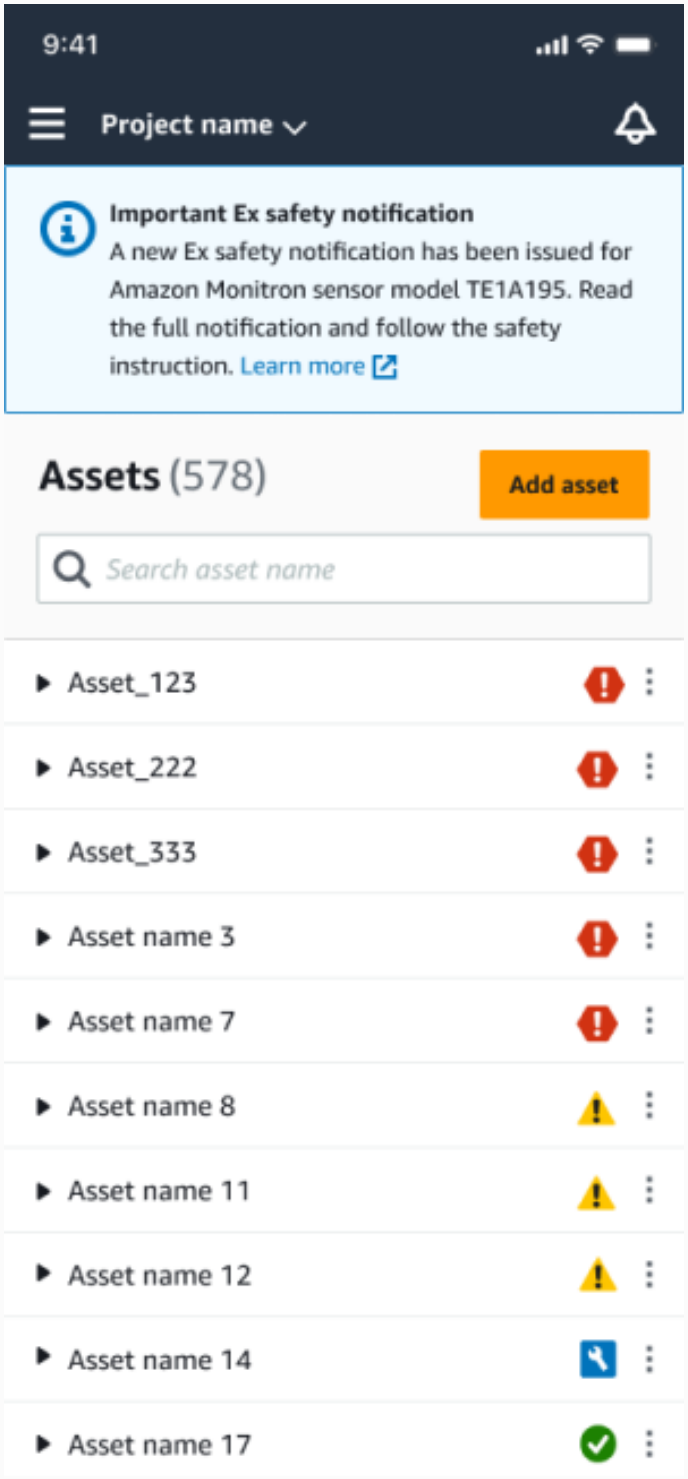


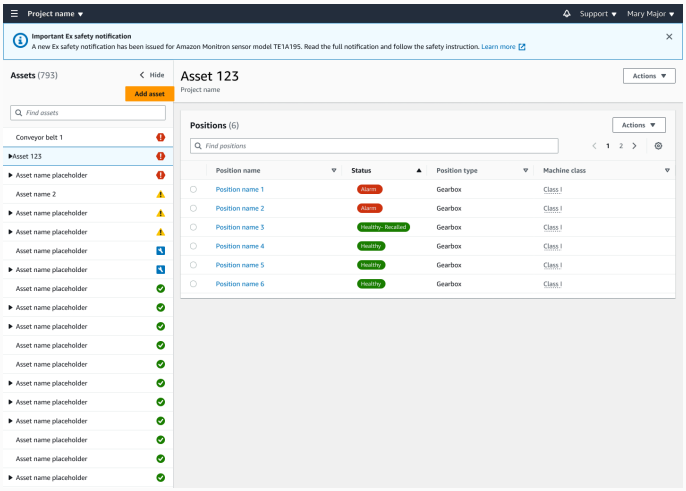
定格超過センサー

> **Warning**
>
> センサーをインストールして使用する前に、すべての警告と手順については、Ex Safety and Compliance Guide を参照してください。

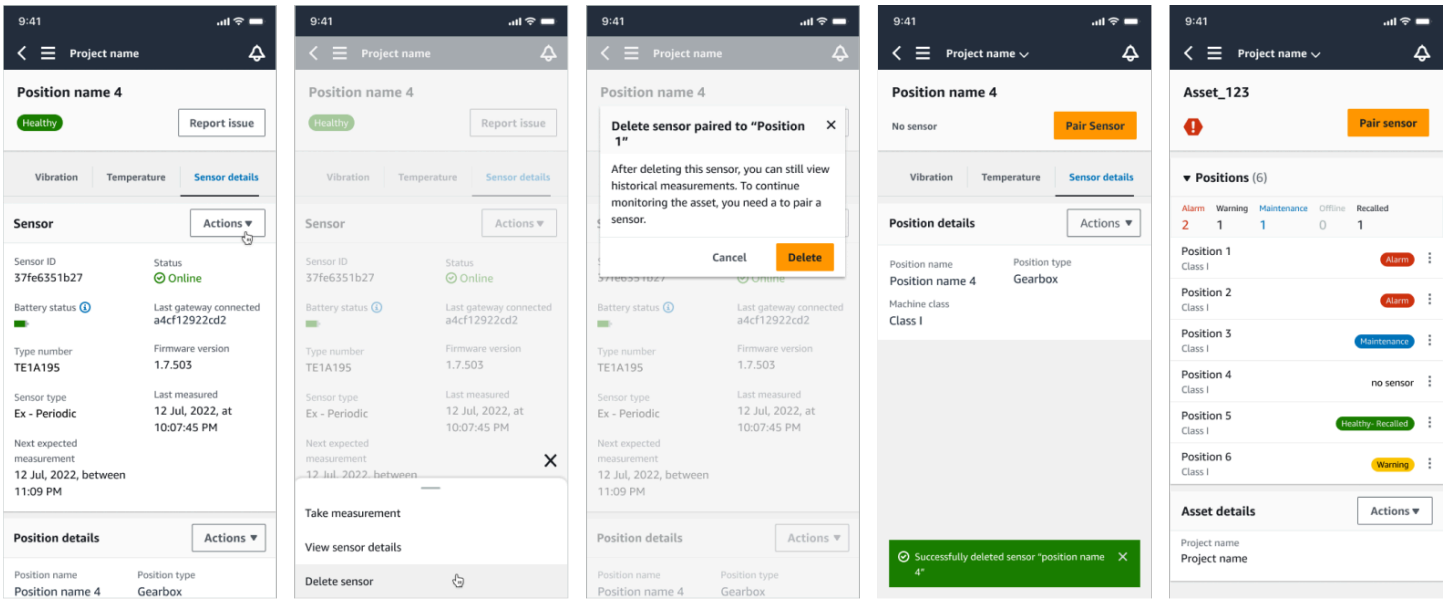
Amazon Monitron は、爆発物や危険なエリアでの安全性に影響を与える可能性のある製品の問題について通知できます。センサーがインストールされた既存の顧客の場合、これらの通知がウェブアプリに表示されます。

センサーに緊急の安全アドバイザリがある場合は、ウェブまたはモバイルアプリにログオンすると通知と説明が表示されます。続行する前に、アドバイザリを確認し、安全警告で推奨されるアクションを実行する必要があります。例えば、センサーは潜在的な点火源となる可能性があるため、危険エリアから物理的にセンサーを削除する必要がある場合があります。





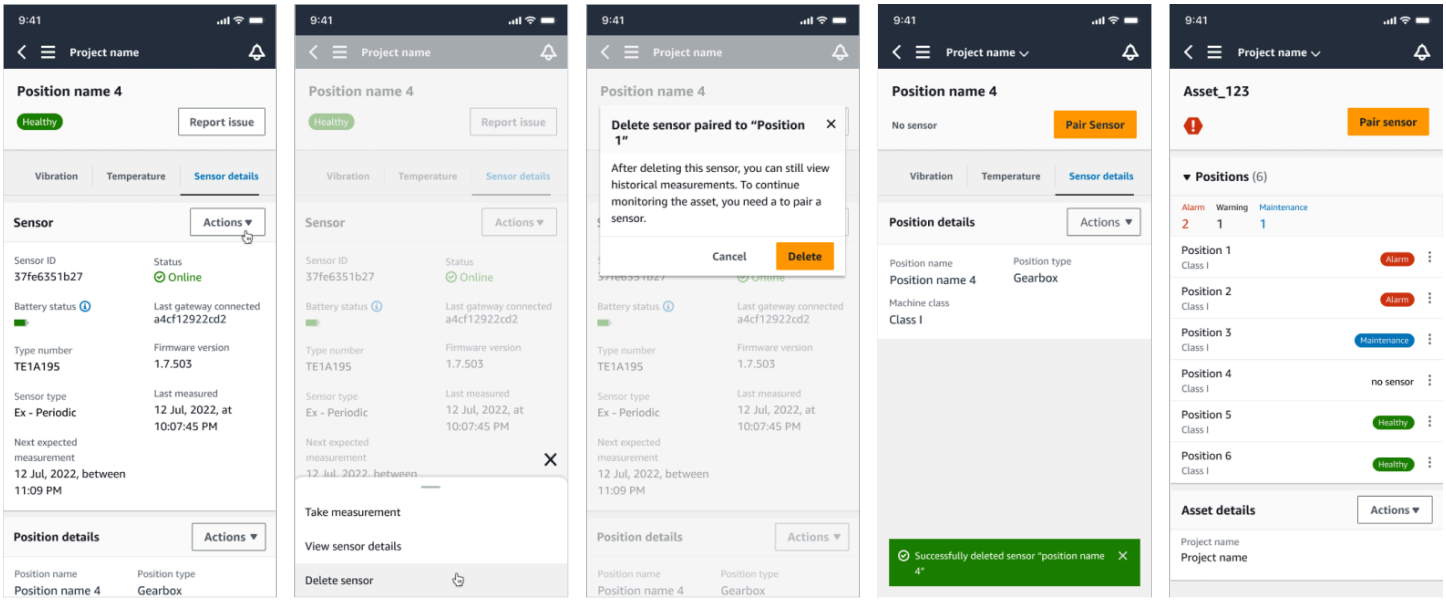
センサーの位置ステータスが正常である場合は、センサーを使用して、測定値の取得、センサーの詳細の表示、センサーの削除を行うことができます。

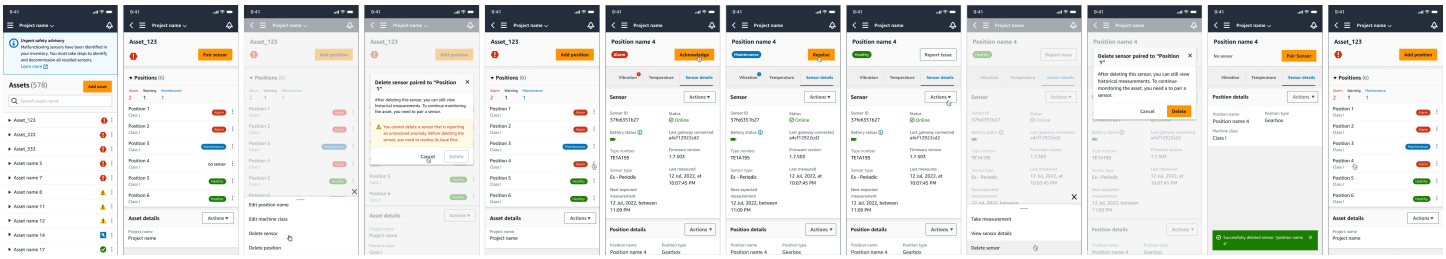


センサーを削除する必要がある場合は、まずセンサーが正常な状態であることを確認します。センサーの位置は、削除する前に正常な状態になっている必要があります。安全通知の対象であるか、正常でないセンサーを削除すると、アラートを最初にクリアする必要があることを説明する通知が送信されます。

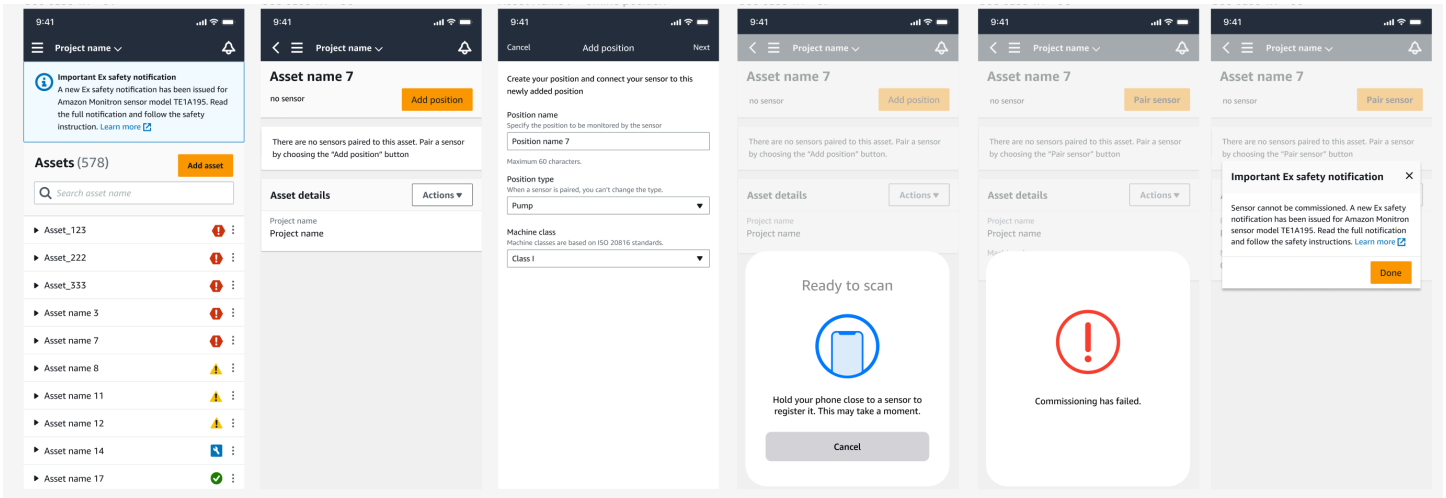
アラートをクリアするには：

1. アセットリストで、異常なセンサーを選択します。
2. エラーを確認します。
3. 確認を選択して、センサーに関連するアクティブなアラートを理解したことを確認します。
4. 解決を選択して、センサーが報告している異常を修正します。問題を解決した後、センサーは正常な状態に戻ります。
5. アセットリストまたは位置の詳細ページからセンサーを削除します。





安全通知に基づいてセンサーをコミッショニングしようとすると、コミッショニングプロセスは失敗します。失敗の理由を説明する通知が届きます。



センサーの測定値とマシンの異常のモニタリングについて

Amazon Monitron は、センサーの温度と振動データをモニタリングし、障害の発生を示す可能性のある異常がないかアセットの状態を監視します。アセットは、 Amazon Monitron ウェブアプリ、またはスマートフォンにダウンロードしてインストールする Amazon Monitron モバイルアプリを使用してモニタリングします。 は、Android 8.0 以降または iOS 14 以降と近距離無線通信 (NFC) および Bluetooth を使用するスマートフォンのみ Amazon Monitron をサポートします。

このトピックでは、センサーの測定値の読み取り、マシン異常の通知への対応、ワンタイム測定を行う方法について説明します。

トピック

- 測定値を表示するプラットフォームの選択
- センサーの測定値の表示
- センサーの測定値について
- アセットステータスについて
- マシンの異常の確認
- 異常の解決
- ワンタイム測定の実施

測定値を表示するプラットフォームの選択

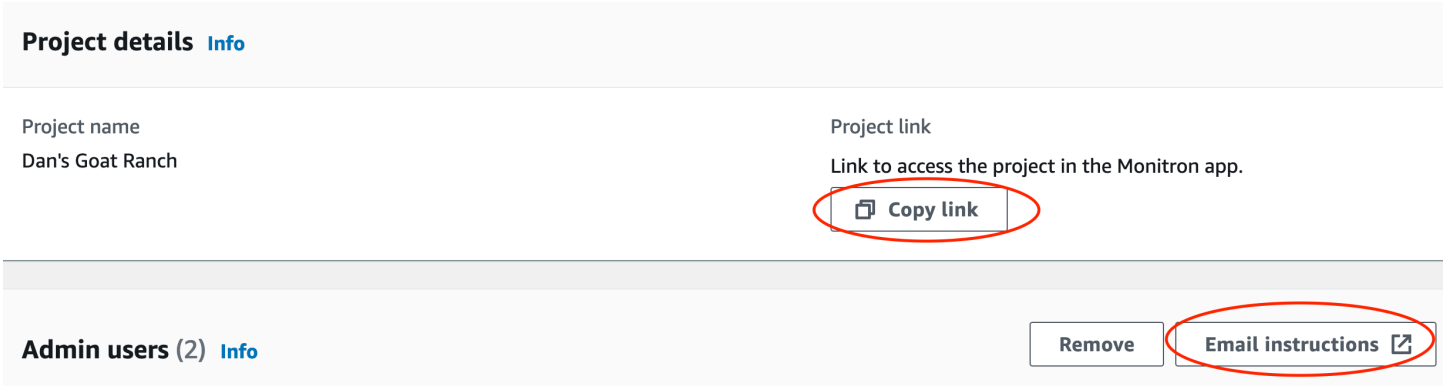
Amazon Monitron を使用してアセットの測定値と異常を表示する方法は 2 つあります。方法があり、それぞれに利点があります。

「Wi-Fi ゲートウェイ」で説明されているように、モバイルアプリではスマートフォンの Bluetooth と近距離無線通信 (NFC) 機能を使用して、ゲートウェイとセンサーをインストールおよび設定します。

ウェブアプリでは、データを .csv ファイルにダウンロードします。また、モニターはおそらくスマートフォンよりも大きいため、測定値を折れ線グラフで確認するにはウェブアプリの方が適している場合があります。

モバイルアプリとウェブアプリのどちらからでも、プロジェクトへのリンクをクリックすることでアクティブ化が可能です。「招待 E メールの送信」で説明されているように、これは管理者がユー

ザーに送信するリンクです。ただし、[プロジェクト] ページでユーザーを選択して [E メールによる指示] を選択するか、[プロジェクトの詳細] の [リンクをコピー] を選択することでリンクを再生成できます。



トピック

- アプリ内更新

アプリ内更新

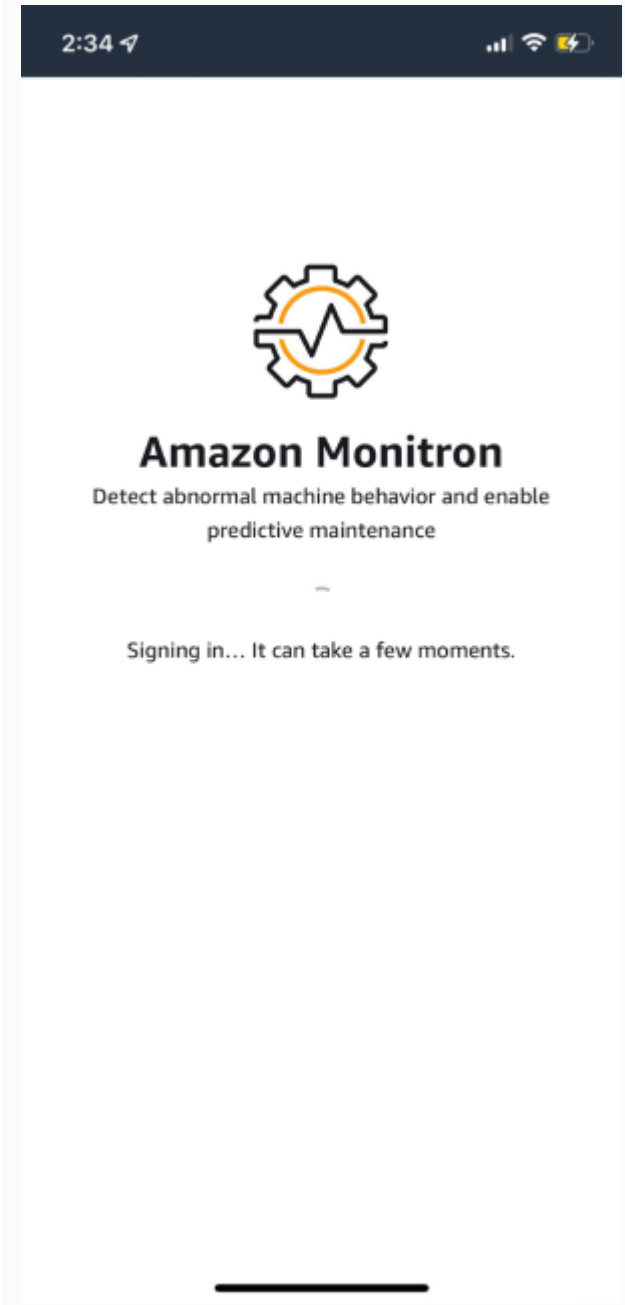
最新の Amazon Monitron 機能にアクセスするには、モバイルデバイスの更新を定期的に確認してください。Amazon Monitron は定期的に新しいアプリケーションのバージョンをリリースします。自動更新を有効にしていない場合は手動で更新する必要があります。これらの通知は、利用可能になり次第ウェブアプリ上で配信されます。

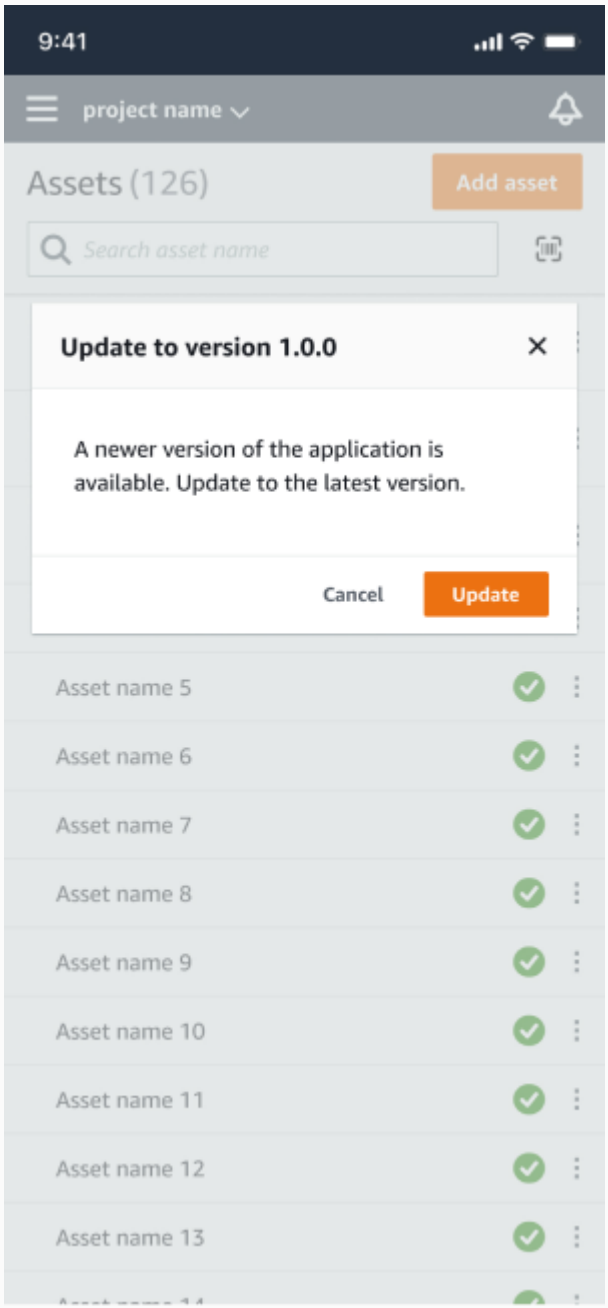
フレキシブル更新と即時更新

Amazon Monitron には、フレキシブル更新と即時更新の 2 種類のアプリ内更新があります。フレキシブル更新 では、サインイン後に Amazon Monitron アプリを更新するかどうかを選択できます。即時更新 にはセキュリティ更新が含まれており、アプリを使用するにはインストールする必要があります。更新は Amazon Monitron アプリからインストールすることも、Google Play やアプリストアから直接インストールすることもできます。

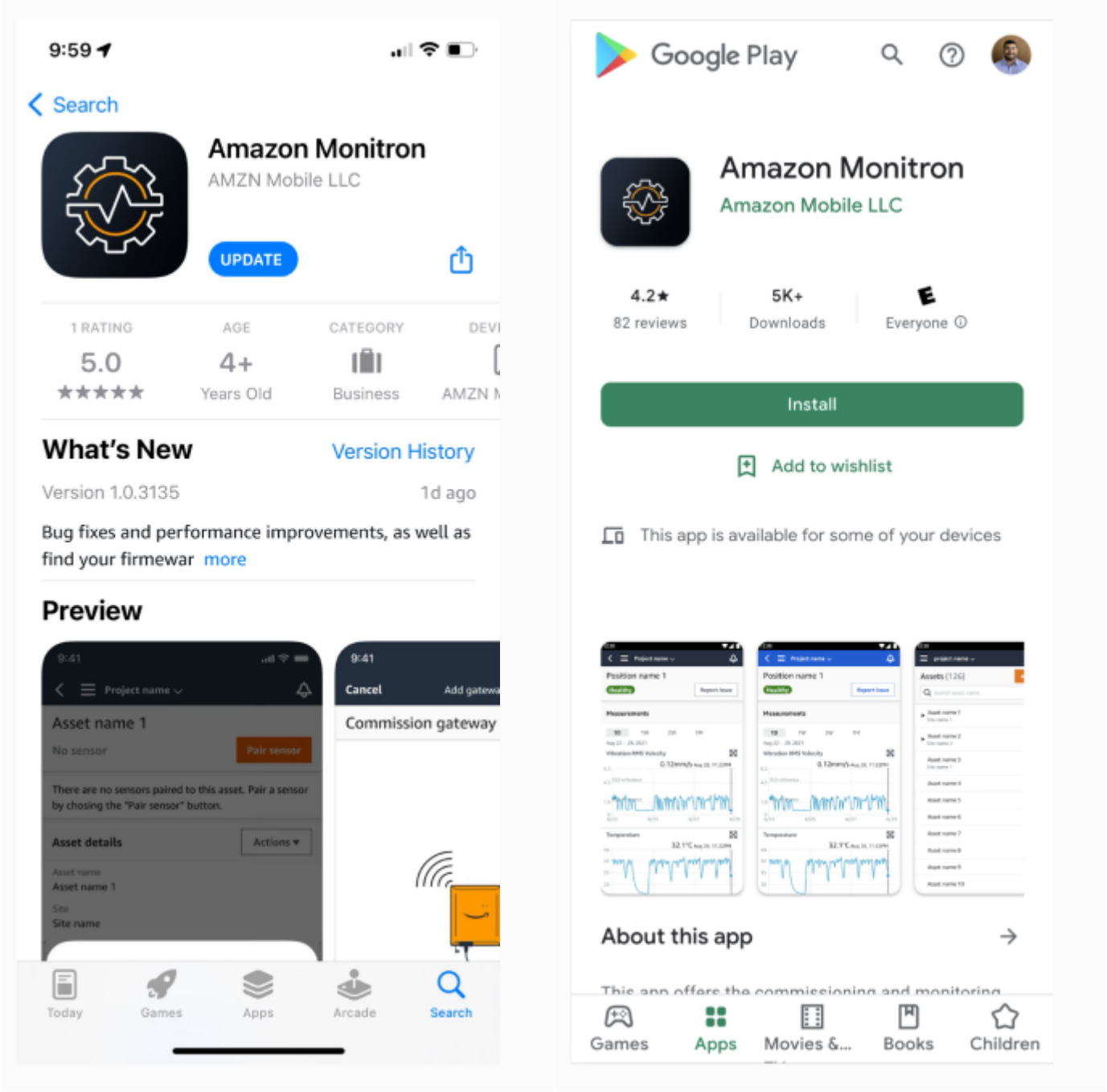
手動で最新の更新をインストールするには:

1. Amazon Monitron アプリにサインインし、[更新] を選択します。

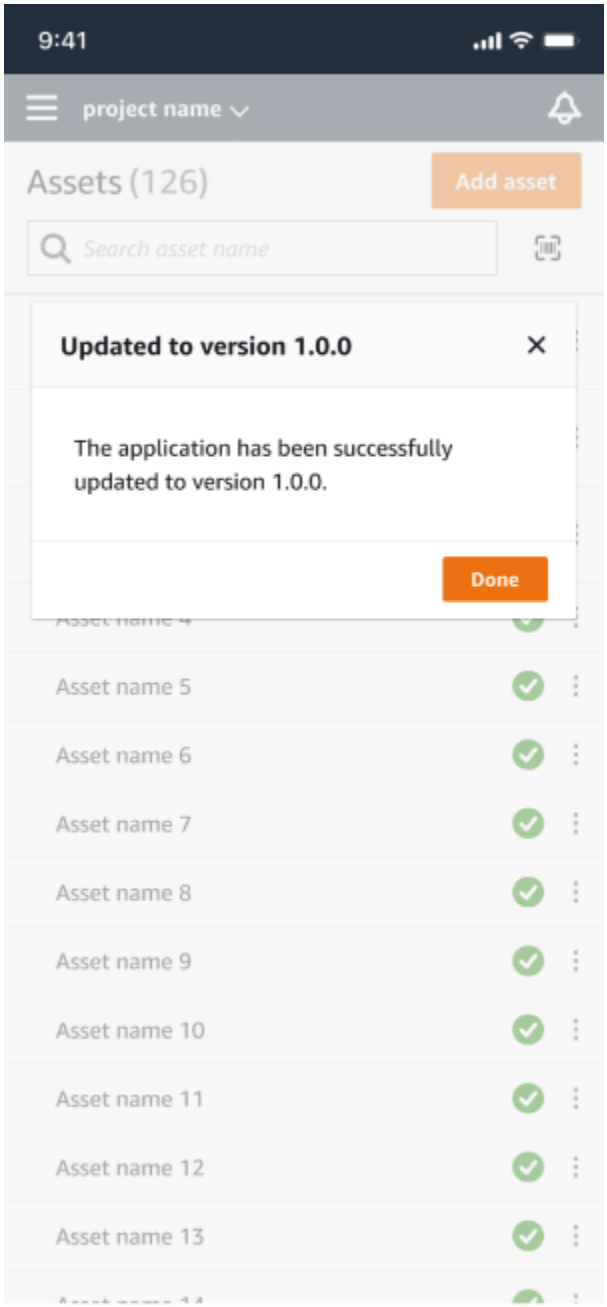




2. [更新] を選択すると、Google Play または App Store に移動します。[更新] または [インストール] を選択して更新を開始します。



3. Amazon Monitron アプリ内で更新プロセスを開始すると、更新のインストール完了後に、アプリに成功メッセージが表示されます。

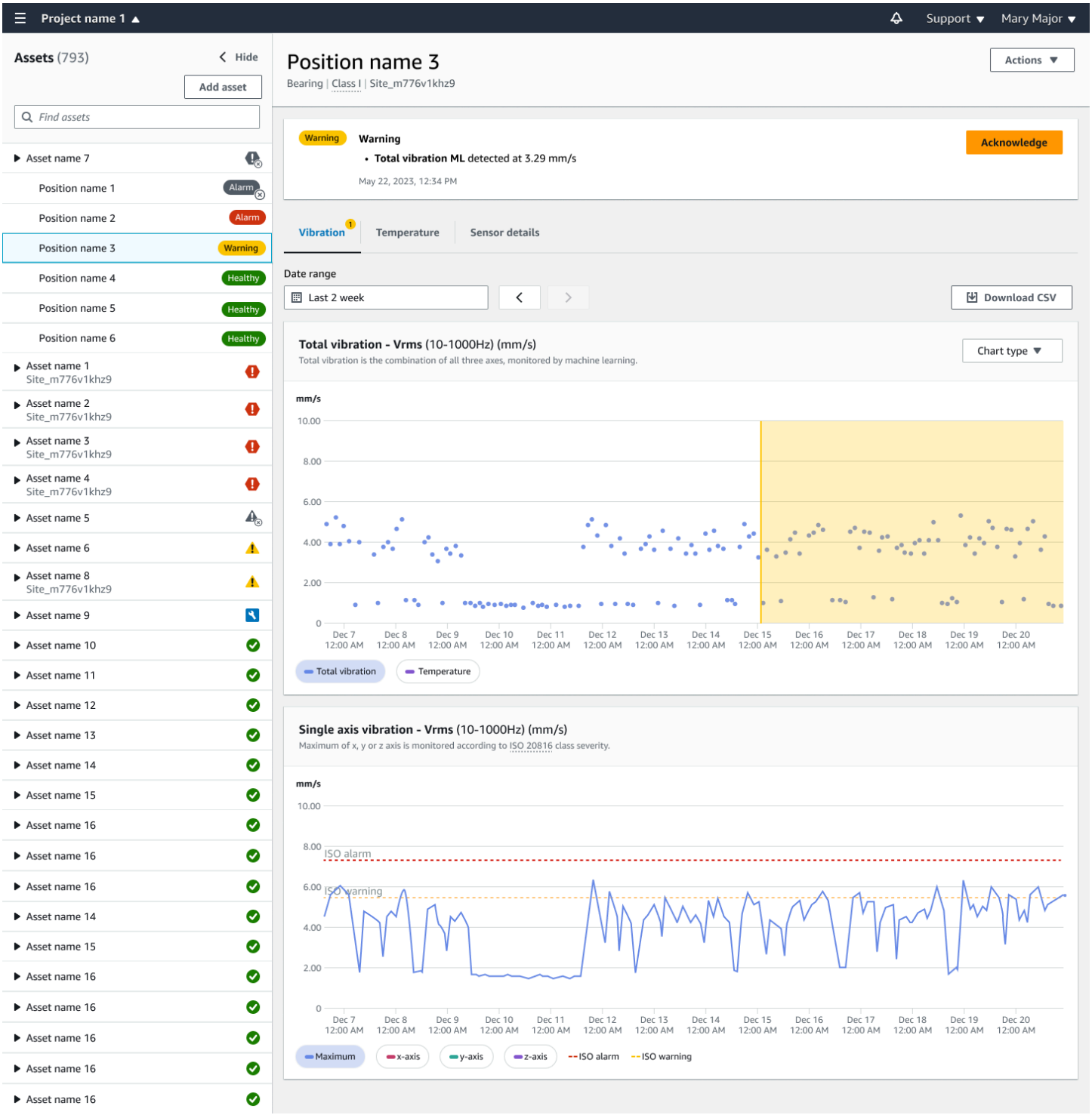


> **Note**
>
> 自動更新の場合、または App Store や Google Play 内で更新プロセスを開始した場合は、成功メッセージは表示されません。

センサーの測定値の表示

センサーの測定データは、散布図と折れ線グラフの 2 つのチャート形式で表示できます。次の画像は、上部に散布図ビュー、下部に折れ線グラフビューを示しています。

> **Note**
>
> センサーの測定値の表示方法は、モバイルアプリとウェブアプリの [グラフのタイプ] メニューから選択できます。


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

センサーの測定値について

センサーが最初にアセットとペアリングされると、 Amazon Monitron は機器から収集された振動と温度のデータから学習し、ベースラインを確立してそのアセットの「正常」なものを決定します。この学習は、今後の潜在的な障害を検出するのに活用されます。

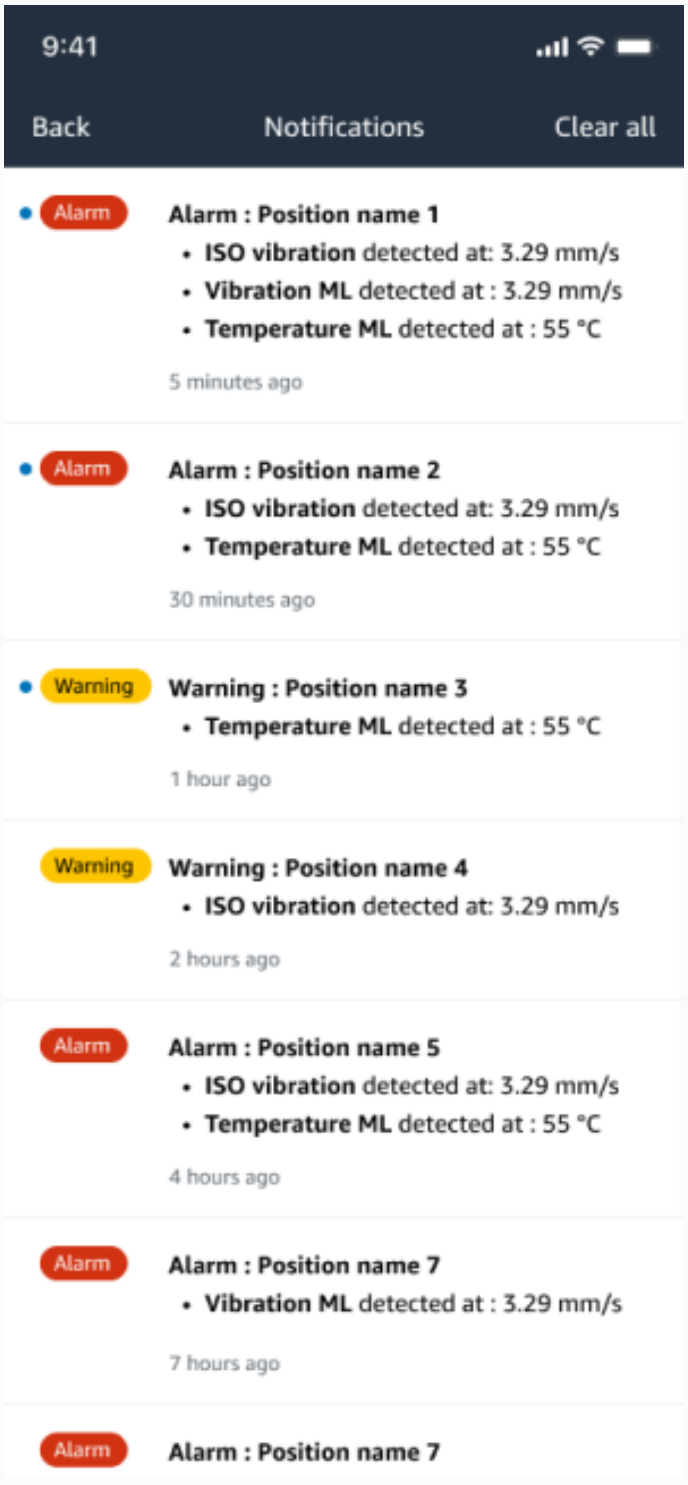
状況、運用シナリオ、ユースケース、アセットの義務サイクルなどのさまざまなパラメータに応じて、このベースラインを確立するには 14～21 日 Amazon Monitron かかります。この初期学習およびトレーニングフェーズでは、アセットは正常であると想定されます。

アセットのベースラインを確立した後、 は収集したデータを Amazon Monitron モニタリングし、潜在的な障害を示すイベントや傾向を探します。特に、温度や振動レベルの上昇、あるいはその両方を監視します。温度と振動の上昇は、マシンの故障を示す主な指標です。多くの場合、マシンの異常はアセットが故障し始めていることを示しています。

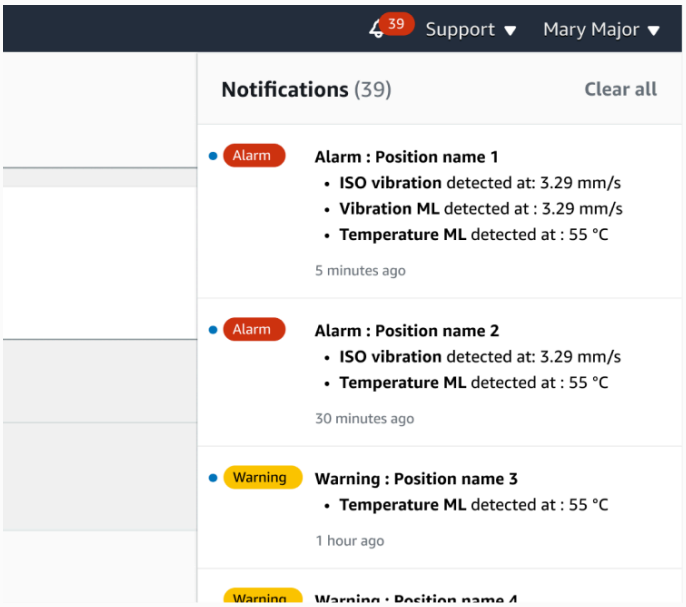
Amazon Monitron は、国際標準化機構 (ISO) によって確立された振動しきい値をお客様の機械クラスに使用します。ISO のしきい値をセルフトレーニングモデルと組み合わせて適用することで、機器に合った実際のしきい値を評価します。たとえば、マシンが少し熱い、または少し冷たい動作をする場合、または標準よりも少し振動する場合、 はしきい値を少し Amazon Monitron 調整して、マシンが異常に動作しているタイミングをより正確に特定できるようにします。

初期学習およびトレーニング期間中に受信するアラームは、(学習期間を必要としない) ISO モデルのアラームだけです。トレーニング期間中の ISO アラームは、他のアラームと同様に扱う必要があります。つまり、アラームを確認して、必要な確認をマシンに実施してから、適切なアクションを実行したコードでアラームを閉じます。その後、 はベースラインの微調整を Amazon Monitron 続行し、センサーがより多くのデータを収集するにつれて「正常」のより良いイメージを構築します。

温度や振動レベルが修正後のしきい値を一貫性なく上回っている場合、障害の可能性はありますが、おそらく差し迫った問題ではないでしょう。この場合、 Amazon Monitron は`Warning`通知を送信します。常にしきい値を上回っている場合、状況は明らかに異常であり、障害の可能性ははるかに高くなります。このような状況では、 はモバイルアプリまたはウェブアプリ`Alarm`に通知 Amazon Monitron を送信します。



モバイルアプリ通知



ウェブアプリ通知

この例では、Position 3 センサーが温度と振動の持続的な上昇を検出しており、潜在的な障害を調査する必要があることを示しています。

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

アセットステータスについて

センサーがマシンの異常を検出すると、アセットのステータスが変更されます。問題が発生すると、Amazon Monitron アプリのアセットリストに表示されます。

トピック

- アセットリスト
- アセットとポジションのステータス
- 通知

アセットリスト

[アセット] リストには、サイトまたはプロジェクト内のすべてのアセットが表示され、現在表示しているサイトまたはプロジェクトのアセットが表示されます。サイトとプロジェクトの詳細については、「モバイルアプリを使用したプロジェクトとサイト間の移動」を参照してください。

Amazon Monitron モバイルアプリを開くと、最後に作業したサイトまたはプロジェクトに関連付けられたアセットのリストが表示されます。アプリ内の別の場所から [アセット] リストに移動するには、次の手順に従います。

モバイルアプリまたはウェブアプリでアセットリストを開くには

1. メニューアイコン (☰) をクリックします。
2. [アセット] を選択します。

   アセットリストが表示されます。

モバイルアプリでのアセットリスト

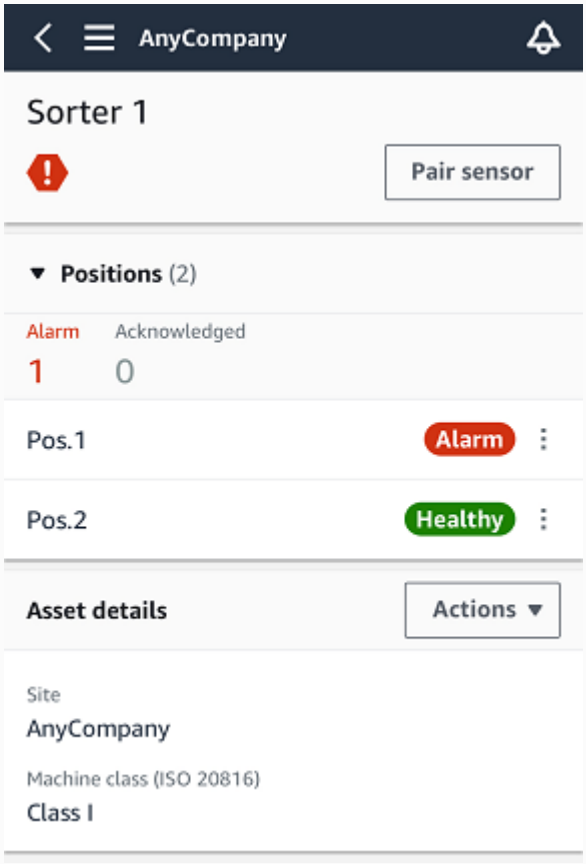
アセットとポジションのステータス

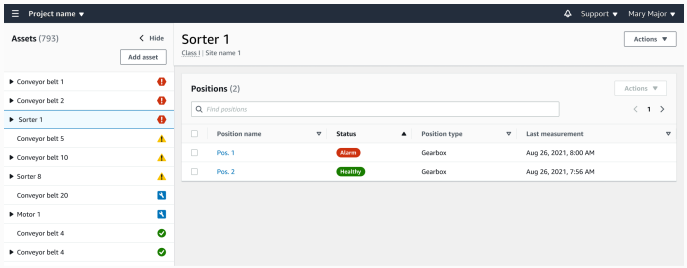
[アセット] リストには、各アセットのステータスが次の表のようなアイコンで表示されます。

ステータス	意味
	正常状態: アセット内のすべてのセンサーポジションのステータスは正常です。
	警告状態: このアセットの位置の 1 つに対して警告がトリガーされました。これは、Amazon Monitron が潜在的な障害の初期兆候を検出したことを示します。 は、機械学習と ISO 振動標準を組み合わせて機器の振動と温度を分析することで警告状態 Amazon Monitron を識別します。
	アラーム状態: このアセットのいずれかのポジションでアラームが発せられました。マシンの振動と温度がそのポジションでは正常範囲外であることを示しています。できるだけ早く問題を調査することが推奨されます。問題が解決されないと、機器に障害が発生する可能性があります。
	確認済み状態: 技術者がポジションの警告またはアラー

ステータス	意味
	ム状態を確認しましたが、アセットの修理はまだ完了していません。
センサーなし	センサーなし: 現在、アセットの少なくとも 1 つのポジションにセンサーがペアリングされていません。

問題の詳細を確認するには、そのアセットを選択し、その中のセンサーポジションのステータスを確認してください。





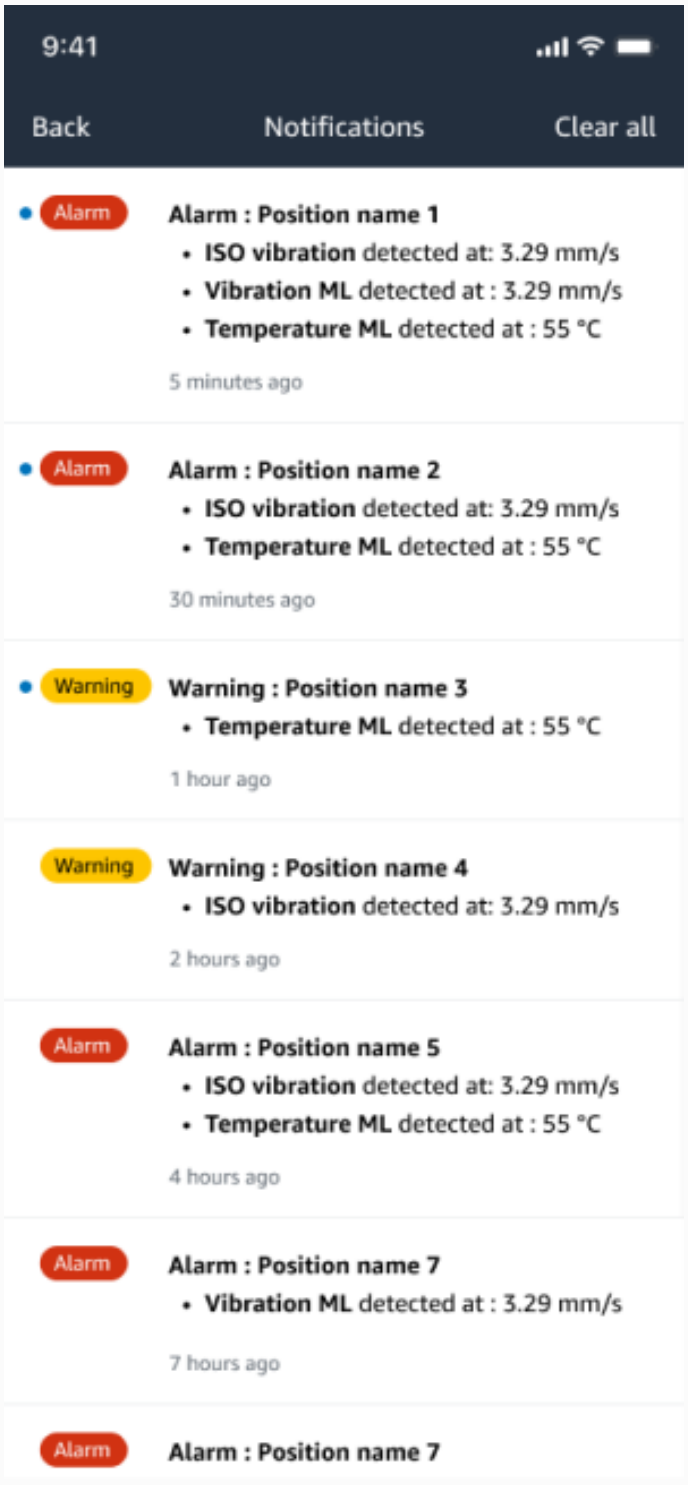
Amazon Monitron は、アセットステータスアイコンのようなアイコンを使用して、センサーの位置のステータスを表示します。

ステータス	意味
Healthy	ポジションは正常です。測定値はすべて正常範囲内です。
	警告状態: このアセットの位置の 1 つに対して警告がトリガーされ、 Amazon Monitron が潜在的な障害の初期兆候を検出したことを示します。 は、機械学習と ISO 振動標準を組み合わせて、機器の振動と温度を分析することで警告状態 Amazon Monitron を識別します。
Alarm	このポジションではマシンの振動と温度が正常範囲外であることを示すアラームが発せられました。できるだけ早く問題を調査することが推奨されます。問題が解決されないと、機器に障害が発生する可能性があります。
Acknowledged	技術者がポジションの警告またはアラーム状態を確認しましたが、アセットの修理はまだ完了していません。
センサーなし	現在、そのポジションとペアリングされているセンサーはありません。

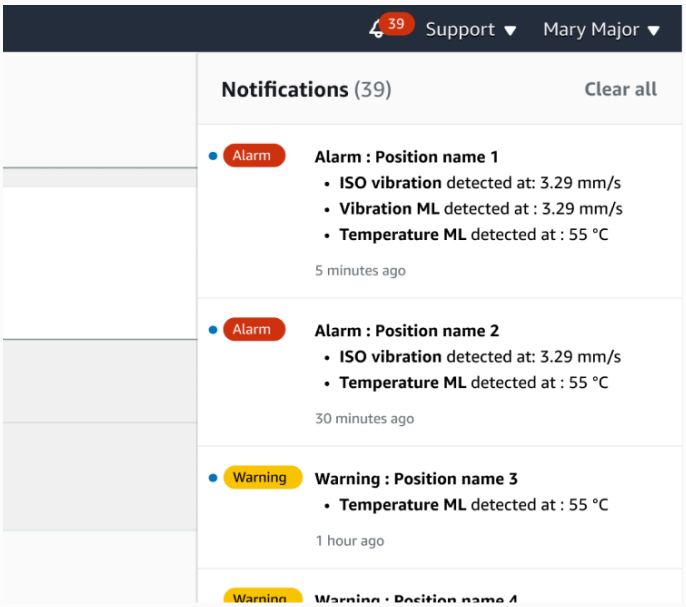
通知

警告またはアラームアラートが生成されると、 はアプリの管理者ユーザーと技術者に通知 Amazon Monitron を送信します。権限のある担当者は、モバイルアプリの通知アイコンにアラートシンボル
( )
が表示されているときにそれを選択することでも通知を確認できます。

通知アイコンをクリックすると [通知] ページが開き、保留中の通知がすべて一覧表示されます。



モバイルアプリの通知



ウェブアプリの通知

マシンの異常の確認

通知を受け取った管理者ユーザーまたは技術者は、通知を確認する必要があります。通知を確認することで、問題が認識されて対応予定であるということを他のユーザーに知らせることができます。

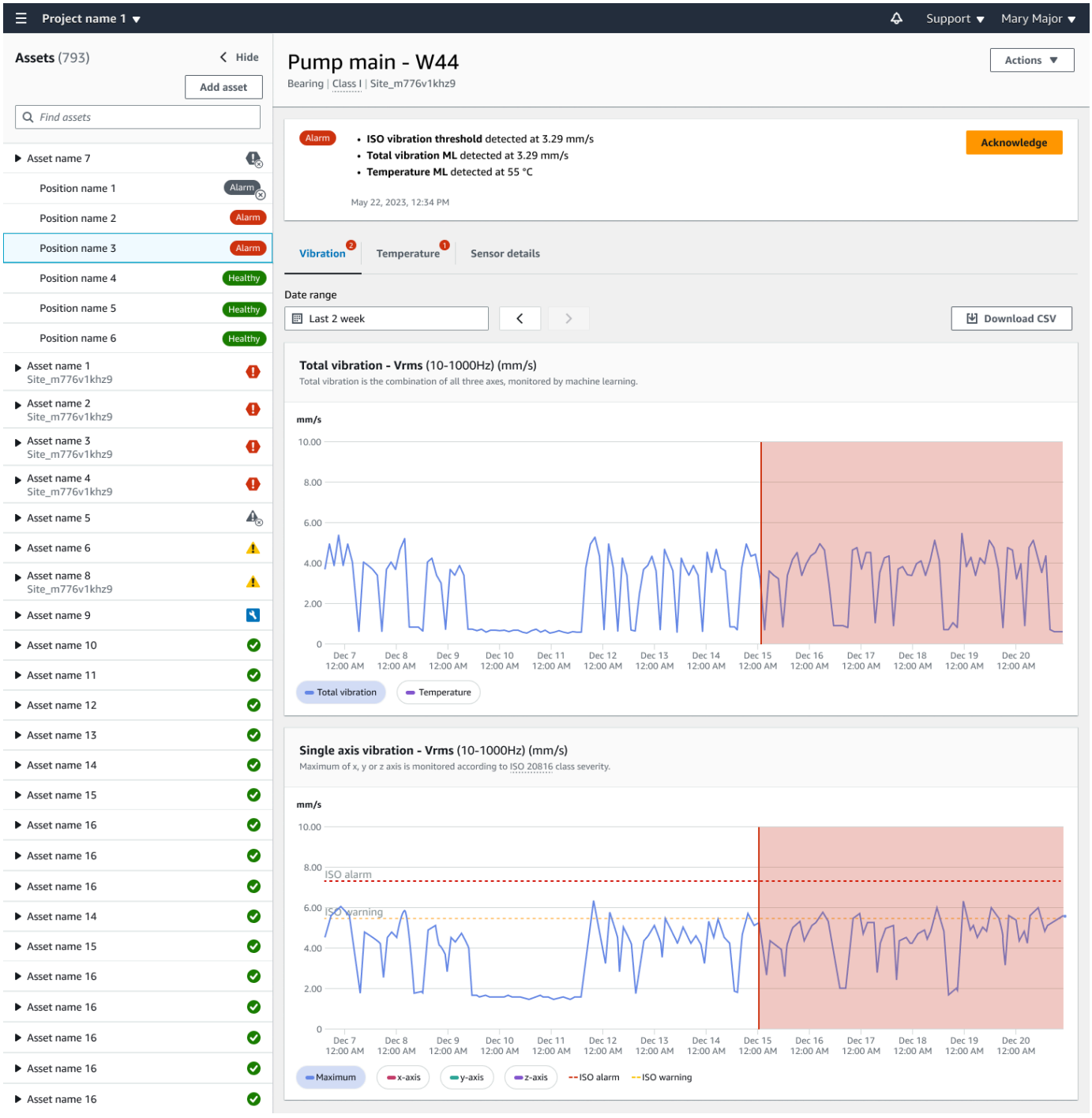
トピック

- マシンの異常を表示して確認するには

マシンの異常を表示して確認するには

1. [アセット] リストから、異常を報告しているアセットを選択します。
2. 問題を表示するには、異常のあるポジションを選択します。

   異常を示すセンサーの測定値が表示されます。



3. [承認] を選択します。

   アセットのステータスが [メンテナンス] に変わります。

異常の解決

異常が発生して確認されたら、それに対処する必要があります。自分で修理するか、専門家に依頼してください。異常を報告したマシンが修正されたら、 Amazon Monitron アプリの異常を解決します。

異常を解決すると、センサーは正常状態に戻ります。また、問題 Amazon Monitron に関する情報を送信して、同様の異常をより正確に予測できるようにします。

障害のタイプ (障害モード) と障害の原因は、複数の一般的な例から選択できます。状況がいずれのモードや原因にも当てはまらない場合は、[その他] を選択してください。

トピック

- 障害モード
- 失敗の原因
- モバイルアプリを使ってマシンの異常を解決するには

障害モード

Amazon Monitron の障害モードまたはタイプは次のとおりです。

- 障害が検出されない (ミュートアラート) : 同じ異常状態が検出された場合、アラートはトリガーされません
- ブロック: 制限された操作を引き起こす障害
- キャビテーション: ポンプの拾い上げ圧力の損失
- 腐食: 湿分腐食、フレッチング、フォールスブリネリング
- 預金: パーティクルの蓄積
- 不均衡: コンポーネントのローテーションのバランスが取れていない
- 注水: 注水不足または不適切な注水
- ずれ: ローテーションアセンブリが整列していない
- その他
- 共鳴: 外部振動ソース
- 回転ルーズネス: ファンブレードやプーリーなどの回転コンポーネントをルーズにする

- 構造的な緩み: コンポーネントのマウントが緩い
- 送信済み障害: 外部力によって発生
- Undetermined (Keep monitoring): 同じ異常状態が検出されると、アラートがトリガーされます。

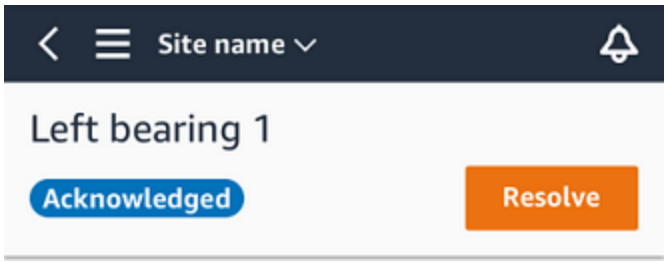
失敗の原因

Amazon Monitron の障害の原因は次のとおりです。

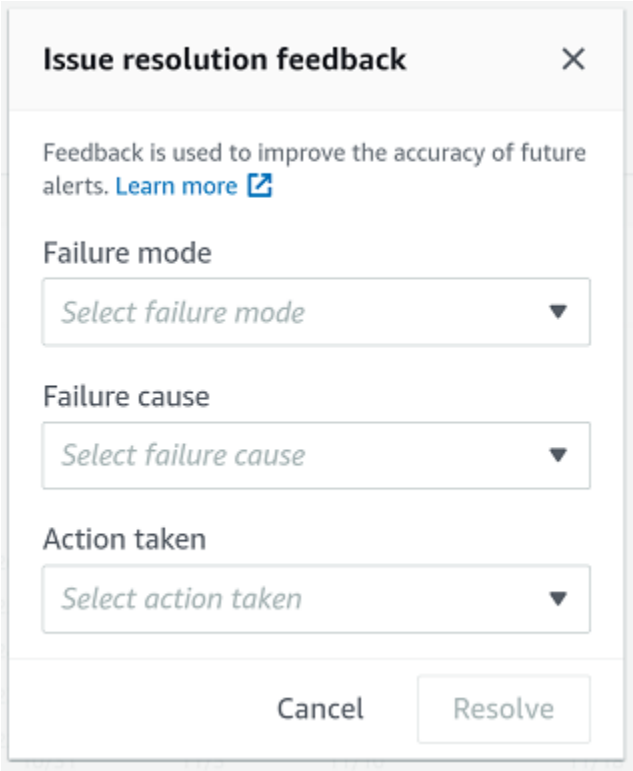
- 管理: 演算子エラー
- 設計: 製造元の設計が不十分
- 作成: アセットが元の状態から変更されました
- メンテナンス: アセットに対して実行されるメンテナンスの欠如
- オペレーション: オペレーション状態の変更
- その他: 保管、輸送 (振動/衝撃)、ベアリングの選定、製造上の懸念、材料に関する懸念
- 品質: 製造元の品質が不十分
- 未確定: 根本原因は特定されていません
- 摩耗: 経時的な分解/分解

モバイルアプリを使ってマシンの異常を解決するには

1. [アセット] リストから、異常を解決したアセットを選択します。
2. 異常が発生したポジションを選択します。
3. [解決] を選択します。



4. [障害モード] では、発生した障害のタイプを選択します。



5. [障害の原因] では、障害の原因を選択します。
6. [実行されたアクション] では、実行したアクションを選択します。
7. [送信] を選択します。

ワンタイム測定の実施

センサーが通常行う測定以外にも、ワンタイム測定でセンサーの値をいつでも確認できます。

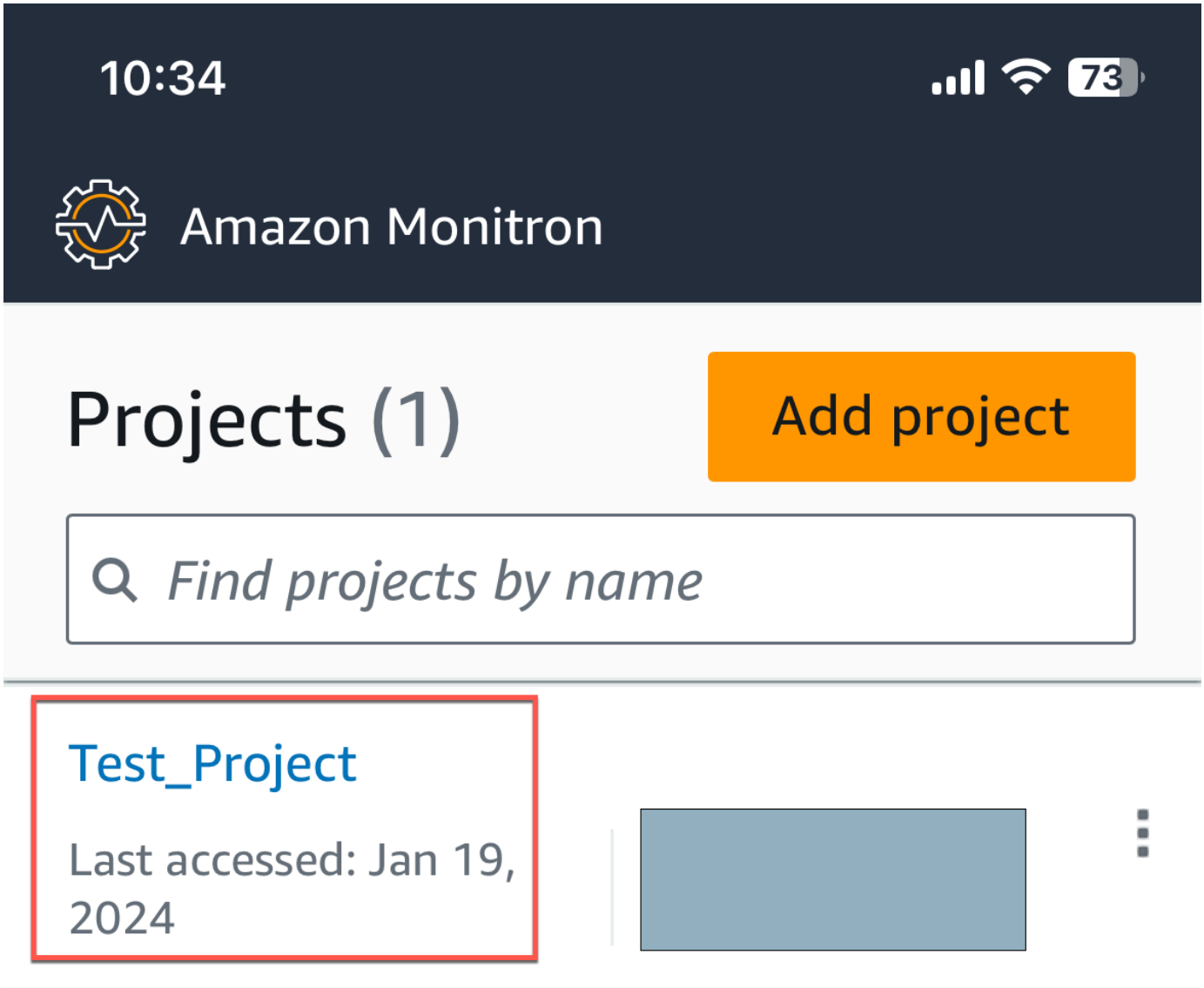
> **Important**
>
> センサー測定は、Amazon Monitron モバイルアプリを使用してのみ実行できます。管理者と技術者の両方がこのアクションを実行できます。

トピック

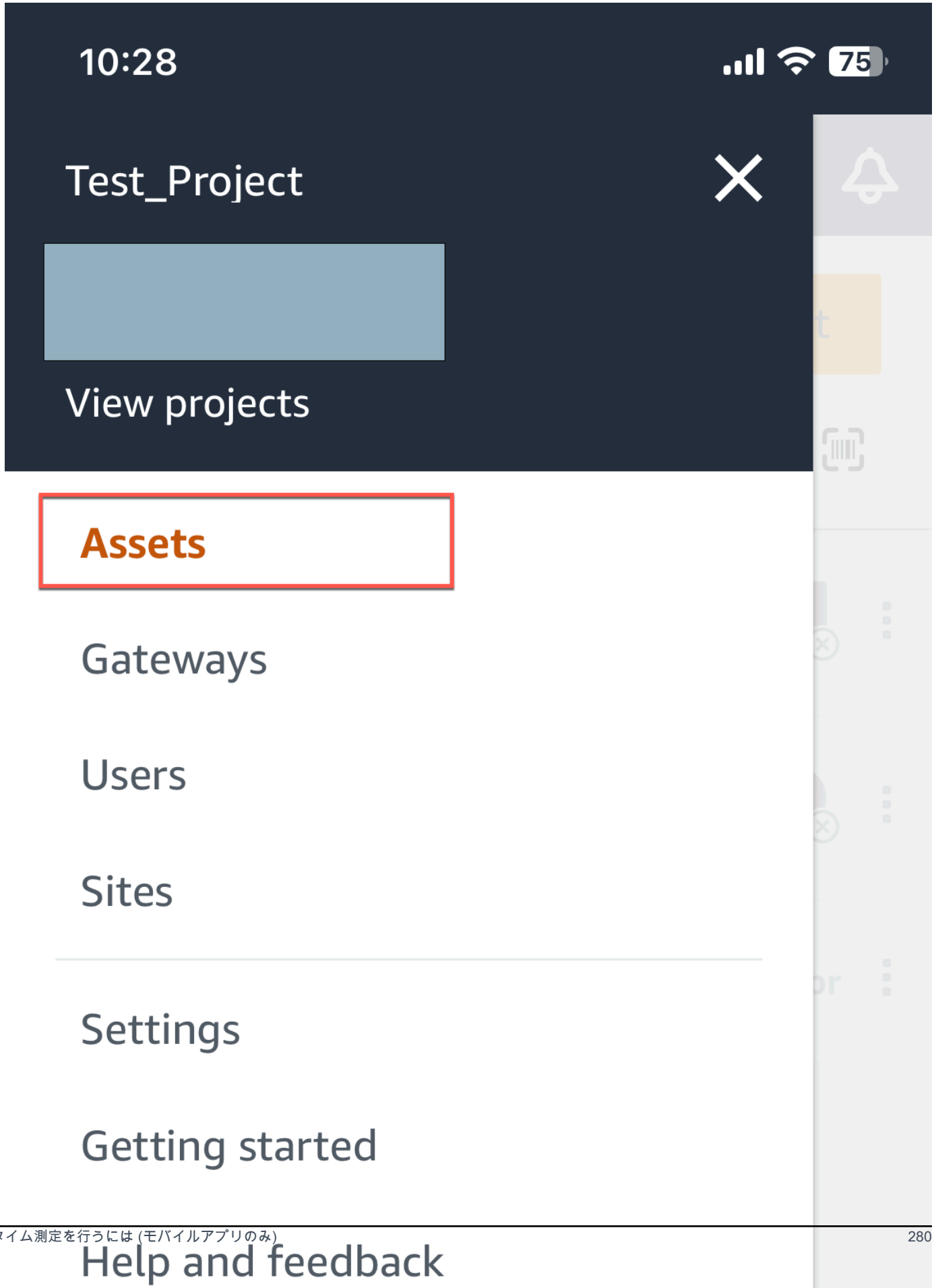
- ワンタイム測定を行うには (モバイルアプリのみ)

ワンタイム測定を行うには (モバイルアプリのみ)

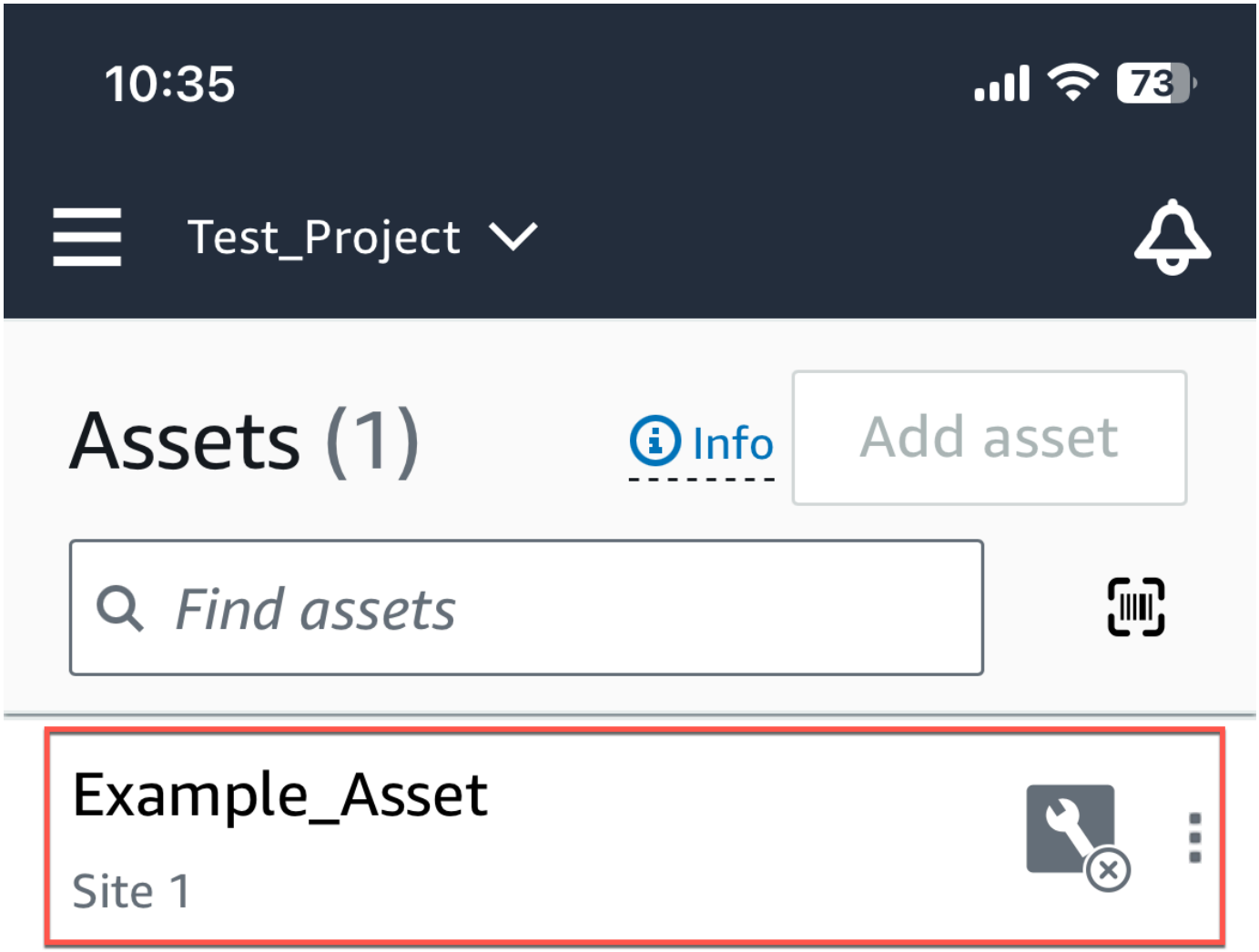
1. Amazon Monitron モバイルアプリから、プロジェクトを選択します。


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

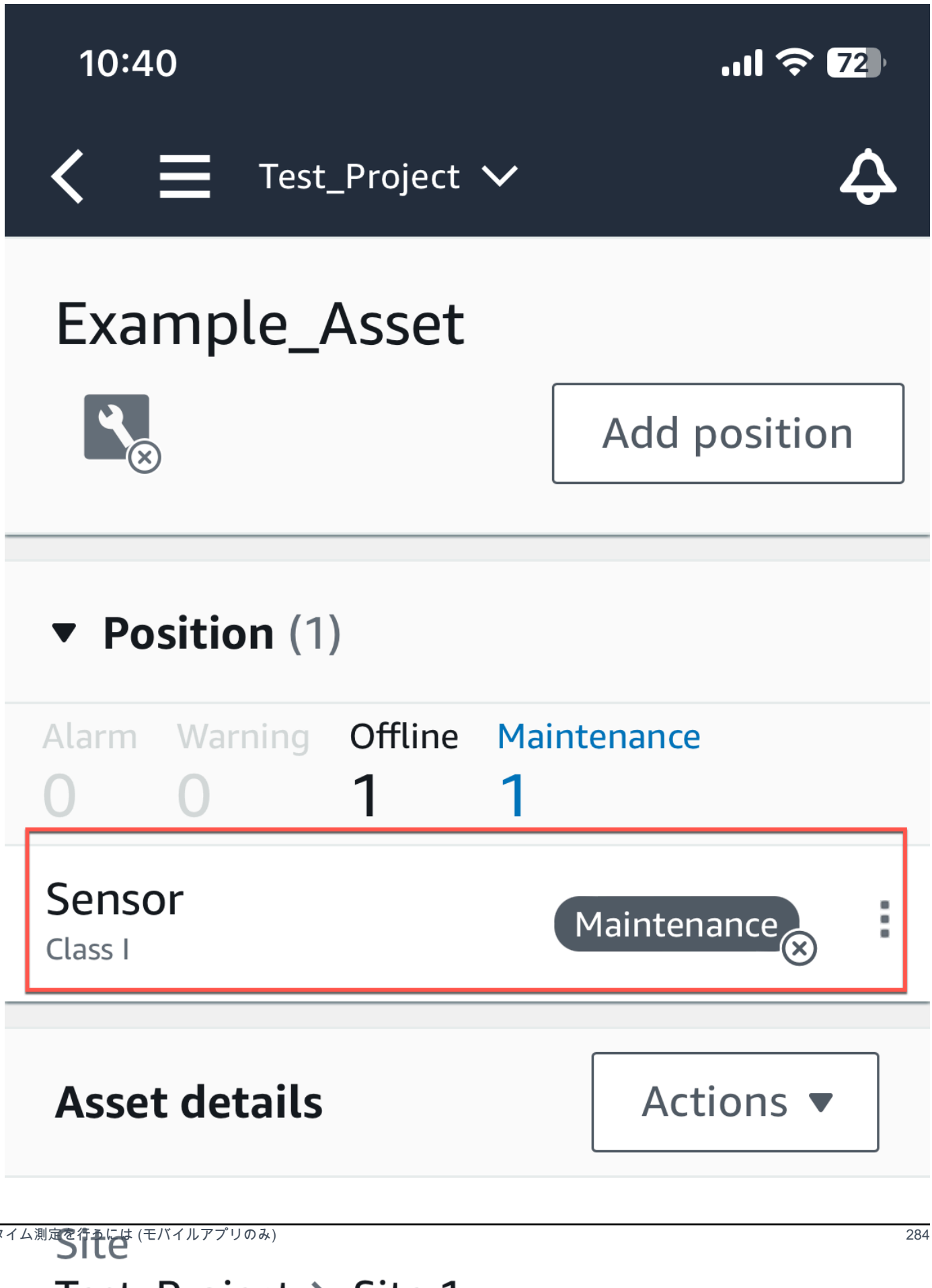
2. Amazon Monitron プロジェクトメニューから、アセット を選択します。


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

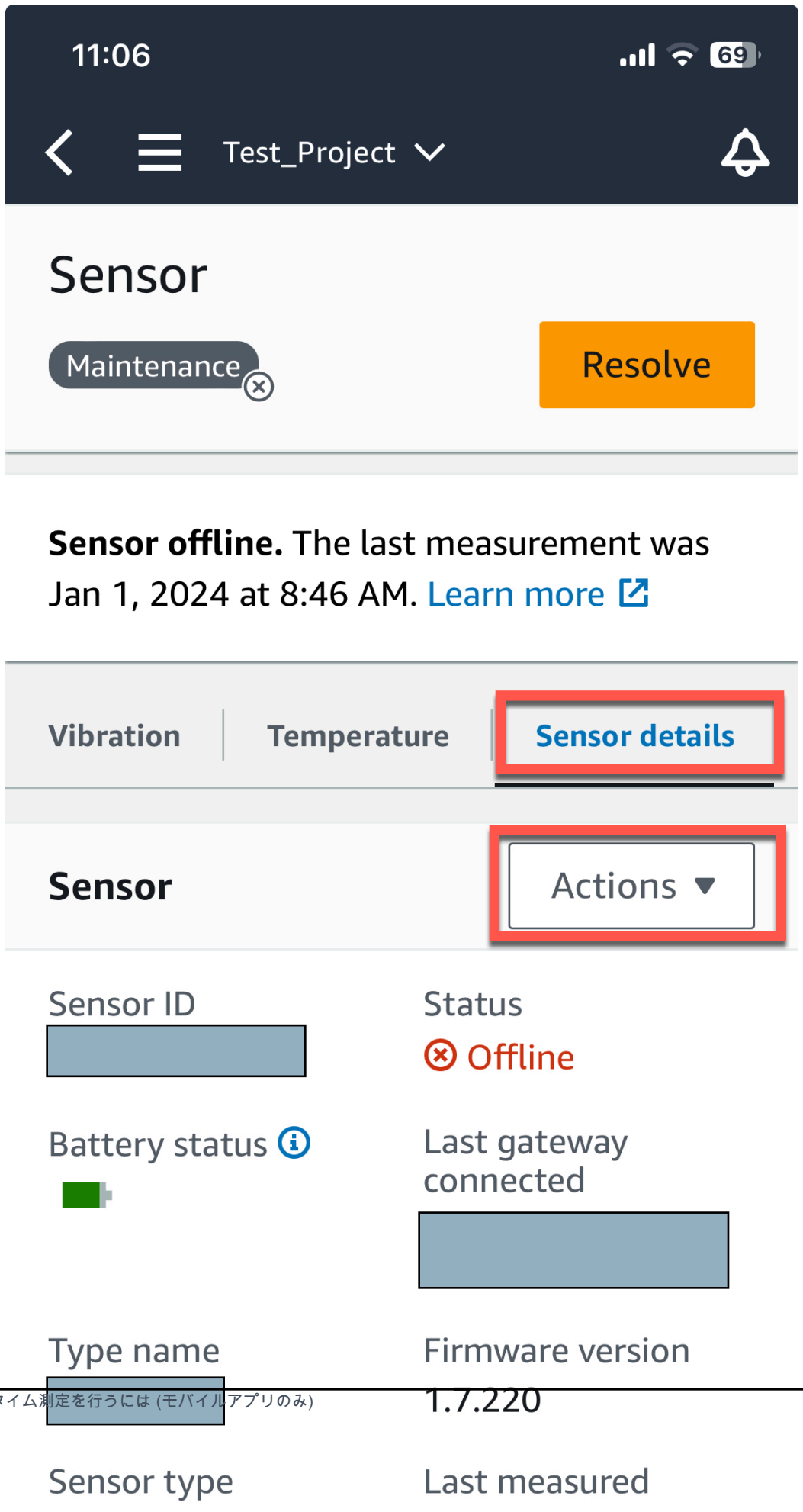
3. アセットのリストから、測定したいセンサーとペアリングされているアセットを選択します。


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

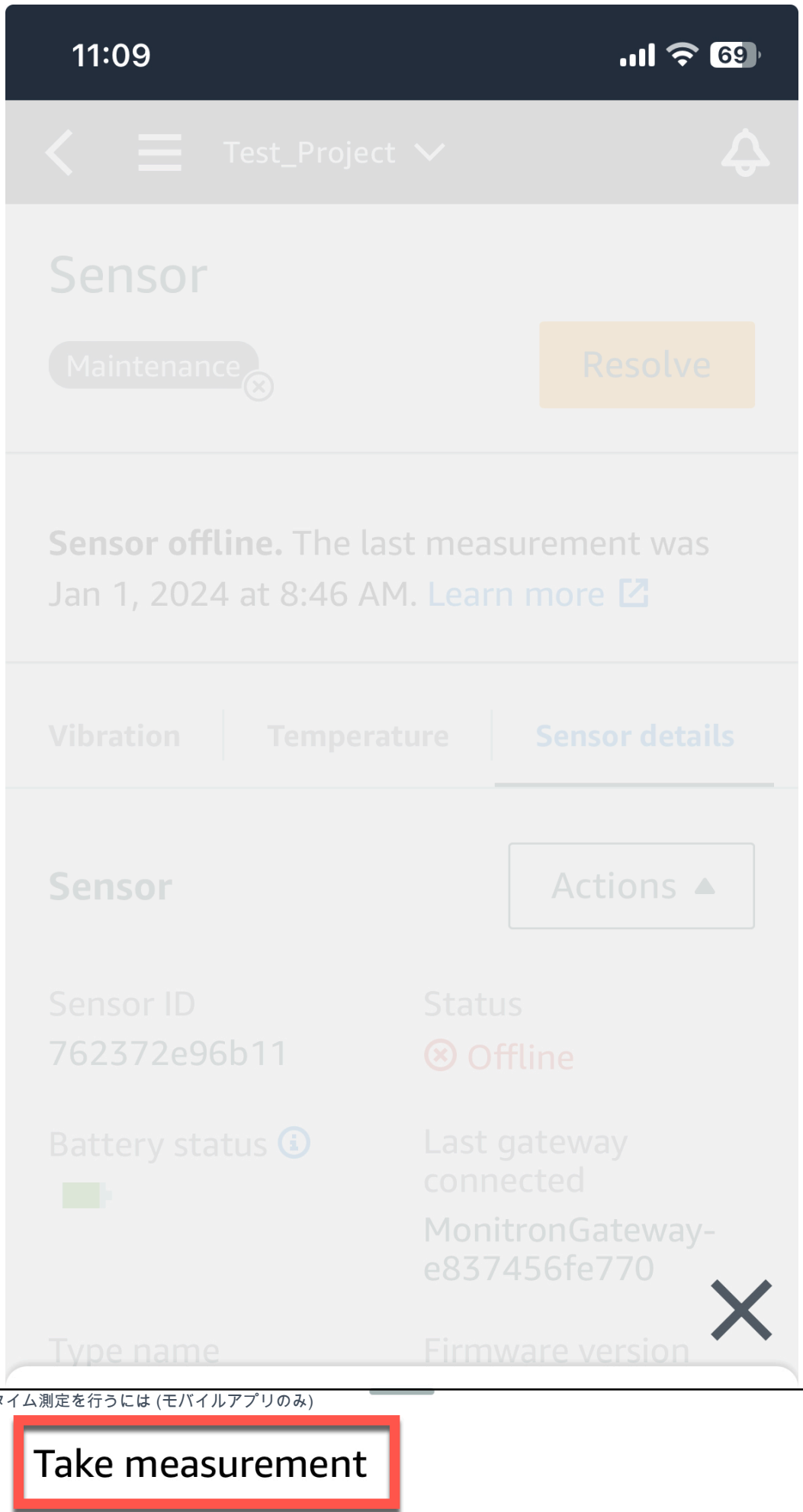
4. 次に、測定に使用するセンサーを選択します。


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

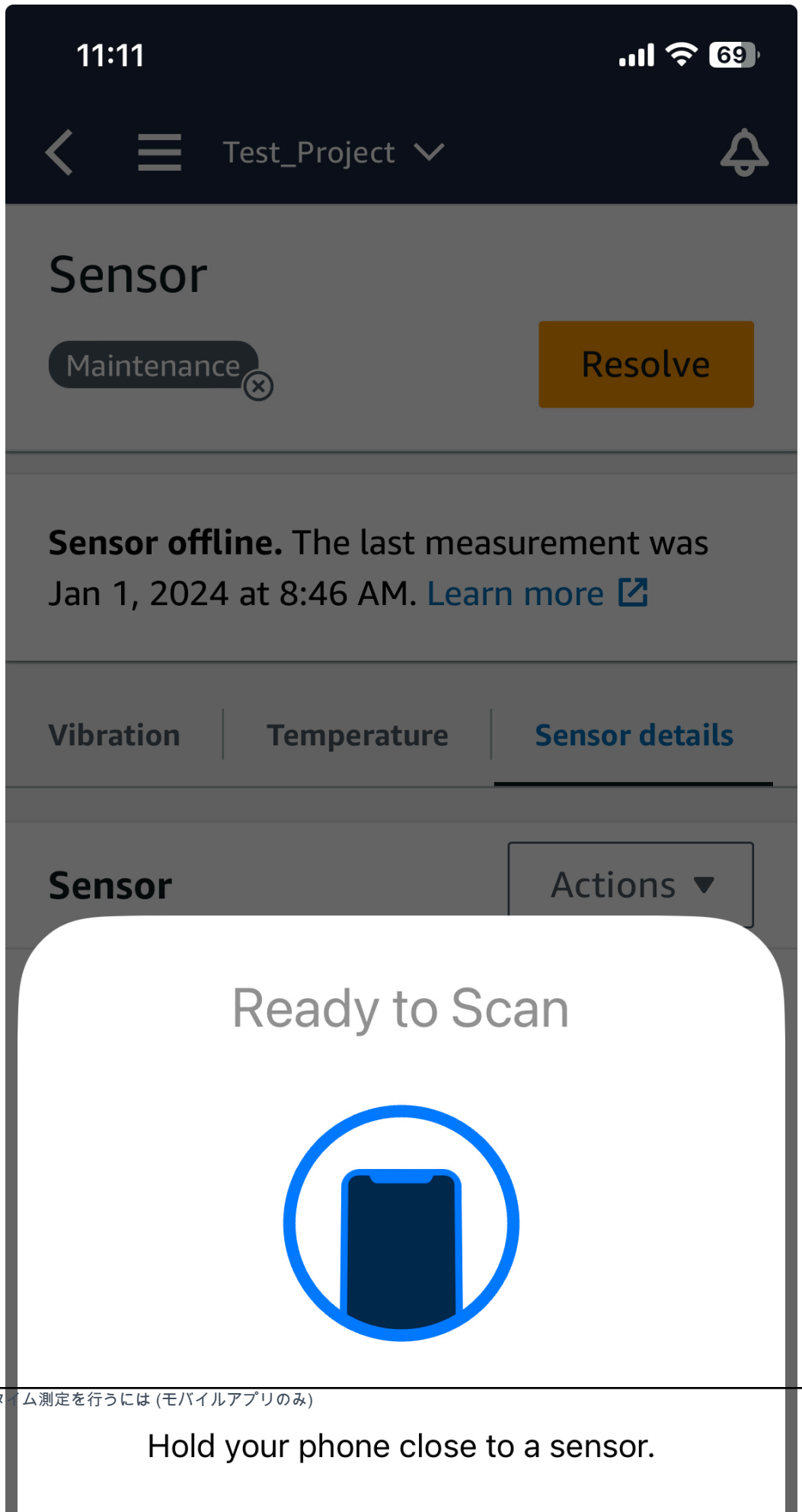
5. センサーページで、センサーの詳細からアクションを選択します。


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

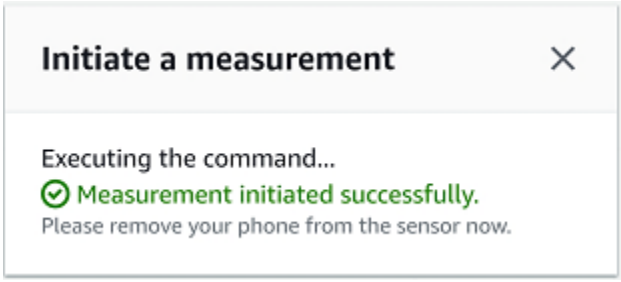
6. アクション から、測定する を選択します。


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. スマートフォンをセンサーに近づけます。


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. 測定が終わったら、スマートフォンをセンサーから離します。



すでにセンサーが収集したデータに新しい測定値が追加されます。

ユーザーの管理

プロジェクトを作成したら、管理を支援する管理者ユーザーを少なくとも 1 人割り当てる必要があります。管理者ユーザーをプロジェクトに追加したり、後でプロジェクトから削除したりすることもできます。コンソールを使用して最初の管理者ユーザーを追加したら、Amazon Monitron モバイルアプリで他の管理者ユーザーをさらに追加できます。

> **Important**
>
> Amazon Monitron では、アプリユーザーごとに E メールアドレスが必要です。Microsoft Active Directory や外部 ID プロバイダーなどのディレクトリを使用する場合は、ユーザーの E メールアドレスが追加され、同期されていることを確認する必要があります。

プロジェクトまたはサイトを作成したら、そこにユーザーを追加する必要があります。管理者ユーザーは、`Admin`、`Technician`、`Viewer` の 3 つの異なるロールにユーザーを追加できます。ユーザーのロールによって、Amazon Monitron で何ができるかが決まります。ユーザーのロールが持つアクセス許可の範囲は、そのロールがプロジェクトレベルで追加されたのか、サイトレベルで追加されたのかによって決まります。プロジェクトレベルでユーザーのロールを設定すると、そのプロジェクトのすべてのサイトに対するアクセス許可がユーザーに付与されます。サイトレベルでユーザーのロールを設定すると、そのサイトに対するアクセス許可のみがユーザーに付与されます。

トピック

- 管理者ユーザーの管理
- 管理者以外のユーザーの管理

管理者ユーザーの管理

プロジェクトを作成したら、管理を支援する管理者ユーザーを少なくとも 1 人割り当てる必要があります。管理者ユーザーをプロジェクトに追加したり、後でプロジェクトから削除したりすることもできます。コンソールを使用して最初の管理者ユーザーを追加したら、Amazon Monitron モバイルアプリで他の管理者ユーザーをさらに追加できます。

> **Important**
>
> Amazon Monitron では、アプリユーザーごとに E メールアドレスが必要です。Microsoft Active Directory や外部 ID プロバイダーなどのディレクトリを使用する場合は、ユーザーの E メールアドレスが追加され、同期されていることを確認する必要があります。

トピック

- ユーザーディレクトリのセットアップ
- ユーザーを管理者として追加する
- 管理者ユーザーとしてのユーザーの管理
- 管理者ユーザーの削除
- 招待 E メールの送信

ユーザーディレクトリのセットアップ

Amazon Monitron は AWS IAM Identity Center を使用してユーザーアクセスを管理します。ユーザーはこの IAM アイデンティティセンターのユーザーディレクトリから追加されます。

管理者ユーザーを追加する方法は、IAM アイデンティティセンターが組織でどのようにセットアップされているかによって異なります。

> **Important**
>
> Amazon Monitron では、アプリユーザーごとに E メールアドレスが必要です。Microsoft Active Directory や外部 ID プロバイダーなどのディレクトリを使用する場合は、ユーザーの E メールアドレスが追加され、同期されていることを確認する必要があります。

トピック

- SSO 要件を理解する
- IAM アイデンティティセンターのネイティブディレクトリを使用して管理者ユーザーを追加する
- Microsoft Active Directory を使用して管理者ユーザーを追加する
- 外部 ID プロバイダーを使用して管理ユーザーを追加する
- IAM アイデンティティセンターを使用して Amazon Monitron に戻る

SSO 要件を理解する

プロジェクトを作成すると、Amazon Monitron は IAM アイデンティティセンターがお客様のアカウントで有効化および設定されているかどうか、そして Amazon Monitron で IAM アイデンティティセンターを使用するためのすべての前提条件が満たされているかどうかを自動的に検出します。これらが実行されていない場合、Amazon Monitron はエラーを生成し、必要な前提条件のリストを提供します。管理者ユーザーを追加する前に、すべての前提条件を満たす必要があります。組織における IAM アイデンティティセンターの有効化と設定の詳細については、「AWS Single Sign-On」を参照してください。

Important

Amazon Monitron は、オプトインリージョンと政府リージョンを除くすべての IAM アイデンティティセンターリージョンをサポートします。以下のリストは、サポートされているリージョンです。

- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (東京)
- アジアパシフィック (ソウル)
- アジアパシフィック (大阪)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- カナダ (中部)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (パリ)
- 欧州 (ストックホルム)
- 南米 (サンパウロ)

IAM アイデンティティセンターの前提条件

IAM アイデンティティセンターをセットアップする前に、以下を行う必要があります。

- 最初に AWS Organizations サービスをセットアップし、すべての機能を有効に設定します。この設定の詳細については、「AWS Organizations ユーザーガイド」の「組織内のすべての機能の有効化」を参照してください。
- IAM Identity Center のセットアップを開始する前に、 AWS Organizations 管理アカウントの認証情報を使用してサインインします。IAM アイデンティティセンターの有効化にはこの認証情報が必要です。詳細については、 AWS Organizations ユーザーガイドの AWS 「組織の作成と管理」を参照してください。組織のメンバーアカウントの認証情報を使用してサインインしている場合は、IAM アイデンティティセンターのセットアップを行えません。
- ID ソースを選択して、ユーザーポータルへの SSO アクセスがあるユーザープールを決定します。ユーザーストアにデフォルトの IAM アイデンティティセンター ID ソースを使用するように選択した場合は、前提条件となるタスクは不要です。IAM アイデンティティセンターを有効にすると、IAM アイデンティティセンターストアがデフォルトで作成され、すぐに使用できる状態になります。このストアを使用してもコストは発生しません。また、Azure Active Directory を使用して、外部 ID プロバイダーに接続することもできます。ユーザーストアの既存の Active Directory に接続する場合は、以下の状態である必要があります。
  - 既存の AD Connector または AWS Managed Microsoft AD ディレクトリが にセットアップされており AWS Directory Service、組織の管理アカウント内に存在する必要があります。一度に接続できる AWS Managed Microsoft AD ディレクトリは 1 つのみです。ただし、いつでも別の AWS Managed Microsoft AD ディレクトリに変更したり、IAM Identity Center ストアに戻したりできます。詳細については、「 管理ガイド」の AWS Managed Microsoft AD 「ディレクトリの作成」を参照してください。 AWS Directory Service
  - AWS Managed Microsoft AD ディレクトリがセットアップされているリージョンで IAM アイデンティティセンターをセットアップすること。IAM アイデンティティセンターでは、割り当てデータをディレクトリと同じリージョンに保存します。IAM アイデンティティセンターを管理するには、IAM アイデンティティセンターをセットアップしたリージョンに切り替える必要があります。また、IAM アイデンティティセンターのユーザーポータルでは、接続されたディレクトリと同じアクセス URL が使用されます。
- 現在、次世代ファイアウォール (NGFW) やセキュアウェブゲートウェイ (SWG) などのウェブコンテンツフィルタリングソリューションを使用して、特定の Amazon Web Service (AWS) ドメインや URL エンドポイントへのアクセスをフィルタリングしている場合、IAM アイデンティティセンターを正しく機能させるには、以下のドメインや URL エンドポイントをウェブコンテンツフィルタリングソリューションの許可リストに追加する必要があります。

特定の DNS ドメイン

- *.awsapps.com (http://awsapps.com/)
- *.signin.aws

特定の URL エンドポイント

- https://[お使いのディレクトリ].awsapps.com/start
- https://[お使いのディレクトリ].awsapps.com/login
- https://[お使いのリージョン].signin.aws/platform/login

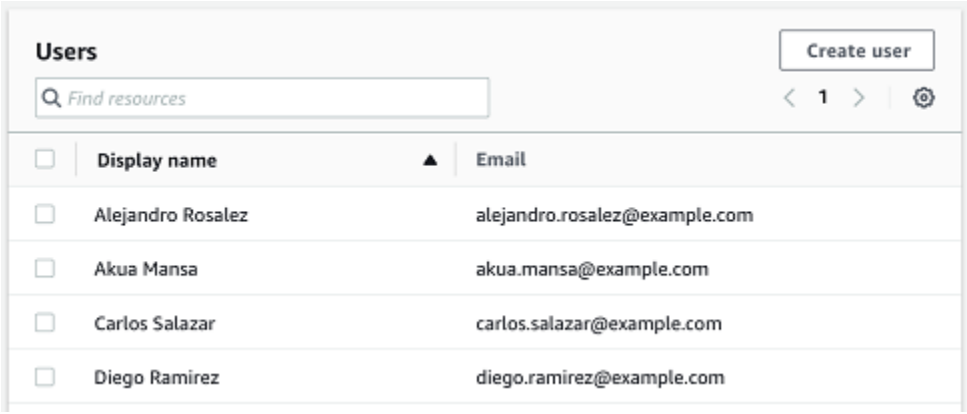
IAM Identity Center を有効にする前に、まず AWS アカウントが IAM ロールのクォータ制限に近づいているかどうかを確認することを強くお勧めします。詳細については、「IAM オブジェクトクォータ」を参照してください。クォータ制限に近づいている場合は、クォータを引き上げることを検討してください。これを行わない場合、IAM ロールの制限を超えたアカウントにアクセス許可セットをプロビジョニングする際に、IAM アイデンティティセンターで問題が発生する可能性があります。

IAM アイデンティティセンターのネイティブディレクトリを使用して管理者ユーザーを追加する

管理者ユーザーをプロジェクトに追加する最も簡単な方法は、IAM アイデンティティセンターのネイティブディレクトリを使用することです。これは Amazon Monitron の使用を開始することで利用でき、IAM アイデンティティセンターを基本レベルで使用できるようになります。Amazon Monitron を使用する前に IAM アイデンティティセンターをセットアップし、ネイティブディレクトリを使用するように設定することもできます。どちらの方法でも、ユーザーを手動で追加でき、名前と E メールアドレス以外のユーザー ID 情報が他の管理者ユーザーに公開される可能性はありません。

IAM アイデンティティセンターのネイティブディレクトリを使用する際に管理者ユーザーを追加するには

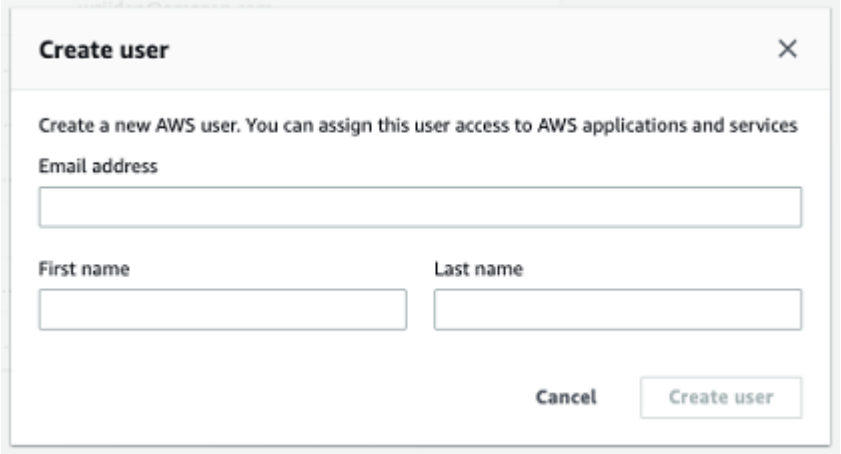
1. Amazon Monitron コンソール (https://console.aws.amazon.com/monitron) を開きます。
2. [プロジェクトを作成] を選択します。
3. ナビゲーションペインで目的のプロジェクトを選択します。
4. [ユーザー] ページで、管理者ユーザーに割り当てるユーザーを選択します。ユーザーが表示されない場合は、そのユーザーを検索します。



選択したユーザーは、[選択されたユーザー] セクションに表示されます。

5. 目的のユーザーがディレクトリにいない場合は、[ユーザーを作成] をクリックしてユーザーを追加します。

   1. [ユーザーを作成] の [E メールアドレス] に、新しい管理者ユーザーのメールアドレスを入力します。



   2. [名] と [姓] に管理者の名前を入力します。
   3. [ユーザーを作成] をクリックします。

6. ユーザー名がディレクトリのリストに表示されたら、[追加] をクリックして選択した管理者ユーザーを追加します。
7. Amazon Monitron モバイルアプリをダウンロードするためのリンクを含む、プロジェクトへの招待 E メールを管理者ユーザーに送信します。詳細については、「招待 E メールの送信」を参照してください。

   Amazon Monitron は、プロジェクトの [プロジェクト] ページに移動します。このページには、すべての管理者ユーザーがリストで表示されています。

8. 管理者ユーザーをさらに追加するには、[管理者を追加] をクリックします。

   管理者ユーザーは誰でも、Amazon Monitron モバイルアプリを使用してその他のユーザーを追加できます。詳細については、「Amazon Monitron ユーザーガイド」の「Adding a User」を参照してください。

Microsoft Active Directory を使用して管理者ユーザーを追加する

組織のプライマリユーザーディレクトリに Microsoft Active Directory (AD) を使用している場合は、Microsoft AD を使用するように IAM アイデンティティセンターを設定できます。IAM Identity Center では、 AWS Directory Service を使用して、セルフマネージド Active Directory を AWS Managed Microsoft AD ディレクトリとして接続できます。この Microsoft AD ディレクトリは、Amazon Monitron コンソール (または Amazon Monitron モバイルアプリ) を使用してユーザーロールを割り当てる際に、プル元の ID プールを提供します。

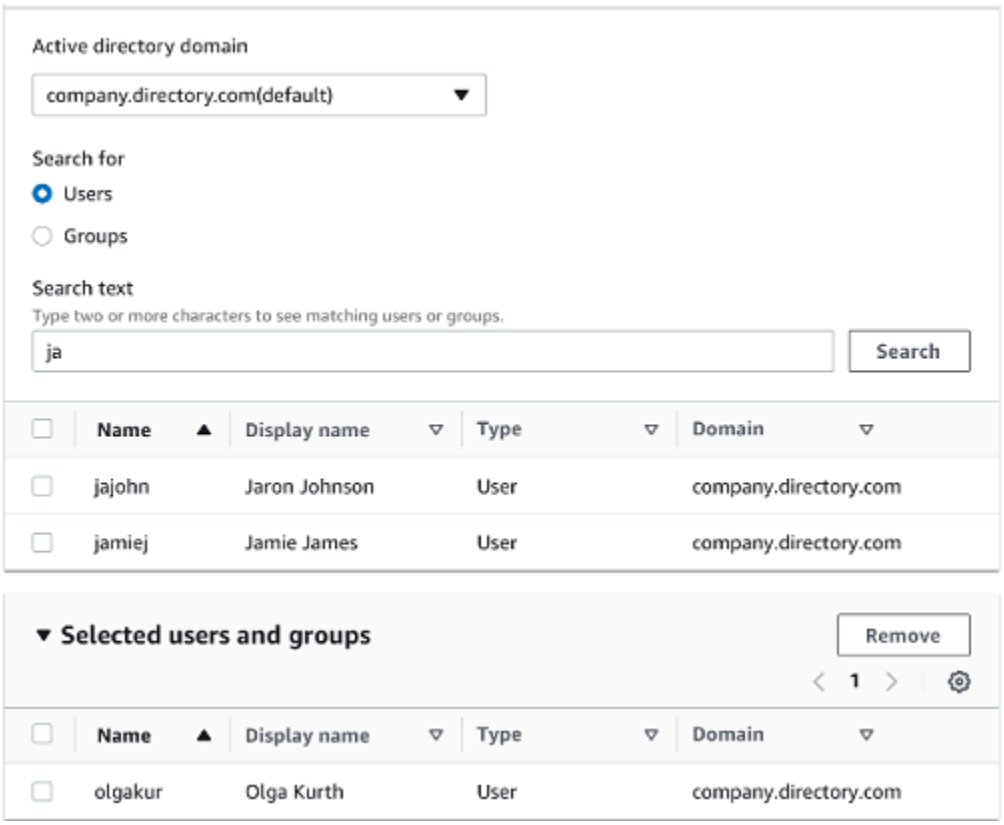
> **Important**
>
> Amazon Monitron では、アプリユーザーごとに E メールアドレスが必要です。ユーザーの E メールアドレスが追加され、同期されていることを確認してください。

すべての Amazon Monitron 管理者ユーザーは、Amazon Monitron の IAM アイデンティティセンターで設定されているユーザーディレクトリの ID 情報にアクセスできます。ユーザーの組織情報へのアクセスを制限したい場合は、独立したディレクトリを使用することを強くお勧めします。

Microsoft Active Directory を使用して管理者ユーザーを追加するには

1. Microsoft Active Directory に接続するように IAM アイデンティティセンターを設定します。これに関連する手順は、セルフマネージド Active Directory と AWS Managed Microsoft AD ディレクトリのどちらを使用しているかによって異なります。詳細については、「Connect to Microsoft AD Directory」を参照してください。
2. Amazon Monitron コンソール (https://console.aws.amazon.com/monitron) を開きます。

3. [プロジェクトを作成] を選択します。
4. ナビゲーションペインで目的のプロジェクトを選択します。
5. [Active Directory ドメイン] で、ID を追加するディレクトリドメインを選択します。



6. ユーザーディレクトリの検索方法に応じて、[ユーザー] または [グループ] を選択します。
7. 検索ボックスに追加する ID の文字列を入力して、[検索] をクリックします。

   返されるユーザーの数を制限するには、検索ボックスに長い文字列を入力します。例えば、検索ボックスに「olg」と入力すると、「Olga Kurth」や「Jamie Folgman」など、名前に「olg」という文字が含まれるすべてのユーザーがリストに表示されます。
8. 管理者ユーザーに割り当てるユーザーを選択します。
9. [追加] をクリックして管理者ユーザーを追加します。

外部 ID プロバイダーを使用して管理ユーザーを追加する

外部 ID プロバイダー (IdP) を使用している場合は、Security Assertion Markup Language (SAML) 2.0 規格を経由して、そのプロバイダーを使用するように IAM アイデンティティセンターを設定できます。これにより、IdP ディレクトリ内の ID プールがわかります。Amazon Monitron コンソール (または Amazon Monitron モバイルアプリ) を使用する際にこのプールを取得し、そこに管理者

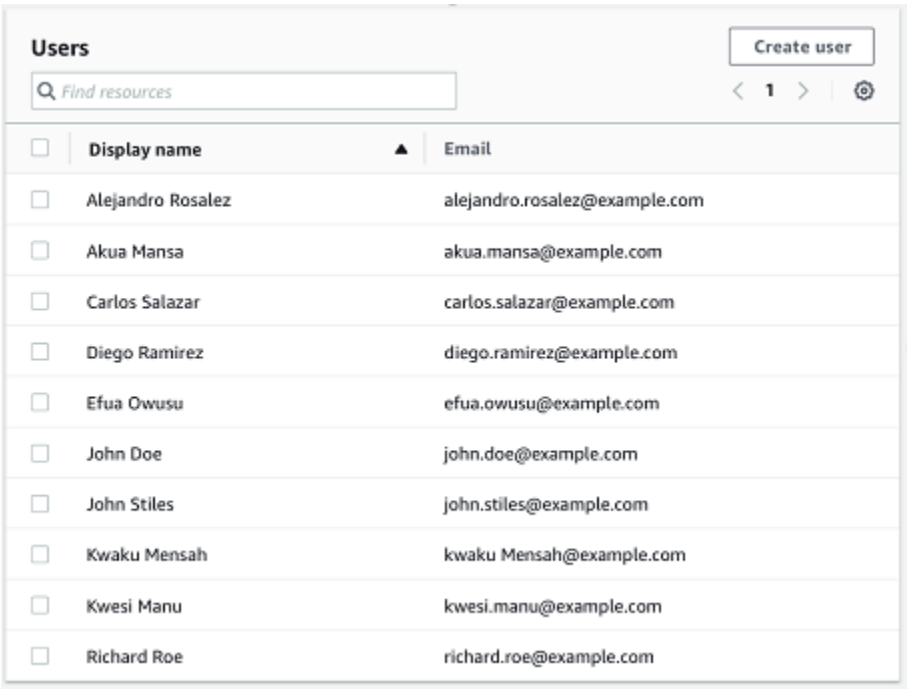
ユーザーを割り当てることができます。これにより、ユーザーは企業の認証情報を使用して Amazon Monitron にサインインできるようになります。

> **Important**
>
> Amazon Monitron では、アプリユーザーごとに E メールアドレスが必要です。ユーザーの E メールアドレスが追加され、同期されていることを確認してください。

すべての Amazon Monitron 管理者ユーザーは、Amazon Monitron の IAM アイデンティティセンターで設定されているユーザーディレクトリの ID 情報にアクセスできます。ユーザーの組織情報へのアクセスを制限したい場合は、独立したディレクトリを使用することを強くお勧めします。

外部 ID プロバイダー (IdP) を使用して管理者ユーザーを追加するには

1. 外部 AWS IdP に接続するように IAM アイデンティティセンターを設定します。これに関連するステップは、使用しているプロバイダーによって異なります。詳細については、「Connect to Your External ID Provider」を参照してください。
2. Amazon Monitron コンソール (https://console.aws.amazon.com/monitron) を開きます。
3. [プロジェクトを作成] を選択します。
4. ナビゲーションペインで目的のプロジェクトを選択します。
5. [ユーザー] ページで、管理者ユーザーに割り当てるユーザーを選択します。ユーザーが表示されない場合は、そのユーザーを検索します。



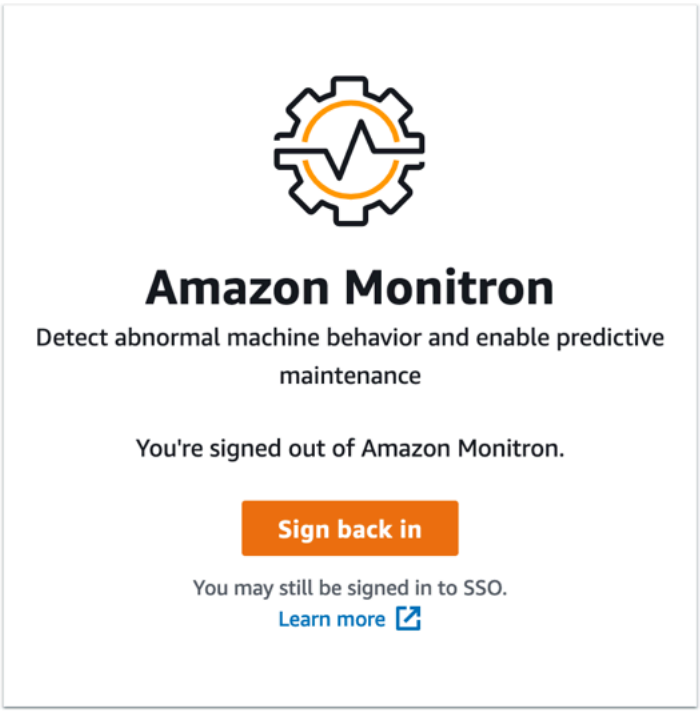
6. [追加] をクリックして管理者ユーザーを追加します。

IAM アイデンティティセンターを使用して Amazon Monitron に戻る

Amazon Monitron ウェブアプリからログアウトしても、 にサインインしている可能性があります AWS IAM Identity Center。ユーザーポータルから開いた他のアプリケーションは開いたままで実行されています。

IAM アイデンティティセンターからログアウトする方法は 2 つあります。

- IAM アイデンティティセンターポータルから直接ログアウトします。
- AWS IAM Identity Center は 1 時間に 1 回、サービスを積極的に使用しているかどうかを確認します AWS 。使用していない場合は、IAM アイデンティティセンターから自動的にログアウトされます。



IAM アイデンティティセンターを使用する管理者ユーザーの詳細については、「ユーザーディレクトリのセットアップ」を参照してください。

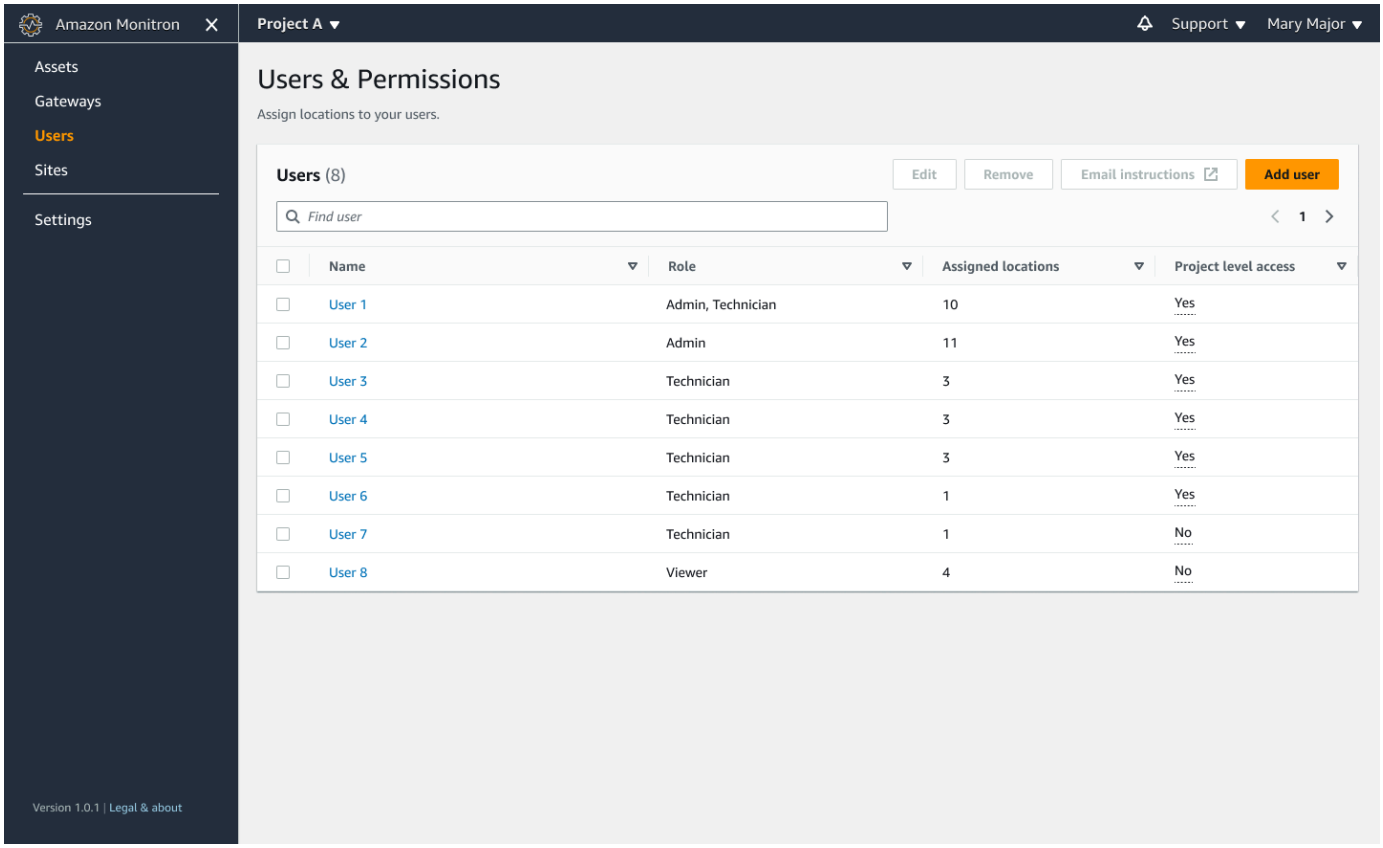
Amazon Monitron と IAM Identity Center のセキュリティのベストプラクティスについては、「 のセキュリティのベストプラクティス Amazon Monitron」を参照してください。

SSO ユーザーポータルの使用方法については、「Using the user portal」を参照してください。

ユーザーを管理者として追加する

管理者は、Amazon Monitron ウェブアプリに他のユーザー (他の管理者ユーザーを含む) を追加できます。

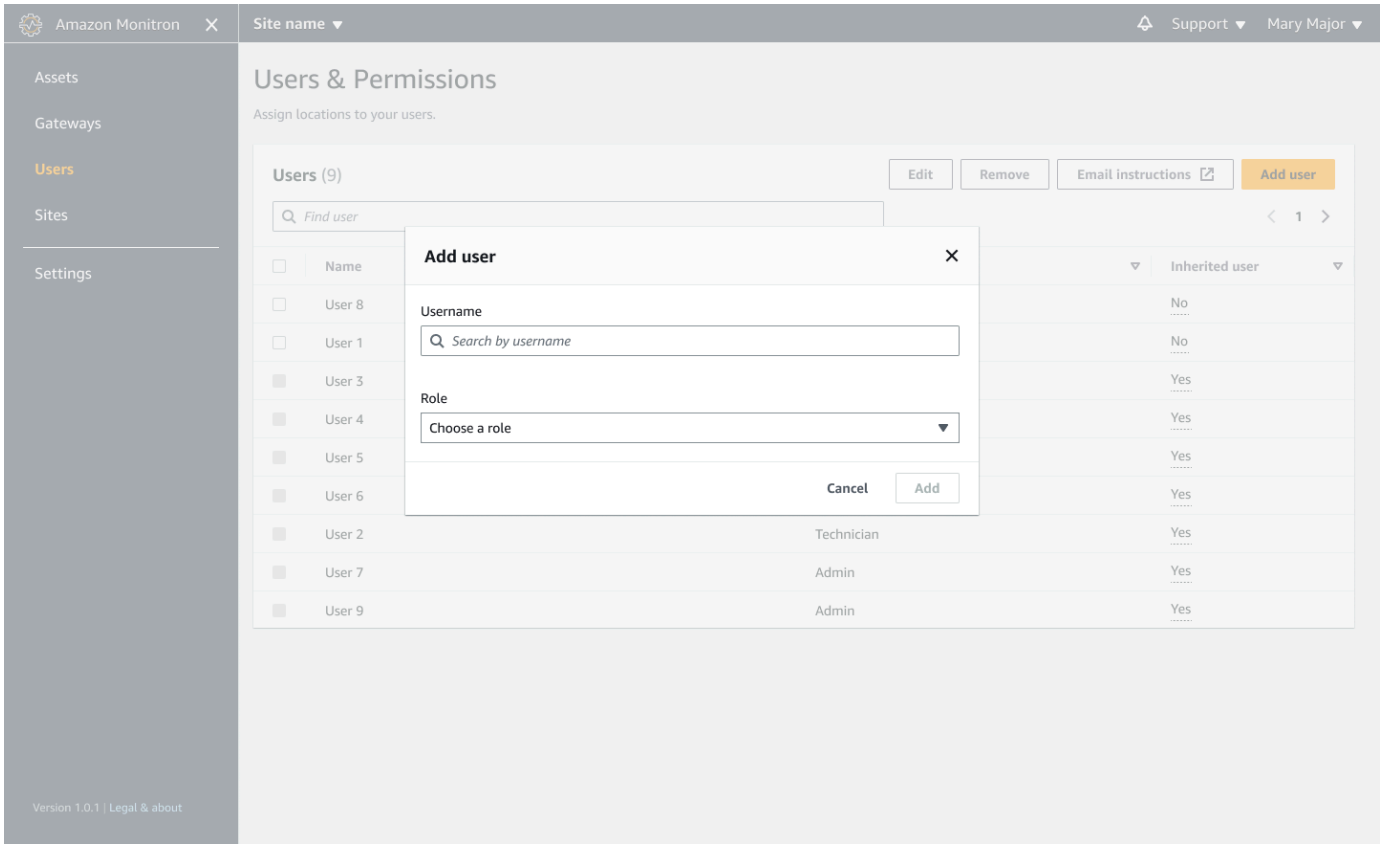
1. ユーザーを追加するプロジェクトまたはサイトに移動し、[ユーザー] のリストに移動します。



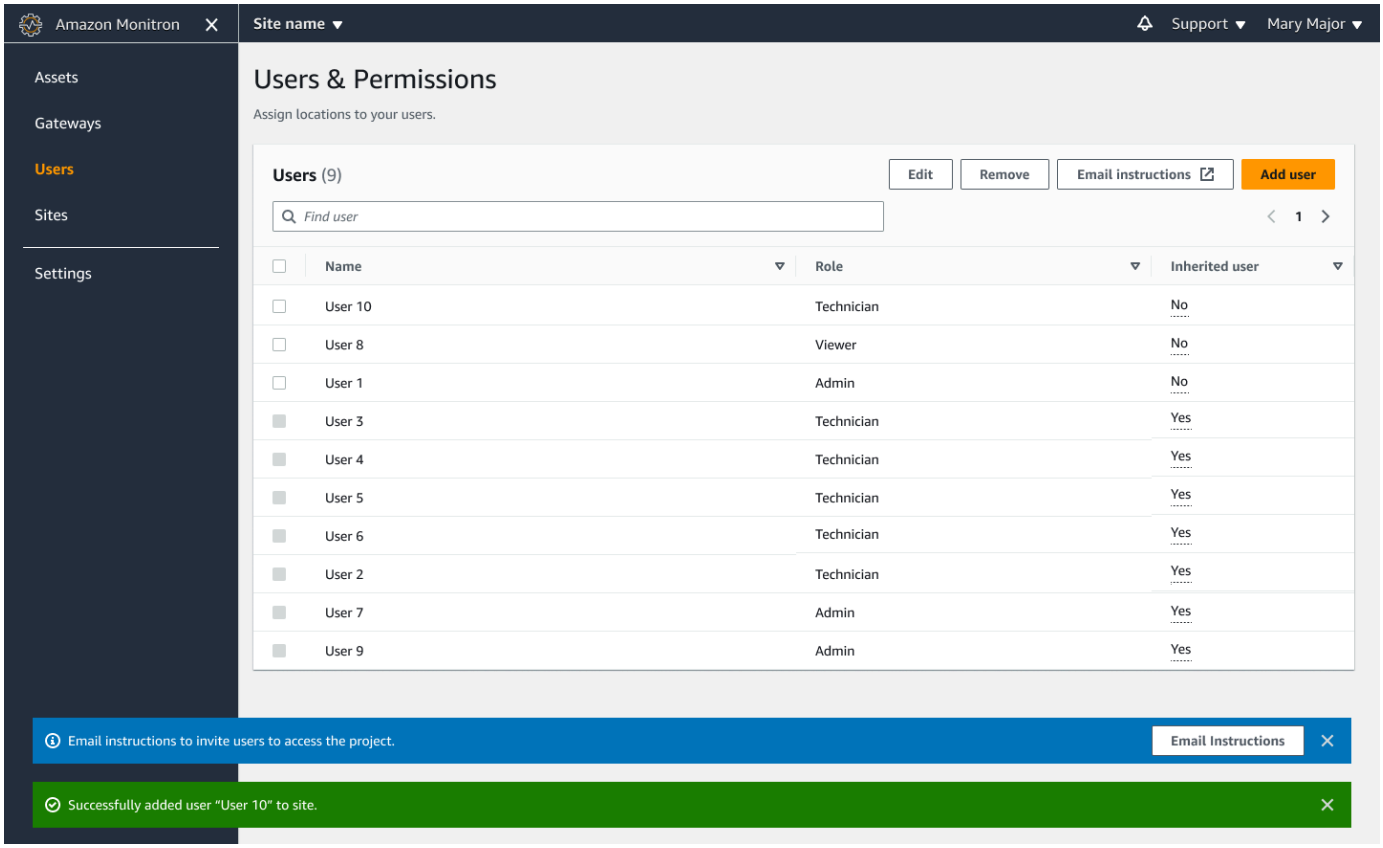
2. ユーザー名を入力します。Amazon Monitron がユーザーディレクトリでユーザーを検索します。

   リストからユーザーを選択し、ユーザーに割り当てるロールを管理者、技術者、またはビューワーを選択します。

   次に、ユーザーの追加を選択します。



3. 新しいユーザーが [ユーザー] のリストに表示されます。



新しいユーザーに、プロジェクトにアクセスして Amazon Monitron モバイルアプリをダウンロードするためのリンクを含む、招待 E メールを送信します。詳細については、「招待 E メールの送信」を参照してください。

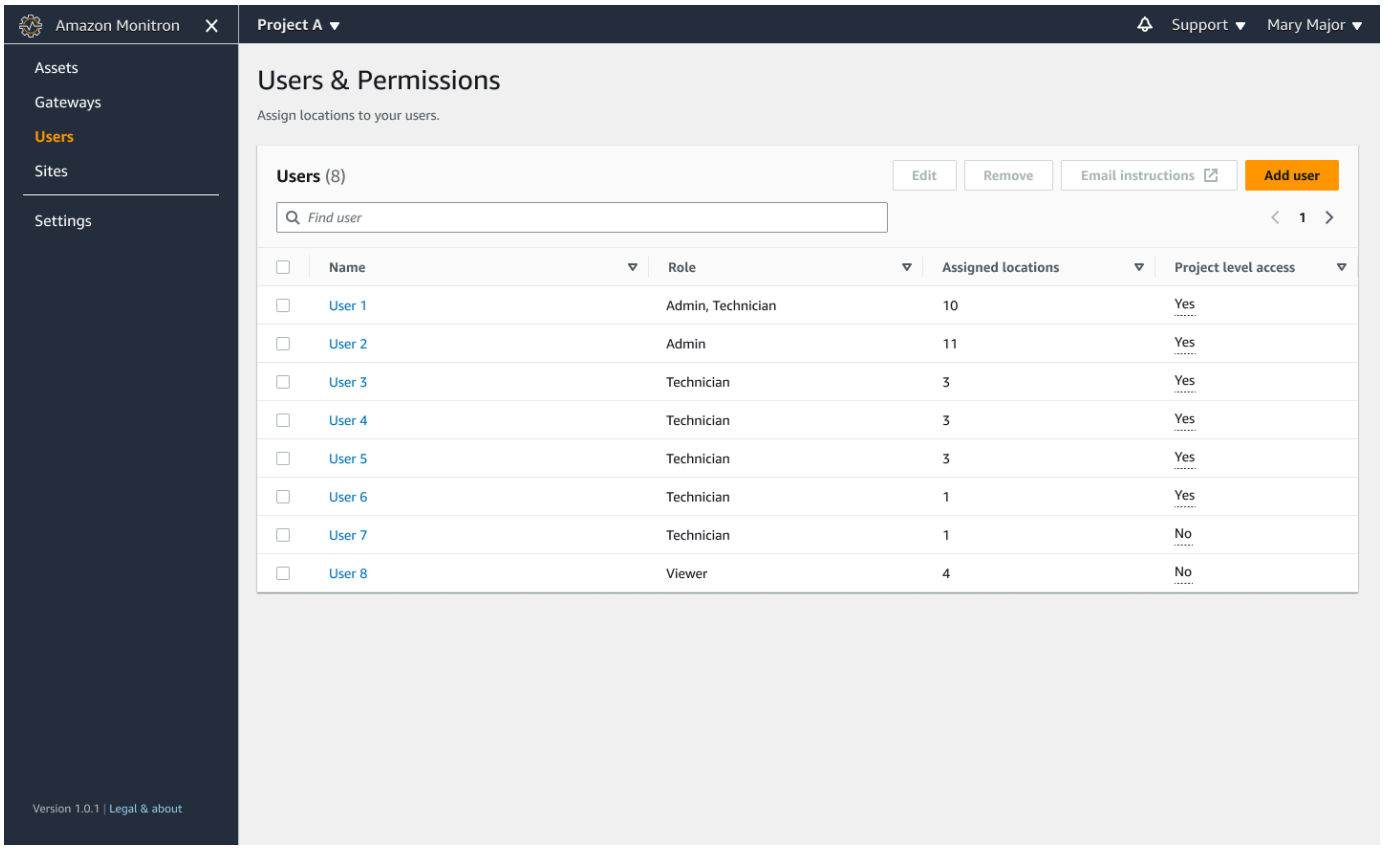
管理者ユーザーとしてのユーザーの管理

管理者は、ユーザーのリストを使用して Amazon Monitron ウェブアプリでユーザーを管理できます。プロジェクトレベルの管理者は、プロジェクトレベルのすべてのユーザーと、特定のサイトレベルのすべてのユーザーを表示できます。

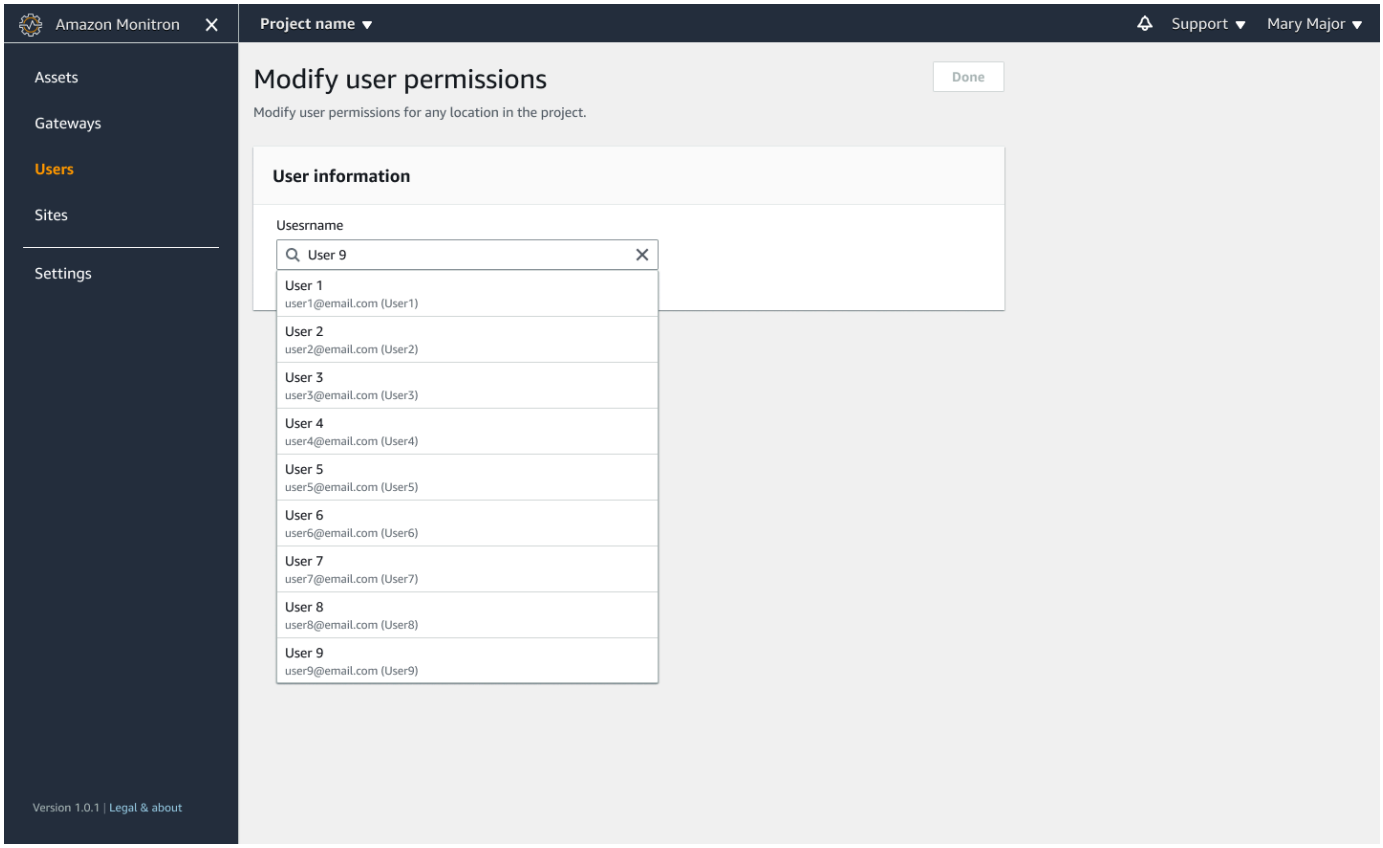
ユーザーとアクセス許可ページには、ユーザー管理を容易にするために以下の情報が表示されます。

- 名前 – ユーザーの名前。
- ロール – 管理者、技術者、閲覧者、またはこれらの組み合わせにかかわらず、ユーザーに割り当てられたロール。
- 割り当てられたロケーション – ユーザーが割り当てられているロケーションの数。
- プロジェクトレベルのアクセス – ユーザーがプロジェクトレベルのアクセスを持っているか、特定のサイトレベルのアクセスのみを持っているか。

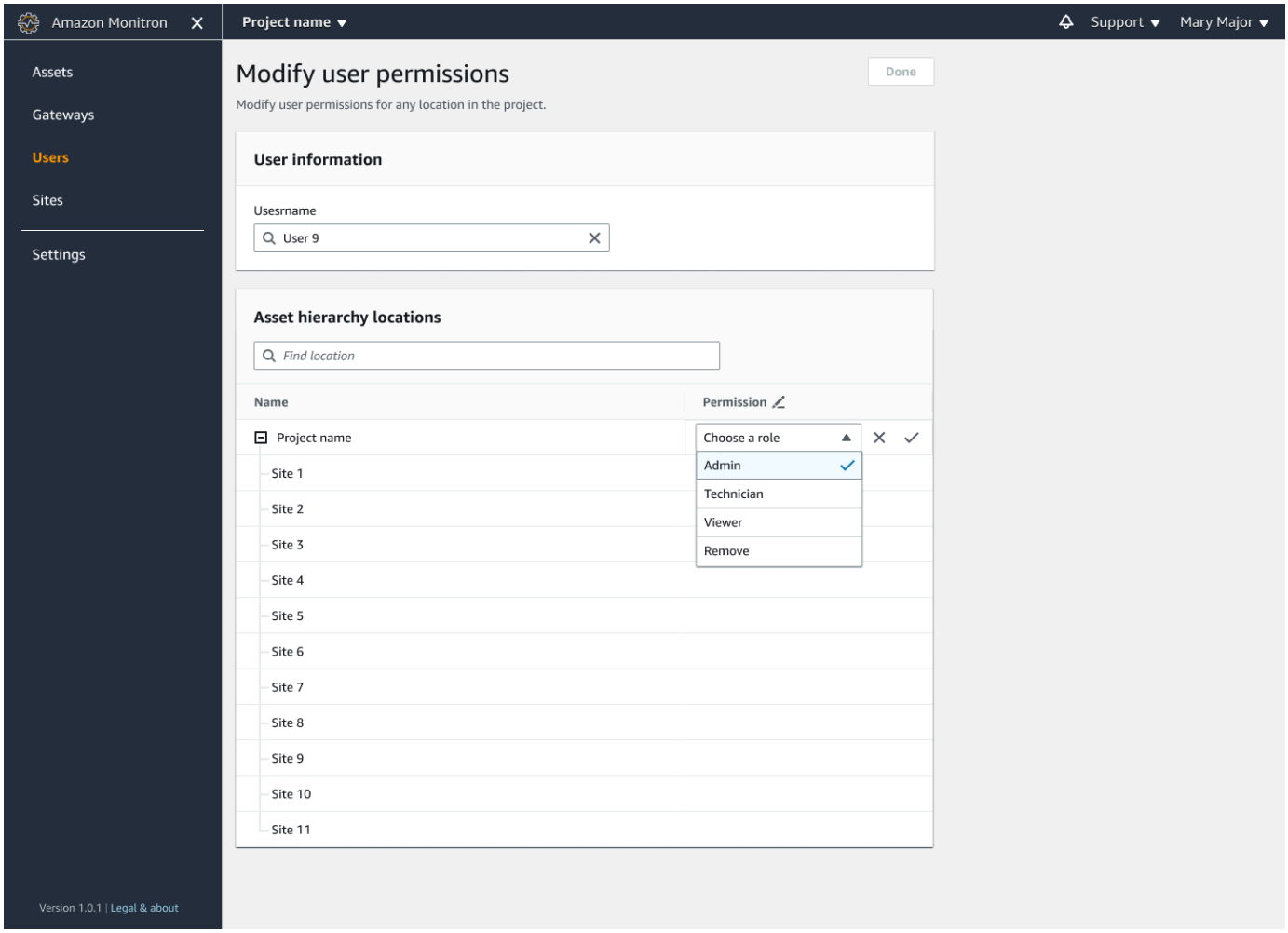
1. ユーザーを追加するプロジェクトまたはサイト、またはユーザーアクセス許可の更新元のプロジェクトまたはサイトに移動し、ユーザーとアクセス許可リストに移動します。



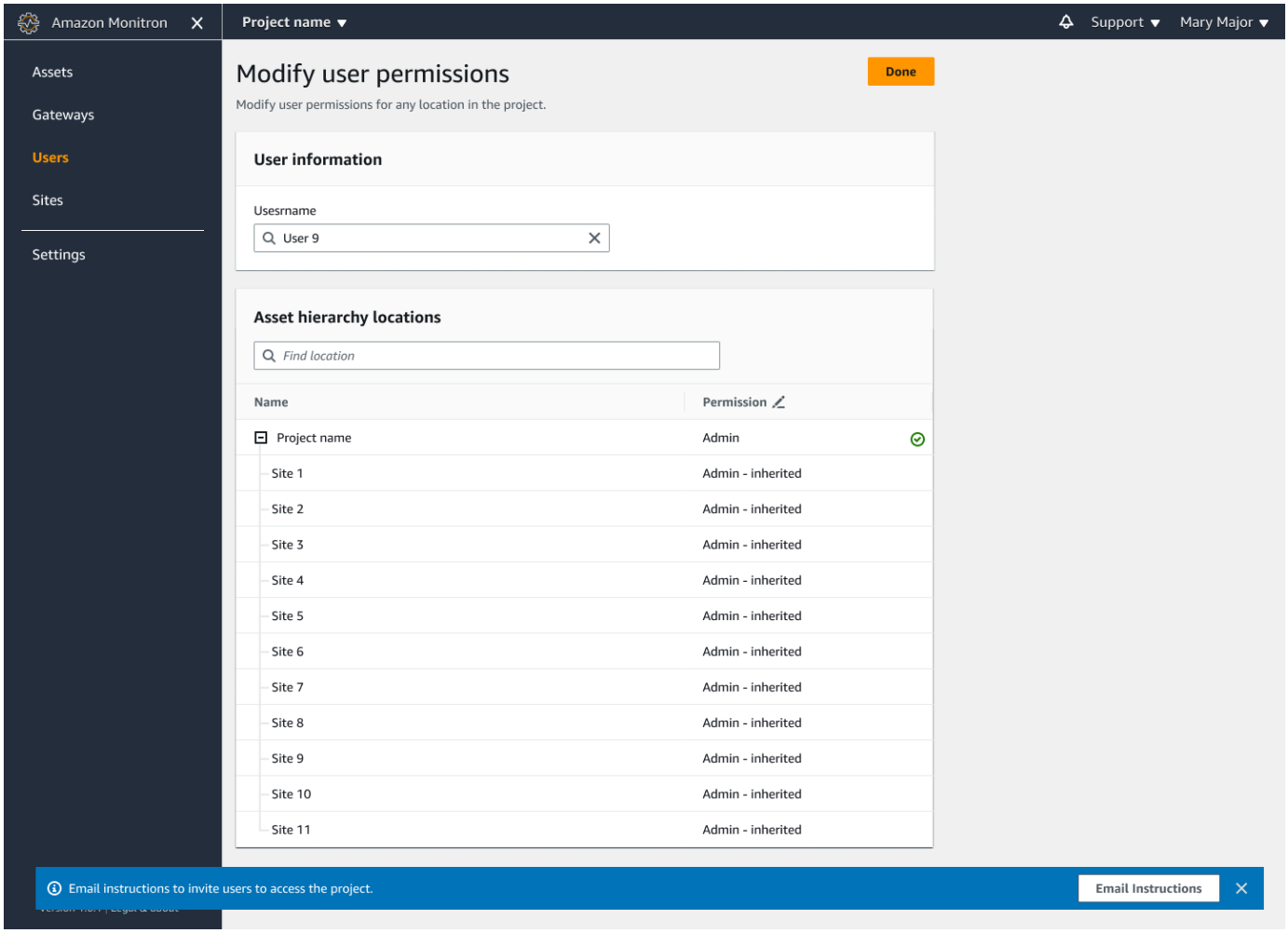
2. [Edit] (編集) を選択します。次に、ユーザー名のユーザーアクセス許可の変更ページから、詳細を表示または編集するユーザーを選択します。Amazon Monitron は、ユーザーが割り当てられている場所のリストを表示します。



3. ユーザーに割り当てられたロールを変更するには、管理者、技術者、閲覧者のいずれかを選択します。または、ユーザーを削除することもできます。次に、[完了] を選択します。



Amazon Monitron は、ユーザーがすべてのロケーションにアクセス許可を割り当てられた方法を示します。プロジェクトレベルで管理者ロールが割り当てられているユーザーは、そのプロジェクト内のすべての場所へのアクセスを継承します。この場合、Amazon Monitron はアクセスレベルを管理者 - 継承として示します。



管理者ユーザーの削除

すべてのプロジェクトには、管理者ユーザーが少なくとも 1 人必要です。プロジェクトから管理者ユーザーを削除する前に、他の管理者ユーザーが少なくとも 1 人割り当てられていることを確認してください。

トピック

- 管理者ユーザーを削除するには

管理者ユーザーを削除するには

1. Amazon Monitron コンソール (https://console.aws.amazon.com/monitron) を開きます。
2. [プロジェクトを作成] を選択します。
3. ナビゲーションペインで目的のプロジェクトを選択します。

4. [管理者ユーザー]のリストから、削除するユーザーを選択します。
5. [削除] をクリックします。
6. [削除] を再度クリックします。

   プロジェクトの管理者ユーザーのリストからユーザーが削除されます。

招待 E メールの送信

Amazon Monitron プロジェクトまたはサイトにユーザーを追加すると、そのユーザーに対して、Amazon Monitron モバイルアプリまたはウェブアプリをダウンロードしてログインするよう招待する E メールが送信されます。この招待 E メールには、プロジェクトに接続するための手順も含まれています。

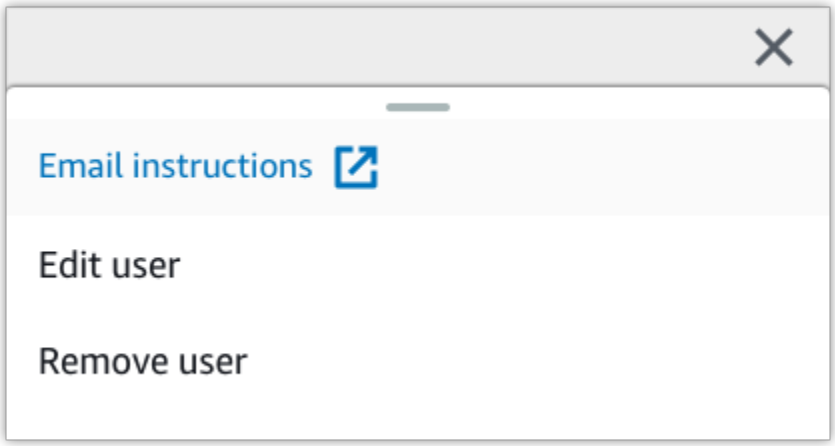
トピック

- モバイルアプリを使用してサイトまたはプロジェクトへの招待 E メールを生成するには
- ウェブアプリを使用してサイトまたはプロジェクトへの招待 E メールを生成するには

モバイルアプリを使用してサイトまたはプロジェクトへの招待 E メールを生成するには

1. ユーザーをサイトまたはプロジェクトに追加します。
2. 追加したユーザーの横にある縦 3 点アイコン

   ( )
   を選択します。
3. [E メールによる指示] を選択します。



E メールアプリケーションが立ち上がり、そのユーザー宛の招待内容の下書きが表示されます。これには、2 つのリンクが含まれます。1 つは、Google Play ストアから Amazon Monitron モバイルアプリをダウンロードするためのリンクです。もう 1 つは、ユーザーが追加されたプロジェクトを開くためのリンクです。

4. E メール内容が正しいことを確認し、ユーザーに送信します。

ウェブアプリを使用してサイトまたはプロジェクトへの招待 E メールを生成するには

1. ユーザーをサイトまたはプロジェクトに追加します。
2. 左側のナビゲーションペインで [ユーザー] を選択します。
3. [E メールによる指示] を選択します。
4. E メールアプリケーションが立ち上がり、そのユーザー宛の招待内容の下書きが表示されます。これには、2 つのリンクが含まれます。1 つは、Google Play ストアから Amazon Monitron モバイルアプリをダウンロードするためのリンクです。もう 1 つは、ユーザーが追加されたプロジェクトを開くためのリンクです。
5. E メール内容が正しいことを確認し、ユーザーに送信します。

> **Warning**
>
> フィッシング攻撃に注意してください。Amazon Monitron プロジェクトの招待 E メールになりすました E メールが攻撃者から届く場合があります。受信するユーザーには、サインイン認証情報を入力する前に、ディレクトリ名がログイン画面に表示されていることを確認するように警告してください。

管理者以外のユーザーの管理

プロジェクトまたはサイトを作成したら、そこにユーザーを追加する必要があります。管理者ユーザーは、Admin、Technician、Viewer の 3 つの異なるロールにユーザーを追加できます。

ユーザーのロールによって、Amazon Monitron で何ができるかが決まります。ユーザーのロールが持つアクセス許可の範囲は、そのロールがプロジェクトレベルで追加されたのか、サイトレベルで追加されたのかによって決まります。ユーザーのロールセットをプロジェクトレベルで設定すると、ユーザーに付与されるアクセス許可は、そのプロジェクト内の全サイトに適用されます。ユーザーのロールをサイトレベルで設定すると、ユーザーに付与されるアクセス許可はそのサイトにのみ適用されます。

トピック

- ユーザーのリストの表示
- ユーザーの追加
- ユーザーロールの変更
- ユーザーの削除

ユーザーのリストの表示

管理者は、ユーザーのリストを使用して Amazon Monitron アプリでユーザーを管理できます。ユーザーのリストを表示するには、3 つのレベルから選択できます (管理者ロールによって異なります)。

- プロジェクトレベルの管理者は、プロジェクトレベルですべてのユーザーを表示できます。
- プロジェクトレベルの管理者は、特定のサイトレベルですべてのユーザーを表示できます。
- サイトレベルの管理者は、特定のサイトレベルですべてのユーザーを表示できます。

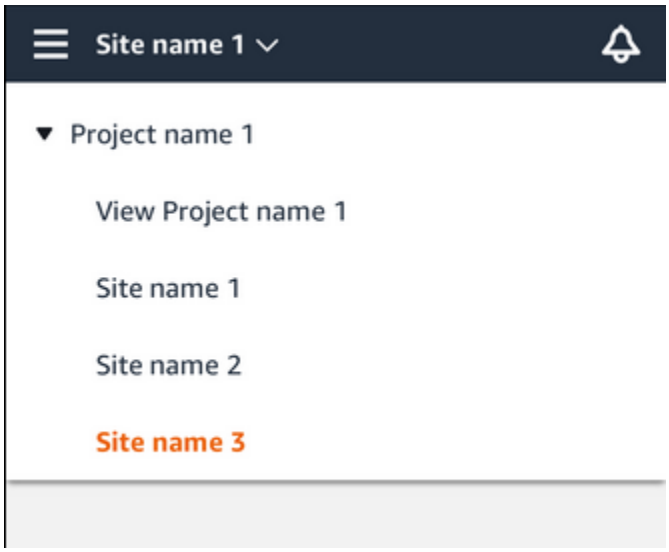
トピック

- ユーザーのリストをモバイルアプリで表示するには
- ユーザーのリストをウェブアプリで表示するには

ユーザーのリストをモバイルアプリで表示するには

1. スマートフォンで Amazon Monitron モバイルアプリにログインします。

2. ユーザーを表示するプロジェクトまたはサイトを選択します。



3. メニューアイコン (☰) をクリックします。

4. [ユーザー] を選択します。

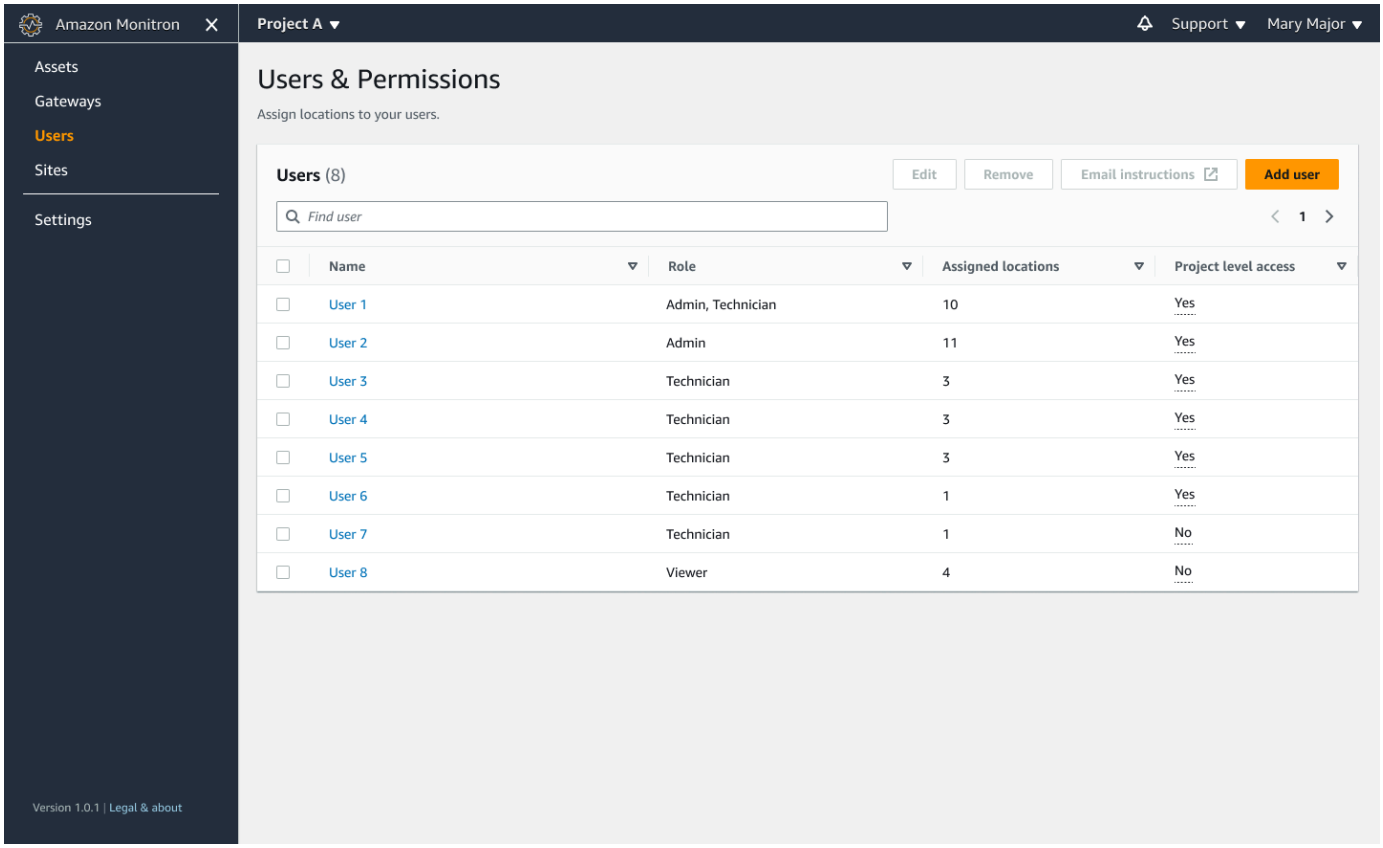
   プロジェクトまたはサイトに関連付けられているすべてのユーザーのリストが表示されます。

ユーザーのリストをウェブアプリで表示するには

ユーザーとアクセス許可ページには、ユーザー管理を容易にするために以下の情報が表示されます。

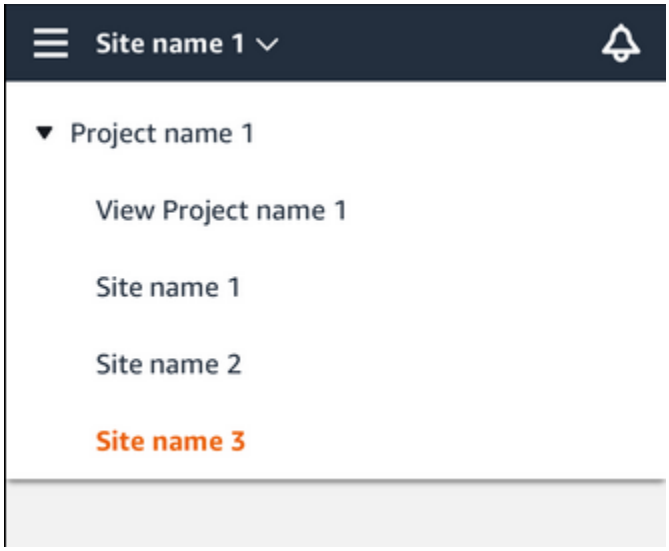
- 名前 – ユーザーの名前。
- ロール – 管理者、技術者、閲覧者、またはこれらの組み合わせにかかわらず、ユーザーに割り当てられたロール。
- 割り当てられたロケーション – ユーザーが割り当てられているロケーションの数。
- プロジェクトレベルのアクセス – ユーザーがプロジェクトレベルのアクセスを持っているか、特定のサイトレベルのアクセスのみを持っているか。

1. Amazon Monitron ウェブアプリにログインします。
2. 左側のナビゲーションペインで [ユーザー] を選択します。ユーザーのリストが表示されます。



3. ユーザーを表示するプロジェクトまたはサイトを選択します。

   プロジェクトまたはサイトに関連付けられているすべてのユーザーのリストが表示されます。



ユーザーの追加

新しいユーザーを追加する際、そのユーザーが持つアクセス許可は選択したロールによって決まります。

ユーザーには、以下のロールを割り当てることができます。

- 管理者: 管理者ユーザーは、自分が追加されたプロジェクトまたはサイト内のすべてのリソースに完全にアクセスできます。他のユーザーの追加、アセットの作成、センサーとアセットのペアリングなどを行うことができます。また、アセットをモニタリングし、異常を認識して解決することもできます。プロジェクトレベルで追加された場合、このユーザーのアクセス許可はプロジェクト全体に及びます。サイトレベルで追加された場合、このユーザーのアクセス許可はそのサイトのみに制限されます。
- 技術者: 技術者ユーザーは、追加先のプロジェクトまたはサイトに対する読み取り専用のアクセス許可と、アセットをモニタリングし、異常を認識して解決するためのアクセス許可を持ちます。プロジェクトレベルで追加された場合、このユーザーのアクセス許可はプロジェクト全体に及びます。サイトレベルで追加された場合、このユーザーのアクセス許可はそのサイトのみに適用されます。
- 読み取り専用: 読み取り専用のアクセス許可を持つユーザーには、追加先のプロジェクトまたはサイト内のすべてのリソースの詳細を読み取るアクセス許可が付与されています (追加、変更、削除はできません)。

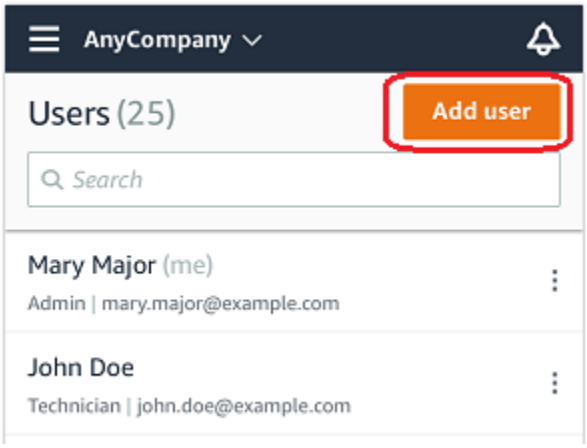
新しいユーザーをプロジェクトまたはサイトに追加する手順は同じです。

トピック

- モバイルアプリを使用してユーザーを追加するには
- ウェブアプリを使用してユーザーを追加するには

モバイルアプリを使用してユーザーを追加するには

1. スマートフォンで Amazon Monitron モバイルアプリにログインします。
2. ユーザーを追加するプロジェクトまたはサイトに移動し、[ユーザー] のリストに移動します。
3. [ユーザーを追加] を選択します。



4. ユーザー名を入力します。

   Amazon Monitron がユーザーディレクトリでユーザーを検索します。

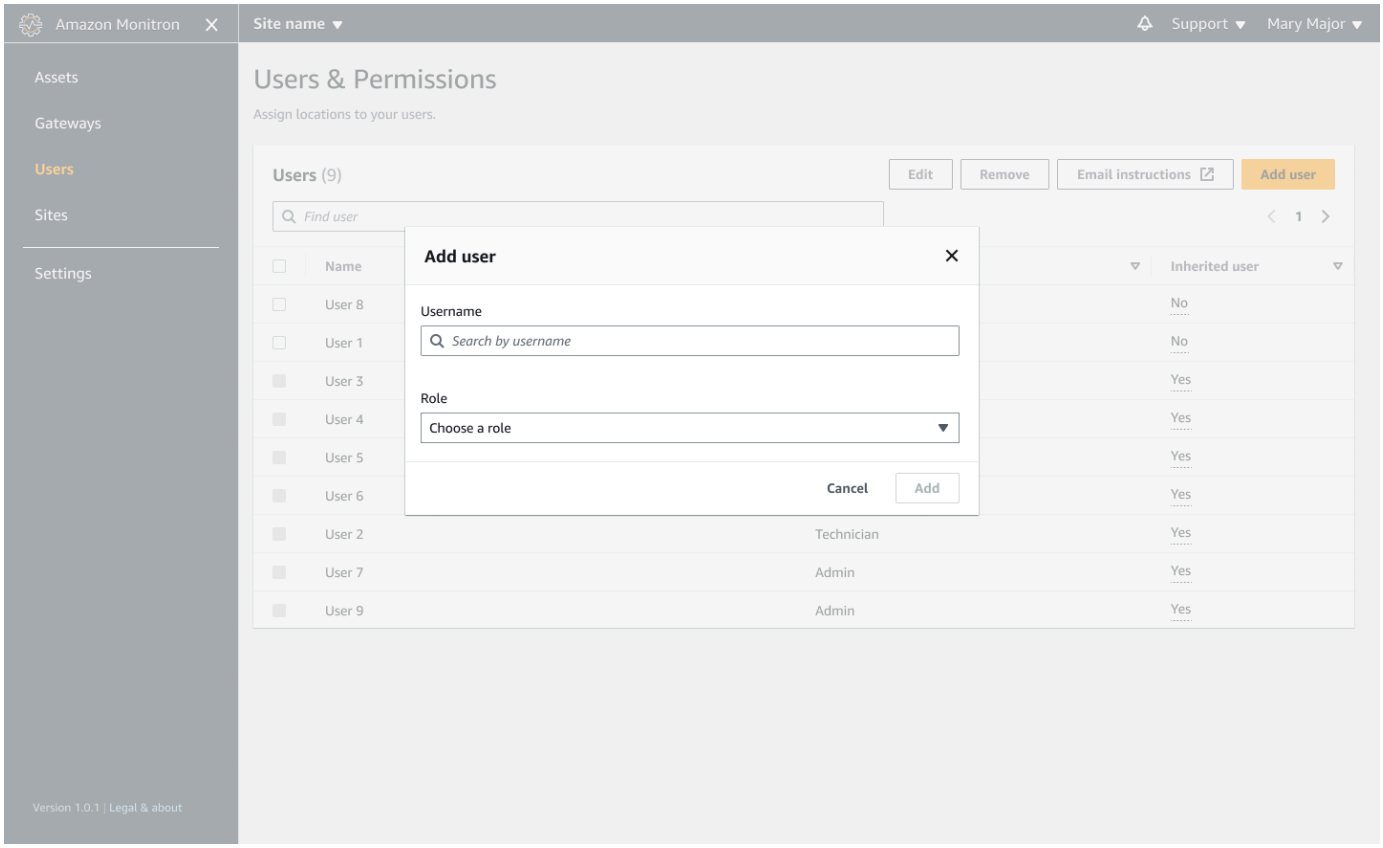
5. リストからユーザーを選択します。
6. ユーザーに割り当てるロールを [管理者]、[技術者]、[閲覧者] から選択します。
7. [追加] を選択します。

   新しいユーザーが [ユーザー] のリストに表示されます。

8. 新しいユーザーに、プロジェクトにアクセスして Amazon Monitron モバイルアプリをダウンロードするためのリンクを含む、招待 E メールを送信します。詳細については、「招待 E メールの送信」を参照してください。

ウェブアプリを使用してユーザーを追加するには

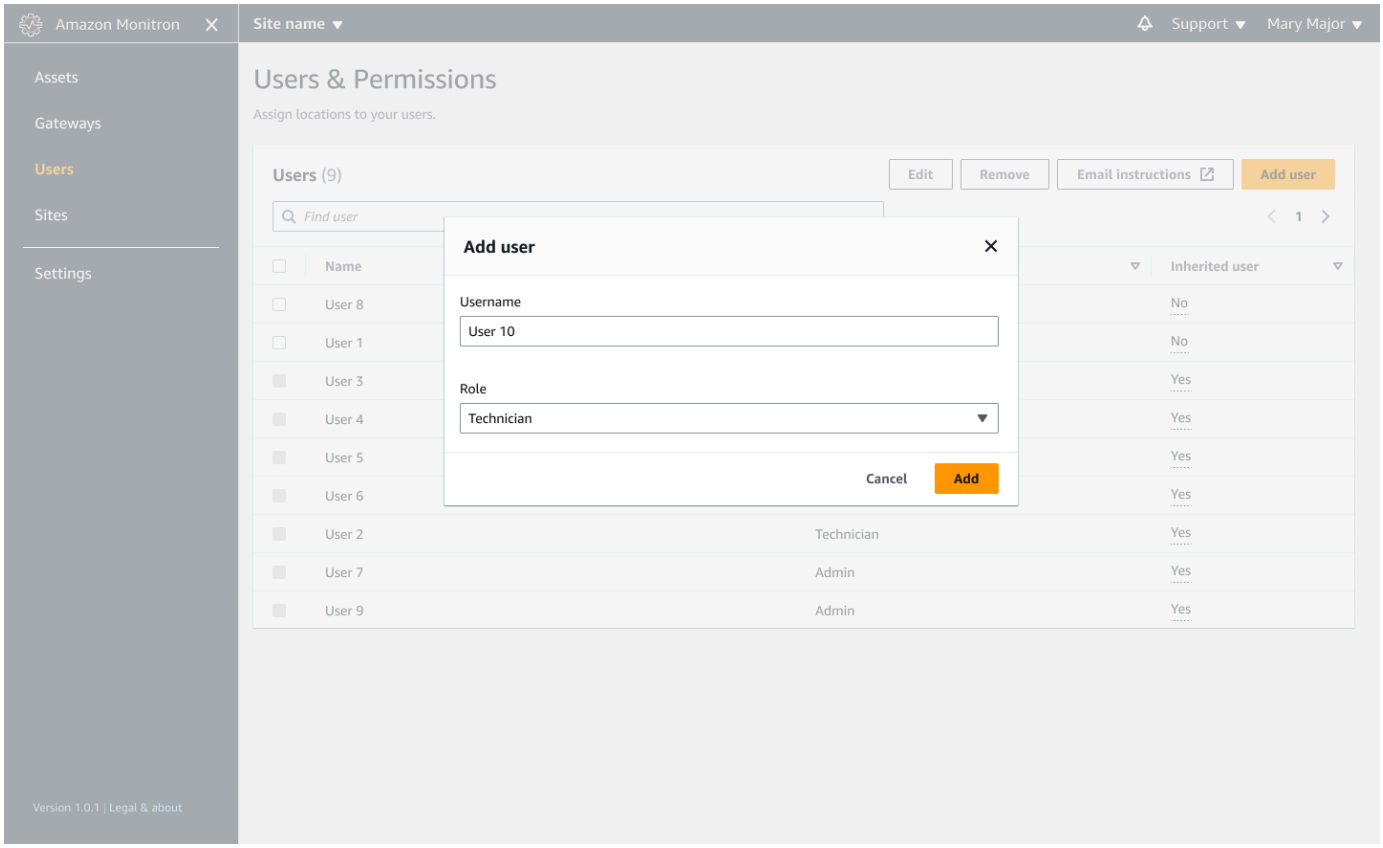
1. ユーザーを追加するプロジェクトまたはサイトに移動し、[ユーザー] のリストに移動します。



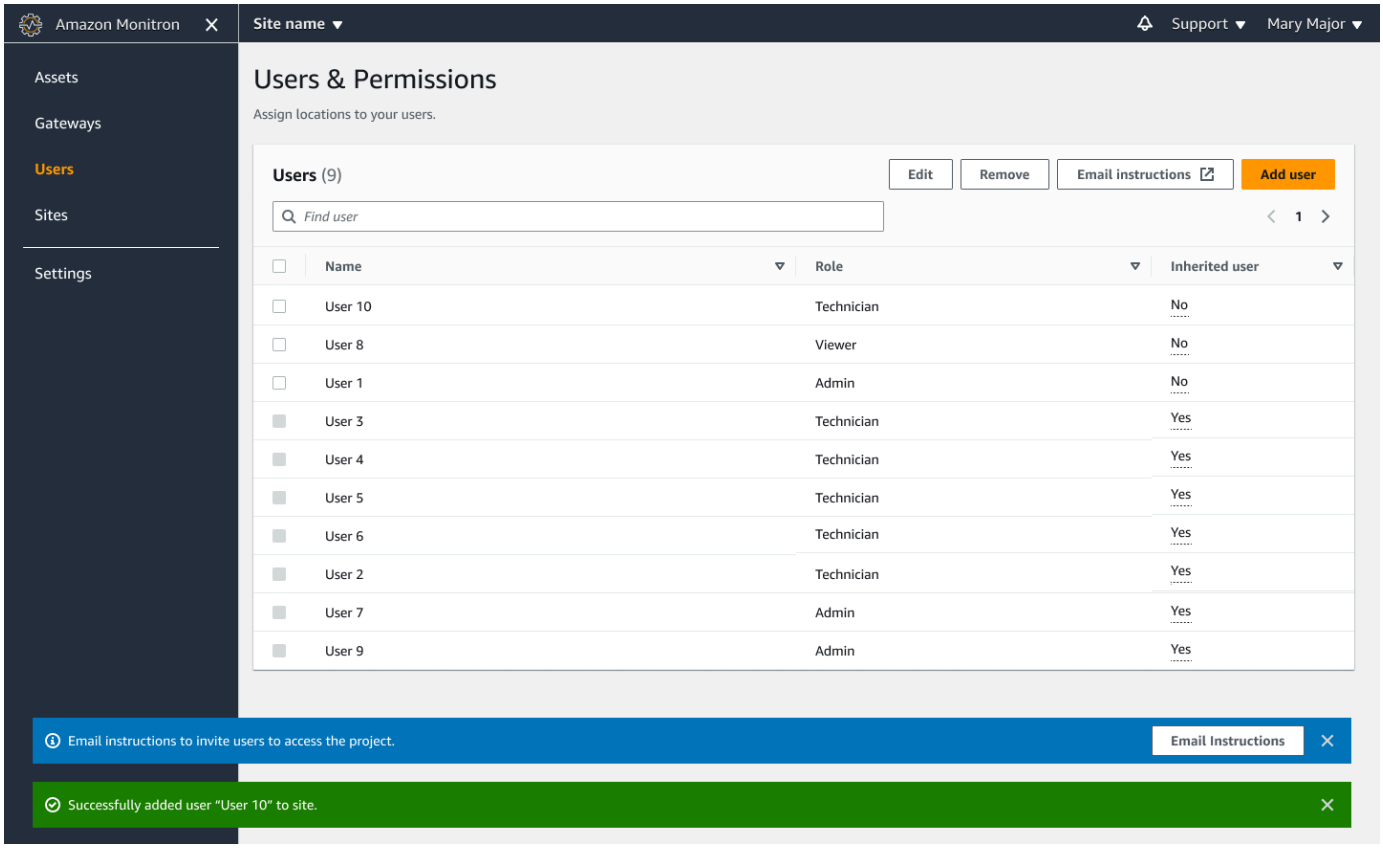
2. ユーザー名を入力します。Amazon Monitron がユーザーディレクトリでユーザーを検索します。

   リストからユーザーを選択し、ユーザーに割り当てるロールを管理者、技術者、または閲覧者を選択します。

   次に、ユーザーの追加を選択します。



3. 新しいユーザーが [ユーザー] のリストに表示されます。



新しいユーザーに、プロジェクトにアクセスして Amazon Monitron モバイルアプリをダウンロードするためのリンクを含む、招待 E メールを送信します。詳細については、「招待 E メールの送信」を参照してください。

ユーザーロールの変更

ユーザーのロールは変更できますが、ユーザーの名前は変更できません。これは、名前が Amazon Monitron によってリンクされているユーザーディレクトリにリンクされているためです。

プロジェクトまたはサイトのユーザーを変更するには、以前のユーザーを削除して、新しいユーザーを追加する必要があります。プロジェクトまたはサイトからユーザーを削除する方法については、「モバイルアプリを使用してユーザーを削除するには」を参照してください。新しいユーザーを追加する方法については、「ユーザーの追加」を参照してください。

トピック

- モバイルアプリを使用してユーザーロールを変更するには
- ウェブアプリを使用してユーザーロールを変更するには

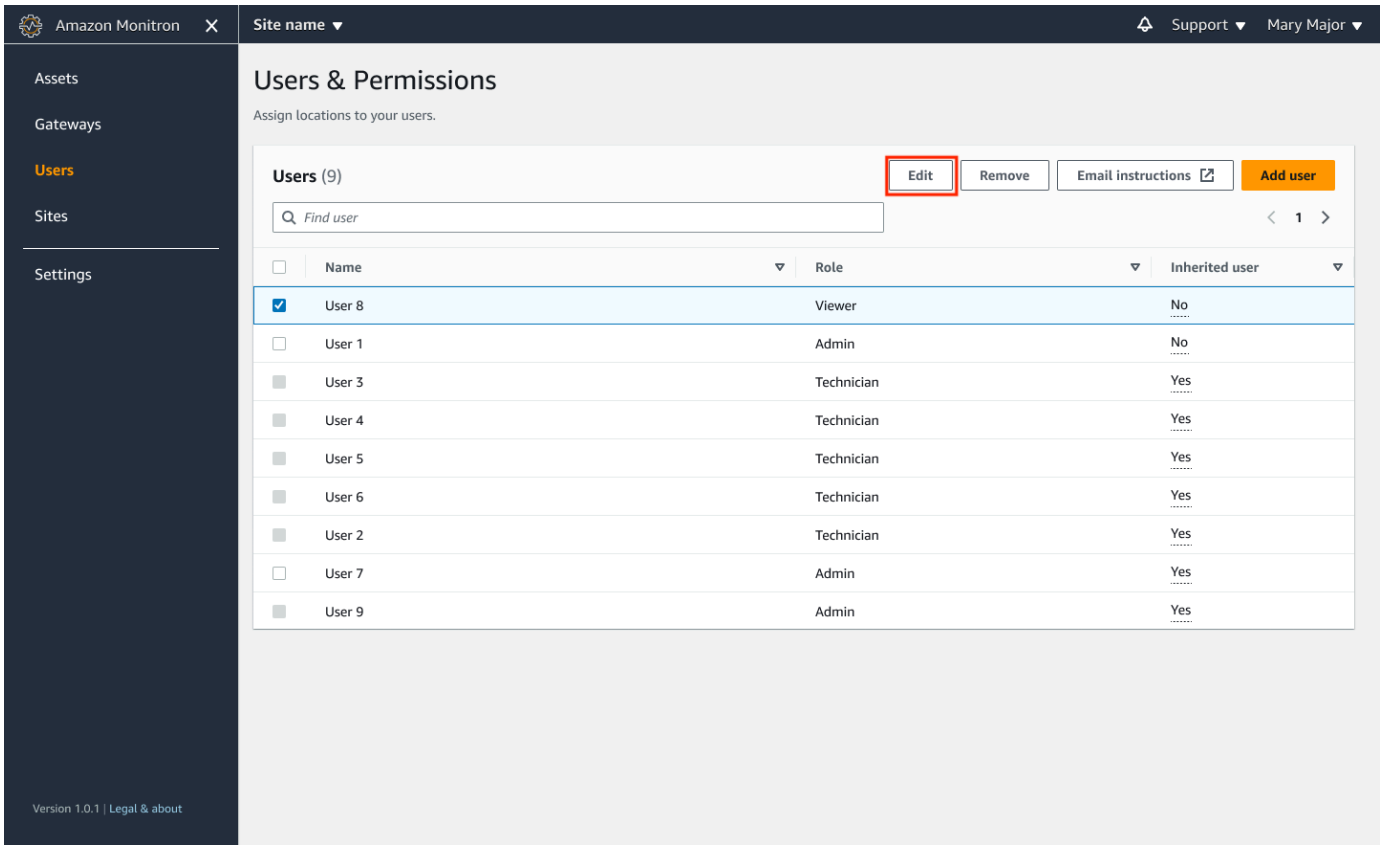
モバイルアプリを使用してユーザーロールを変更するには

1. スマートフォンで Amazon Monitron モバイルアプリにログインします。
2. ロールを変更するユーザーのプロジェクトまたはサイトに移動し、[ユーザー] のリストに移動します。
3. ロールを変更するユーザーの名前の横にある縦 3 点アイコン

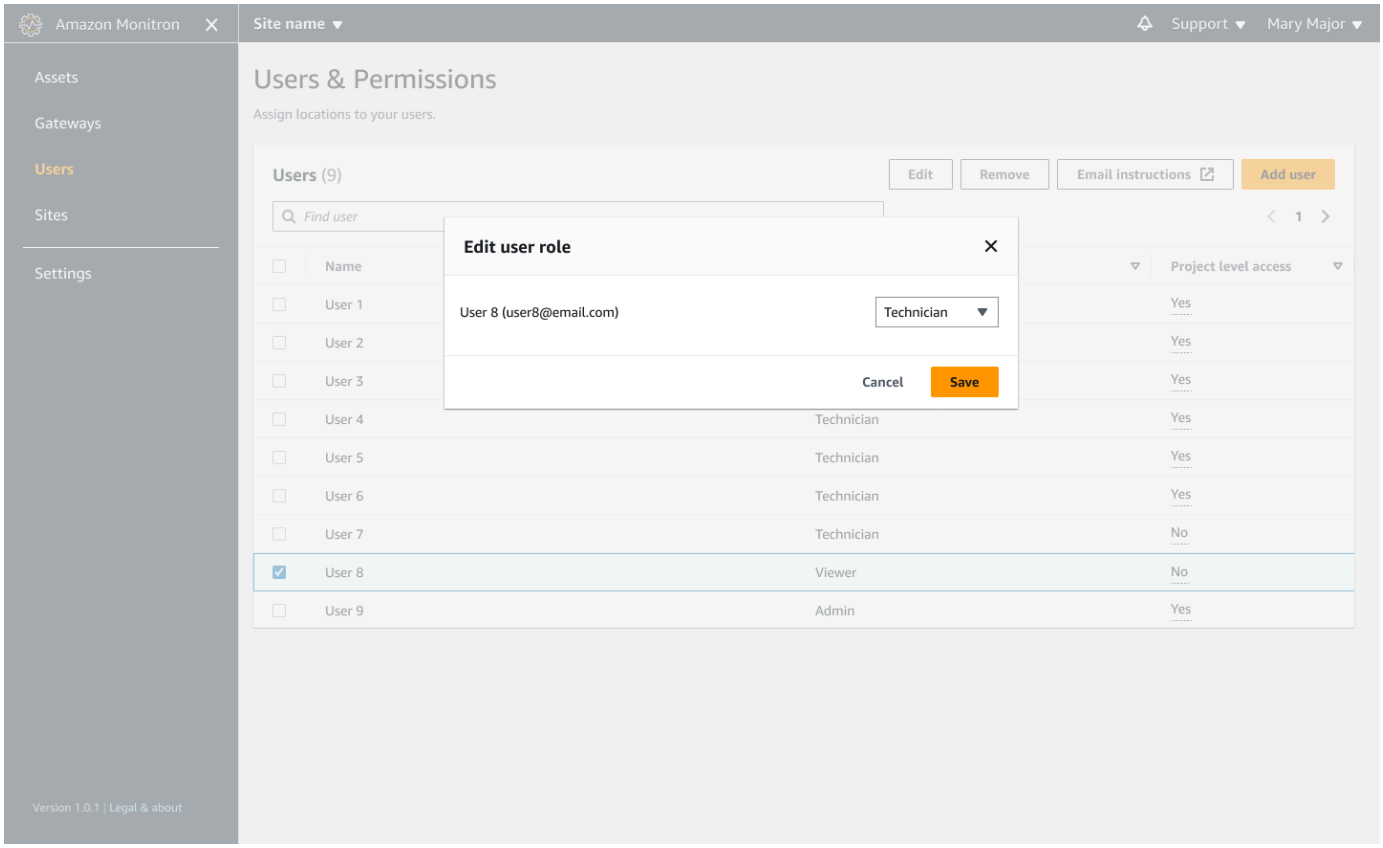
   ( )
   をクリックします。
4. [ユーザーを編集] を選択します。
5. ユーザーの新しいロールを [管理者]、[技術者]、[読み取り専用] から選択します。
6. [保存] をクリックします。

ウェブアプリを使用してユーザーロールを変更するには

1. ナビゲーションペインで [ユーザー] を選択します。



2. [ユーザーロールを編集] を選択します。
3. 管理者、技術者、または閲覧者のいずれかのユーザーの新しいロールを選択します。



4. [Save] を選択します。

ユーザーの削除

ユーザーを削除すると、そのユーザーのサイトまたはプロジェクトへのアクセス許可が削除されます。ユーザーディレクトリには影響しません。また、ユーザーが他のサイトやプロジェクトに対するアクセス許可を持っている場合、それらのアクセス許可は削除されません。

トピック

- モバイルアプリを使用してユーザーを削除するには
- ウェブアプリを使用してユーザーを削除するには

モバイルアプリを使用してユーザーを削除するには

1. スマートフォンで Amazon Monitron モバイルアプリにログインします。

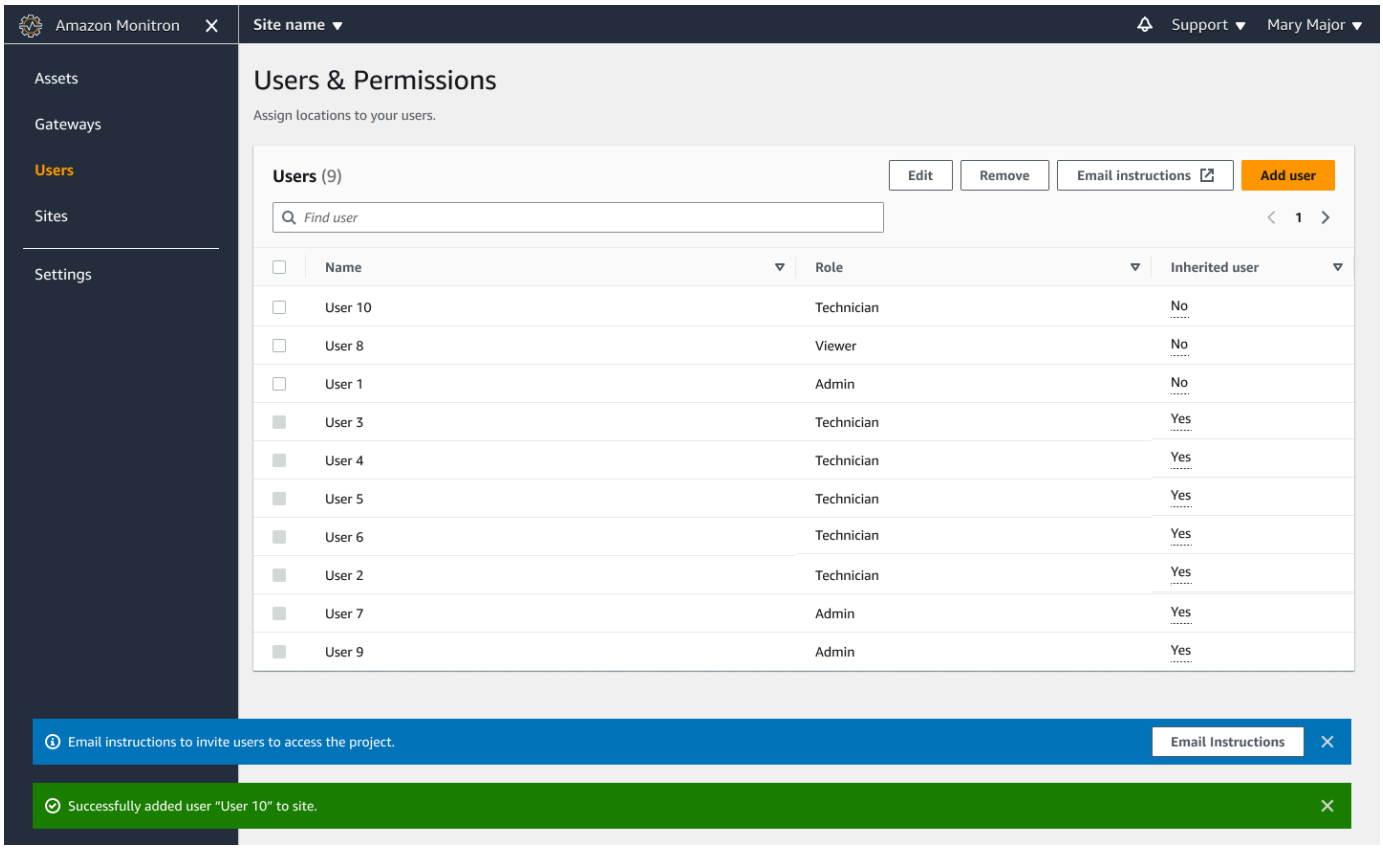
2. プロジェクトまたはサイトに移動し、[ユーザー] のリストページに移動します。
3. ユーザー名の横にある縦 3 点アイコン

   ( )

   を選択します。
4. [ユーザーを削除] を選択します。
5. [確認] ページで、[削除] をクリックします。

ウェブアプリを使用してユーザーを削除するには

1. ナビゲーションペインで [ユーザー] を選択します。



2. 削除するユーザーを選択します。
3. [削除] をクリックします。

Amazon Monitron のネットワーキングについて

ローカルネットワークを計画し、そのネットワークに Amazon Monitron をどのように組み込むかを決定する際には、各コンポーネント間の関係を理解しておくと役立つ場合があります。

トピック

- モバイルデバイスとのネットワーキング
- ネットワークのセキュリティ強化

モバイルデバイスとのネットワーキング

ネットワーキングの観点から見ると、センサーやゲートウェイをプロビジョニングするプロセスは次のようになります。

トピック

- モバイルアプリでの Monitron ネットワーク基盤のセットアップ
- ゲートウェイのセットアップ
- センサーのセットアップ

モバイルアプリでの Monitron ネットワーク基盤のセットアップ

1. モバイルデバイスは Wi-Fi または施設外からの信号 (衛星やタワーなど) を使用してインターネットに接続します。
2. インターネット経由で、Amazon Monitron モバイルアプリをモバイルデバイスにインストールします。(これはデバイスごとに 1 回だけ行う必要があります)
3. インターネット経由で、モバイルデバイスの Monitron アプリは AWS インフラストラクチャに接続し、 で認証します AWS IAM Identity Center。
4. AWS インフラストラクチャ内で認証されると、アプリケーションは Amazon Monitron バックエンドに接続します。
5. 認証済みアプリケーションを使用して、ローカルの Amazon Monitron セットアップのフレームワークを識別します。これには、ローカルネットワークに名前を付け、そのネットワーク内のゲートウェイの数を特定することが含まれます。

ゲートウェイのセットアップ

1. (認証された安全なインターネット経由で) モバイルアプリで、ゲートウェイを追加するオプションを選択します。
2. モバイルアプリに、モバイルデバイスの Bluetooth 機能にアクセスする権限を付与します。
3. デバイス上のモバイルアプリは Bluetooth を使用してローカルゲートウェイに接続します。
4. アプリでローカルネットワークの名前を指定します (Wi-Fi のみ) 。
5. アプリにローカルネットワークのパスワードを渡します。
6. アプリは、安全なインターネット経由で、ゲートウェイの情報を Monitron のバックエンドと通信します。
7. フロントエンドでは、モバイルデバイスの Bluetooth 経由で、アプリがゲートウェイに Monitron バックエンドとの通信に必要なトークンを渡します。
8. ゲートウェイはローカルネットワーク (イーサネットまたは Wi-Fi) を使用して、ローカルのインターネットアクセスポイント経由でインターネットに接続します。
9. 安全なインターネット経由で、ゲートウェイが Monitron バックエンドに登録されます。
10. これで、ゲートウェイがネットワークの一部としてアプリに表示されるようになりました。

センサーのセットアップ

1. モバイルアプリで、アセットの名前とクラスを指定します (アセットごとに 1 回)。
2. モバイルアプリで、センサーに名前を付けます。
3. 施設で、ペアリングされていないセンサーをアセットに物理的に取り付けます。
4. デバイスの NFC を使用して、モバイルアプリからセンサーに接続します。
5. モバイルアプリは、デバイスの NFC を使用して、すでにセットアップされているローカルの Monitron ゲートウェイの情報をセンサーに伝えます。
6. モバイルアプリは、安全なインターネット経由で、Monitron バックエンドにセンサーの情報を伝えます。
7. センサーは、Bluetooth を使用して、ゲートウェイに対してアセットに関するデータの送信を開始します。
8. ゲートウェイは、安全なインターネット経由で、センサーのデータを Monitron バックエンドに送信します。
9. 安全なインターネット経由で、アセットの分析データをモバイルアプリ (またはウェブアプリ) で表示できるようになりました。

ネットワークのセキュリティ強化

Amazon Monitron ゲートウェイが AWS にデータを送り返せるようにするには、ローカルネットワークトラフィックに関して次の許可が必要です。

- UDP プロトコル、ポート 53 - 標準 DNS ポート
- UDP プロトコル、ポート 67 と 68 - 標準 DHCP ポート
- TCP ポート 443 と 8883
- 2024 年 1 月 19 日より前にコミッショニングされた Amazon Monitron ゲートウェイの場合：
  - 末尾が `*.amazonaws.com` のドメイン
- 2024 年 1 月 19 日以降にコミッショニングされた Amazon Monitron ゲートウェイの場合：
  - アジアパシフィック (シドニー) (ap-southeast-2) – 54.79.215.104 および 54.79.23.89
  - 欧州 (アイルランド) (eu-west-1) – 54.72.131.46、34.251.27.192、52.213.71.97
  - 米国東部 (バージニア北部) (us-east-1) – 3.215.69.205、52.86.131.66、および 18.210.44.199

> **Note**
>
> で終わる IP ドメイン `*.amazonaws.com` (の新しい静的 IPs ドメインが既に含まれている) に対して既に許可されているため、以前にコミッショニングされたデバイスに対して新しい静的 IP がデフォルトで有効になっている場合、リグレッションはありませんamazonaws.com。ゲートウェイを廃止して再コミッショニングすると、ゲートウェイは静的 IP に切り替わります。ゲートウェイネットワーク設定を静的 IP から動的 IP に戻すことはできません。

Android モバイルデバイスを使用してゲートウェイやセンサーをプロビジョニングする場合は、ローカルネットワークトラフィックに関して次の許可が必要です。

- TCP ポート 443、5228、5229、5230
- 末尾が `*.google.com` や `*.googleapis.com` のドメイン
- 通信事業者が必要とするすべてのポート
- 次の端末で使用される SSL 通信用の TCP ポート 5094

  ボーダフォンデバイス

Apple 製モバイルデバイスを使用してゲートウェイやセンサーをプロビジョニングする場合は、ローカルネットワークトラフィックに関して次の許可が必要です。

- TCP ポート 443、2197、5223
- サブネット 17.249.0.0/16、17.252.0.0/16、17.57.144.0/22、17.188.128.0/18、17.188.20.0/23
- Apple 製品が使用するポートとホストのリストも参照してください。

注意: Amazon Monitron、Android、Apple (のそれぞれのドキュメント) によると、次のポートを開く必要はありません。

- UDP ポート 443
- TCP ポート 80

Amazon Monitron データへのアクセスする

Amazon Monitron の外部から Amazon Monitron の raw データにアクセスするには 2 つの方法があります。

データに継続的にアクセスして、他の場所でも使用したい場合もあるでしょう。その場合は、自動的にデータを Kinesis ストリームに追加できるよう Amazon Monitron を設定できます。そこから、データを Amazon S3 や Lambda など、さまざまな宛先に移植することができます。このプロセスには設定が必要であり、その設定には Kinesis データストリームを理解する必要があります。ただし、すべての要素を満足のいくように配置できたら、データを自動的にストリーミングし続けることができます。

また、 AWS上に保存して分析しているデータの種類を明確に把握するために、ときどきデータにアクセスしたい場合もあるかもしれません。その場合は、 AWS サポートにデータを手動で Amazon S3 にコピーするよう依頼できます。このプロセスに必要な設定は少ないですが、自動化することはできません。Amazon Monitron がこれまでに蓄積してきたデータのみを、1 つのチャンクにまとめて提供します。

トピック

- Amazon Monitron データを Amazon S3 にエクスポートする
- Amazon Monitron Kinesis データエクスポート v1
- Amazon Monitron Kinesis データエクスポート v2

Amazon Monitron データを Amazon S3 にエクスポートする

AWSでどのような種類のデータを安全に保存しているかを正確に把握するために、Amazon Monitron が保存している raw データへのアクセスが必要な場合があります。

にサポートチケットを提出し AWS、データを配信するアクセス許可を Amazon Monitron に付与することで、未加工データを取得できます。

プログラムで消費できる Amazon Monitron リソースのリアルタイムの運用データを取得するには、Kinesis ストリームを使用してデータをエクスポートすることを検討してください。詳細については、「Amazon Monitron Kinesis データエクスポート v2」を参照してください。

トピック

- 前提条件
- AWS CloudFormation (推奨オプション) を使用してデータをエクスポートする
- コンソールを使用してデータをエクスポートする
- CloudShell を使用してデータをエクスポートする

前提条件

Amazon Monitron データを正常にエクスポートするには、次の前提条件を満たす必要があります。

- 同じリージョンで (Amazon Monitron データの) 別のエクスポートがすでに実行中でないこと。
- 過去 24 時間以内に同じリージョンで別のエクスポートを実行していないこと。

AWS CloudFormation (推奨オプション) を使用してデータをエクスポートする

トピック

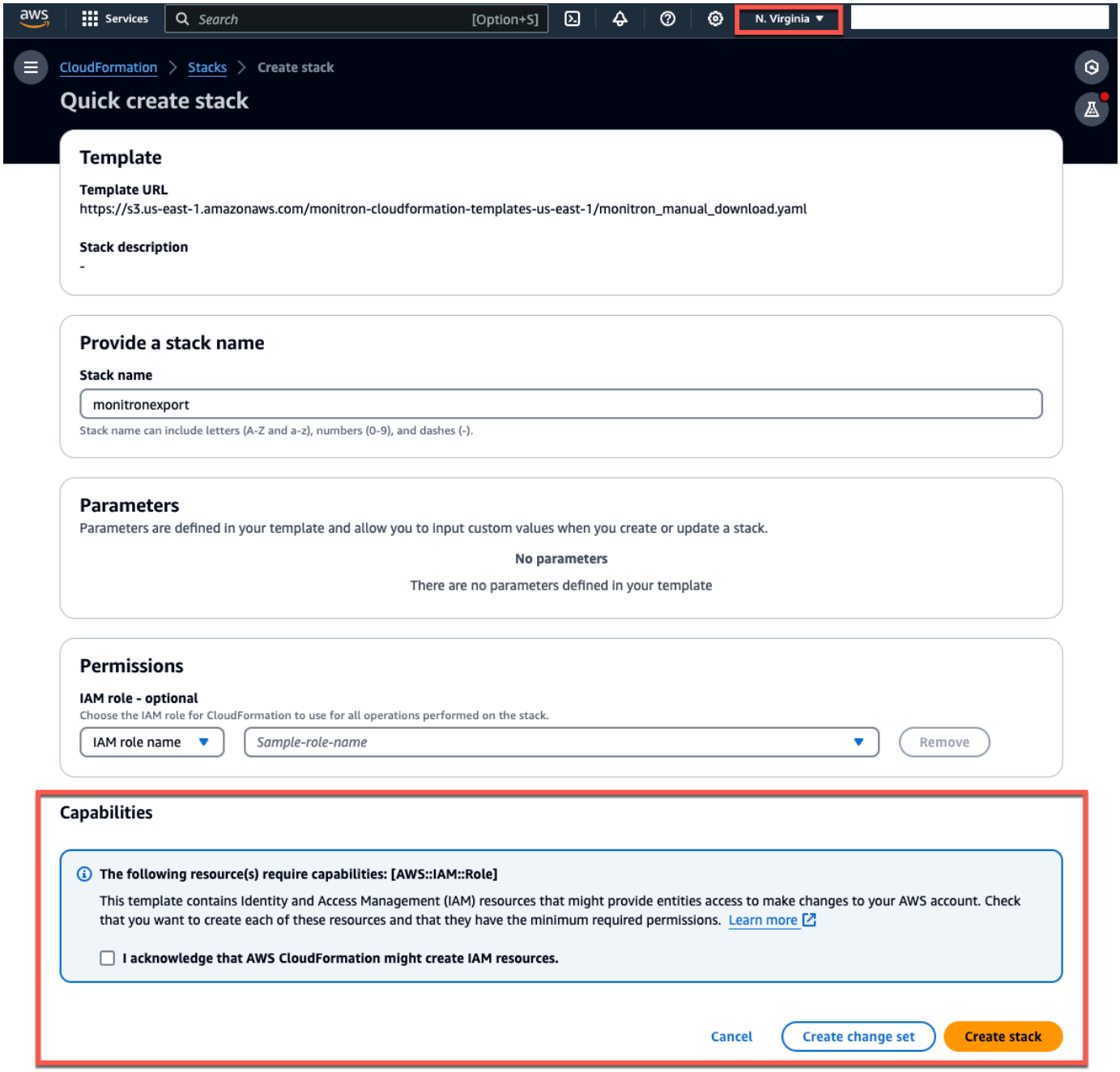
- ステップ 1: Amazon S3 バケット、IAM ロール、IAM ポリシーを作成します。
- ステップ 2: リソースのメモを作成する
- ステップ 3: サポートケースを作成する

ステップ 1: Amazon S3 バケット、IAM ロール、IAM ポリシーを作成します。

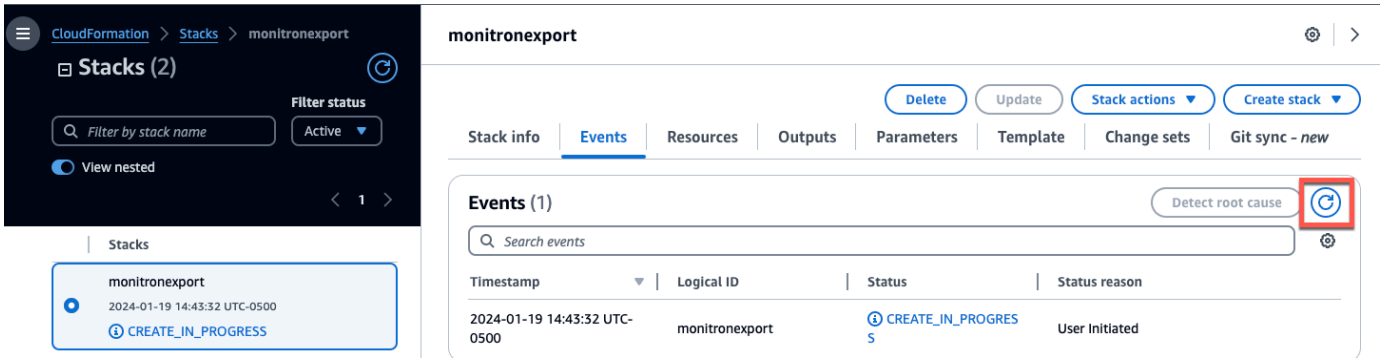
1. AWS アカウントにサインインします。
2. 次の URL で新しいブラウザタブを開きます。

```
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. 開いた AWS CloudFormation ページの右上隅で、Amazon Monitron を使用しているリージョンを選択します。
4. [スタックの作成] を選択してください。

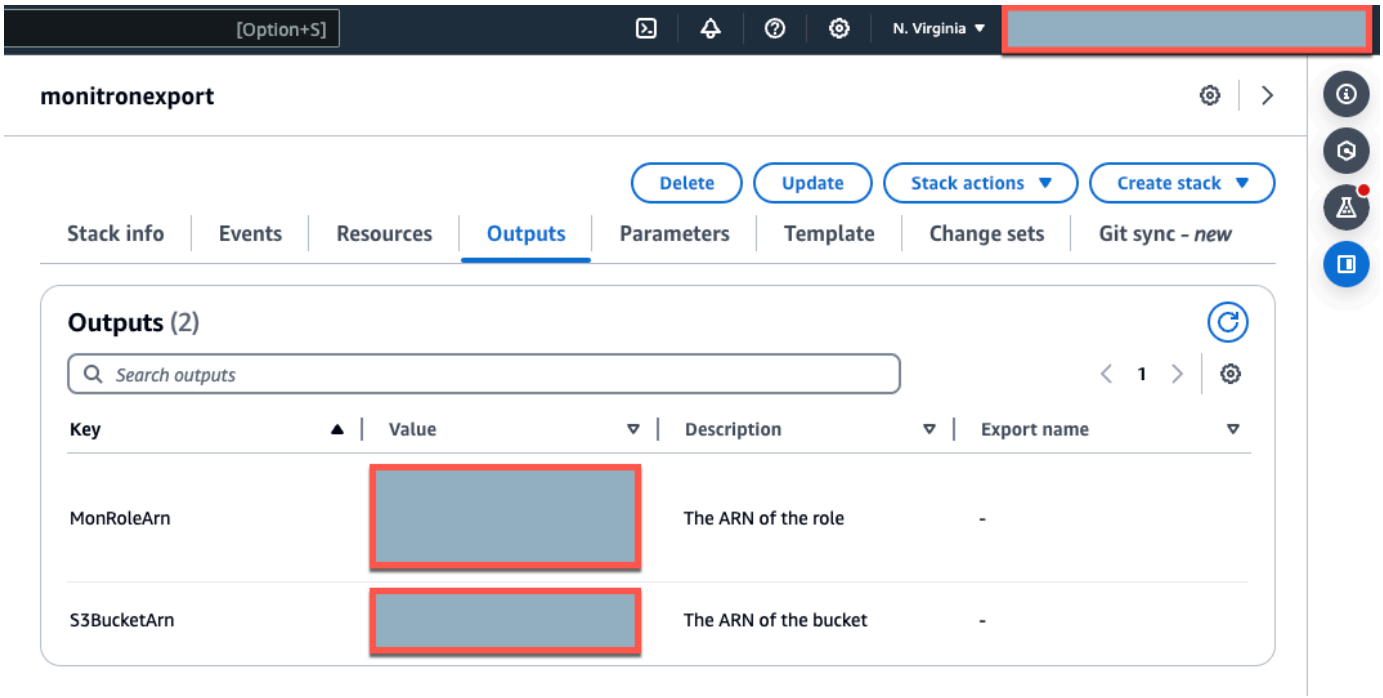


5. 次のページで、スタックのステータス (monitronexport) が CREATE_COMPLETE になるまで、必要に応じて更新アイコンを選択します。



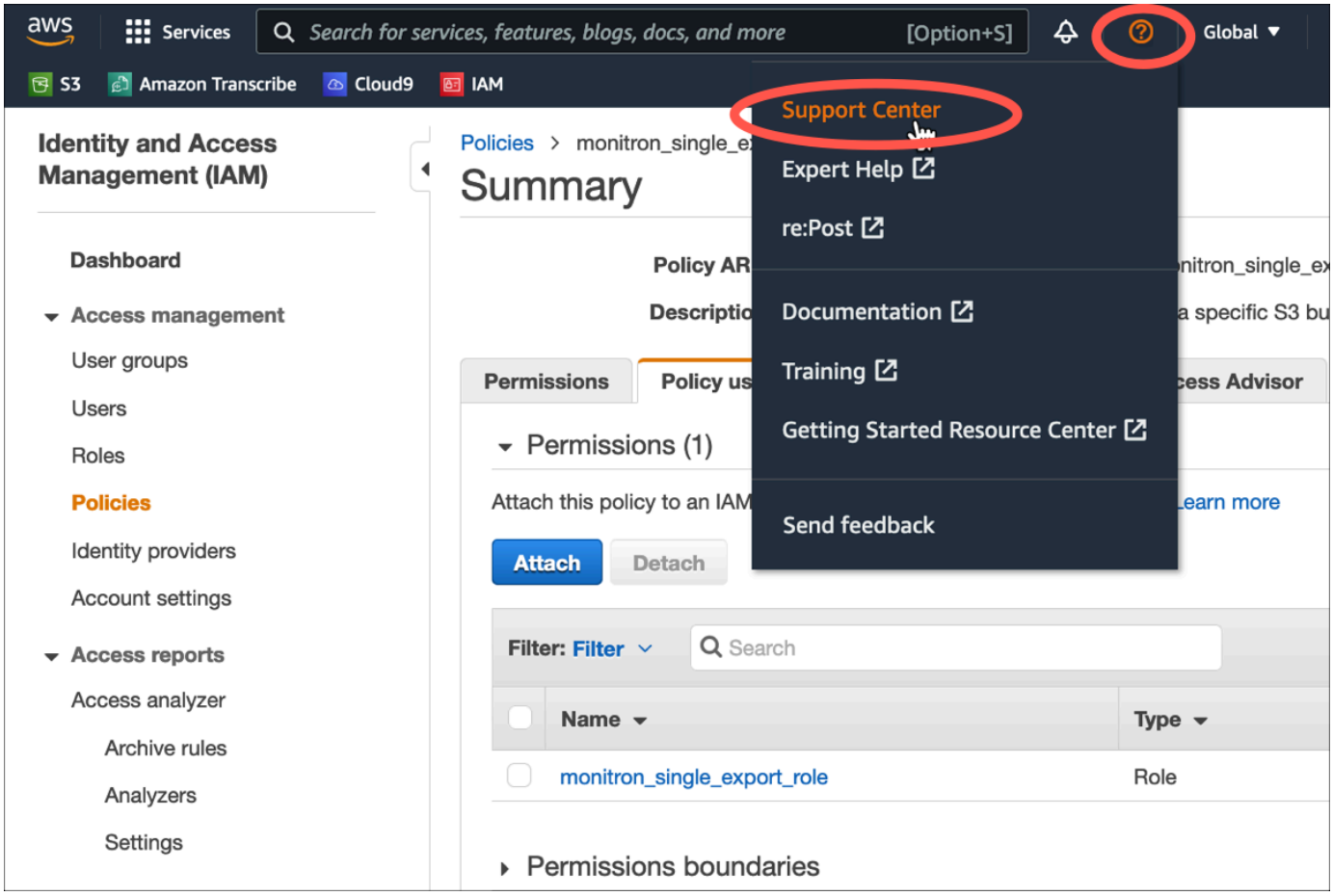
ステップ 2: リソースのメモを作成する

1. [出力] タブを選択します。
2. キー MonRoleArn の値をメモします。
3. キー S3BucketArn の値をメモします。
4. ページの右上隅にあるアカウント ID をメモします。
5. ステップ 1 で選択したリージョンをメモします。ページ上部のアカウント ID の左側にも選択したリージョンが表示されるようになりました。

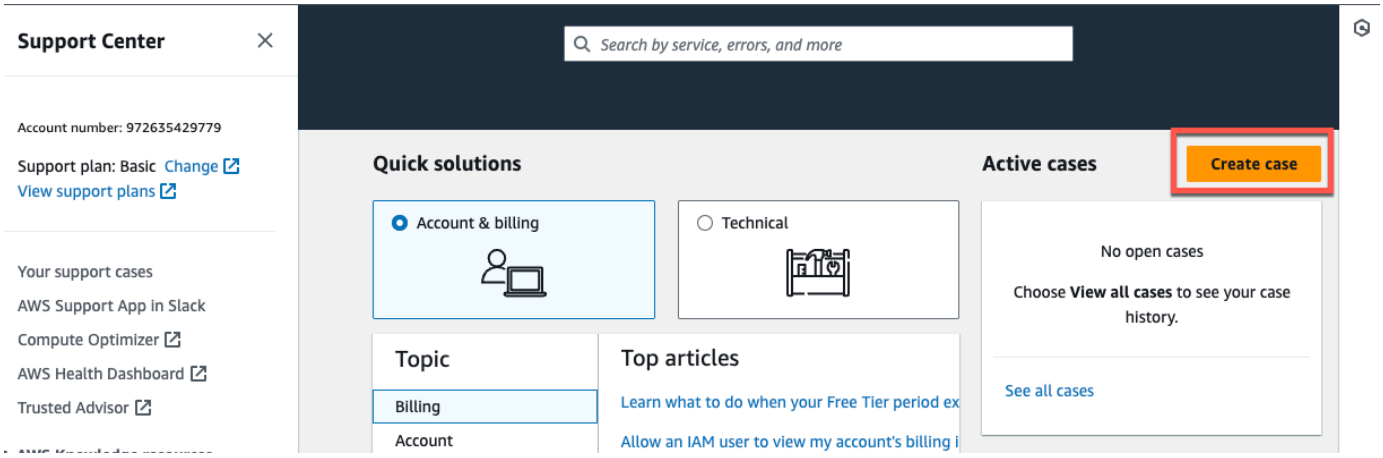


ステップ 3: サポートケースを作成する

1. AWS コンソールから、任意のページの右上隅にある疑問符アイコンを選択し、サポートセンターを選択します。

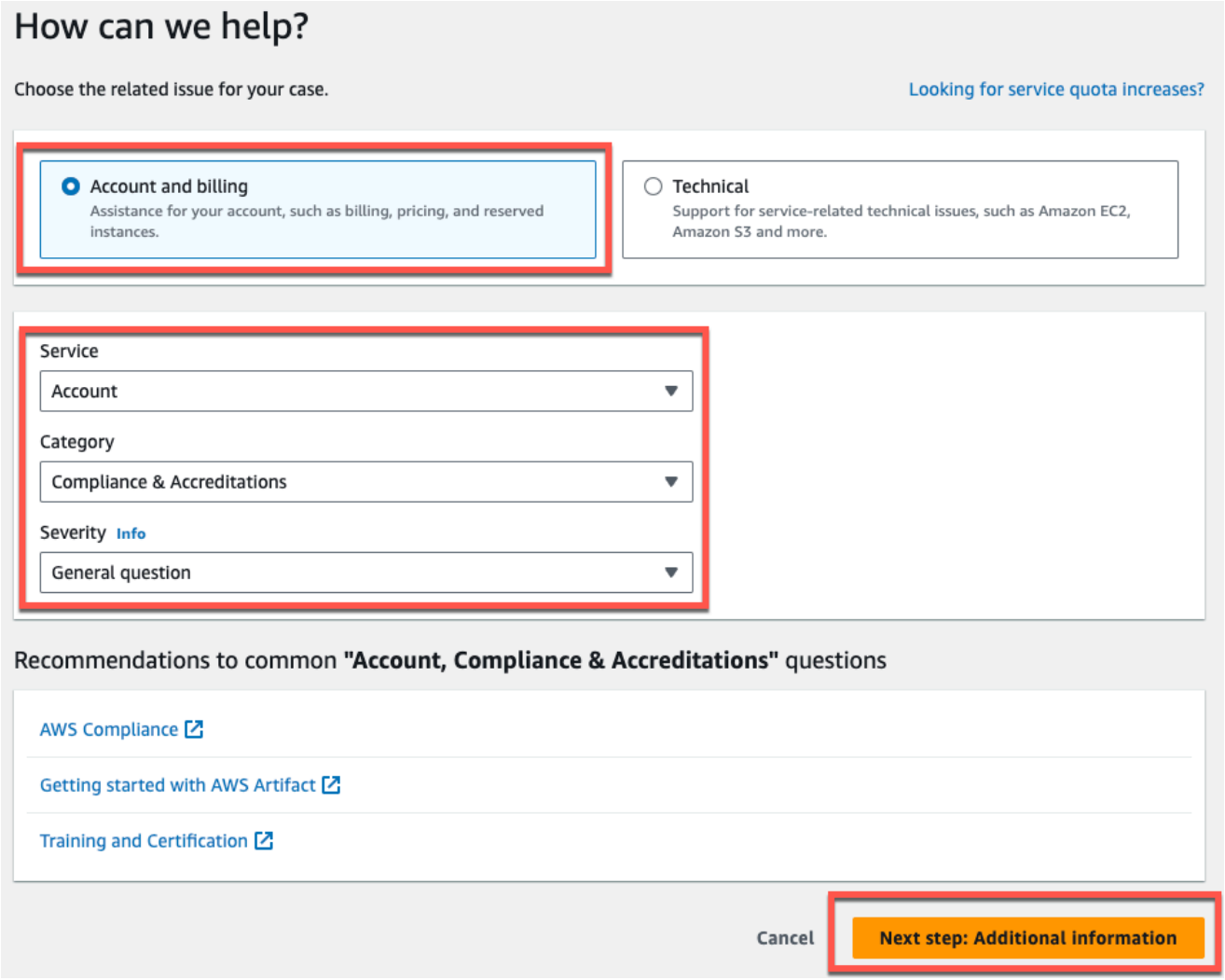


2. 次のページで、[ケースの作成] を選択します。



3. どのように支援できるか ページで、次の操作を行います。

a. [アカウントおよび請求サポート] を選択します。
b. サービスで、アカウントを選択します。
c. [カテゴリ] で、[コンプライアンスと認定] を選択します。
d. サポート契約に基づいてそのオプションが利用できる場合は、[重要度] を選択します。
e. [Next step: Additional information] (次のステップ:追加情報) を選択します。

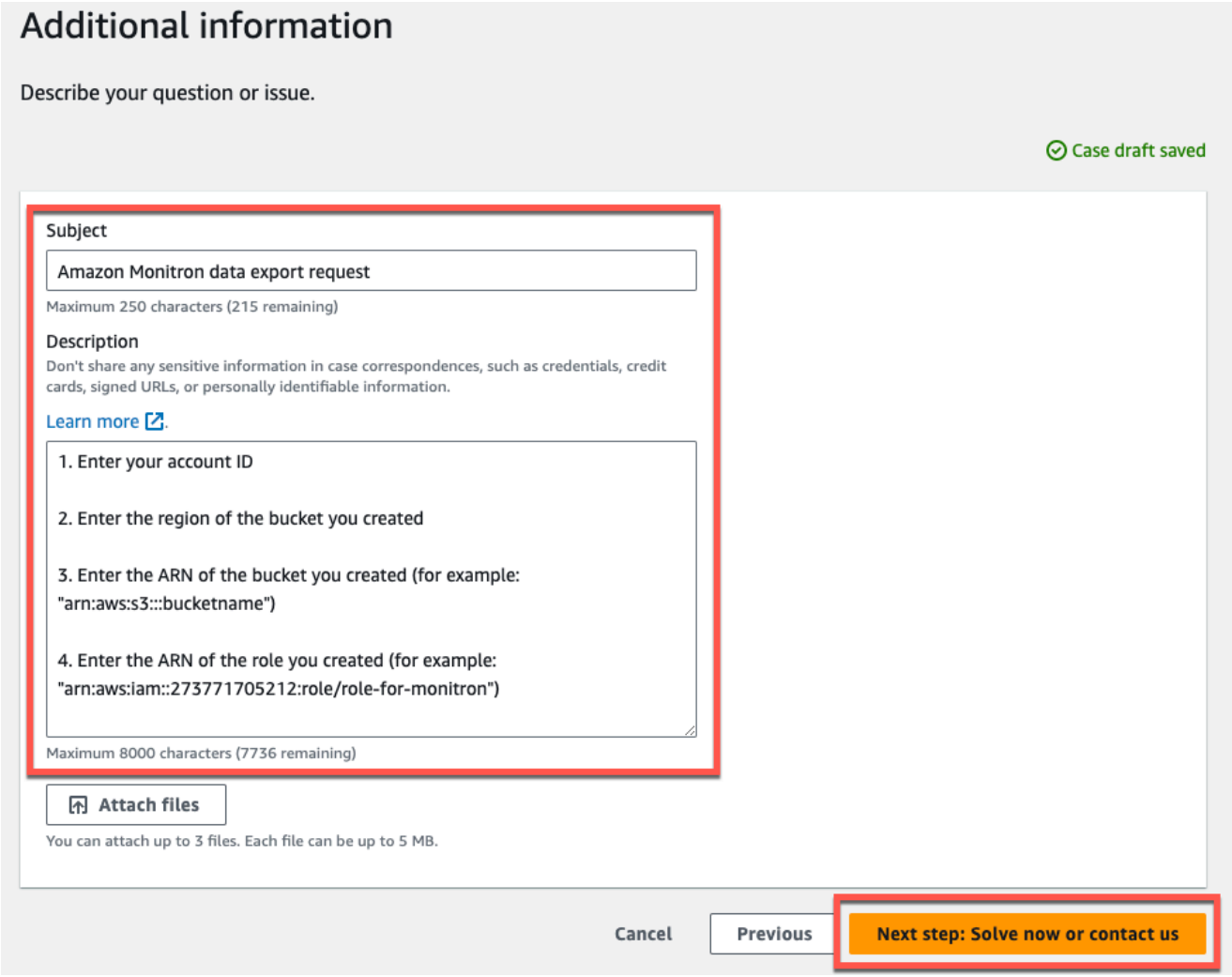


4. 「追加情報」では、次の操作を行います。

a. [件名] に Amazon Monitron data export request と入力します。
b. [説明] フィールドに、次のように入力します。

1. アカウント ID
2. 作成したバケットのリージョン
3. 作成したバケットの ARN (例:「arn:aws:s3:::bucketname」)

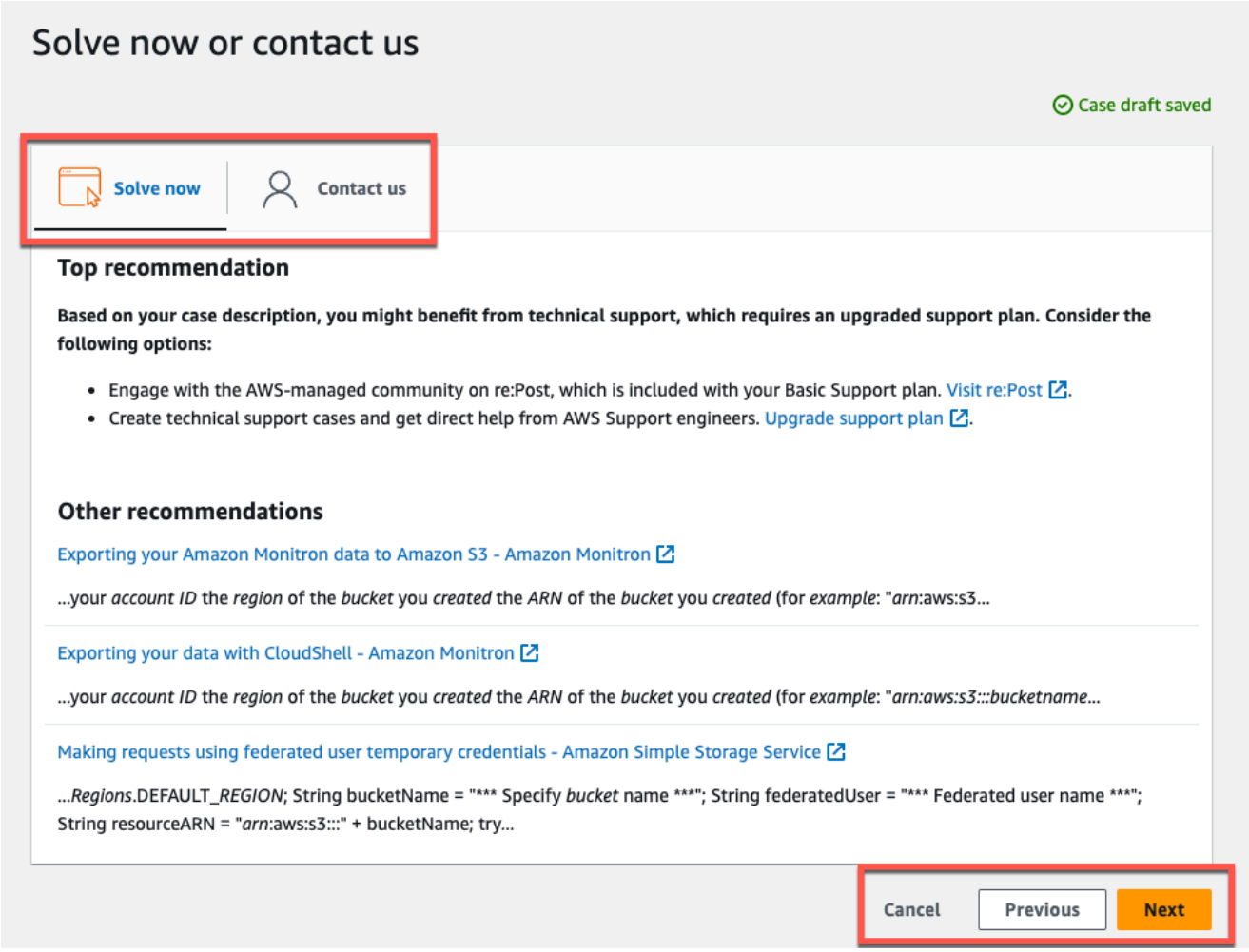
4. 作成したロールの ARN (例:「arn:aws:iam::273771705212:role/role-for-monitron」)



c. [次のステップ: 今すぐ解決またはお問い合わせ] を選択します。

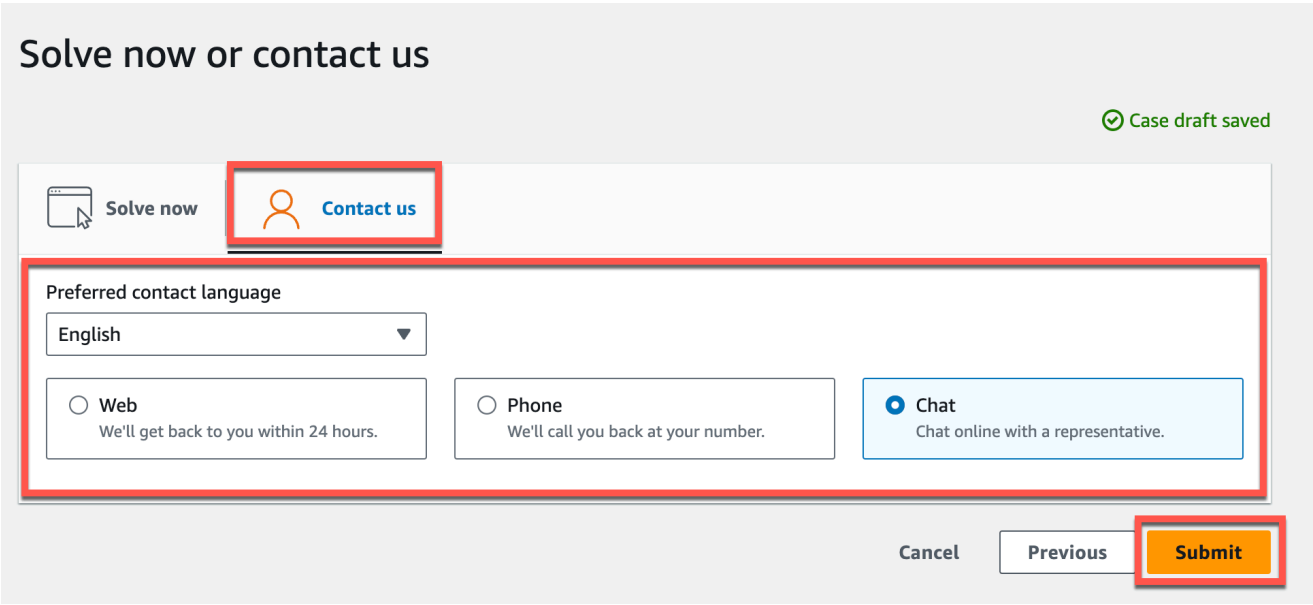
5. 今すぐ解決するか、お問い合わせください。以下を実行します。

a. 今すぐ解決で、次へを選択します。



b. Contact us で、希望する問い合わせ言語と希望する問い合わせ方法を選択します。

c. [Submit] を選択してください。ケース ID と詳細を含む確認画面が表示されます。



AWS カスタマーサポートスペシャリストができるだけ早くご連絡します。記載されている手順に問題がある場合、スペシャリストが詳細情報を伺うことがあります。必要な情報がすべて提供されている場合は、上記で作成した Amazon S3 バケットにデータがコピーされ次第、スペシャリストからご連絡いたします。

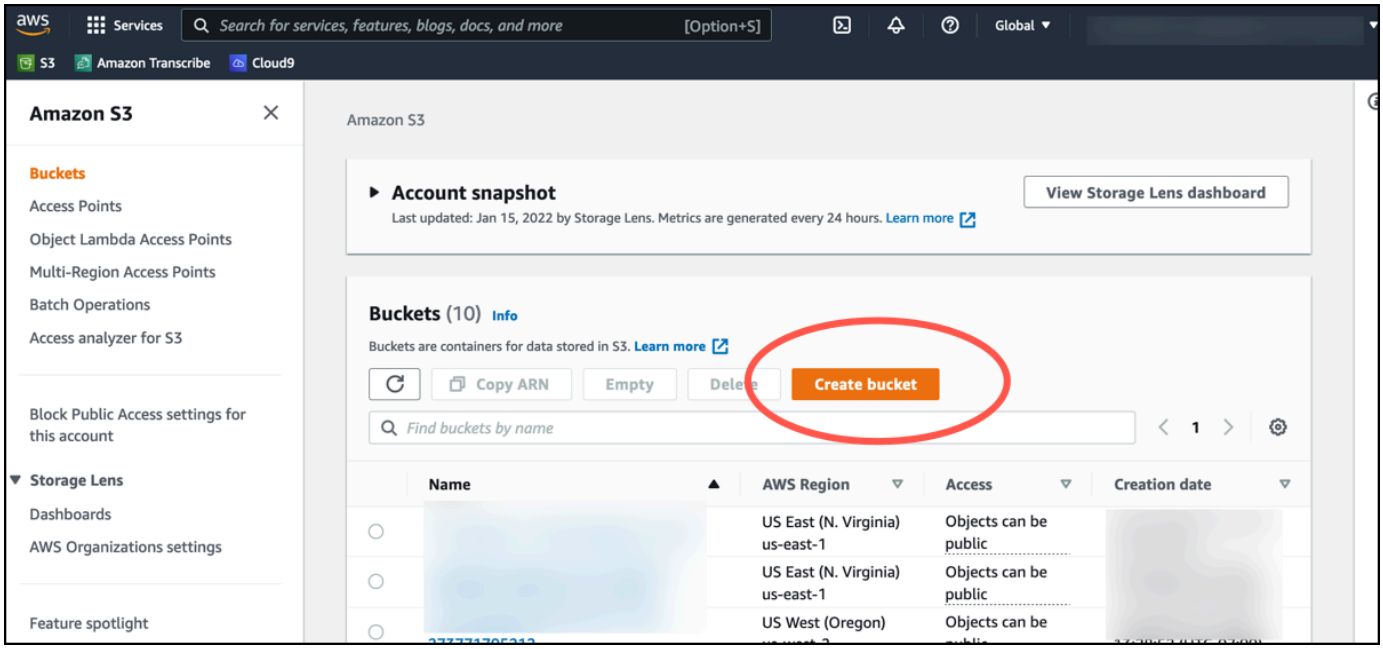
コンソールを使用してデータをエクスポートする

トピック

- ステップ 1: Amazon S3 バケットを設定する
- ステップ 2: Amazon Monitron に Amazon S3 へのアクセス権限を付与する
- ステップ 3: ロールを作成する
- ステップ 4: 信頼ポリシーを作成する
- ステップ 5: サポートケースを作成する

ステップ 1: Amazon S3 バケットを設定する

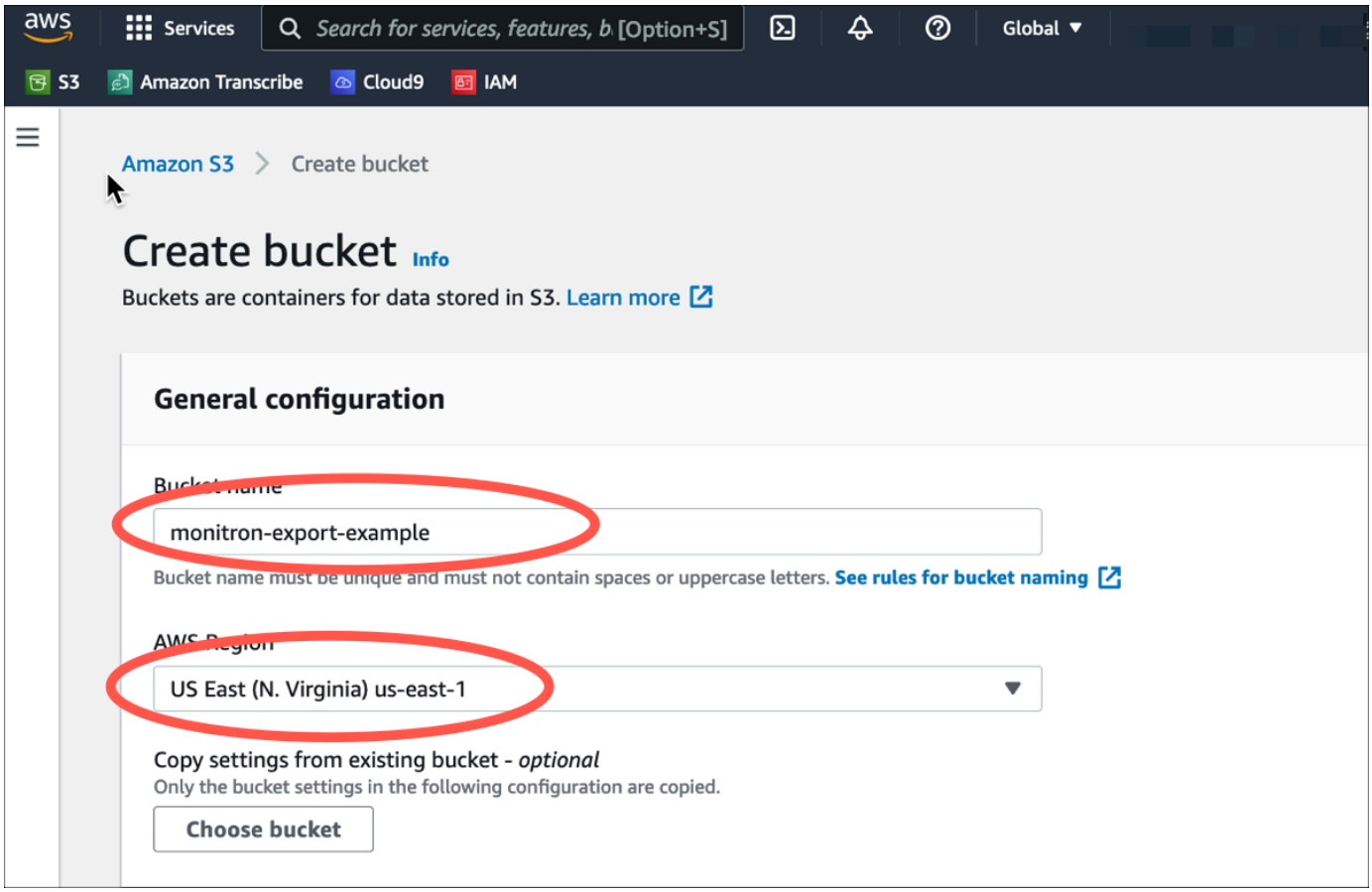
1. Amazon S3 コンソールを開きます。
2. [バケットを作成する] を選択します。



3. バケットに名前を付け、適切なリージョンを選択します。ページ下部にある [バケットの作成] を選択します。

> **Important**
>
> 現時点では、Amazon Monitron は次の 3 つのリージョンでのみサポートされています。
>
> - 米国東部 (バージニア北部) us-east-1
> - 欧州 (アイルランド) eu-west-1
> - アジアパシフィック (シドニー) ap-south-east-2
>
> そのため、Amazon S3 バケットはそれらのリージョンのいずれかでなければなりません。

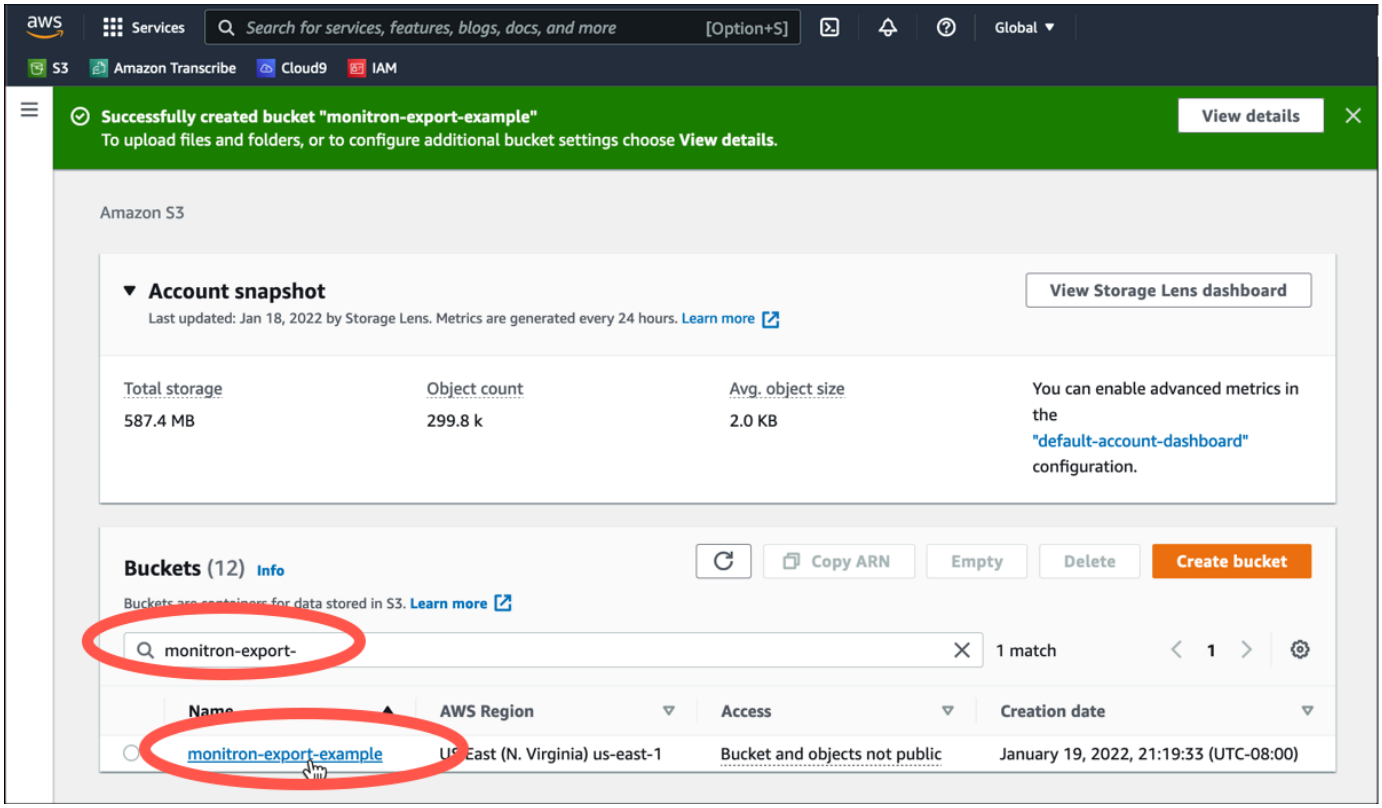
また、Amazon Monitron サービスを使用しているリージョンと同じリージョンである必要があります。



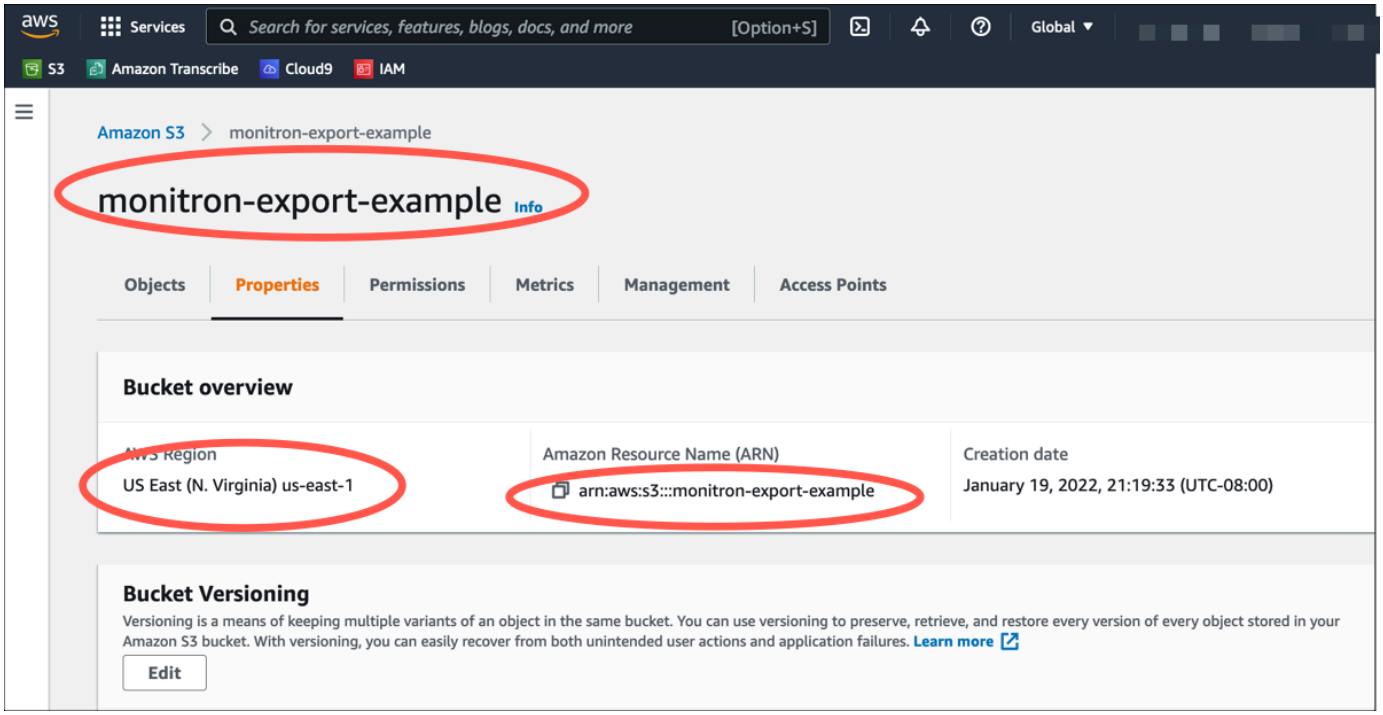
4. ページにある残りのオプションを確認し、セキュリティのニーズとポリシーに応じて適切な選択を行います。

> **Important**
>
> ユーザーはデータを保護するための適切な措置を講じる責任があります。サーバー側の暗号化を使用し、バケットへのパブリックアクセスをブロックすることを強くお勧めします。

5. 検索ボックスを使用して、先ほど作成したバケットを検索し、選択します。

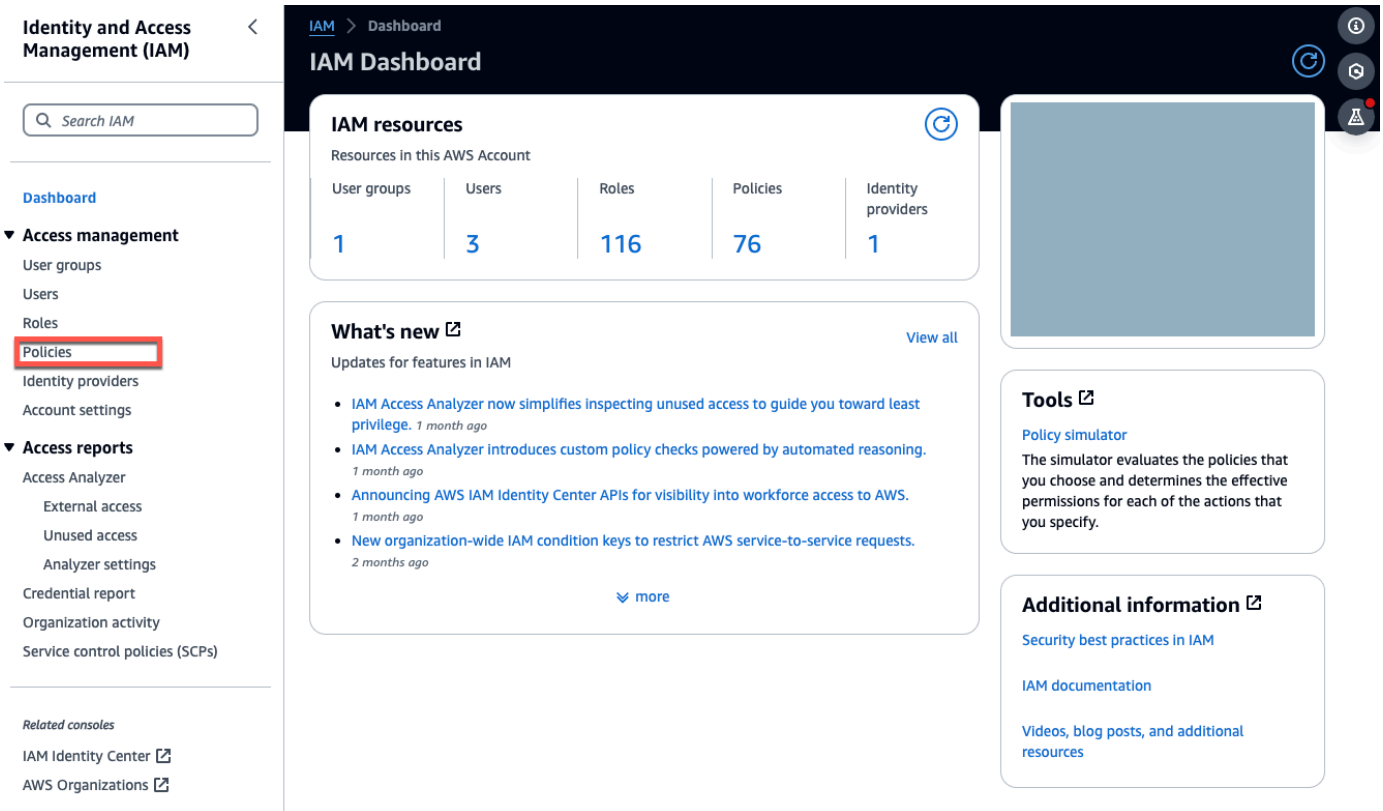


6. [プロパティ] タブから、バケットの名前、ARN、リージョンをメモします。

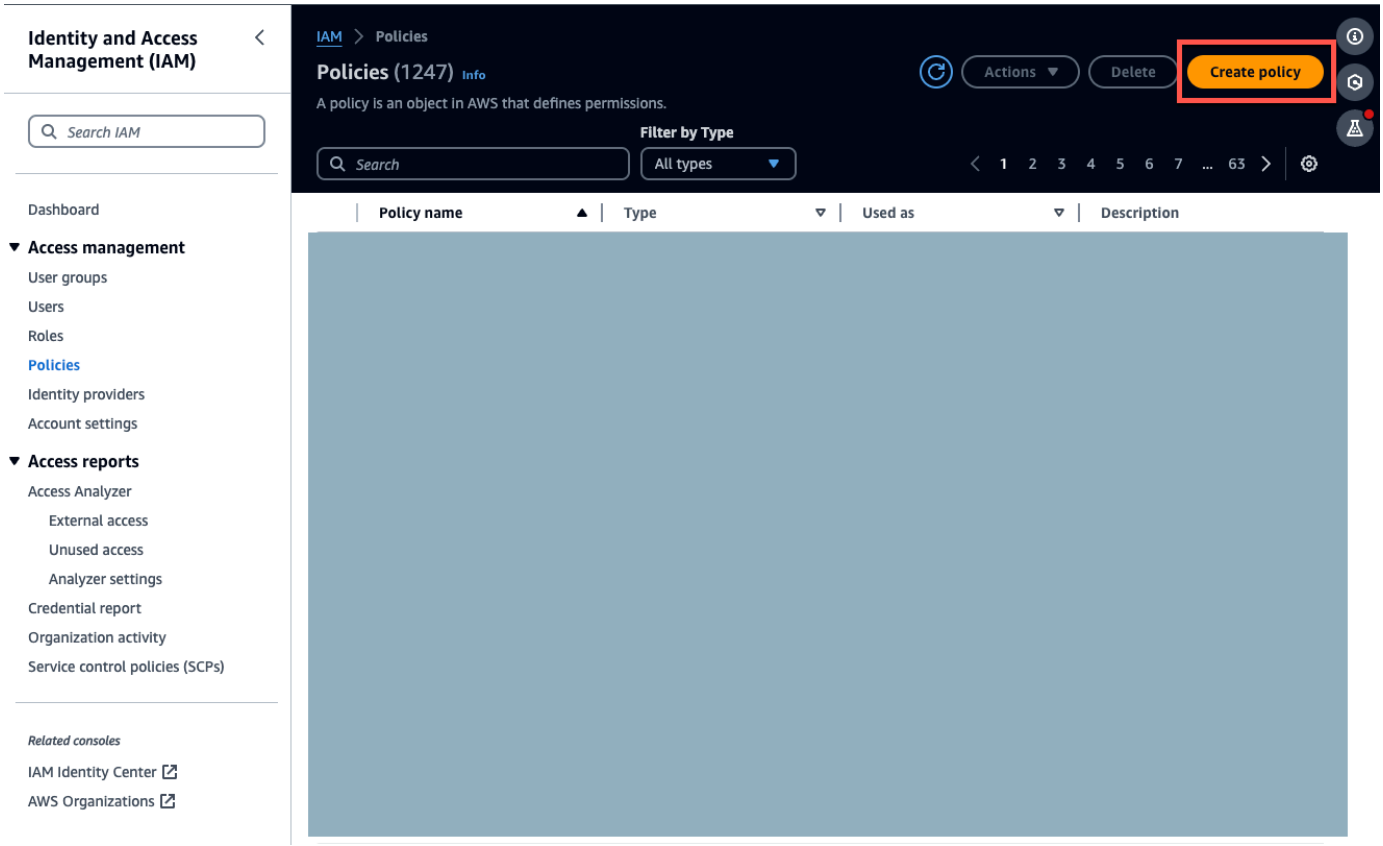


ステップ 2: Amazon Monitron に Amazon S3 へのアクセス権限を付与する

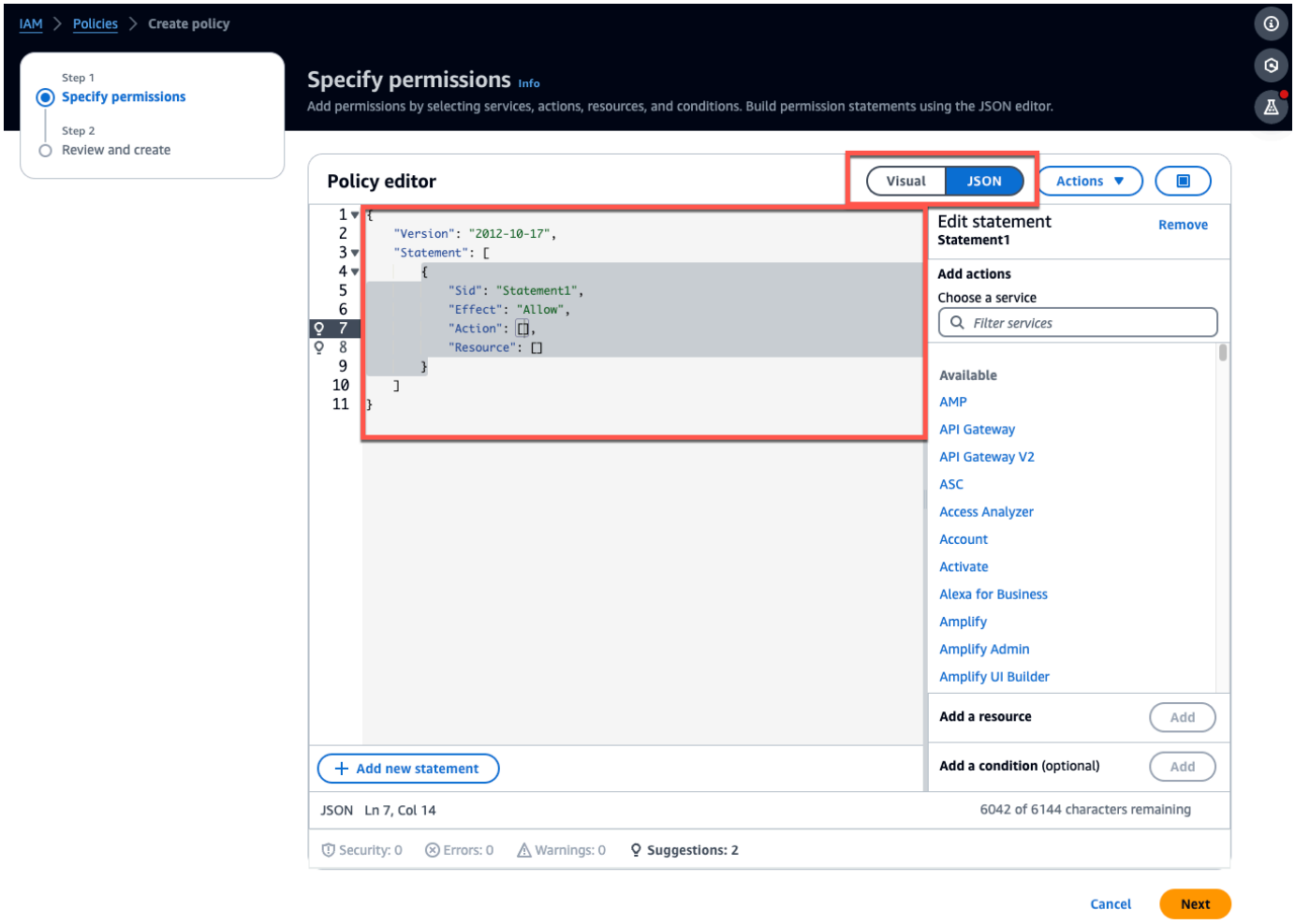
1. IAM コンソールを開き、[ポリシー] を選択します。



2. [Create policy] (ポリシーの作成) を選択します。



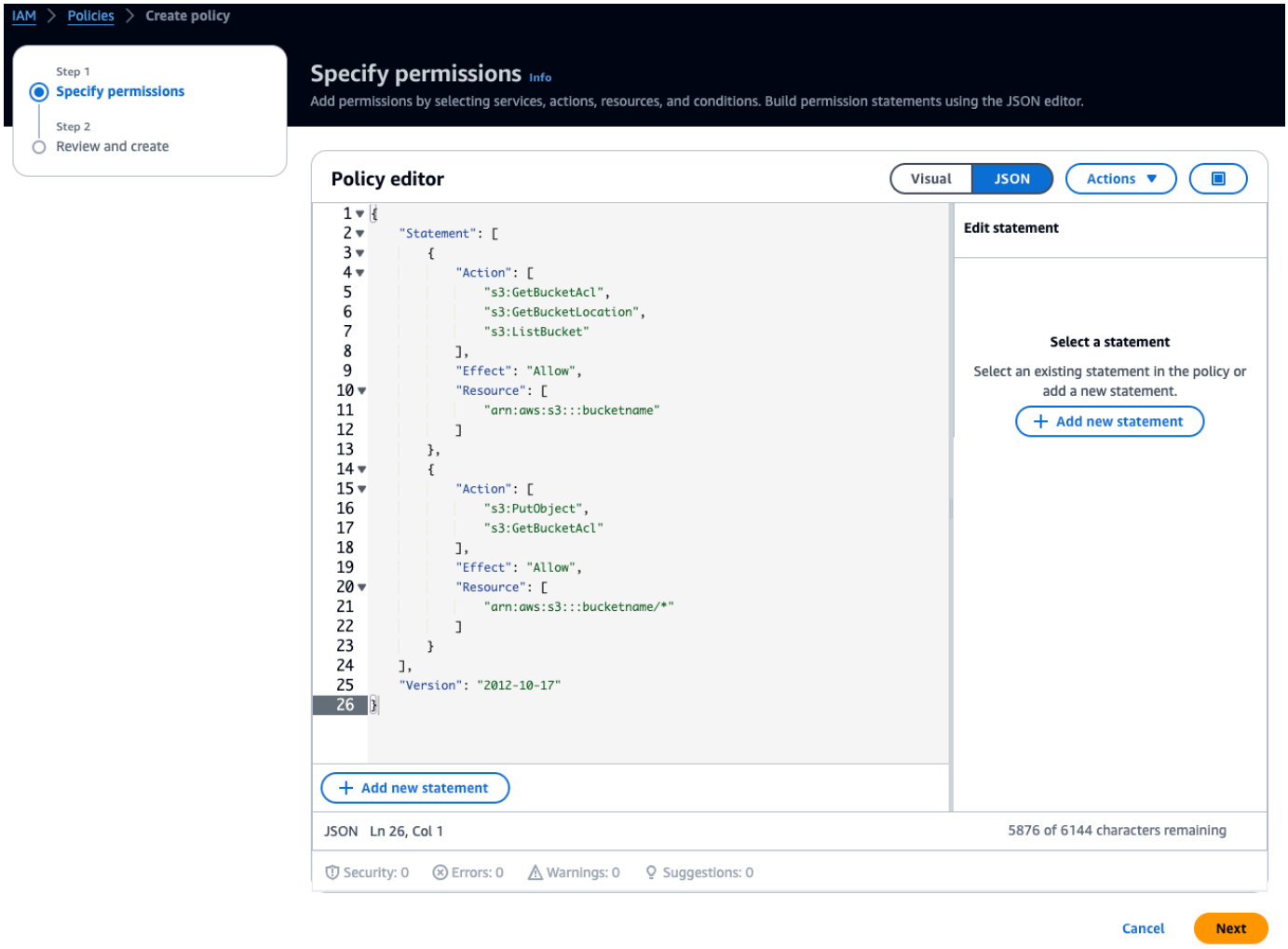
3. [JSON] タブを選択します。



4. デフォルトの JSON テキストを削除して、フォームを空にします。
5. バケットアクセスポリシーを貼り付けます。

```
{
    "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"
}
```



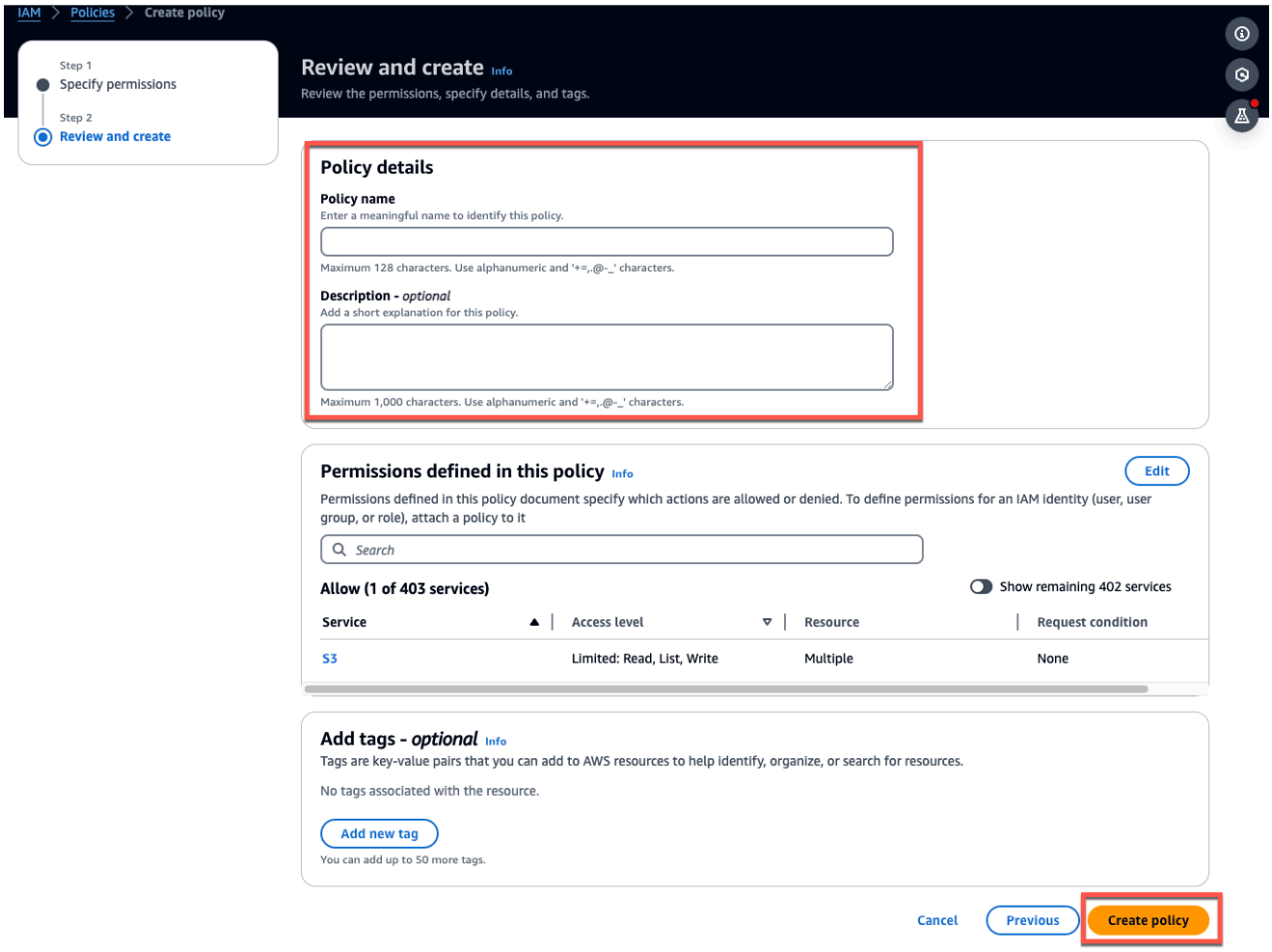
6. [次へ] を選択してください。
7. [レビューと作成] ページで、以下の操作を実行します。

a. ポリシーの詳細に、ポリシー名とオプションの説明を入力します。

b. このポリシーセクションで定義されているアクセス許可はそのままにしておきます。

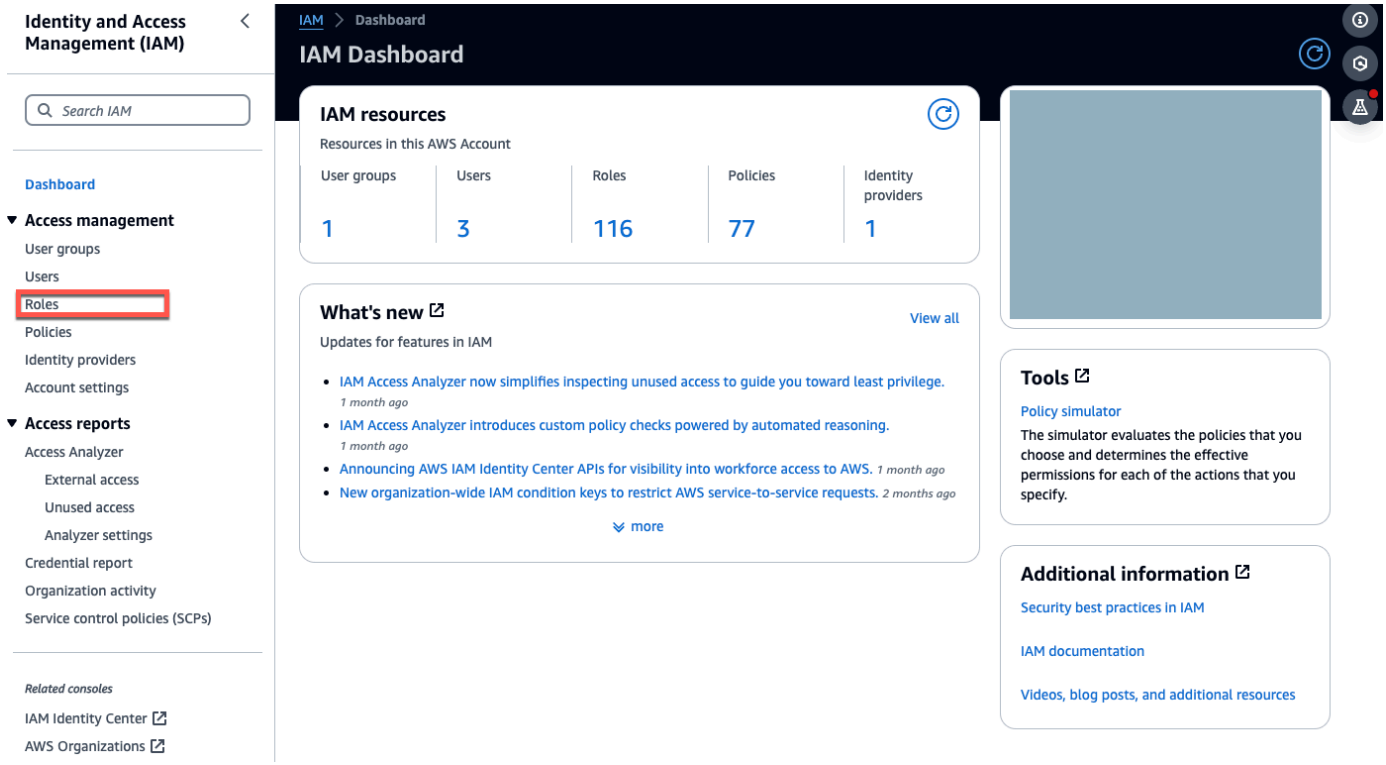
c. タグの追加 — オプションで、リソースを追跡するためにタグを追加できます。

d. [Create policy] (ポリシーの作成) を選択します。

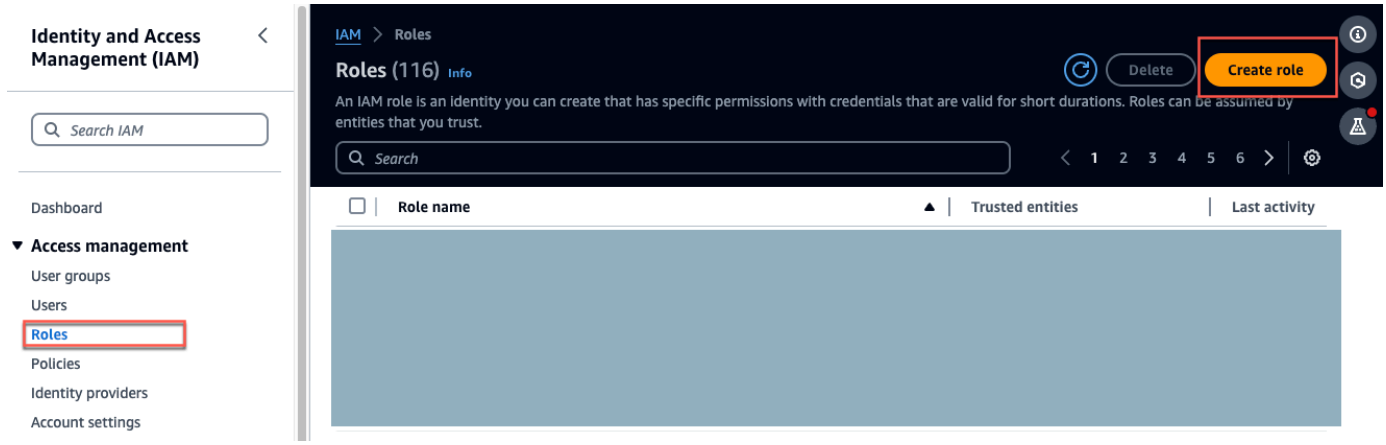


ステップ 3: ロールを作成する

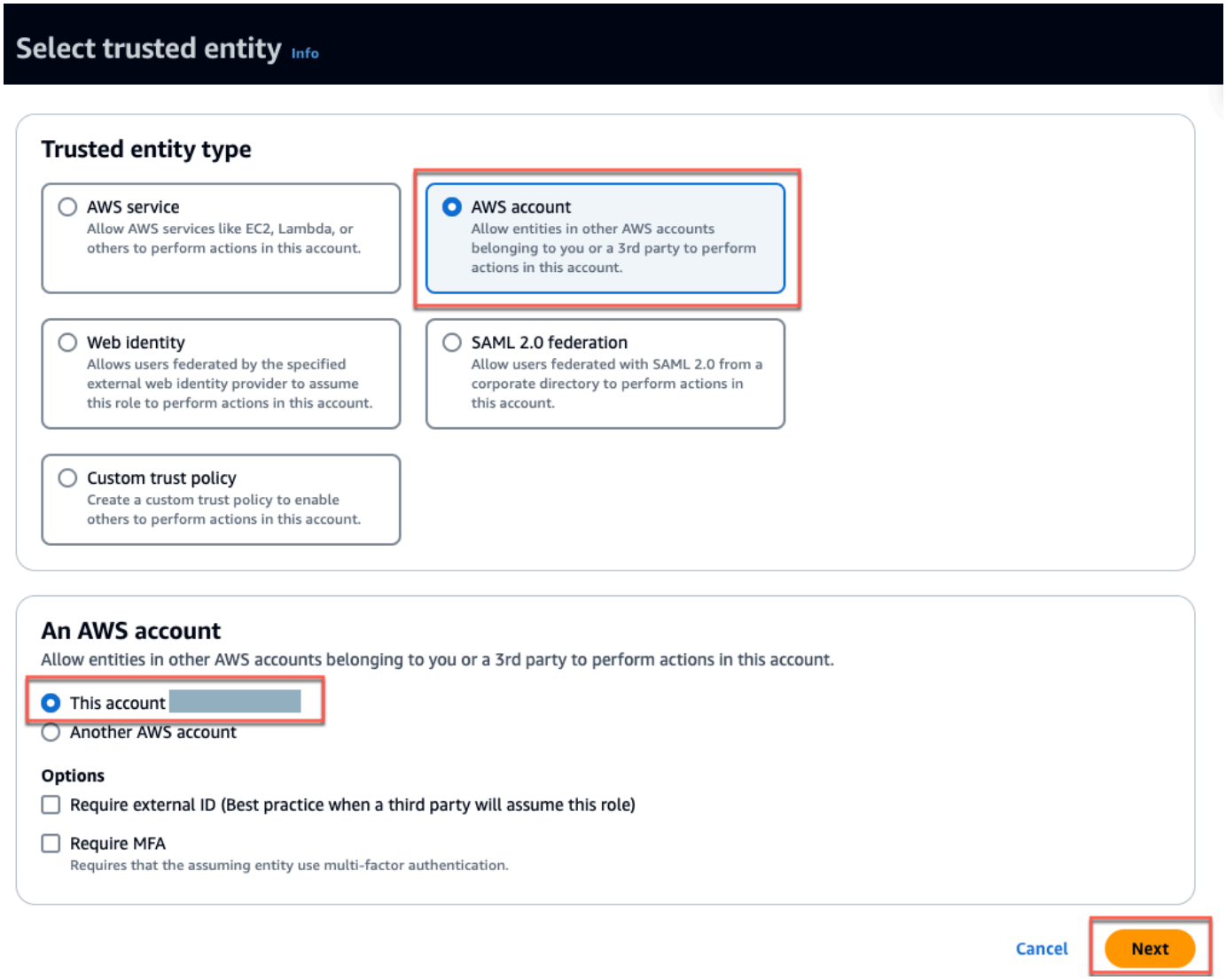
1. IAM コンソールを開き、ロールを選択します。



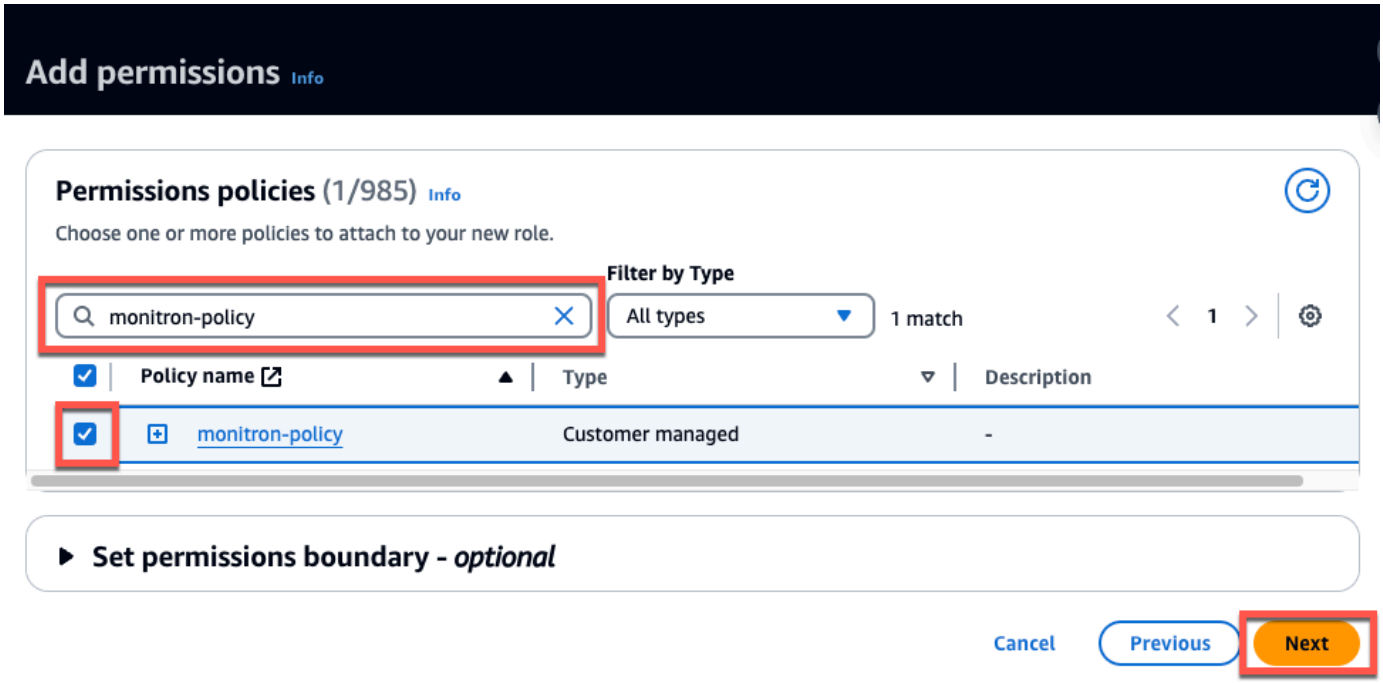
2. [ロールの作成] を選択してください。



3. 信頼されたエンティティを選択 の信頼されたエンティティタイプで、AWS アカウントを選択します。
4. AWS アカウントで、このアカウントを選択します。オプションを使用して追加の設定をカスタマイズできます。
5. [次へ] を選択します。



6. アクセス許可の追加で、アクセス許可ポリシーで、検索ボックスで作成したポリシーを検索し、ポリシーを選択します。



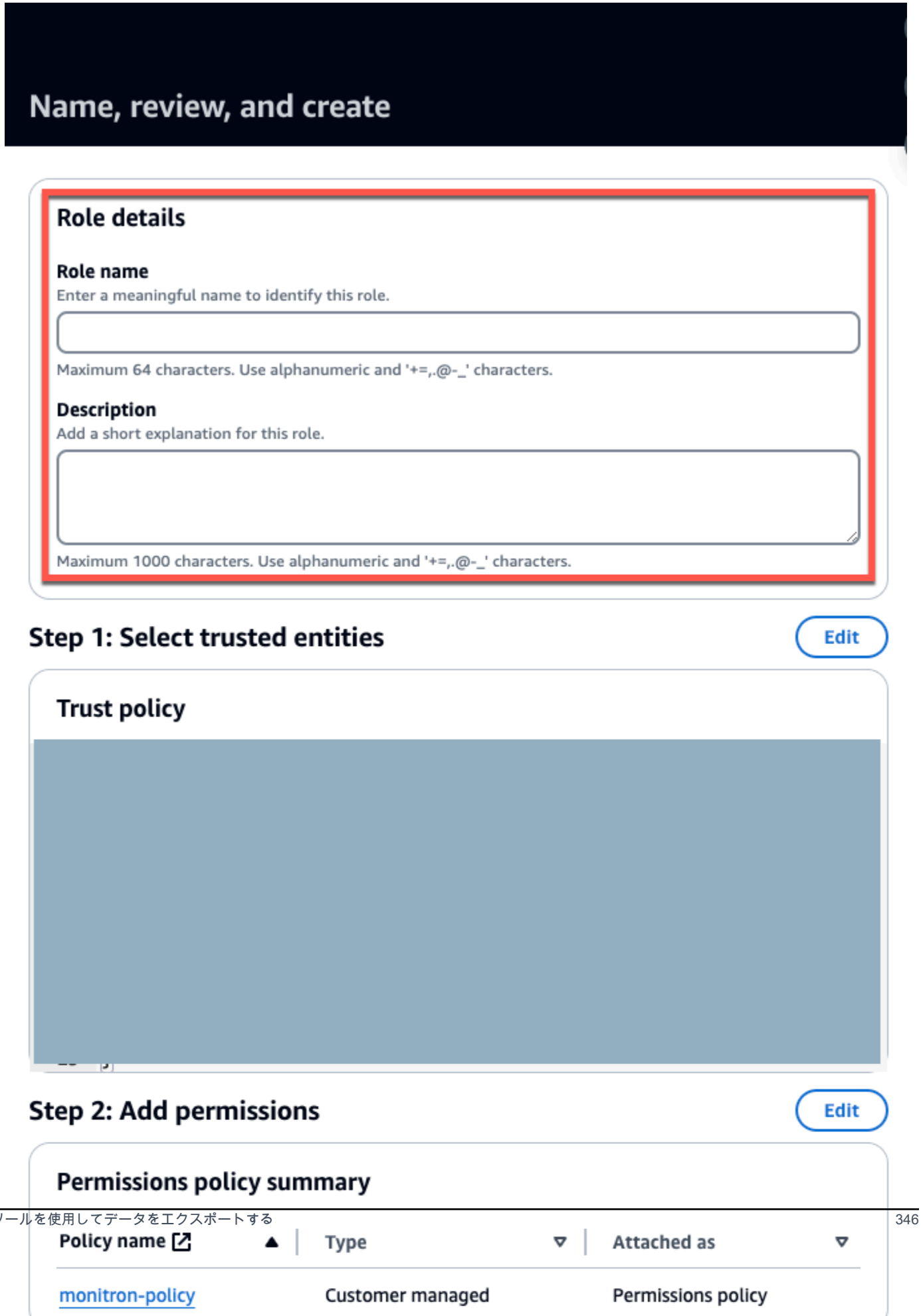
7. 名前、確認、作成ページで、次の操作を行います。

   a. ロールの詳細に、ロール名とオプションの説明を入力します。

   b. ステップ 1: 信頼されたエンティティを選択する、ステップ 2: 許可を追加する を無視することを選択できます。

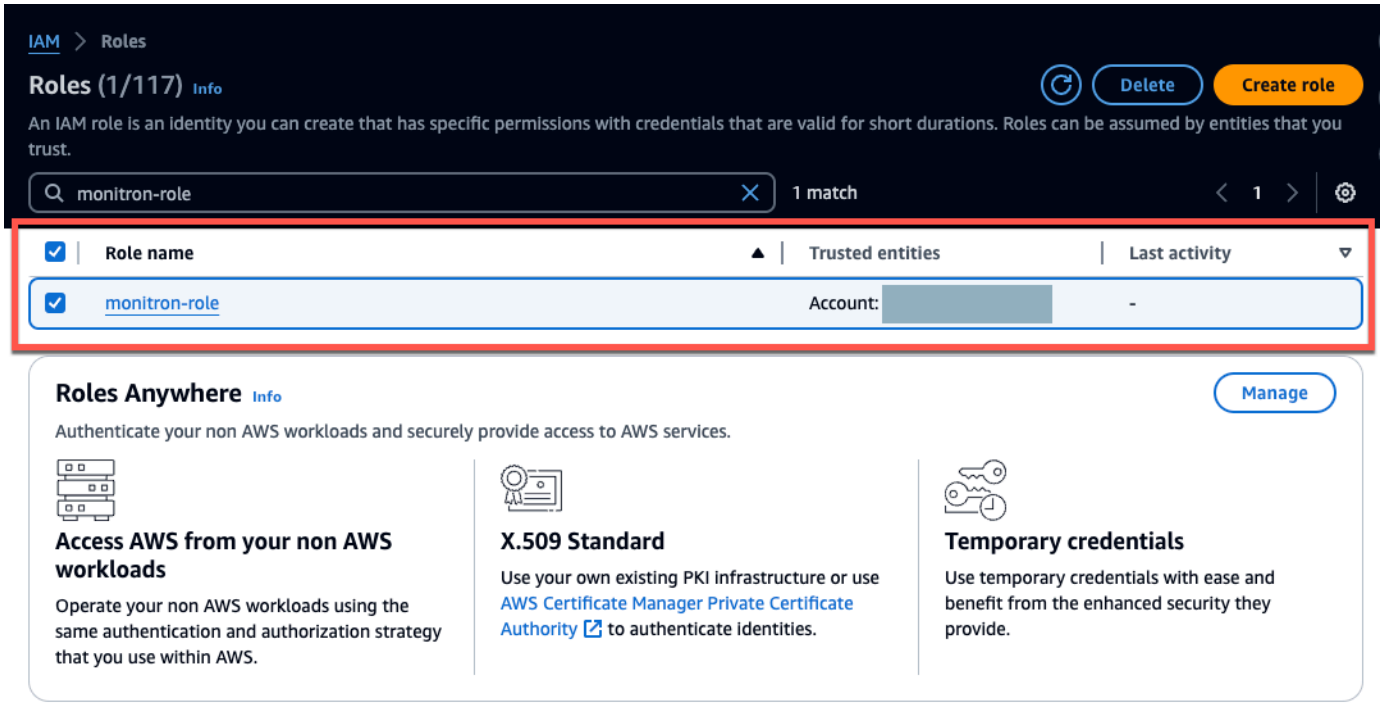
   c. ステップ 3: タグを追加する では、タグを追加する - オプションで、オプションのタグを追加してリソースを追跡します。

8. [ロールの作成] を選択してください。

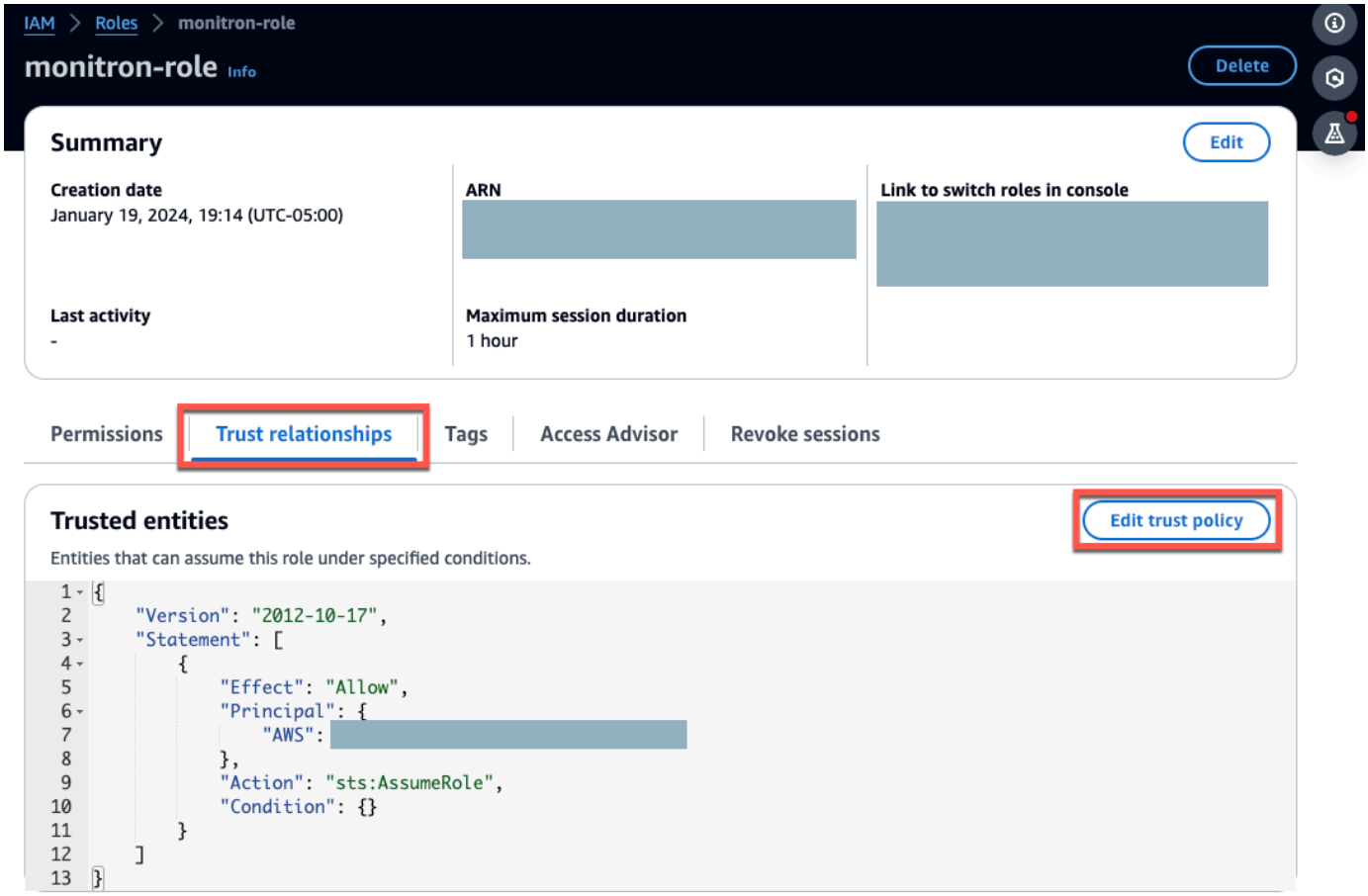

Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Step 1: Select trusted entities
Edit
Trust policy
Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
monitron-policy
Customer managed
Permissions policy

ステップ 4: 信頼ポリシーを作成する

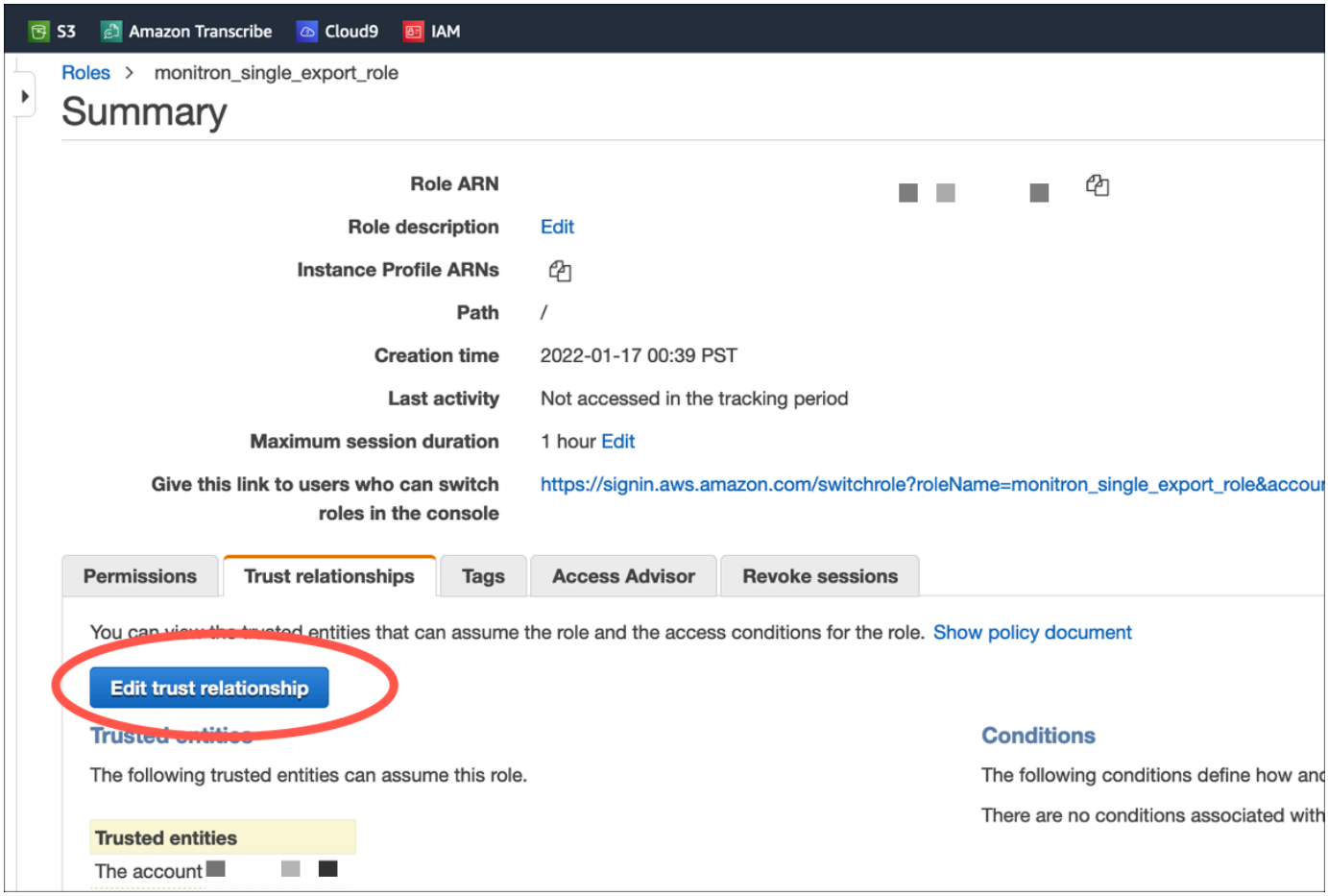
1. 先ほど作成したロールを検索し、選択します。



2. [信頼関係] タブを選択します。

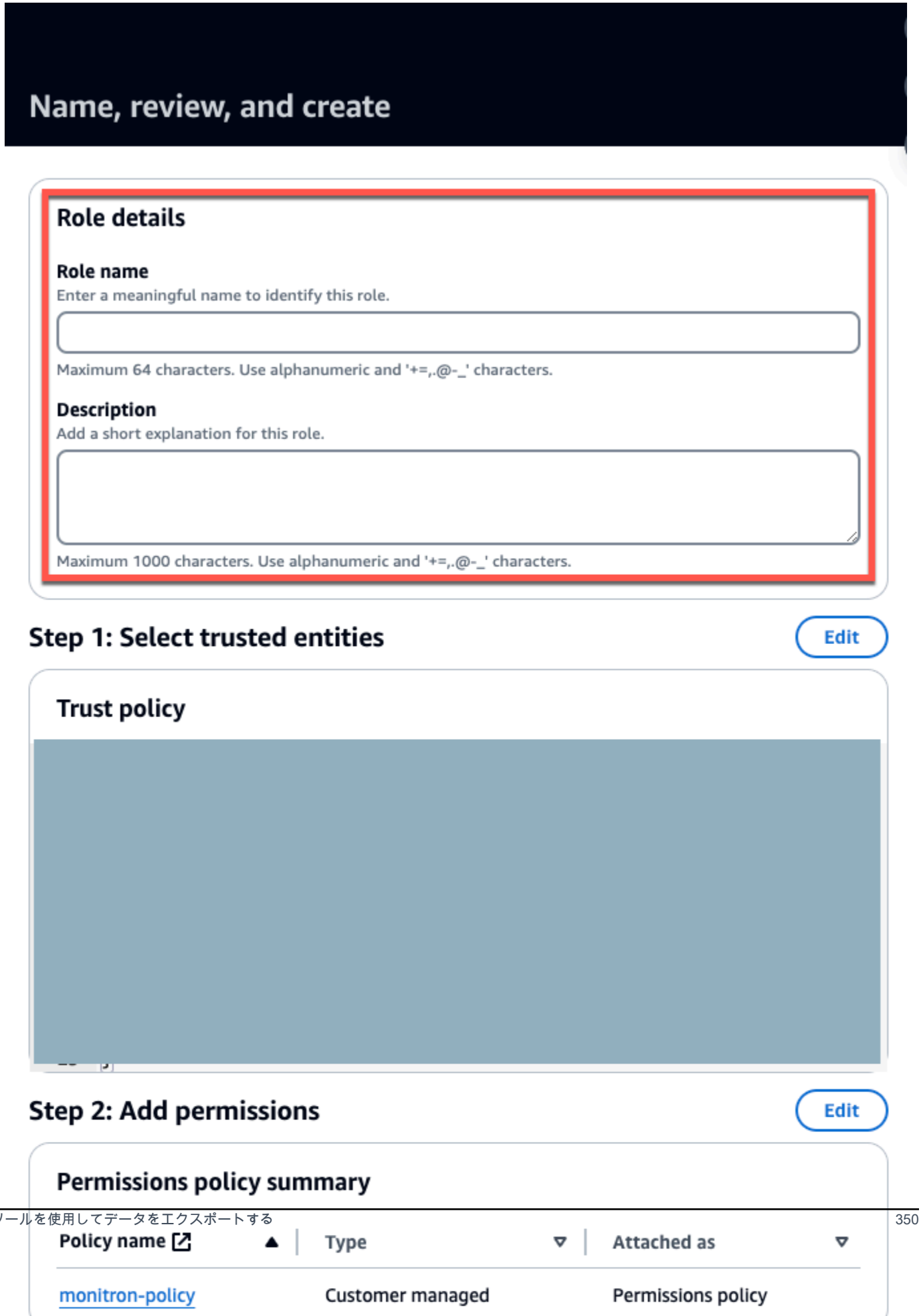


3. [Edit trust relationship (信頼関係の編集)] を選択します。



4. デフォルトの JSON テキストを消去して、フォームを空にします。
5. Amazon Monitron がロールを引き受けることを許可するポリシーを貼り付けます。

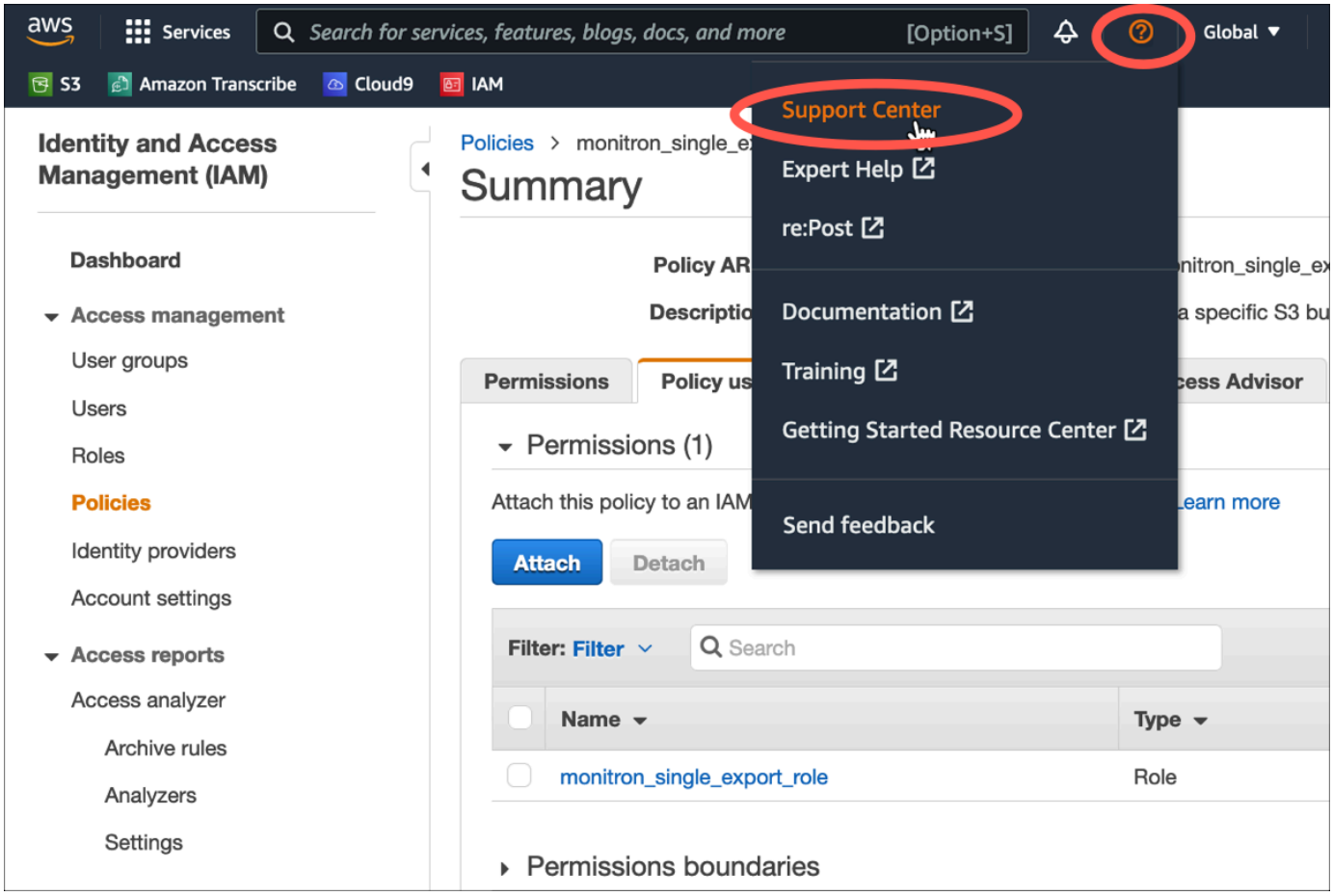
```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Principal": {
   "Service": ["monitron.amazonaws.com"]
  },
  "Action": "sts:AssumeRole"
 }]
}
```


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

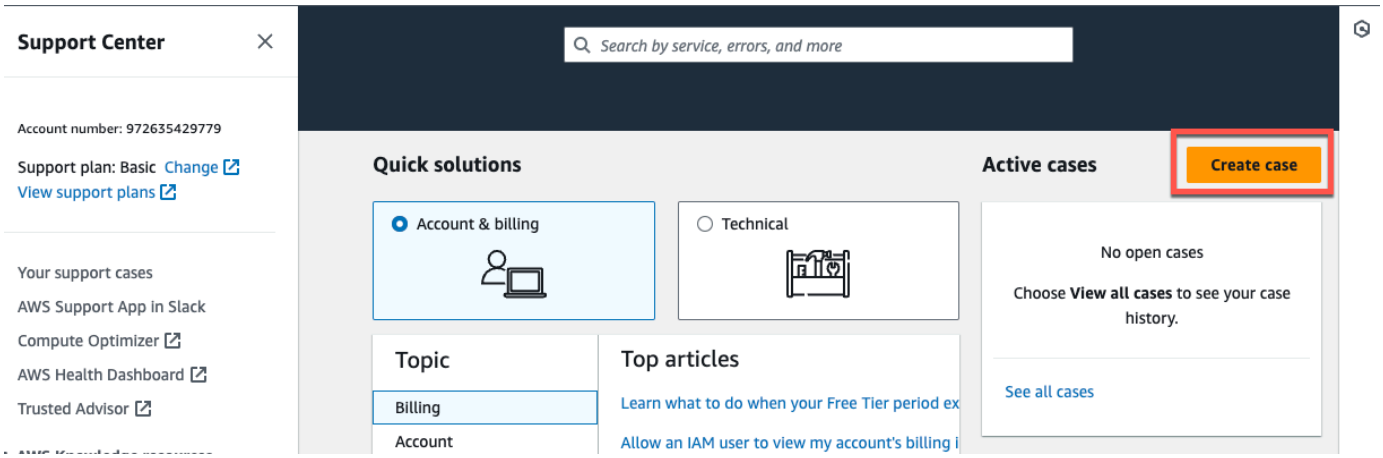
6. 信頼ポリシーの更新 を選択します。

ステップ 5: サポートケースを作成する

1. AWS コンソールから、任意のページの右上隅にある疑問符アイコンを選択し、サポートセンターを選択します。



2. 次のページで、[ケースの作成] を選択します。



3. どのようにサポートできるか ページで、次の操作を行います。

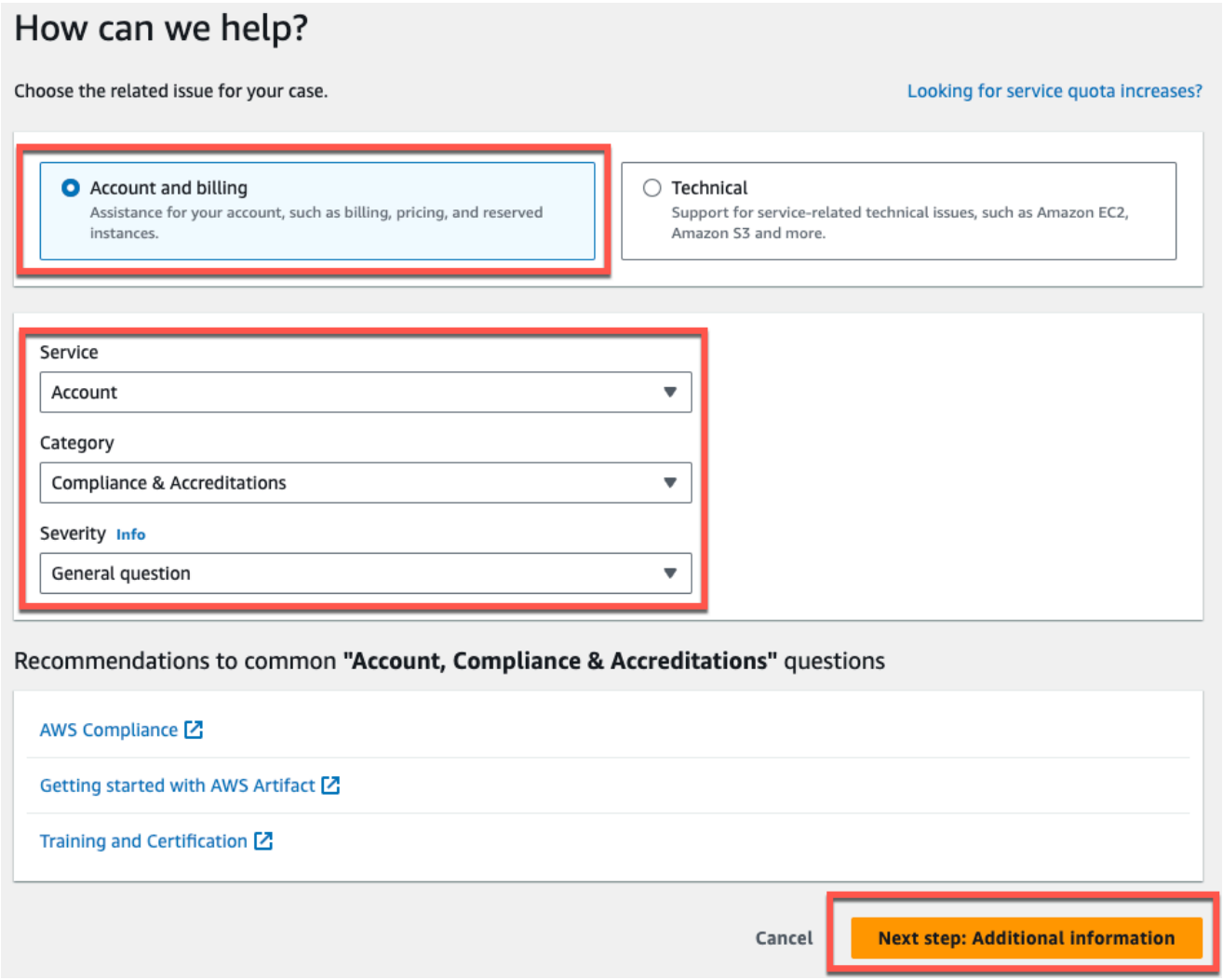
   a. [アカウントおよび請求サポート] を選択します。

   b. サービスで、アカウントを選択します。

   c. [カテゴリ] で、[コンプライアンスと認定] を選択します。

   d. サポート契約に基づいてそのオプションが利用できる場合は、[重要度] を選択します。

   e. [Next step: Additional information] (次のステップ:追加情報) を選択します。



4. 「追加情報」では、次の操作を行います。

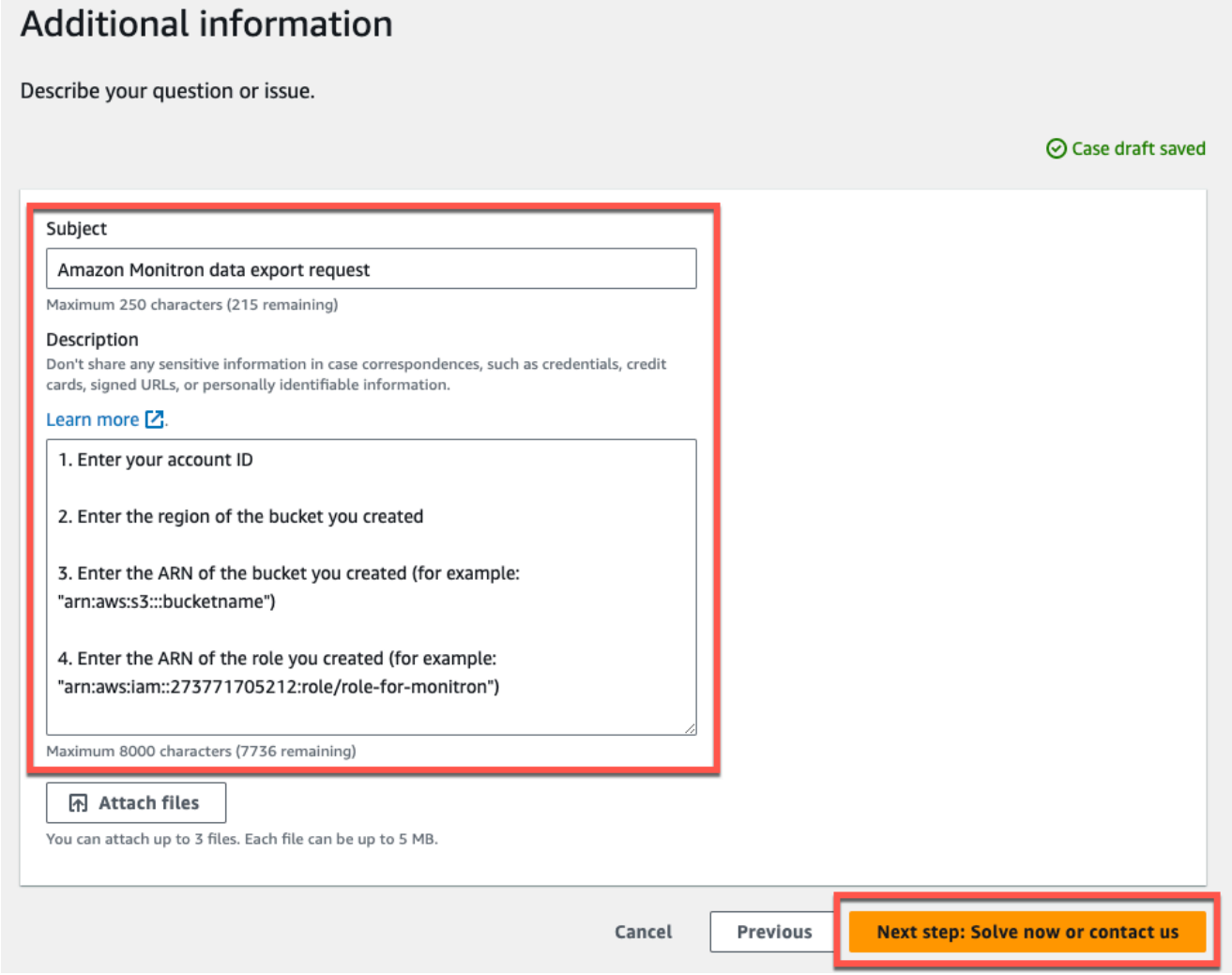
   a. [件名] に Amazon Monitron data export request と入力します。

   b. [説明] フィールドに、次のように入力します。

      1. アカウント ID

      2. 作成したバケットのリージョン

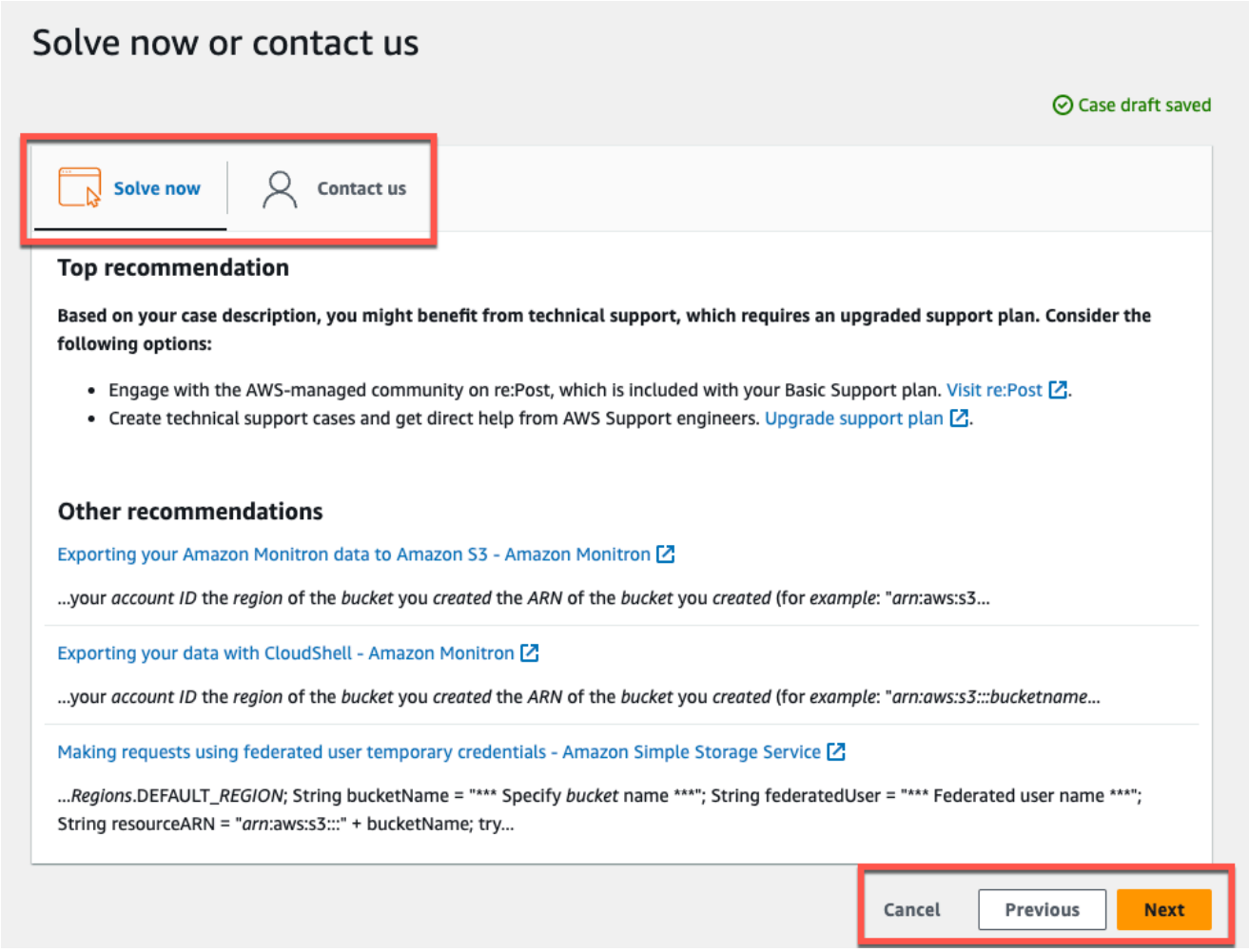
3. 作成したバケットの ARN (例:「arn:aws:s3:::bucketname」)
4. 作成したロールの ARN (例:「arn:aws:iam::273771705212:role/role-for-monitron」)



c. [次のステップ: 今すぐ解決またはお問い合わせ] を選択します。

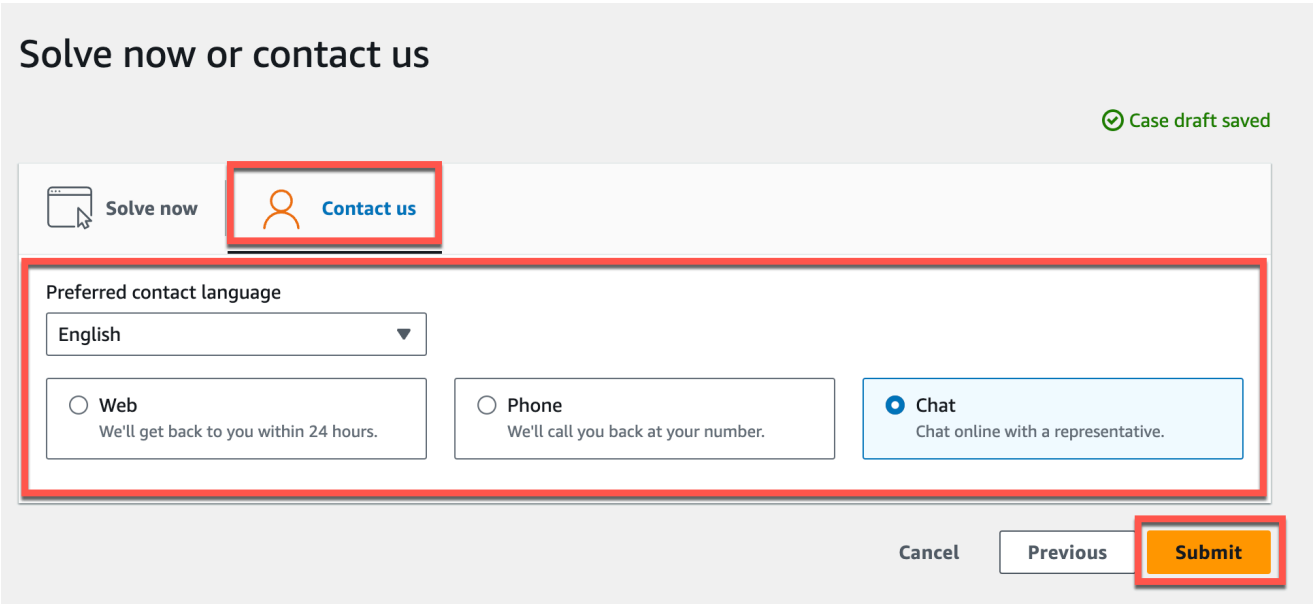
5. 今すぐ解決するか、お問い合わせください。以下を実行します。

a. 今すぐ解決で、次へを選択します。



b. Contact us で、希望する問い合わせ言語と希望する問い合わせ方法を選択します。

c. [Submit] を選択してください。ケース ID と詳細を含む確認画面が表示されます。



AWS カスタマーサポートスペシャリストができるだけ早くご連絡します。記載されている手順に問題がある場合、スペシャリストが詳細情報を伺うことがあります。必要な情報がすべて提供されている場合は、上記で作成した Amazon S3 バケットにデータがコピーされ次第、スペシャリストからご連絡いたします。

CloudShell を使用してデータをエクスポートする

トピック

- ステップ 1: Amazon S3 バケットを作成する (AWS CloudShellを使用)
- ステップ 2: Amazon Monitron に Amazon S3 バケットへのアクセスを許可する (を使用 AWS CloudShell)
- ステップ 3: サポートチケットを作成する

ステップ 1: Amazon S3 バケットを作成する (AWS CloudShellを使用)

1. AWS コンソールにログインします。
2. AWS CloudShellを開きます。

   AWS CloudShell はブラウザ内で動作するコマンドライン環境です。内では AWS CloudShell、AWS Command Line Interface を使用して多くの AWS サービスを起動および設定できます。
3. AWS CloudShellに次のコマンドを入力します。ここで、bucketname は作成するバケットの名前です。

   ```
   $ aws s3api create-bucket --bucket bucketname --region us-east-1
   ```

   このコマンドで、raw データを保存する Amazon S3 バケットを作成します。コンソールから簡単にバケットへアクセスできるようになり、適宜データをダウンロードできるようになります。詳細については、「Amazon S3 バケットの作成、設定、操作」を参照してください。

   > **Important**
   >
   > ユーザーはデータを保護するための適切な措置を講じる責任があります。サーバー側の暗号化を使用し、バケットへのパブリックアクセスをブロックすることを強くお勧めします。

上記のコマンドは、米国東部 (バージニア北部) リージョンにバケットを作成します。必要に応じて、リクエストボディに別のリージョンを指定できます。詳細については、「リージョン、アベイラビリティーゾーン、および Local Zones」を参照してください。

次のような出力が表示されます。

```
{ "Location": "/bucketname" }
```

4. 作成したバケットの Amazon リソースネーム (ARN) を次のように指定します。

```
arn:aws:s3:::bucketname
```

ステップ 2: Amazon Monitron に Amazon S3 バケットへのアクセスを許可する (を使用 AWS CloudShell)

1. 以下のコードをテキストエディタに貼り付け、「monitron-assumes-role.json.」と名前をつけて保存します。Microsoft Word は使用しないでください。余分な文字が追加されてしまいます。メモ帳や TextEdit などシンプルなテキストエディタを使用してください。

   このポリシーでは、S3 バケットへアクセスできるロールを引き受ける権限を Amazon Monitron に付与します。詳細については、「IAM のポリシーとアクセス許可」を参照してください。

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Principal": {
   "Service": ["monitron.amazonaws.com"]
  },
  "Action": "sts:AssumeRole"
 }]
}
```

2. 以下のテキストをテキストエディタに貼り付け、「monitron-role-accesses-s3.json」と名前をつけて保存します。

   このポリシーで、Amazon Monitron は (上記で作成したロールを使用して) Amazon S3 バケットにアクセスできるようになります。

```
{
    "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. 作成したテキストファイルでは、*#####*が出現する箇所をすべて自分のバケット名に置き換えます。

   例えば、バケットの名前が「relentless」の場合、ファイルは次のようになります。

```
{
    "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. 作成したばかりの JSON ファイルを両方とも、ホームディレクトリの CloudShell にアップロードします。

   ファイルをアップロードするには、CloudShell コンソールページの右上隅から [アクション] を選択し、[ファイルのアップロード] を選択します。

5. CloudShell のコマンドラインで次のとおりに入力します。

   aws iam create-role --role-name role-for-monitron --assume-role-policy-document "cat monitron-assumes-role.json"

   このコマンドはロールを作成し、monitron-assumes-role ポリシーをアタッチします。

   次のような出力が表示されます。

```
{
"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"
   }]
  }
 }
}
```

作成したロールの ARN 値をメモします。後で必要になります。

この例では、ARN 値は `arn:aws:iam::273771705212:role/role-for-monitron` です。

6. CloudShell のコマンドラインで次のとおりに入力します。

aws iam create-policy --policy-name role-uses-bucket --policy-document "cat role-uses-bucket.json"

このコマンドでは monitron-role-accesses-s3 ポリシーを作成します。

次のような出力が表示されます。

```
 {
 "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"
 }
}
```

作成したポリシーの ARN 値をメモします。次のステップで必要になります。

この例では、ARN 値は次の通りです。

```
arn:aws:iam::273771705212:policy/role-uses-bucket
```

7. CloudShell のコマンドラインに以下を入力し、ARN を role-uses-bucket ポリシーの ARN に置き換えます。

```
aws iam attach-role-policy --role-name role-for-monitron --policy-arn
     arn:aws:iam::273771705212:policy/role-uses-bucket
```

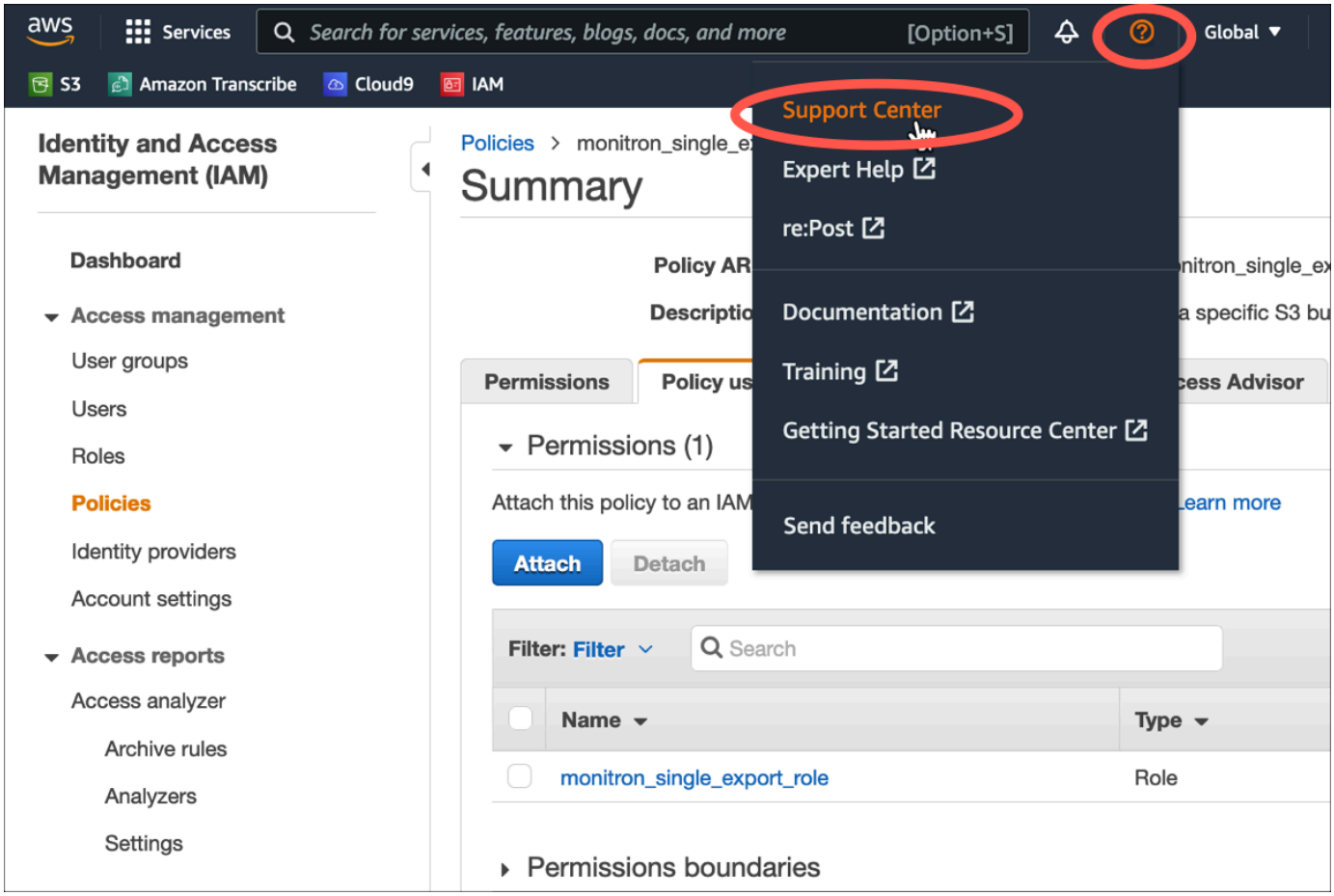
このコマンドでは、作成したロールに monitron-role-accesses-s3 ポリシーがアタッチされます。

これで、Amazon S3 バケット、Amazon Monitron が引き受けることができるロール、Amazon Monitron がそのロールを引き受けることを許可するポリシー、およびそのロールを使用するサービスが Amazon S3 バケットを使用することを許可する別のポリシーを作成し、プロビジョニングすることができました。

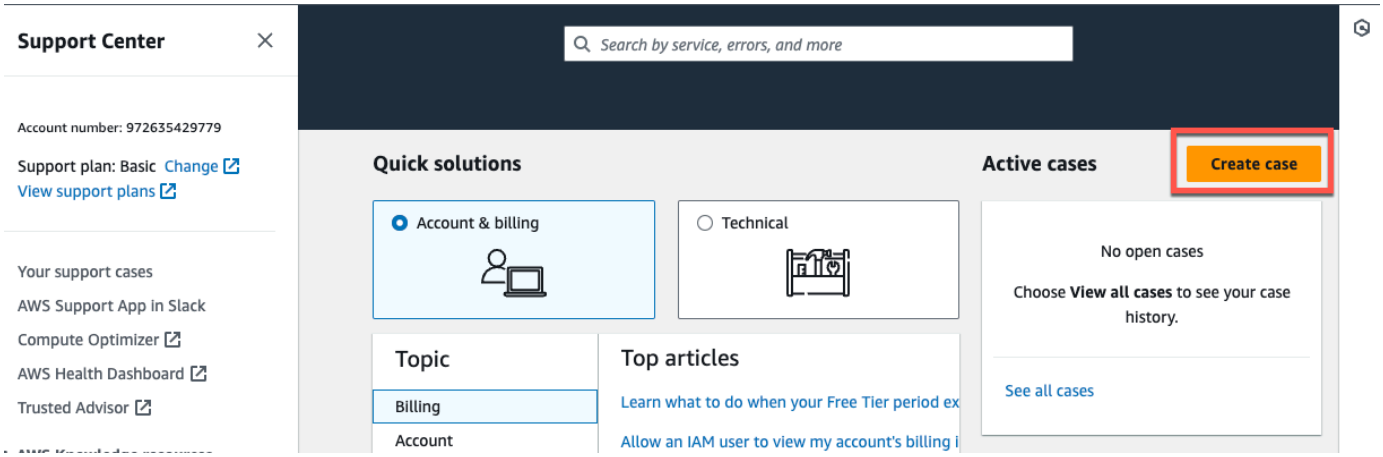
ユーザーはデータを保護するための適切な措置を講じる責任があります。サーバー側の暗号化を使用し、バケットへのパブリックアクセスをブロックすることを強くお勧めします。詳細については「パブリックアクセスのブロック」を参照してください。

ステップ 3: サポートチケットを作成する

1. AWS コンソールから、任意のページの右上隅にある疑問符アイコンを選択し、サポートセンターを選択します。



2. 次のページで、[ケースの作成] を選択します。



3. どのように支援できるか ページで、次の操作を行います。

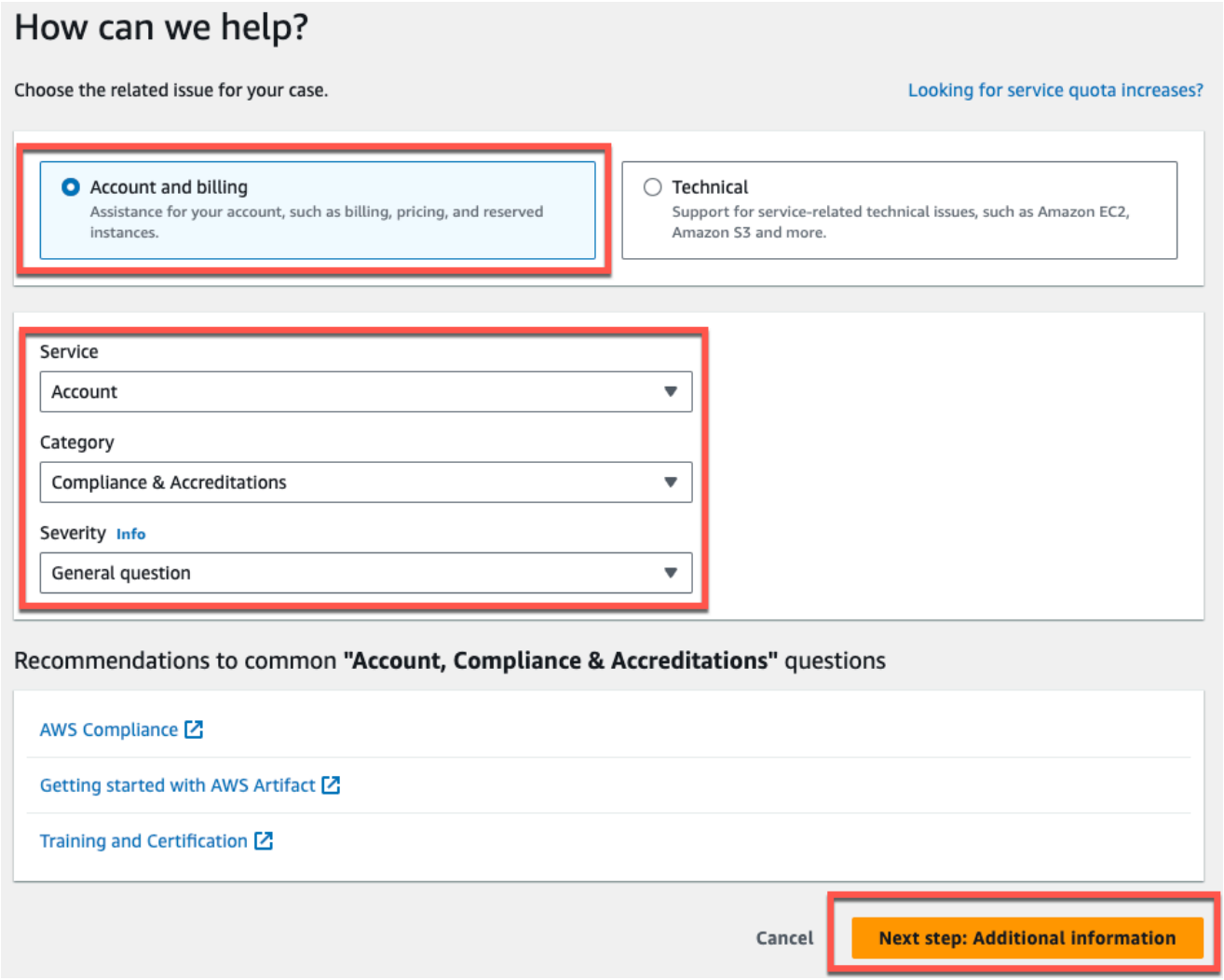
   a. [アカウントおよび請求サポート] を選択します。

   b. サービスで、アカウントを選択します。

   c. [カテゴリ] で、[コンプライアンスと認定] を選択します。

d. サポート契約に基づいてそのオプションが利用できる場合は、[重要度] を選択します。

e. [Next step: Additional information] (次のステップ:追加情報) を選択します。

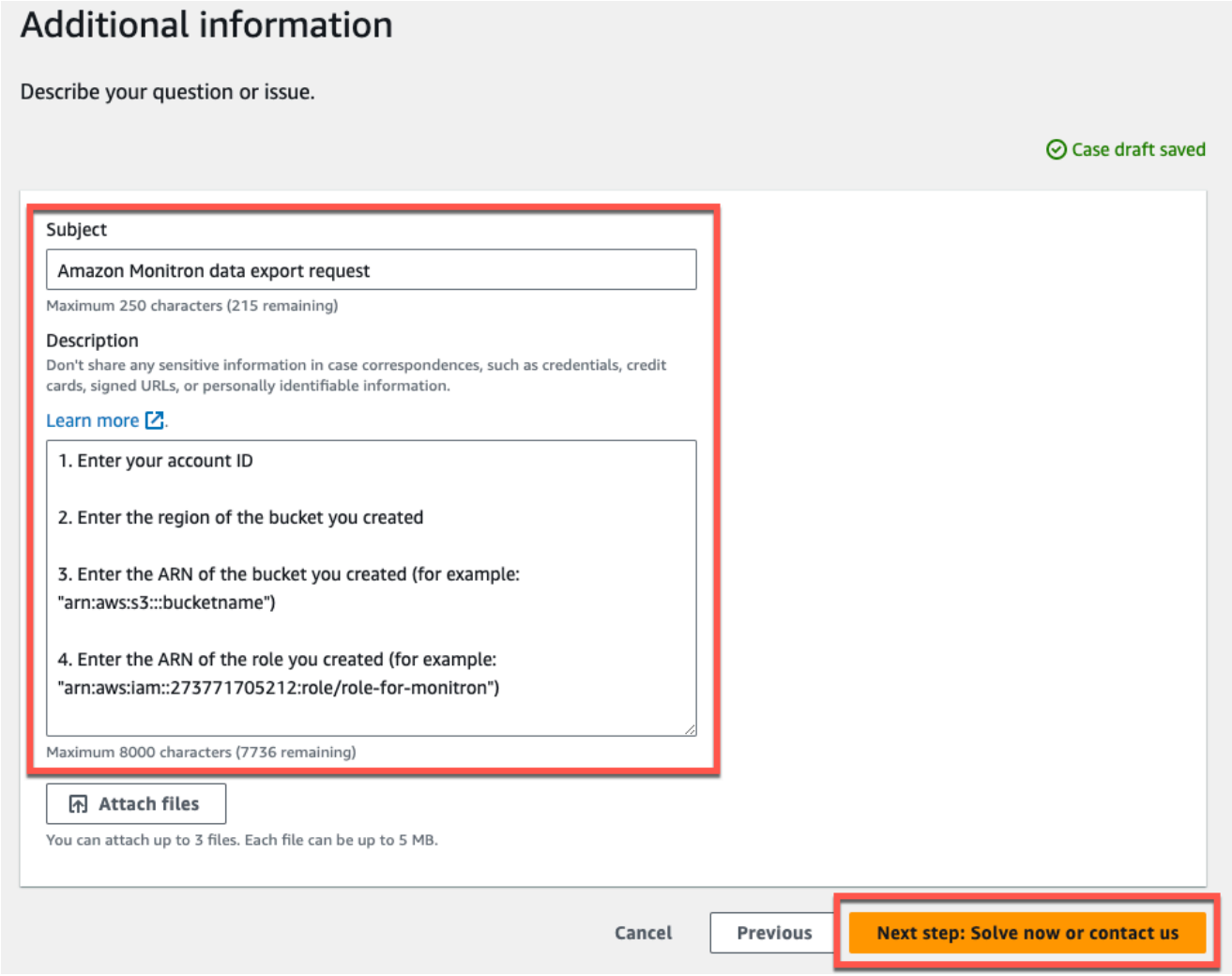


4. 「追加情報」では、次の操作を行います。

a. [件名] に Amazon Monitron data export request と入力します。

b. [説明] フィールドに、次のように入力します。

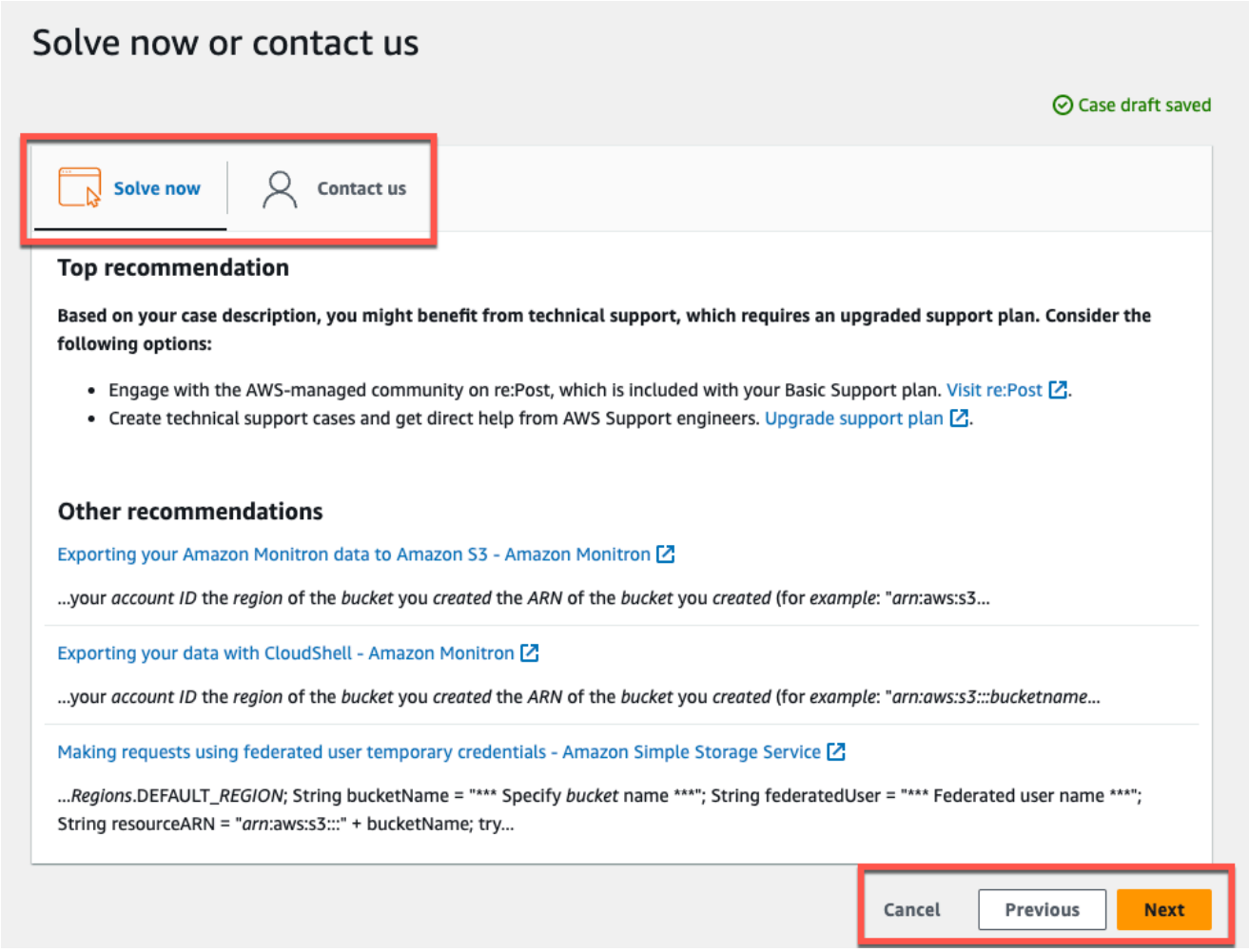
1. アカウント ID
2. 作成したバケットのリージョン
3. 作成したバケットの ARN (例:「arn:aws:s3:::bucketname」)
4. 作成したロールの ARN (例:「arn:aws:iam::273771705212:role/role-for-monitron」)



c. [次のステップ: 今すぐ解決またはお問い合わせ] を選択します。

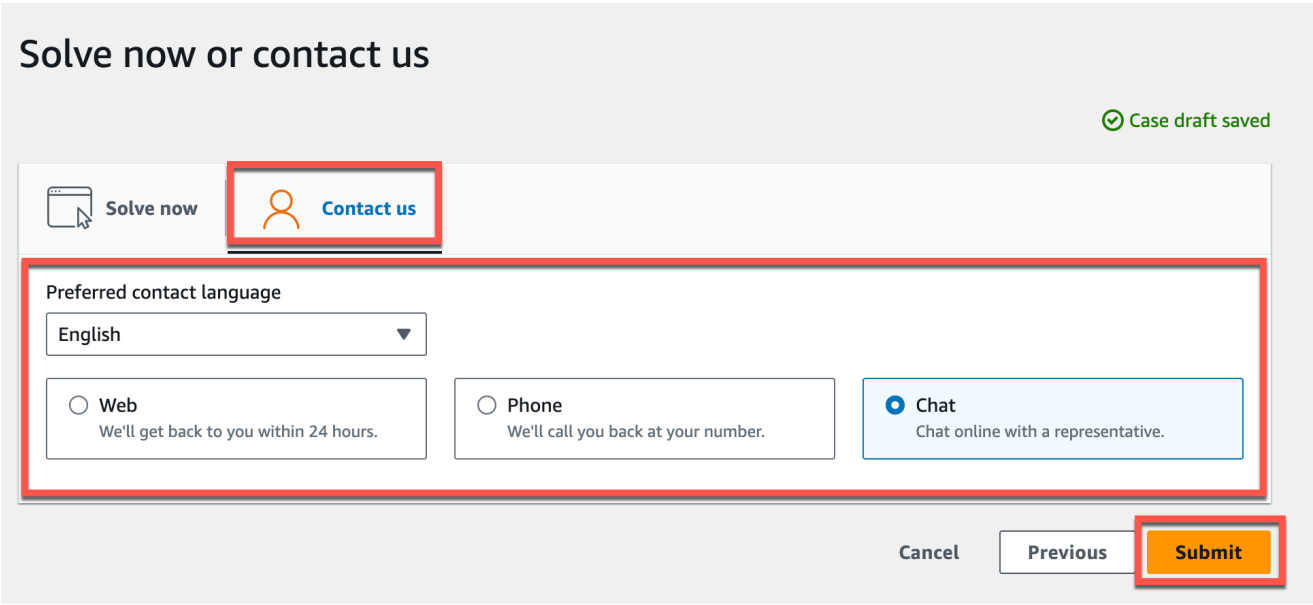
5. 今すぐ解決するか、お問い合わせください。以下を実行します。

a. 今すぐ解決で、次へを選択します。



b. Contact us で、希望する問い合わせ言語と希望する問い合わせ方法を選択します。

c. [Submit] を選択してください。ケース ID と詳細を含む確認画面が表示されます。



AWS カスタマーサポートスペシャリストができるだけ早くご連絡します。記載されている手順に問題がある場合、スペシャリストが詳細情報を伺うことがあります。必要な情報がすべて提供されている場合は、上記で作成した Amazon S3 バケットにデータがコピーされ次第、スペシャリストからご連絡いたします。

Amazon Monitron Kinesis データエクスポート v1

> **Note**
>
> Amazon Monitron の Kinesis データエクスポートスキーマ v1 は廃止されました。v2 データエクスポートスキーマの詳細を参照してください。

受信した測定データとそれに対応する推論結果を Amazon Monitron からエクスポートして、リアルタイムで分析ができます。データのエクスポートでは、ライブデータが Kinesis にストリーミングされます。

トピック

- Kinesis ストリームへデータをエクスポートする
- ライブデータエクスポート設定を編集する
- ライブデータエクスポートを停止する
- データエクスポートのエラーを表示する
- Kinesis ストリームへのサーバー側の暗号化の使用
- Amazon CloudWatch Logs による のモニタリング
- エクスポートしたデータを Amazon S3 に保存する
- Lambda でデータを処理する
- v1 データエクスポートスキーマを理解する

Kinesis ストリームへデータをエクスポートする

1. プロジェクトのメインページの下部、右側にある [ライブデータのエクスポートを開始] を選択します。
2. [Amazon Kinesis データストリームの選択] で、次のいずれかの操作を行います。
   - 検索ボックスに既存のストリーム名を入力して、ステップ 5 に進みます。

- [新しいデータストリームを作成] を選択します。

3. [データストリームの作成] ページの [データストリームの設定] で、データストリーム名を入力します。
4. [データストリーム容量] で、[容量モード] を選択します。

   - データストリームのスループット要件が予測不可能で変動する場合は、[オンデマンド] を選択します。
   - データストリームのスループット要件を確実に見積もることができる場合は、[プロビジョニング済み] を選択してください。次に、[プロビジョニングされたシャード] で、作成するシャード数を入力するか、[シャードの見積もり] を選択します。
5. [データストリームの作成] を選択します。

ライブデータエクスポート設定を編集する

ライブデータエクスポート設定を編集するには、

1. Amazon Monitron コンソールを開きます。
2. ナビゲーションペインで、[プロジェクト] を選択します。
3. プロジェクトが複数ある場合は、エクスポート設定を編集するプロジェクトを選択します。
4. プロジェクトのメインページにある、[ライブデータエクスポート] の [アクション] のドロップダウンメニューから、[ライブデータエクスポート設定の編集] を選択します。

ライブデータエクスポートを停止する

1. Amazon Monitron コンソールを開きます。
2. ナビゲーションペインで、[プロジェクト] を選択します。
3. プロジェクトが複数ある場合は、エクスポート設定を編集するプロジェクトを選択します。
4. プロジェクトのメインページにある、[ライブデータエクスポート] の [アクション] のドロップダウンメニューから [ライブデータのエクスポートを停止] を選択します。
5. ポップアップウィンドウで、[停止] を選択します。

データエクスポートのエラーを表示する

CloudWatch Logs のインターフェイスでエラーメッセージを表示するには、

- Amazon Monitron コンソールで、プロジェクトのメインページにある [ライブデータのエクスポート] から、[CloudWatch ロググループ] を選択します。

Kinesis ストリームへのサーバー側の暗号化の使用

Kinesis データのエクスポートをセットアップする前に、Kinesis ストリームに対してサーバー側の暗号化を有効にできます。ただし、Kinesis データのエクスポートをセットアップした後にサーバー側の暗号化を有効にすると、Amazon Monitron はストリームに公開できなくなります。これは、Amazon Monitron に Kinesis に送信されたデータを暗号化できる kms:GenerateDataKey を呼び出す権限がないためです。

この問題を回避するには、設定を変更せず、??? に記載の指示に従ってください。設定した暗号化をエクスポート設定に関連付けることができます。

Amazon CloudWatch Logs による のモニタリング

Amazon CloudWatch Logs を使用して、Amazon Monitron のライブデータエクスポートをモニタリングできます。測定値のエクスポートに失敗すると、Amazon Monitron は CloudWatch Logs にログイベントを送信します。エラーログにメトリクスフィルタを設定してメトリクスを生成し、アラームを設定することもできます。アラームは特定のしきい値を監視し、これらのしきい値に達したときに通知を送信したりアクションを実行したりできます。詳細については、『CloudWatch ユーザーガイド』を参照してください。

Amazon Monitron は、/aws/monitron/data-export/{HASH_ID} ロググループにログイベントを送信します。

ログイベントには次の JSON 形式があります。

```
{
    "assetDisplayName": "string",
    "destination": "string",
    "errorCode": "string",
    "errorMessage": "string",
    "eventId": "string",
    "positionDisplayName": "string",
    "projectDisplayName": "string",
    "projectName": "string",
    "sensorId": "string",
    "siteDisplayName": "string",
    "timestamp": "string"
```

```
}
```

assetDisplayName

- アプリに表示されるアセット名
- タイプ: 文字列

destination

- Kinesis データストリームの ARN
- タイプ: 文字列
- パターン: arn:aws:kinesis:{{REGION}}:{{AWS_ACCOUNT_ID}}:stream/{{STREAM_NAME}}

errorCode

- エラーコード
- 型: 文字列
- 有効な値：`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

- 詳しいエラーメッセージ
- タイプ: 文字列

eventId

- 各測定値のエクスポートに対応する固有のイベント ID
- タイプ: 文字列

positionDisplayName

- アプリに表示されるセンサーの配置名
- タイプ: 文字列

sensorId

- 測定値の送信元となるセンサーの物理 ID
- タイプ: 文字列

siteDisplayName

- アプリに表示されるサイト名
- タイプ: 文字列

timestamp

- Amazon Monitron サービスが測定値を受信したときのタイムスタンプ (UTC 時間)
- タイプ: 文字列
- パターン: yyyy-mm-dd hh:mm:ss.SSS

エクスポートしたデータを Amazon S3 に保存する

トピック

- 事前定義された CloudFormation テンプレートを使用する
- コンソールで Kinesis を手動で設定する

事前定義された CloudFormation テンプレートを使用する

Amazon Monitron には、Kinesis データストリームから Amazon S3 バケットにデータを配信するように Firehose をすばやくセットアップするための事前定義された AWS CloudFormation テンプレートが用意されています。このテンプレートによって動的パーティショニングが可能になり、配信される Amazon S3 オブジェクトでは Amazon Monitron が推奨する以下のキーフォーマットが使用されます: `/project={projectName}/site={siteName}/time={yyyy-mm-dd 00:00:00}/{filename}`

1. AWS アカウントにサインインします。
2. 以下の URL で新しいブラウザタブを開きます。

```
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. 開いた AWS CloudFormation ページの右上隅で、Amazon Monitron を使用しているリージョンを選択します。
4. デフォルトでは、Amazon S3 にデータを配信するのに必要なその他のリソースとともに、新しい Kinesis データストリームと S3 バケットがテンプレートで作成されます。パラメータを変更して既存のリソースを使用できます。
5. が IAM リソースを作成する AWS CloudFormation 可能性があることを確認するチェックボックスをオンにします。

6. [スタックの作成] を選択してください。
7. 次のページで、スタックのステータスが CREATE_COMPLETE になるまで必要に応じて更新アイコンを選択します。

コンソールで Kinesis を手動で設定する

1. AWS マネジメントコンソールにサインインし、https://https://console.aws.amazon.com/kinesis.https://www.kit で Kinesis コンソールを開きます。
2. ナビゲーションペインで、[配信ストリーム] を選択します。
3. [Create delivery stream (配信ストリームの作成)] を選択します。
4. [ソース] で、[Amazon Kinesis Data Streams] を選択します。
5. [送信先] で、[Amazon S3] を選択します。
6. [ソースの設定] の [Kinesis Data Stream] で、Kinesis データストリームの ARN を入力します。
7. [配信ストリーム名] に、Kinesis データストリーム名を入力します。
8. [送信先の設定] で [Amazon S3 バケット] を選択するか、バケット URI を入力します。
9. (任意) JSON のインライン解析を使用して動的パーティショニングを有効にします。このオプションは、ソース情報とタイムスタンプに基づいて、ストリーミング測定データを分割する場合に適しています。例：

   - [動的パーティショニング] で [有効] を選択します。
   - [改行の区切り文字] で [有効] を選択します。
   - [JSON のインライン解析] で [有効] を選択します。
   - [動的パーティショニングキー] に以下を追加します。

キー名	JQ 式
プロジェクト	.projectDisplayName| "project=\(.)"
site	.siteDisplayName| "site=\(.)"
時間	.timestamp| sub("[0-9]{2}:[0-9]{2}:[0-9]{2}.[0-9]{3}$"; "00:00:00")| "time=\(.)"

10. [動的パーティショニングキーを適用] を選択し、生成された Amazon S3 バケットプレフィックスが `!{partitionKeyFromQuery:project}/!{partitionKeyFromQuery:site}/!{partitionKeyFromQuery:time}/` であることを確認します。
11. Amazon S3 で、オブジェクトは次のキー形式を使用します: `/project={projectName}/site={siteName}/time={yyyy-mm-dd 00:00:00}/{filename}`
12. [Create delivery stream (配信ストリームの作成)] を選択します。
13. (任意) より詳細なパスを使用してください。

    動的パーティションを選択した場合、 AWS Glue と Athena を使用してデータをクエリする場合は、前の Amazon S3 キー形式を使用します。より詳細なキー形式を選択することもできますが、Amazon Athena クエリでは効率的ではありません。より詳細な Amazon S3 のキーパスを設定する例を次に示します。

    [動的パーティショニングキー] に以下を追加します。

キー名	JQ 式
プロジェクト	.projectDisplayName| "project=\(.)"
site	.siteDisplayName| "site=\(.)"
アセット	.assetDisplayName| "asset=\(.)"
position	.sensorPositionDisplayName| "position=\(.)"
センサー	.sensor.physicalId | "sensor=\(.)"
date	.timestamp| sub(" [0-9]{2}:[0-9]{2}:[0-9]{2}.[0-9]{3}$"; "")| "date=\(.)"

    Amazon S3 で、オブジェクトは次のキー形式を使用します: `/project={projectName}/site={siteName}/asset={assetName}/position={positionName}/sensor={sensorId}/date={yyyy-mm-dd}/time={HH:MM:SS}/{filename}`

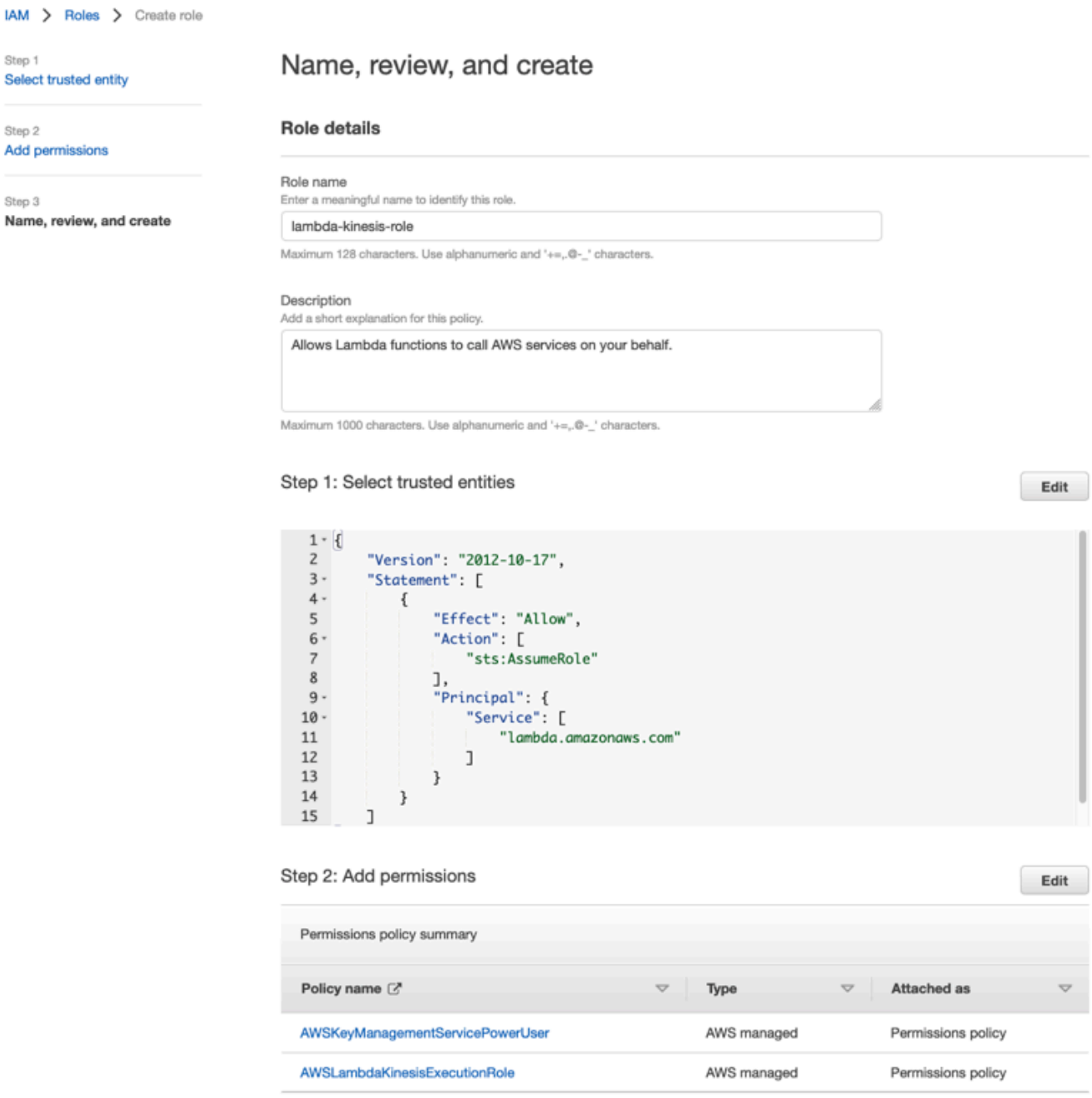
Lambda でデータを処理する

トピック

- ステップ 1: AWS リソースにアクセスするためのアクセス許可を関数に付与する IAM ロールを作成する。
- ステップ 2 : Lambda 関数を作成する
- ステップ 3: Lambda 関数を設定する
- ステップ 4: AWS Lambda コンソールで Kinesis トリガーを有効にする

ステップ 1: AWS リソースにアクセスするためのアクセス許可を関数に付与する IAM ロールを作成する。

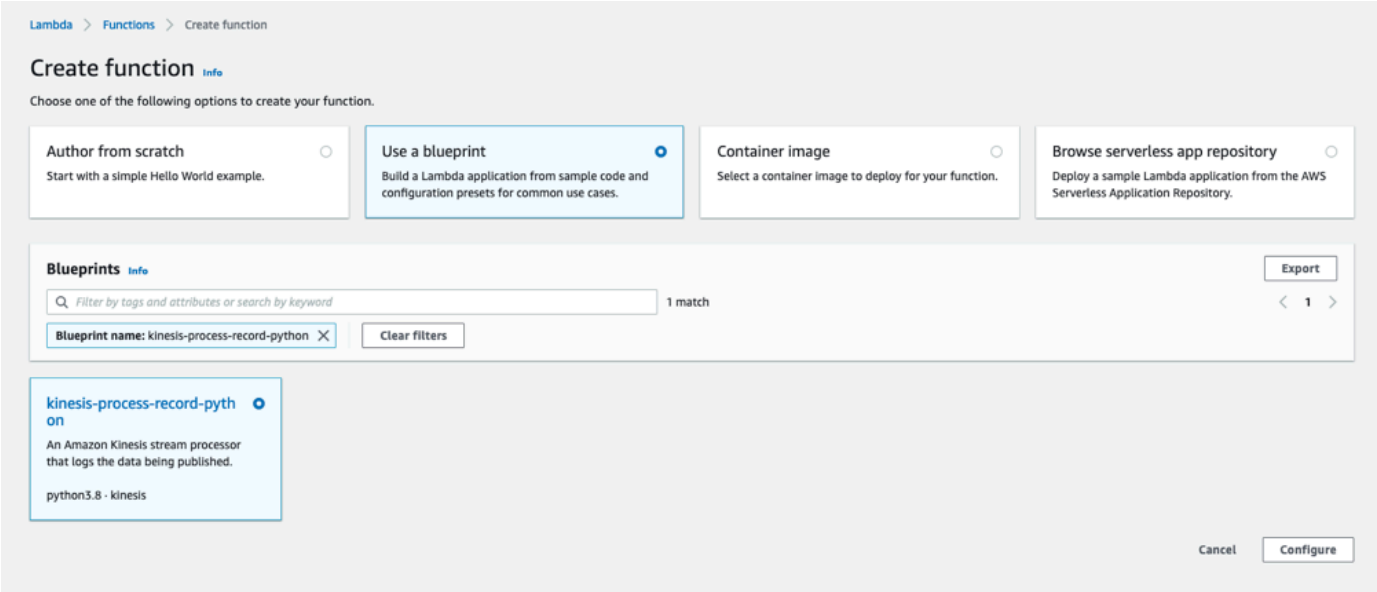
1. IAM コンソールの [ロールページ] を開きます。
2. [ロールの作成] を選択します。
3. 次のプロパティでロールを作成します。
   - 信頼されたエンティティ: Lambda
   - 権限: AWSLambdaKinesisExecutionRole (Kinesis ストリームが暗号化されている場合は、AWSKeyManagementServicePowerUser)
   - ロール名: lambda-kinesis-role



ステップ 2 : Lambda 関数を作成する

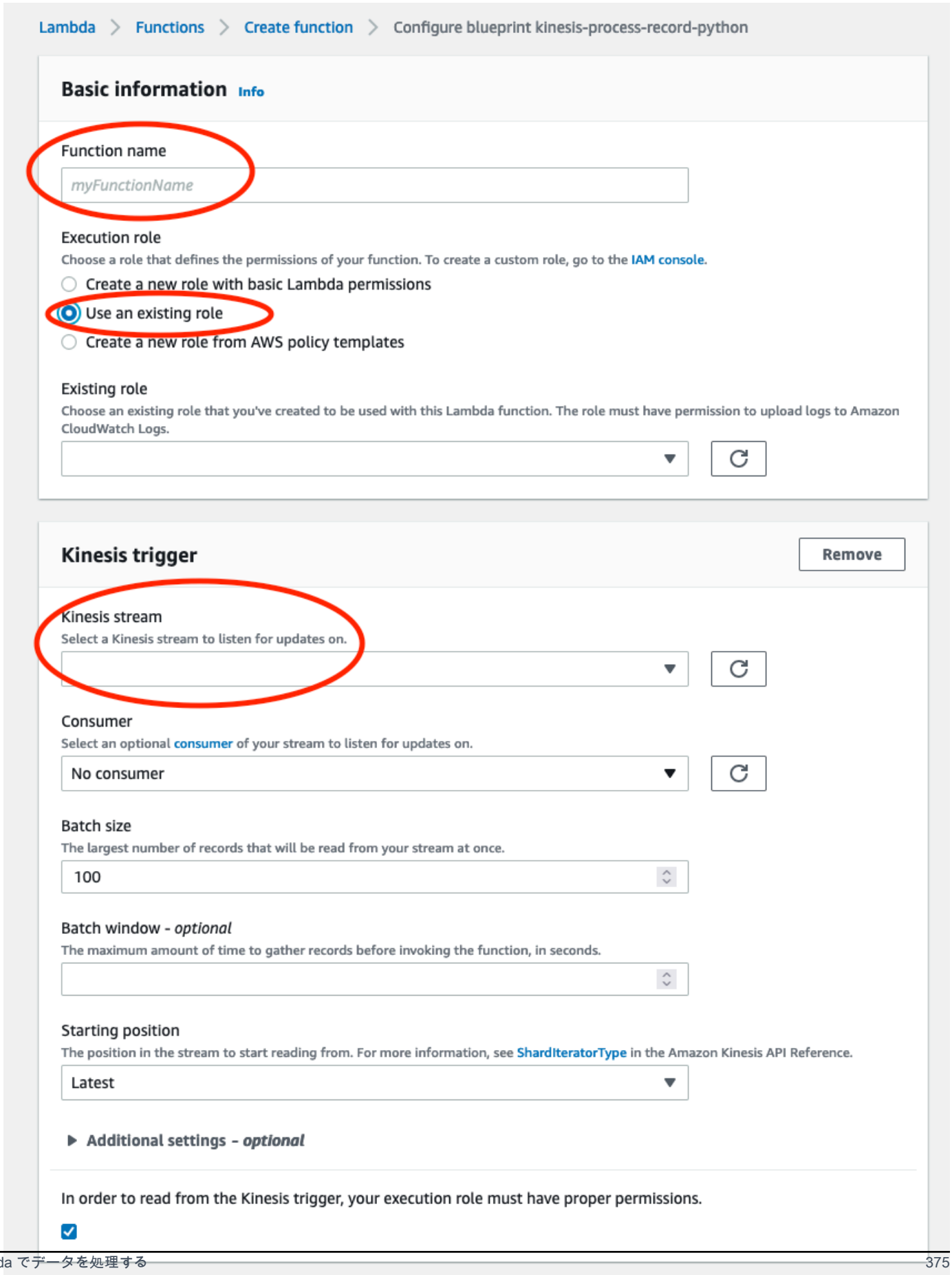
1. Lambda コンソールの [関数] ページを開きます。
2. [Create function] (関数の作成) を選択します。
3. [設計図の使用] を選択します。

4. Blueprints の検索ボックスで、kinesis-process-record (nodejs) または kinesis-process-record-python を検索して選択します。
5. [設定] を選択します。



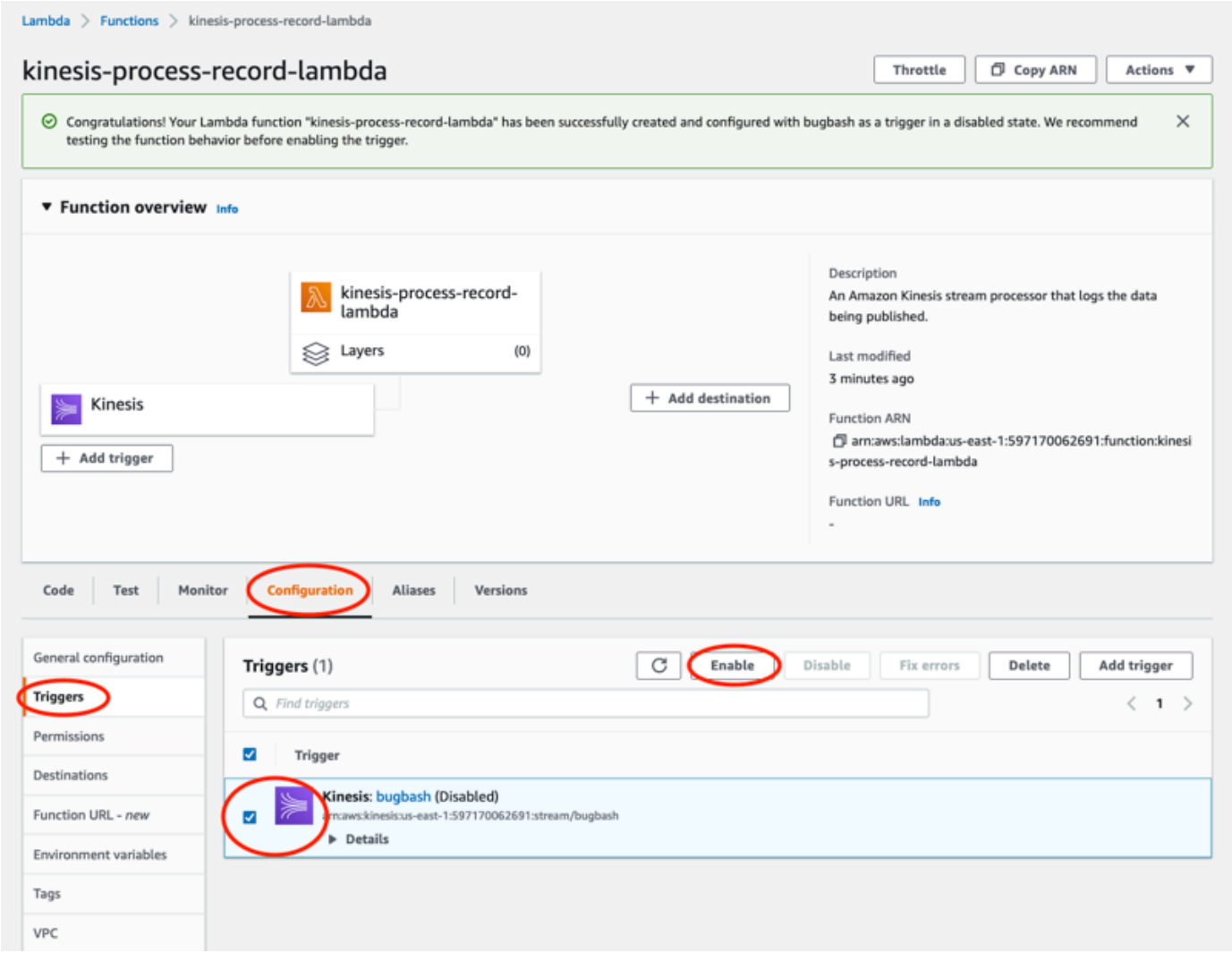
ステップ 3: Lambda 関数を設定する

1. [関数名] を選択します。
2. 最初のステップで作成したロールを [実行ロール] として選択します。
3. Kinesis トリガーを設定します。
    1. Kinesis ストリーミングを選択します。
    2. [関数の作成] を選択します。


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.

ステップ 4: AWS Lambda コンソールで Kinesis トリガーを有効にする

1. [設定] タブで、[トリガー] を選択します。
2. Kinesis ストリーミング名の横にあるボックスにチェックを入れ、[有効] を選択します。



この例で使用されているブループリントは、選択したストリームの口グデータのみを消費します。後で Lambda 関数コードを追加編集して、より複雑なタスクを実行できます。

v1 データエクスポートスキーマを理解する

> **Note**
>
> Amazon Monitron の Kinesis データエクスポートスキーマ v1 は廃止されました。v2 データエクスポートスキーマの詳細を参照してください。

各測定データとそれに対応する推論結果は、1 つの Kinesis データストリームレコードとして JSON 形式でエクスポートされます。

トピック

- v1 スキーマ形式
- v1 スキーマパラメータ

v1 スキーマ形式

```
{
    "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 スキーマパラメータ

timestamp

- Monitron サービスが測定値を受信したときのタイムスタンプ (UTC時間)
- タイプ: 文字列
- パターン: yyyy-mm-dd hh:mm:ss.SSS

eventId

- 各測定値に割り当てられる固有のデータエクスポートイベント ID。受信した Kinesis ストリームレコードを重複排除するのに使用できます。
- タイプ: 文字列

version

- スキーマバージョニング
- タイプ: 文字列
- 現在の値: 1.0

projectDisplayName

- アプリとコンソールに表示されるプロジェクト名
- タイプ: 文字列

siteDisplayName

- アプリに表示されるサイト名
- タイプ: 文字列

assetDisplayName

- アプリに表示されるアセット名
- タイプ: 文字列

sensorPositionDisplayName

- アプリに表示されるセンサーの配置名
- タイプ: 文字列

sensor.physicalId

- 測定値の送信元となるセンサーの物理 ID
- タイプ: 文字列

sensor.rssi

- 信号強度のインジケータ値を受信する Bluetooth センサー
- タイプ: 数値
- 単位: dBm

gateway.physicalId

- Amazon Monitron サービスへのデータ送信に使用されるゲートウェイの物理 ID
- タイプ: 文字列

measurement.features.acceleration.band0To6000Hz.xAxis.rms

- X 軸の 0 ~ 6000 Hz の周波数帯域で観測された加速度の二乗平均平方根
- タイプ: 数値
- 単位: m/s^2

measurement.features.acceleration.band0To6000Hz.yAxis.rms

- Y 軸の 0 ~ 6000 Hz の周波数帯域で観測された加速度の二乗平均平方根
- タイプ: 数値
- 単位: m/s^2

measurement.features.acceleration.band0To6000Hz.zAxis.rms

- Y 軸の 0 ~ 6000 Hz の周波数帯域で観測された加速度の二乗平均平方根
- タイプ: 数値
- 単位: m/s^2

measurement.features.acceleration.band10To1000Hz.resultantVector.absMax

- 10 ~ 1000 Hz の周波数帯域で観測された絶対最大加速度
- タイプ: 数値
- 単位: m/s^2

measurement.features.acceleration.band10To1000Hz.resultantVector.absMin

- 10 ~ 1000 Hz の周波数帯域で観測された絶対最小加速度
- タイプ: 数値
- 単位: m/s^2

measurement.features.acceleration.band10To1000Hz.resultantVector.crestFactor

- 10 ~ 1000 Hz の周波数帯域で観測された加速度の波高率
- タイプ: 数値

measurement.features.acceleration.band10To1000Hz.resultantVector.rms

- 10 ~ 1000 Hz の周波数帯域で観測された加速度の二乗平均平方根
- タイプ: 数値
- m/s^2

measurement.features.acceleration.band10To1000Hz.xAxis.rms

- X 軸の 10 ~ 1000 Hz の周波数帯域で観測された加速度の二乗平均平方根
- タイプ: 数値
- m/s^2

measurement.features.acceleration.band10To1000Hz.yAxis.rms

- Y 軸の 10 ~ 1000 Hz の周波数帯域で観測された加速度の二乗平均平方根
- タイプ: 数値
- m/s^2

measurement.features.acceleration.band10To1000Hz.zAxis.rms

- Z 軸の 10 ~ 1000 Hz の周波数帯域で観測された加速度の二乗平均平方根
- タイプ: 数値

- m/s^2

measurement.features.temperature

- 観測された温度
- タイプ: 数値
- °C/摂氏

measurement.features.velocity.band10To1000Hz.resultantVector.absMax

- 10 ~ 1000 Hz の周波数帯域で観測された絶対最大速度
- タイプ: 数値
- mm/秒

measurement.features.velocity.band10To1000Hz.resultantVector.absMin

- 10 ~ 1000 Hz の周波数帯域で観測された絶対最小速度
- タイプ: 数値
- mm/秒

measurement.features.velocity.band10To1000Hz.resultantVector.crestFactor

- 10 ~ 1000 Hz の周波数帯域で観測された速度の波高率
- タイプ: 数値

measurement.features.velocity.band10To1000Hz.resultantVector.rms

- 10 ~ 1000 Hz の周波数帯域で観測された速度の二乗平均平方根
- タイプ: 数値
- mm/秒

measurement.features.velocity.band10To1000Hz.xAxis.rms

- X 軸の 10 ~ 1000 Hz の周波数帯域で観測された速度の二乗平均平方根
- タイプ: 数値
- mm/秒

measurement.features.velocity.band10To1000Hz.yAxis.rms

- Y 軸の 10 ~ 1000 Hz の周波数帯域で観測された速度の二乗平均平方根
- タイプ: 数値
- mm/秒

measurement.features.velocity.band10To1000Hz.zAxis.rms

- Z 軸の 10 ~ 1000 Hz の周波数帯域で観測された速度の二乗平均平方根

- タイプ: 数値
- mm/秒

measurement.sequenceNo

- 測定のシーケンス番号
- タイプ: 数値

models.temperatureML.persistentClassificationOutput

- 機械学習ベースの温度モデルからの永続的な分類出力
- タイプ: 数値
- 有効な値 : `UNKNOWN | HEALTHY | WARNING | ALARM`

models.temperatureML.pointwiseClassificationOutput

- 機械学習ベースの温度モデルからのポイントごとの分類出力
- 型: 文字列
- 有効な値 : `UNKNOWN | INITIALIZING | HEALTHY | WARNING | ALARM`

models.vibrationISO.isoClass

- ISO ベースの振動モデルで使用される ISO 20816 クラス (機械振動の測定と評価に関する規格)
- 型: 文字列
- 有効な値 : `CLASS1 | CLASS2 | CLASS3 | CLASS4 | FAN_BV2`

models.vibrationISO.mutedThreshold

- ISO ベースの振動モデルからの通知をミュートするしきい値
- 型: 文字列
- 有効な値 : `WARNING | ALARM`

models.vibrationISO.persistentClassificationOutput

- ISO ベースの振動モデルからの永続的な分類出力
- 型: 文字列
- 有効な値 : `UNKNOWN | HEALTHY | WARNING | ALARM`

models.vibrationISO.pointwiseClassificationOutput

- ISO ベースの振動モデルからのポイントごとの分類出力
- 型: 文字列
- 有効な値 : `UNKNOWN | HEALTHY | WARNING | ALARM | MUTED_WARNING | MUTED_ALARM`

models.vibrationML.persistentClassificationOutput

- 機械学習ベースの振動モデルからの永続的な分類出力
- 型: 文字列
- 有効な値：UNKNOWN | HEALTHY | WARNING | ALARM

models.vibrationML.pointwiseClassificationOutput

- 機械学習ベースの振動モデルからのポイントごとの分類出力
- 型: 文字列
- 有効な値：UNKNOWN | INITIALIZING | HEALTHY | WARNING | ALARM

assetState.newState

- 測定を処理した後の機械の状態
- 型: 文字列
- 有効な値：UNKNOWN | HEALTHY | NEEDS_MAINTENANCE | WARNING | ALARM

assetState.previousState

- 測定を処理する前の機械の状態
- 型: 文字列
- 有効な値：UNKNOWN | HEALTHY | NEEDS_MAINTENANCE | WARNING | ALARM

Amazon Monitron Kinesis データエクスポート v2

受信した測定データとそれに対応する推論結果を Amazon Monitron からエクスポートして、リアルタイムで分析ができます。データのエクスポートでは、ライブデータが Kinesis にストリーミングされます。

トピック

- Kinesis ストリームへデータをエクスポートする
- ライブデータエクスポート設定を編集する
- ライブデータエクスポートを停止する
- データエクスポートのエラーを表示する
- Kinesis ストリームへのサーバー側の暗号化の使用
- Amazon CloudWatch Logs による のモニタリング
- エクスポートしたデータを Amazon S3 に保存する
- Lambda でデータを処理する

- v2 データエクスポートスキーマを理解する
- Kinesis v1 から v2 への移行

Kinesis ストリームへデータをエクスポートする

1. プロジェクトのメインページの下部、右側にある [ライブデータのエクスポートを開始] を選択します。
2. [Kinesis データストリームの選択] で、次のいずれかの操作を行います。
   - 検索ボックスに既存のストリーム名を入力して、ステップ 5 に進みます。
   - [新しいデータストリームを作成] を選択します。
3. [データストリームの作成] ページの [データストリームの設定] で、データストリーム名を入力します。
4. [データストリーム容量] で、[容量モード] を選択します。
   - データストリームのスループット要件が予測不可能で変動する場合は、[オンデマンド] を選択します。
   - データストリームのスループット要件を確実に見積もることができる場合は、[プロビジョニング済み] を選択してください。次に、[プロビジョニングされたシャード] で、作成するシャード数を入力するか、[シャードの見積もり] を選択します。
5. [データストリームの作成] を選択します。

ライブデータエクスポート設定を編集する

ライブデータエクスポート設定を編集するには、

1. Amazon Monitron コンソールを開きます。
2. ナビゲーションペインで、[プロジェクト] を選択します。
3. プロジェクトが複数ある場合は、エクスポート設定を編集するプロジェクトを選択します。
4. プロジェクトのメインページにある、[ライブデータエクスポート] の [アクション] のドロップダウンメニューから、[ライブデータエクスポート設定の編集] を選択します。

ライブデータエクスポートを停止する

1. Amazon Monitron コンソールを開きます。

2. ナビゲーションペインで、[プロジェクト] を選択します。
3. プロジェクトが複数ある場合は、エクスポート設定を編集するプロジェクトを選択します。
4. プロジェクトのメインページにある、[ライブデータエクスポート] の [アクション] のドロップダウンメニューから [ライブデータのエクスポートを停止] を選択します。
5. ポップアップウィンドウで、[停止] を選択します。

データエクスポートのエラーを表示する

CloudWatch Logs のインターフェイスでエラーメッセージを表示するには、

- Amazon Monitron コンソールで、プロジェクトのメインページにある [ライブデータのエクスポート] から、[CloudWatch ロググループ] を選択します。

Kinesis ストリームへのサーバー側の暗号化の使用

Kinesis データのエクスポートをセットアップする前に、Kinesis ストリームに対してサーバー側の暗号化を有効にできます。ただし、Kinesis データのエクスポートをセットアップした後にサーバー側の暗号化を有効にすると、Amazon Monitron はストリームに公開できなくなります。これは、Amazon Monitron に Kinesis に送信されたデータを暗号化できる kms:GenerateDataKey を呼び出す権限がないためです。

この問題を回避するには、設定を変更せず、??? に記載の指示に従ってください。設定した暗号化をエクスポート設定に関連付けることができます。

Amazon CloudWatch Logs による のモニタリング

Amazon CloudWatch Logs を使用して、Amazon Monitron のライブデータエクスポートをモニタリングできます。測定値のエクスポートに失敗すると、Amazon Monitron は CloudWatch Logs にログイベントを送信します。エラーログにメトリクスフィルタを設定してメトリクスを生成し、アラームを設定することもできます。アラームは特定のしきい値を監視し、これらのしきい値に達したときに通知を送信したりアクションを実行したりできます。詳細については、『CloudWatch ユーザーガイド』を参照してください。

Amazon Monitron は、/aws/monitron/data-export/{HASH_ID} ロググループにログイベントを送信します。

ログイベントには次の JSON 形式があります。

```
{
    "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

- アプリに表示されるアセット名
- タイプ: 文字列

destination

- Kinesis データストリームの ARN
- タイプ: 文字列
- パターン: arn:aws:kinesis:{{REGION}}:{{AWS_ACCOUNT_ID}}:stream/{{STREAM_NAME}}

errorCode

- エラーコード
- 型: 文字列
- 有効な値 : `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

- 詳しいエラーメッセージ
- タイプ: 文字列

eventId

- 各測定値のエクスポートに対応する固有のイベント ID
- タイプ: 文字列

eventType

- 現在のイベントタイプ
- 型: 文字列
- 有効な値: `measurement | gatewayConnected | gatewayDisconnected | sensorConnected | sensorDisconnected | assetStateTransition`

positionName

- アプリに表示されるセンサーの配置名
- タイプ: 文字列

projectName

- アプリとコンソールに表示されるプロジェクト名
- タイプ: 文字列

projectID

- Amazon Monitron プロジェクトに対応する任意のプロジェクト ID
- タイプ: 文字列

sensorID

- 測定値の送信元となるセンサーの物理 ID
- タイプ: 文字列

gatewayID

- Amazon Monitron サービスへのデータ送信に使用されるゲートウェイの物理 ID
- タイプ: 文字列

siteName

- アプリに表示されるサイト名
- タイプ: 文字列

timestamp

- Amazon Monitron サービスが測定値を受信したときのタイムスタンプ (UTC 時間)
- タイプ: 文字列
- パターン: yyyy-mm-dd hh:mm:ss.SSS

エクスポートしたデータを Amazon S3 に保存する

エクスポートしたデータを Amazon S3 に保存する場合は、以下の手順に従います。

トピック

- コンソールで Kinesis を手動で設定する

コンソールで Kinesis を手動で設定する

1. AWS マネジメントコンソールにサインインし、https://https://console.aws.amazon.com/kinesis.https://www.kit で Kinesis コンソールを開きます。
2. ナビゲーションペインで、[配信ストリーム] を選択します。
3. [Create delivery stream (配信ストリームの作成)] を選択します。
4. [ソース] で、[Amazon Kinesis Data Streams] を選択します。
5. [送信先] で、[Amazon S3] を選択します。
6. [ソースの設定] の [Kinesis Data Stream] で、Kinesis データストリームの ARN を入力します。
7. [配信ストリーム名] に、Kinesis データストリーム名を入力します。
8. [送信先の設定] で [Amazon S3 バケット] を選択するか、バケット URI を入力します。
9. (任意) JSON のインライン解析を使用して動的パーティショニングを有効にします。このオプションは、ソース情報とタイムスタンプに基づいて、ストリーミング測定データを分割する場合に適しています。例：

   - [動的パーティショニング] で [有効] を選択します。
   - [改行の区切り文字] で [有効] を選択します。
   - [JSON のインライン解析] で [有効] を選択します。
   - [動的パーティショニングキー] に以下を追加します。

キー名	JQ 式
プロジェクト	.projectName| "project=\(.)"
site	.eventPayload.siteName| "site=\(.)"
時間	.timestamp| sub("[0-9]{2}:[0-9]{2}:[0-9]{2}.[0-9]{3}$"; "00:00:00")| "time=\(.)"

10. [動的パーティショニングキーを適用] を選択し、生成された Amazon S3 バケットプレフィックスが `!{partitionKeyFromQuery:project}/!{partitionKeyFromQuery:site}/!{partitionKeyFromQuery:time}/` であることを確認します。

11. Amazon S3 で、オブジェクトは次のキー形式を使用します: `/project={projectName}/site={siteName}/time={yyyy-mm-dd 00:00:00}/{filename}`
12. [Create delivery stream (配信ストリームの作成)] を選択します。

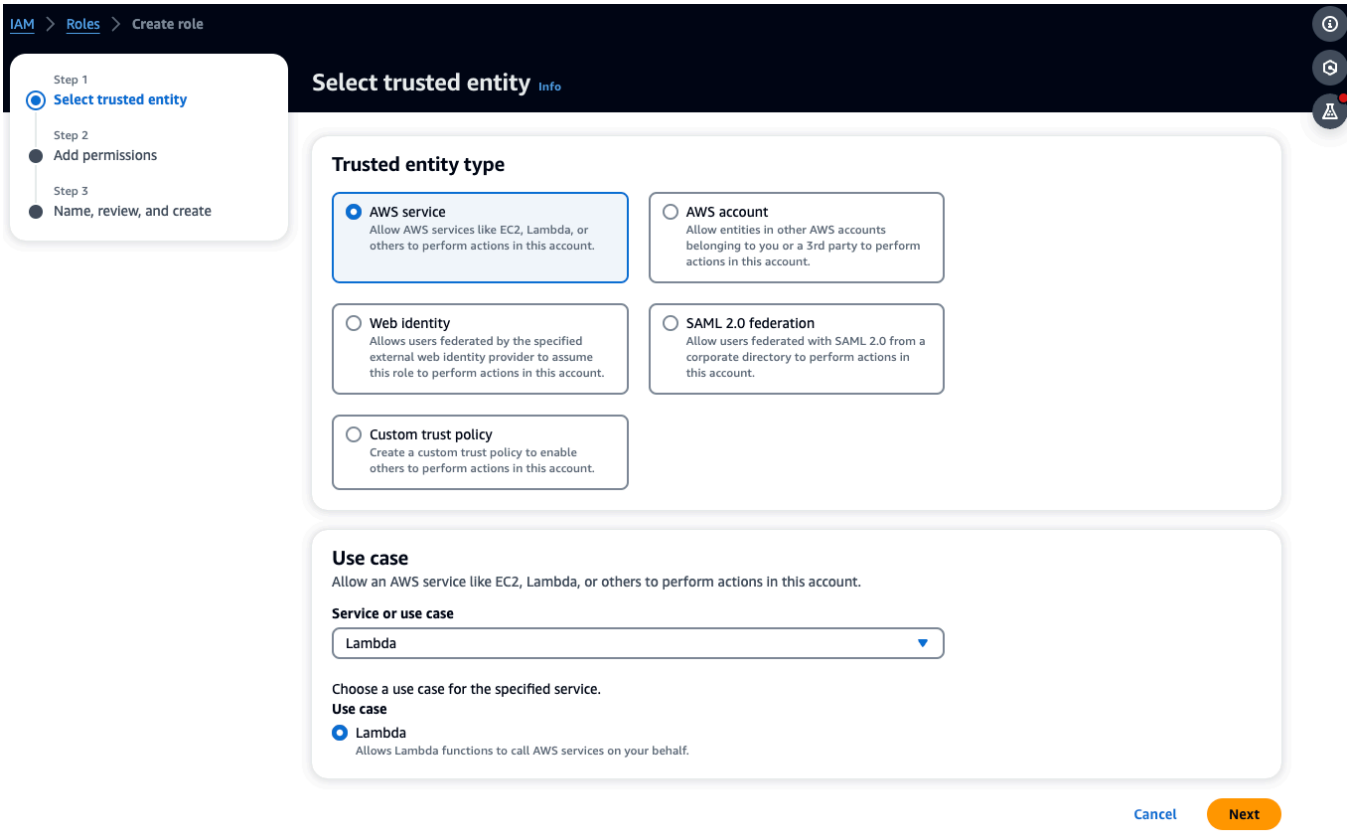
Lambda でデータを処理する

トピック

- ステップ 1: AWS リソースにアクセスするためのアクセス許可を関数に付与する IAM ロールを作成する。
- ステップ 2 : Lambda 関数を作成する
- ステップ 3: Lambda 関数を設定する
- ステップ 4: AWS Lambda コンソールで Kinesis トリガーを有効にする

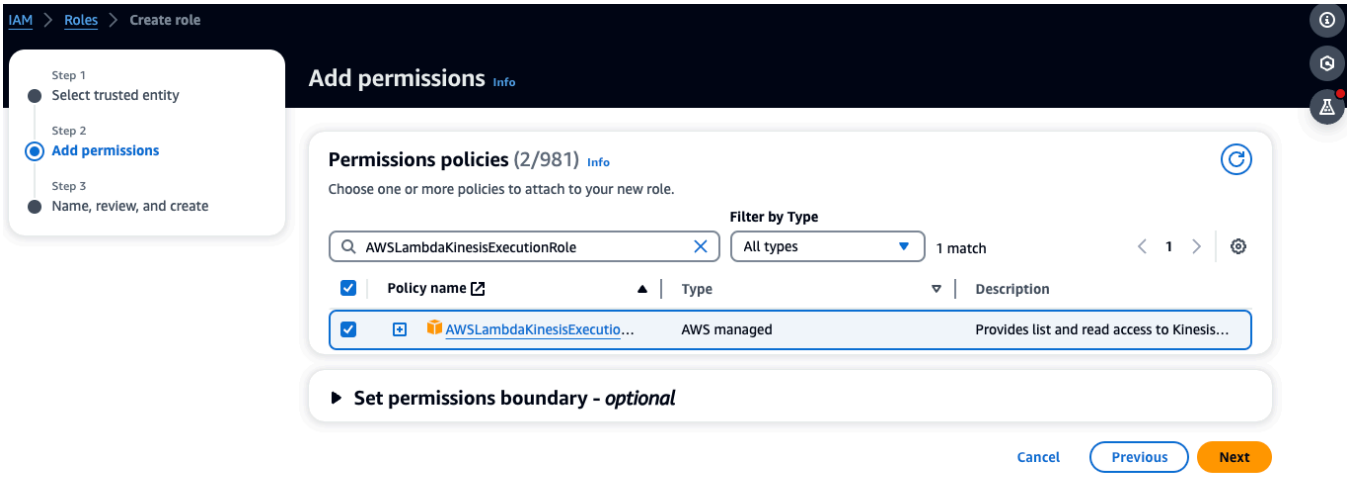
ステップ 1: AWS リソースにアクセスするためのアクセス許可を関数に付与する IAM ロールを作成する。

1. IAM コンソールの [ロールページ] を開きます。
2. [ロールの作成] を選択してください。
3. [信頼されたエンティティを選択] ページで、以下の操作を実行してください :
   - 信頼されたエンティティタイプで、AWS サービスを選択します。
   - ユースケースでは、サービスまたはユースケースで Lambda を選択します。
   - [次へ] を選択します。



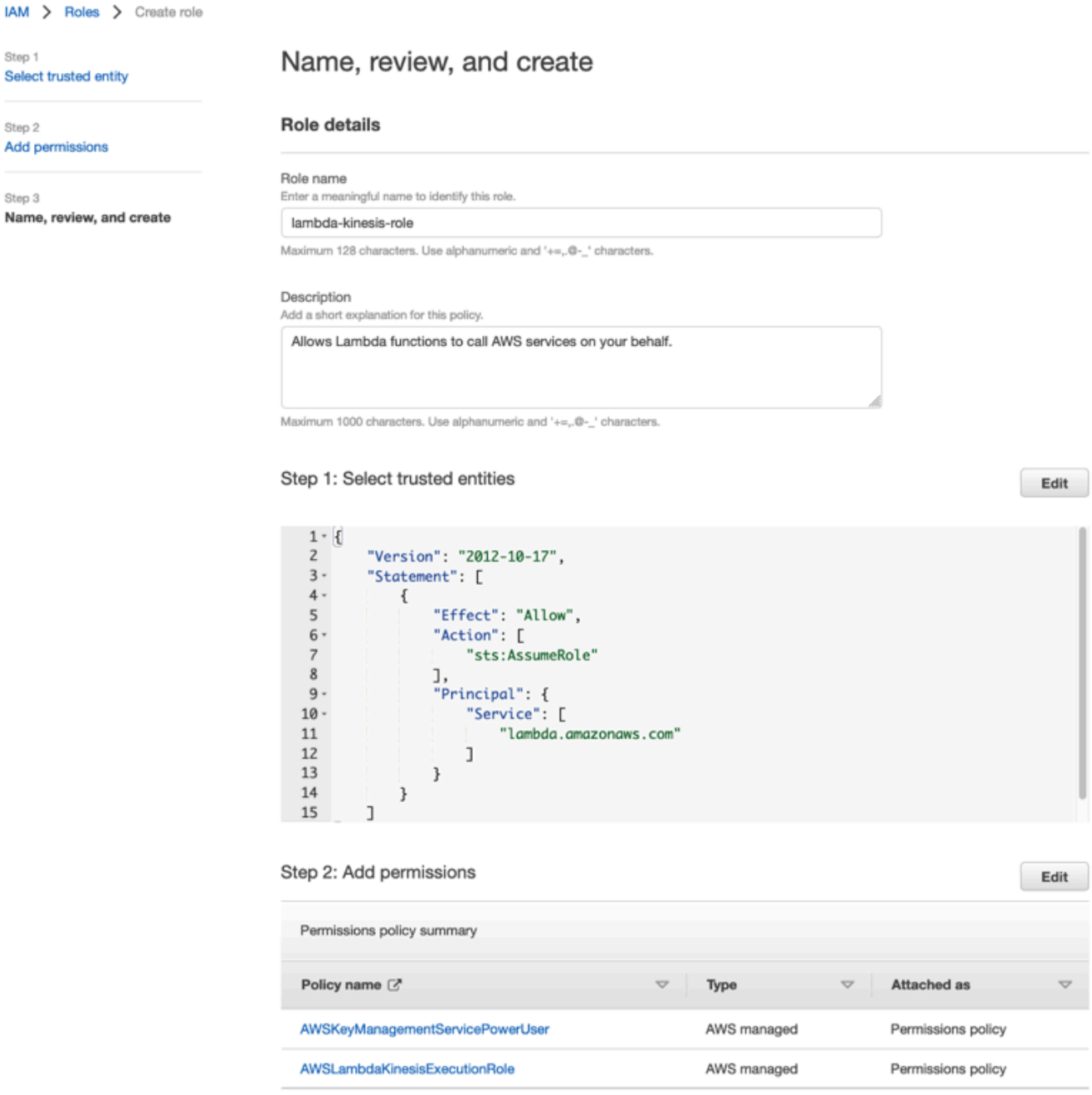
4. アクセス許可の追加ページで、次の操作を行います。

   - アクセス許可ポリシーで、AWSLambdaKinesisExecutionRole (および Kinesis ストリームが暗号化されている場合は AWSKeyManagementServicePowerUser) を選択します。
   - 「アクセス許可の境界をそのまま設定する」を参照してください。
   - [次へ] を選択します。



5. 名前、確認、および作成ページで、次の操作を行います。

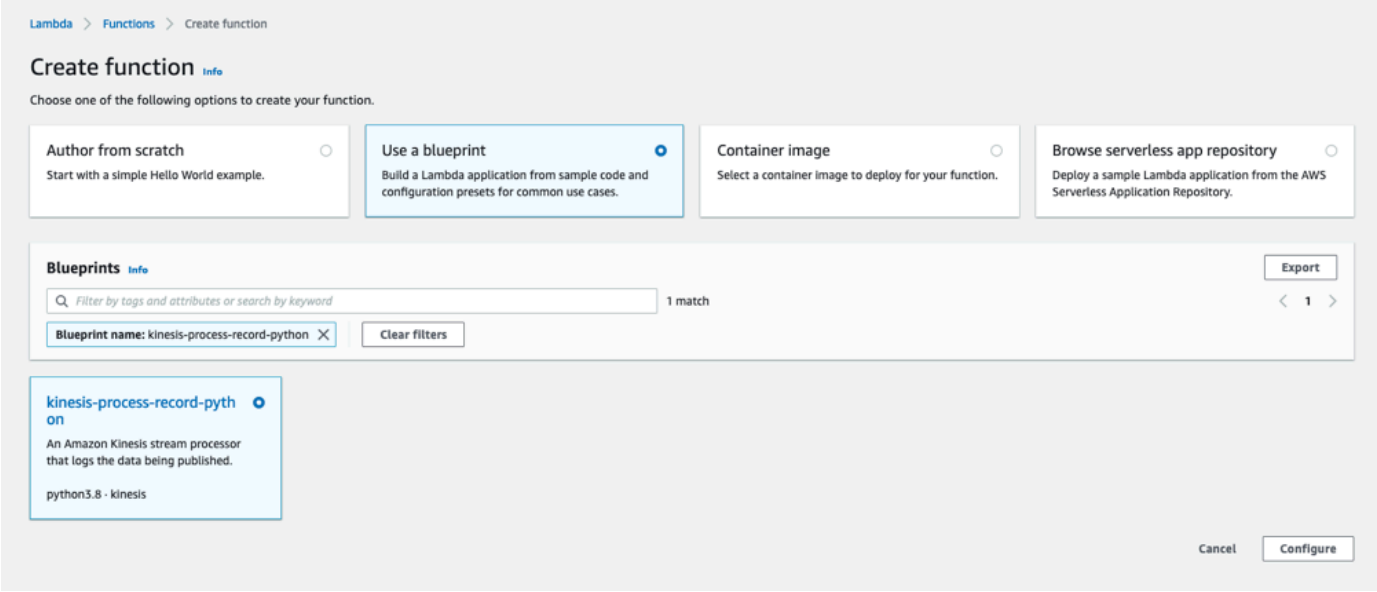
   - ロールの詳細で、ロール名にロールの名前を入力します。例えば、*lambda-kinesis-role* です。オプションの 説明を追加することもできます。
   - ステップ 1: 信頼されたエンティティを選択し、ステップ 2: アクセス許可をそのまま追加するの設定のままにします。ステップ 3: リソースを追跡するためのタグを追加する を選択できます。



6. [Create role] (ロールの作成) を選択します。

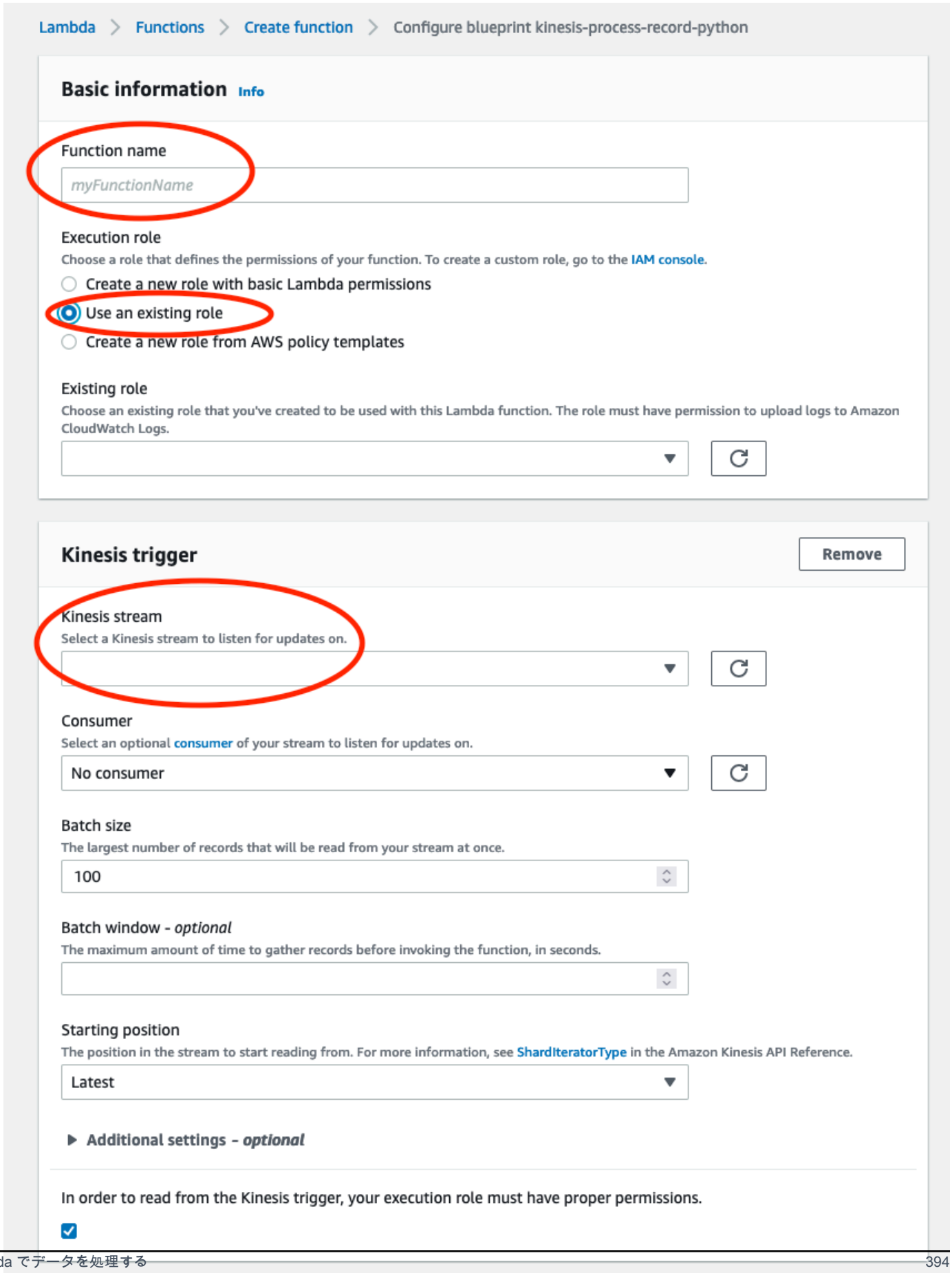
ステップ 2 : Lambda 関数を作成する

1. Lambda コンソールの [関数] ページを開きます。
2. [Create function] (関数の作成) を選択します。
3. [設計図の使用] を選択します。
4. Blueprints の検索ボックスで、kinesis-process-record (nodejs) または kinesis-process-record-python を検索して選択します。
5. [設定] を選択します。



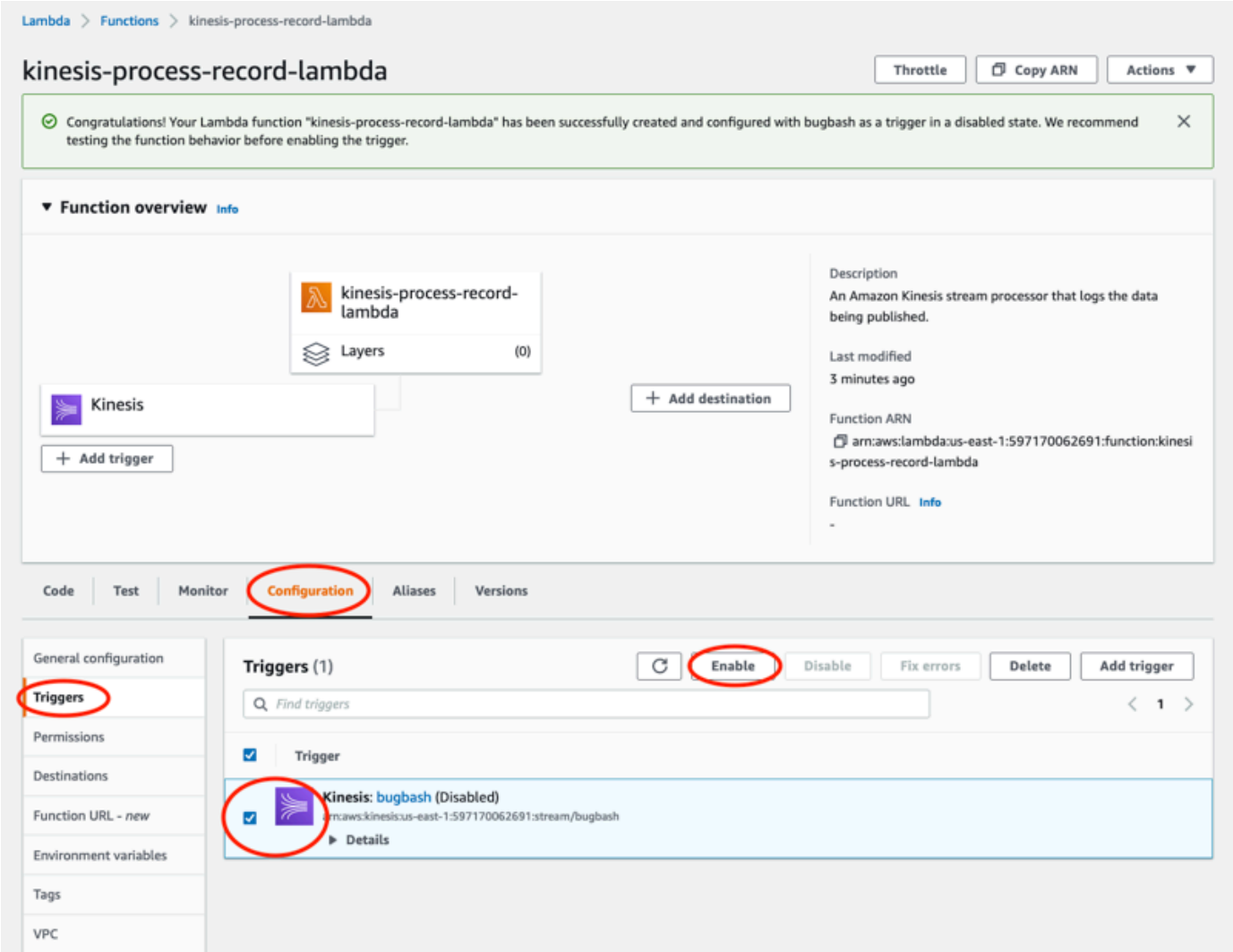
ステップ 3: Lambda 関数を設定する

1. [関数名] を選択します。
2. 最初のステップで作成したロールを [実行ロール] として選択します。
3. Kinesis トリガーを設定します。
   1. Kinesis ストリーミングを選択します。
   2. [関数の作成] を選択します。


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.

ステップ 4: AWS Lambda コンソールで Kinesis トリガーを有効にする

1. [設定] タブで、[トリガー] を選択します。
2. Kinesis ストリーミング名の横にあるボックスにチェックを入れ、[有効] を選択します。



この例で使用されているブループリントは、選択したストリームの口グデータのみを消費します。後で Lambda 関数コードを追加編集して、より複雑なタスクを実行できます。

v2 データエクスポートスキーマを理解する

各測定データ、それに対応する推論結果、ゲートウェイの接続/切断、およびセンサーの接続/切断のイベントは、1 つの Kinesis データストリームレコードとして JSON 形式でエクスポートされます。

トピック

- v2 スキーマ形式
- v2 スキーマパラメータ

v2 スキーマ形式

```
{
    "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 スキーマパラメータ

Amazon Monitron の Kinesis データエクスポートスキーマ v2 には、以下のスキーマパラメータが含まれています。v1 から更新されたパラメータもあれば、v2 に固有のパラメータもあります。例えば、`siteName` は v1 の第 1 レベルのパラメータでしたが、v2 では `eventPayload` エンティティ下の第 2 レベルのパラメータです。

timestamp

- Amazon Monitron サービスが測定値を受信したときのタイムスタンプ (UTC 時間)
- タイプ: 文字列
- パターン: yyyy-mm-dd hh:mm:ss.SSS

eventId

- 各測定値に割り当てられる固有のデータエクスポートイベント ID。受信した Kinesis ストリームレコードを重複排除するのに使用できます。
- タイプ: 文字列

version

- スキーマバージョニング
- タイプ: 文字列
- 値: 1.0 または 2.0

accountId

- Monitron プロジェクトの 12 桁の AWS アカウント ID
- タイプ: 文字列

projectName

アプリとコンソールに表示されるプロジェクト名。

タイプ: 文字列

projectId

Amazon Monitron プロジェクトの一意の ID。

タイプ: 文字列

eventType

- 現在のイベントストリーム。各イベントタイプには専用の `eventPayload` 形式があります。

- タイプ: 文字列
- 使用できる値:
  `measurement`、`gatewayConnected`、`gatewayDisconnected`、`sensorConnected`、`sensorDi`

`eventType: measurement`

eventPayload.features.acceleration.band0To6000Hz.xAxis.rms

- X 軸の 0 ~ 6000 Hz の周波数帯域で観測された加速度の二乗平均平方根
- タイプ: 数値
- 単位: m/s^2

eventPayload.features.acceleration.band0To6000Hz.yAxis.rms

- Y 軸の 0 ~ 6000 Hz の周波数帯域で観測された加速度の二乗平均平方根
- タイプ: 数値
- 単位: m/s^2

eventPayload.features.acceleration.band0To6000Hz.zAxis.rms

- Z 軸の 0 ~ 6000 Hz の周波数帯域で観測された加速度の二乗平均平方根
- タイプ: 数値
- 単位: m/s^2

eventPayload.features.acceleration.band10To1000Hz.resultantVector.absMax

- 10 ~ 1000 Hz の周波数帯域で観測された絶対最大加速度
- タイプ: 数値
- 単位: m/s^2

eventPayload.features.acceleration.band10To1000Hz.resultantVector.absMin

- 10 ~ 1000 Hz の周波数帯域で観測された絶対最小加速度
- タイプ: 数値
- 単位: m/s^2

eventPayload.features.acceleration.band10To1000Hz.resultantVector.crestFactor

- 10 ~ 1000 Hz の周波数帯域で観測された加速度の波高率
- タイプ: 数値

eventPayload.features.acceleration.band10To1000Hz.resultantVector.rms

- 10 ~ 1000 Hz の周波数帯域で観測された加速度の二乗平均平方根

- タイプ: 数値
- m/s^2

eventPayload.features.acceleration.band10To1000Hz.xAxis.rms

- X 軸の 10 ~ 1000 Hz の周波数帯域で観測された加速度の二乗平均平方根
- タイプ: 数値
- m/s^2

eventPayload.features.acceleration.band10To1000Hz.yAxis.rms

- Y 軸の 10 ~ 1000 Hz の周波数帯域で観測された加速度の二乗平均平方根
- タイプ: 数値
- m/s^2

eventPayload.features.acceleration.band10To1000Hz.zAxis.rms

- Z 軸の 10 ~ 1000 Hz の周波数帯域で観測された加速度の二乗平均平方根
- タイプ: 数値
- m/s^2

eventPayload.features.temperature

- 観測された温度
- タイプ: 数値
- °C/摂氏

eventPayload.features.velocity.band10To1000Hz.resultantVector.absMax

- 10 ~ 1000 Hz の周波数帯域で観測された絶対最大速度
- タイプ: 数値
- mm/秒

eventPayload.features.velocity.band10To1000Hz.resultantVector.absMin

- 10 ~ 1000 Hz の周波数帯域で観測された絶対最小速度
- タイプ: 数値
- mm/秒

eventPayload.features.velocity.band10To1000Hz.resultantVector.crestFactor

- 10 ~ 1000 Hz の周波数帯域で観測された速度の波高率
- タイプ: 数値

eventPayload.features.velocity.band10To1000Hz.resultantVector.rms

- 10 ~ 1000 Hz の周波数帯域で観測された速度の二乗平均平方根
- タイプ: 数値
- mm/秒

eventPayload.features.velocity.band10To1000Hz.xAxis.rms

- X 軸の 10 ~ 1000 Hz の周波数帯域で観測された速度の二乗平均平方根
- タイプ: 数値
- mm/秒

eventPayload.features.velocity.band10To1000Hz.yAxis.rms

- Y 軸の 10 ~ 1000 Hz の周波数帯域で観測された速度の二乗平均平方根
- タイプ: 数値
- mm/秒

eventPayload.features.velocity.band10To1000Hz.zAxis.rms

- Z 軸の 10 ~ 1000 Hz の周波数帯域で観測された速度の二乗平均平方根
- タイプ: 数値
- mm/秒

eventPayload.sequenceNo

- 測定のシーケンス番号
- タイプ: 数値

eventPayload.assetPositionId

- 測定値が送信されるセンサー位置の識別子。
- タイプ: 文字列

eventPayload.companyName

- アセットを使用する会社の名前。
- タイプ: 文字列

eventPayload.geoLocation.latitude

- サイトの物理的な場所の緯度。
- タイプ: 数値

eventPayload.geoLocation.longitude

- サイトの物理的な場所の経度。

- タイプ: 数値

eventPayload.address

- サイトのアドレス。
- タイプ: 文字列

eventPayload.serialNumber

- アセットのシリアル番号。
- タイプ: 文字列

eventPayload.make

- アセットのメーカー。
- タイプ: 文字列

eventPayload.model

- アセットのモデル。
- タイプ: 文字列

`eventType: sensorConnected`

siteName

- アプリに表示されるサイト名
- タイプ: 文字列

assetName

- アプリに表示されるアセット名
- タイプ: 文字列

positionName

- アプリに表示されるセンサーの配置名
- タイプ: 文字列

assetPositionURL

- アプリに表示されるセンサー URL
- タイプ: 文字列

physicalID

- 測定値の送信元となるセンサーの物理 ID

- タイプ: 文字列

eventPayload.assetPositionId

- 状態が変更されたセンサー位置の識別子。
- タイプ: 文字列

eventPayload.companyName

- アセットを使用する会社の名前。
- タイプ: 文字列

eventPayload.geoLocation.latitude

- サイトの物理的な場所の緯度。
- タイプ: 数値

eventPayload.geoLocation.longitude

- サイトの物理的な場所の経度。
- タイプ: 数値

eventPayload.address

- サイトのアドレス。
- タイプ: 文字列

eventPayload.serialNumber

- アセットのシリアル番号。
- タイプ: 文字列

eventPayload.make

- アセットのメーカー。
- タイプ: 文字列

eventPayload.model

- アセットのモデル。
- タイプ: 文字列

`eventType: sensorDisconnected`

siteName

- アプリに表示されるサイト名

- タイプ: 文字列

assetName

- アプリに表示されるアセット名
- タイプ: 文字列

positionName

- アプリに表示されるセンサーの配置名
- タイプ: 文字列

assetPositionURL

- アプリに表示されるセンサー URL
- タイプ: 文字列

physicalID

- 測定値の送信元となるセンサーの物理 ID
- タイプ: 文字列

eventPayload.assetPositionId

- 状態が変更されたセンサー位置の識別子。
- タイプ: 文字列

eventPayload.companyName

- アセットを使用する会社名。
- タイプ: 文字列

eventPayload.geoLocation.latitude

- サイトの物理的な場所の緯度。
- タイプ: 数値

eventPayload.geoLocation.longitude

- サイトの物理的な場所の経度。
- タイプ: 数値

eventPayload.address

- サイトのアドレス。
- タイプ: 文字列

eventPayload.serialNumber

- アセットのシリアル番号。

- タイプ: 文字列

eventPayload.make

- アセットのメーカー。
- タイプ: 文字列

eventPayload.model

- アセットのモデル。
- タイプ: 文字列

`eventType: gatewayConnected`

eventPayload.siteName

- アプリに表示されるサイト名
- タイプ: 文字列

eventPayload.gatewayName

- アプリケーションに表示されるゲートウェイ名
- タイプ: 文字列

eventPayload.gatewayListURL

- アプリに表示されるゲートウェイ URL
- タイプ: 文字列

eventPayload.gateway.physicalID

- Amazon Monitron サービスへのデータ送信のために接続したゲートウェイの物理 ID
- タイプ: 文字列

eventPayload.companyName

- アセットを使用する会社名。
- タイプ: 文字列

eventPayload.geoLocation.latitude

- サイトの物理的な場所の緯度。
- タイプ: 数値

eventPayload.geoLocation.longitude

- サイトの物理的な場所の経度。

- タイプ: 数値

eventPayload.address

- サイトのアドレス。
- タイプ: 文字列

eventType: gatewayDisconnected

siteName

- アプリに表示されるサイト名
- タイプ: 文字列

gatewayName

- アプリケーションに表示されるゲートウェイ名
- タイプ: 文字列

gatewayListURL

- アプリに表示されるゲートウェイ URL
- タイプ: 文字列

physicalID

- Amazon Monitron サービスへのデータ送信のために接続したゲートウェイの物理 ID
- タイプ: 文字列

eventPayload.companyName

- アセットを使用する会社名。
- タイプ: 文字列

eventPayload.geoLocation.latitude

- サイトの物理的な場所の緯度。
- タイプ: 数値

eventPayload.geoLocation.longitude

- サイトの物理的な場所の経度。
- タイプ: 数値

eventPayload.address

- サイトのアドレス。

- タイプ: 文字列

eventType: assetStateTransition

eventPayload.siteName

- アプリに表示されるサイト名
- タイプ: 文字列

eventPayload.assetName

- アプリに表示されるアセット名
- タイプ: 文字列

eventPayload.positionName

- アプリに表示されるセンサーの配置名
- タイプ: 文字列

eventPayload.assetPositionURL

- アプリに表示されるセンサー URL
- タイプ: 文字列

eventPayload.sensor.physicalID

- 測定値の送信元となるセンサーの物理 ID
- タイプ: 文字列

eventPayload.assetTransitionType

- アセットの状態遷移の理由
- タイプ: 文字列
- 使用できる値: `measurement` または `userInput`

eventPayload.assetState.newState

- アセットの新しい状態
- タイプ: 文字列

eventPayload.assetState.previousState

- アセットの以前の状態
- タイプ: 文字列

eventPayload.closureCode.failureMode

- この障害を確認するときにユーザーが選択した障害モード

- タイプ: 文字列
- 使用できる値: NO_ISSUE | BLOCKAGE | CAVITATION | CORROSION | DEPOSIT | IMBALANCE | LUBRICATION | MISALIGNMENT | OTHER | RESONANCE | ROTATING_LOOSENESS | STRUCTURAL_LOOSENESS | TRANSMITTED_FAULT | UNDETERMINED

eventPayload.closureCode.failureCause

- 障害を確認するときにユーザーがアプリのドロップダウンで選択した障害の原因。
- タイプ: 文字列
- 使用できる値: ADMINISTRATION | DESIGN | FABRICATION | MAINTENANCE | OPERATION | OTHER | QUALITY | UNDETERMINED | WEAR

eventPayload.closureCode.actionTaken

- アプリのドロップダウンでユーザーが選択した、この異常をクローズするときに実行されるアクション。
- タイプ: 文字列
- 使用できる値: ADJUST | CLEAN | LUBRICATE | MODIFY | NO_ACTION | OTHER | OVERHAUL | REPLACE

eventPayload.closureCode.resolvedModels

- 問題が発生したモデルのセット。
- タイプ: 文字列のリスト
- 使用できる値: vibrationISO | vibrationML | temperatureML

eventPayload.assetPositionId

- 状態が変更されたアセット位置の識別子。
- タイプ: 文字列

models.temperatureML.persistentClassificationOutput

- 機械学習ベースの温度モデルからの永続的な分類出力
- タイプ: 数値
- 有効な値 : UNKNOWN | HEALTHY | WARNING | ALARM

models.temperatureML.pointwiseClassificationOutput

- 機械学習ベースの温度モデルからのポイントごとの分類出力
- 型: 文字列
- 有効な値 : UNKNOWN | INITIALIZING | HEALTHY | WARNING | ALARM

models.vibrationISO.isoClass

- ISO ベースの振動モデルで使用される ISO 20816 クラス (機械振動の測定と評価に関する規格)
- 型: 文字列
- 有効な値 : `CLASS1 | CLASS2 | CLASS3 | CLASS4`

models.vibrationISO.mutedThreshold

- ISO ベースの振動モデルからの通知をミュートするしきい値
- 型: 文字列
- 有効な値 : `WARNING | ALARM`

models.vibrationISO.persistentClassificationOutput

- ISO ベースの振動モデルからの永続的な分類出力
- 型: 文字列
- 有効な値 : `UNKNOWN | HEALTHY | WARNING | ALARM`

models.vibrationISO.pointwiseClassificationOutput

- ISO ベースの振動モデルからのポイントごとの分類出力
- 型: 文字列
- 有効な値 : `UNKNOWN | HEALTHY | WARNING | ALARM | MUTED_WARNING | MUTED_ALARM`

models.vibrationML.persistentClassificationOutput

- 機械学習ベースの振動モデルからの永続的な分類出力
- 型: 文字列
- 有効な値 : `UNKNOWN | HEALTHY | WARNING | ALARM`

models.vibrationML.pointwiseClassificationOutput

- 機械学習ベースの振動モデルからのポイントごとの分類出力
- 型: 文字列
- 有効な値 : `UNKNOWN | INITIALIZING | HEALTHY | WARNING | ALARM`

assetState.newState

- 測定を処理した後の機械の状態
- 型: 文字列
- 有効な値 : `UNKNOWN | HEALTHY | NEEDS_MAINTENANCE | WARNING | ALARM`

assetState.previousState

- 測定を処理する前の機械の状態
- 型: 文字列
- 有効な値：UNKNOWN | HEALTHY | NEEDS_MAINTENANCE | WARNING | ALARM

eventPayload.companyName

- アセットを使用する会社名。
- タイプ: 文字列

eventPayload.geoLocation.latitude

- サイトの物理的な場所の緯度。
- タイプ: 数値

eventPayload.geoLocation.longitude

- サイトの物理的な場所の経度。
- タイプ: 数値

eventPayload.address

- サイトのアドレス。
- タイプ: 文字列

eventPayload.serialNumber

- アセットのシリアル番号。
- タイプ: 文字列

eventPayload.make

- アセットのメーカー。
- タイプ: 文字列

eventPayload.model

- アセットのモデル。
- タイプ: 文字列

Kinesis v1 から v2 への移行

現在 v1 データスキーマを使用している場合は、すでに Amazon S3 へデータを送信しているか、Lambda を使ってデータストリームのペイロードの処理を進めているかもしれません。

トピック

- データスキーマを v2 に更新する
- Lambda を使ってデータ処理を更新する

データスキーマを v2 に更新する

すでに v1 スキーマでデータストリームを設定している場合は、次の手順でデータエクスポートプロセスを更新できます。

1. Amazon Monitron コンソールを開きます。
2. プロジェクトに移動します。
3. 現在のライブデータのエクスポートを停止します。
4. ライブデータエクスポートを開始して、新しいデータストリームを作成します。
5. 新しく作成したデータストリームを選択します。
6. [ライブデータエクスポートを開始] を選択します。この時点で、新しいスキーマによってペイロードがデータストリーム経由で送信されます。
7. (任意) Kinesis コンソールに移動し、古いデータストリームを削除します。
8. v2 スキーマを使用して、新しく作成したデータストリーム用の新しい配信方法を設定します。

これで、新しいストリームで v2 スキーマに準拠したペイロードを新しいバケットに配信できます。バケット内のすべてのデータを処理したい場合に備えて、形式を統一するために 2 つの異なるバケットを使用することをおすすめします。例えば、Athena や などの他の サービスの使用などです AWS Glue。

> **Note**
>
> データを Amazon S3 に配信していた場合、v2 スキーマを使用して Amazon S3 にデータを配信する方法の詳細については、「エクスポートしたデータを Amazon S3 に保存する」で手順をご確認ください。

> **Note**
>
> Lambda 関数を使用してペイロードを処理していた場合は、「Lambda でデータを処理する」で手順をご確認ください。Lambda を使って更新するセクションでは、より詳細な情報が記載されていますので、合わせて参照してください。

Lambda を使ってデータ処理を更新する

Lambda でデータ処理を更新するためには、v2 データストリームがイベントベースになったことを考慮する必要があります。最初の v1 Lambda コードは次のようなコードになっているかもしれません。

```
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
        # ...
```

v1 データスキーマは廃止予定であるため、以前の Lambda コードはすべての新しいデータストリームで機能するわけではありません。

以下の Python サンプルコードでは、データスキーマ v2 を使用して Kinesis ストリームからのイベントを処理します。このコードは、新しい `eventType` パラメーターを使用して、処理を適切なハンドラーに向けます。

```
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
```

コストのモニタリング

Amazon Monitron はAWS、 によって生成されたタグを各センサーに割り当てます。プロジェクトタグとサイトタグです。AWS Cost Explorer を使用する場合は、これらの割り当てられたタグ値を使用して、特定の Amazon Monitron プロジェクトやサイトにフィルタリングされたコストレポートを取得できます。

トピック

- 概念の概要
- 請求タグキーとタグ値
- プロジェクトタグ値の取得
- サイトタグ値の取得
- 請求タグのアクティブ化
- コストレポートを表示する

概念の概要

をセットアップすると Amazon Monitron、 Amazon Monitron リソースを設定してインストールするプロジェクトが作成されます。すべてのプロジェクトは、ミューリプルサイトにリンクすることも、共通の場所または関数に基づいてリンクされたアセット、ゲートウェイ、センサーの整理されたコレクションにリンクすることもできます。

各サイトには、複数のアセットまたはマシンにアタッチされた複数の Amazon Monitron センサーを含めることができ、複数のゲートウェイを介して収集されたアセットデータを送信します。

すべてのサイト、アセット、ゲートウェイ、センサーは 1 つのプロジェクト内に便利に存在しますが、実際には Amazon Monitron セットアップがより分散されている可能性があります。例えば、地理的に異なる場所にあるサイトをモニタリングしたり、さまざまなビジネスユースケースやニーズ別にグループ化したりするために、1 つのプロジェクトを所有している場合があります。または、それぞれに固有の設定を持つ複数のプロジェクトを所有することもできます。統合するパートナーは Amazon Monitron、プロジェクトをそれぞれの顧客に割り当てることもできます。

Amazon Monitron コストを全体的に理解することは役立ちますが、ビジネスに必要なのは、各プロジェクト、場所、またはビジネスユースケースにアタッチされた使用量とコストをより詳細に理解することです。これは、異なる部門間の内部コスト配分の目的にも必要になる場合があります。

このような状況では、AWS Cost Explorer で Amazon Monitron 割り当てられたAWS生成されたタグを使用すると、ビジネスリソースをよりよく理解し、計画するのに役立ちます。

請求タグキーとタグ値

Amazon Monitron はAWS、 によって生成されたタグを使用して、プロジェクトレベルとサイトレベルのタグ値を内部的に割り当てます。これらのタグを使用して、 AWS Cost Explorer コンソールでプロジェクトとサイトを検索できます。タグキーの形式は次のとおりです。

- プロジェクト - `aws:monitron:project`
- サイト – `aws:monitron:location_level4`

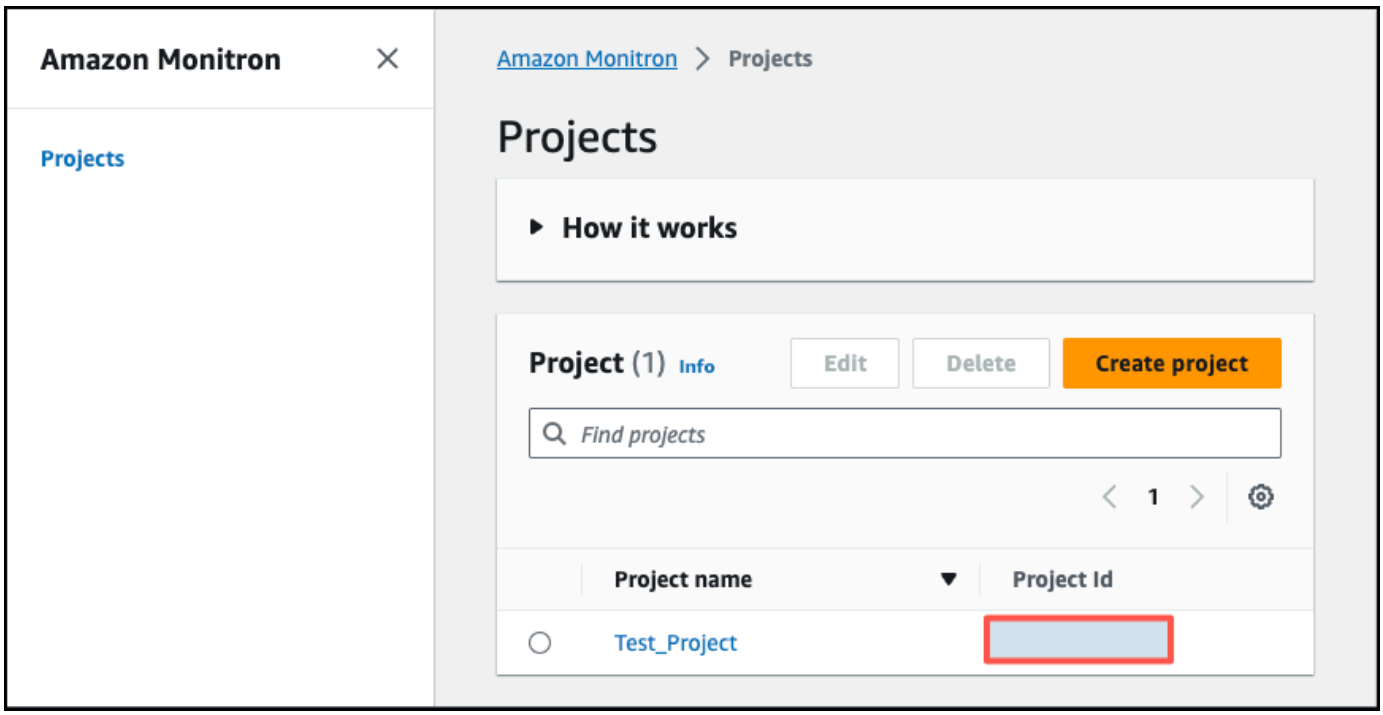
プロジェクトタグ値の取得

割り当てられたプロジェクト値は、 Amazon Monitron ウェブアプリを使用して取得できます。プロジェクトのタグ値はプロジェクト ID です。

プロジェクトに割り当てられた Amazon Monitron 特定のタグ値を取得するには：

1. Amazon Monitron コンソールを https://console.aws.amazon.com/monitron://https://https://https://https://https
2. [プロジェクトの作成] を選択します。
3. ナビゲーションペインで、[プロジェクト] を選択します。

   プロジェクトのリストが [プロジェクト] の下に表示されます。



4. 詳細を取得するプロジェクトを選択します。
5. プロジェクト ID からタグ値をコピーします。

   このプロジェクト ID を使用して、 AWS Cost Explorer コンソールでコストをフィルタリングできます。

サイトタグ値の取得

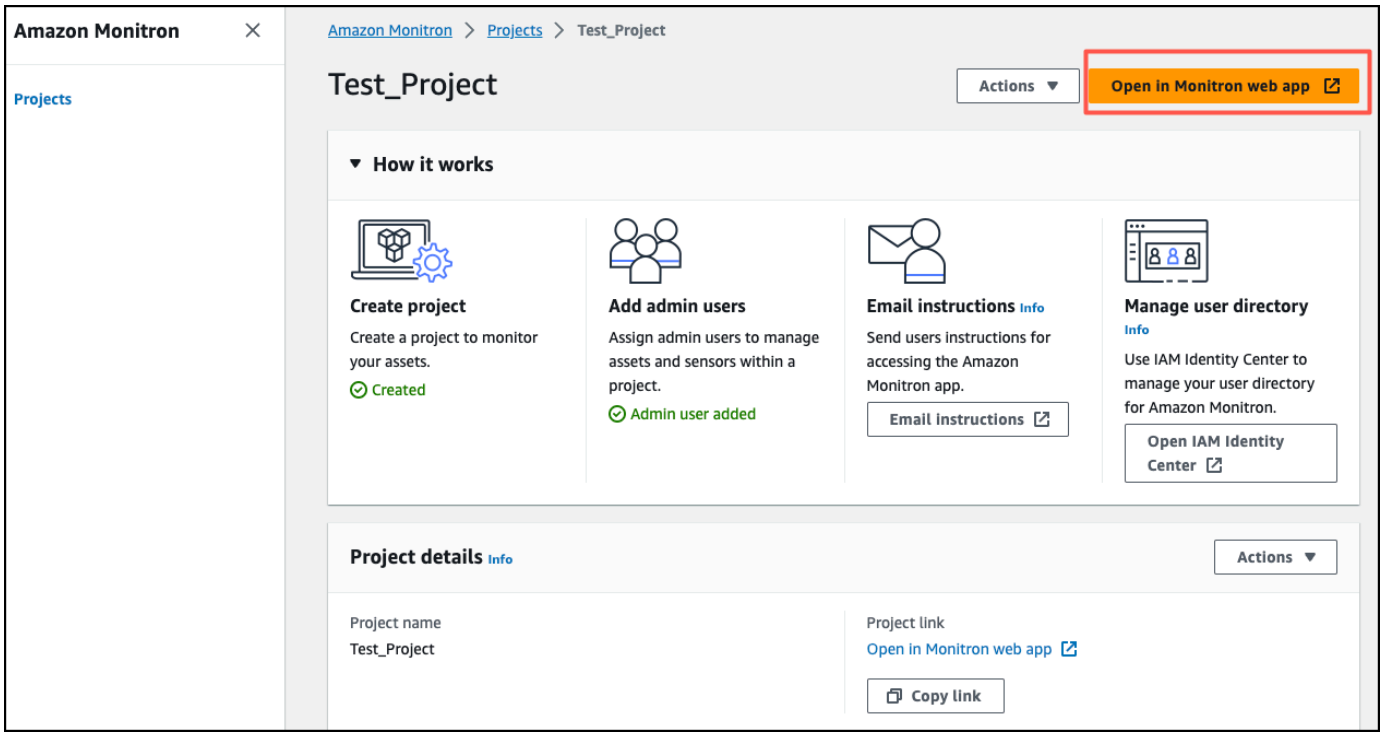
割り当てられたサイトタグ値は、 Amazon Monitron ウェブアプリを使用して取得できます。サイトのタグ値は ID です。

サイトに割り当てられた Amazon Monitron 特定のタグ値を取得するには：

1. Amazon Monitron コンソールを https://console.aws.amazon.com/monitron://www.com で開きます。
2. [プロジェクトを作成] を選択します。
3. プロジェクトを初めて作成する場合は、「プロジェクトの作成」で説明されているステップに従います。

   既存のプロジェクトを選択する場合は、左側のナビゲーションメニューからプロジェクトを選択し、カスタムアセットクラスを作成するプロジェクトを選択します。

4. プロジェクトの詳細ページから、Amazon Monitron ウェブアプリケーションで開くを選択します。



5. 左側のナビゲーションペインから、サイトを選択します。

   サイトのリストが表示されます。

6. 詳細を取得するサイトを選択します。
7. ID からタグ値をコピーします。

   この ID を使用して、 AWS Cost Explorer コンソールでコストをフィルタリングできます。

請求タグのアクティブ化

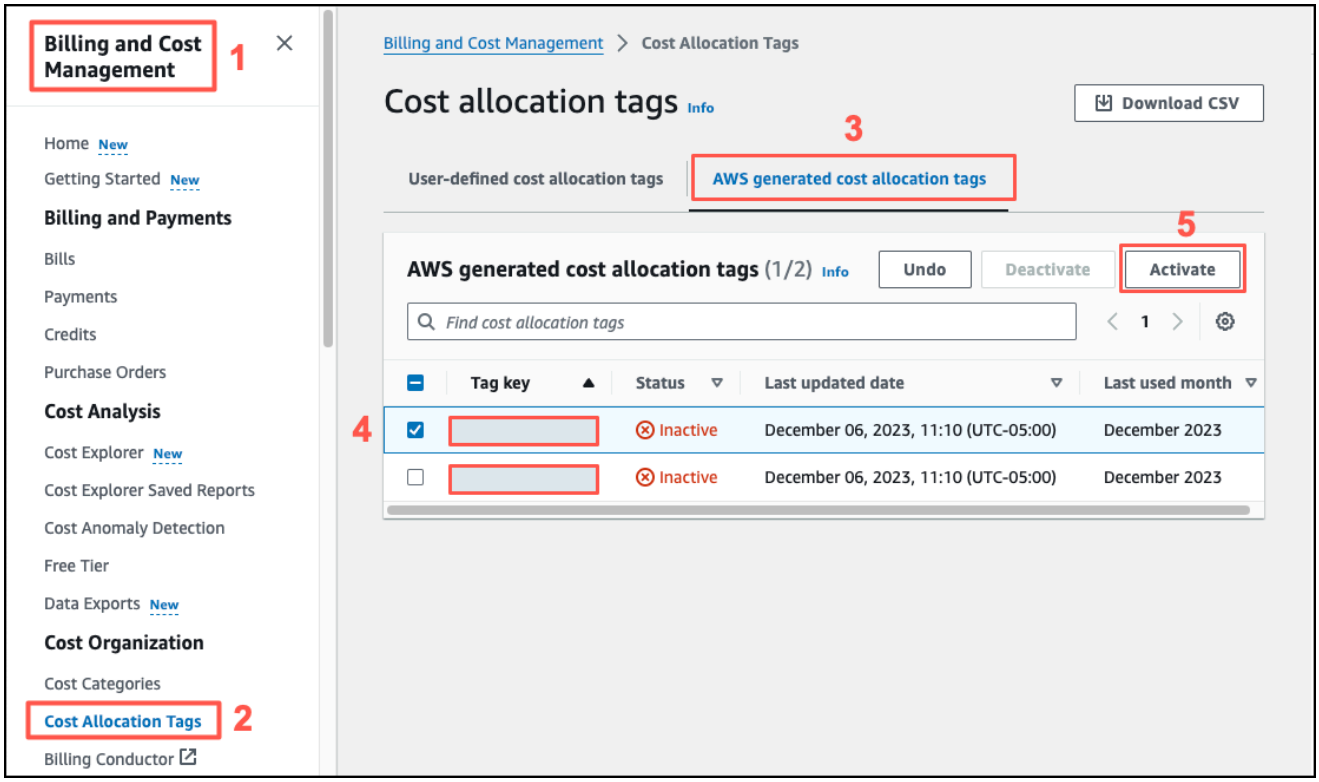
プロジェクトレベルとサイトレベルのコストトラッカータグの使用を開始するには、以下を実行する必要があります。

1. 前提条件 – で AWS Cost Explorer をアクティブ化する必要があります AWS Management Console。これには最小限のセットアップが必要です。AWS コスト管理ガイドで説明されているステップに従うことをお勧めします。
2. AWSが生成したタグを Amazon Monitron 請求アカウントでアクティブ化します。 AWS

   Billing AWS and Cost Management の左側のナビゲーションペインから、次の操作を行います。

   a. Cost Organization から、コスト配分タグを選択します。AWS 生成されたコスト配分タグは、このセクションにあります。

   b. 使用するタグを選択し、アクティブ化を選択します。



> **Note**
>
> タグがアクティブ化されるまでに最大 96 時間かかります。請求データは、タグがアクティブになった後にのみタグ付けが開始されます。

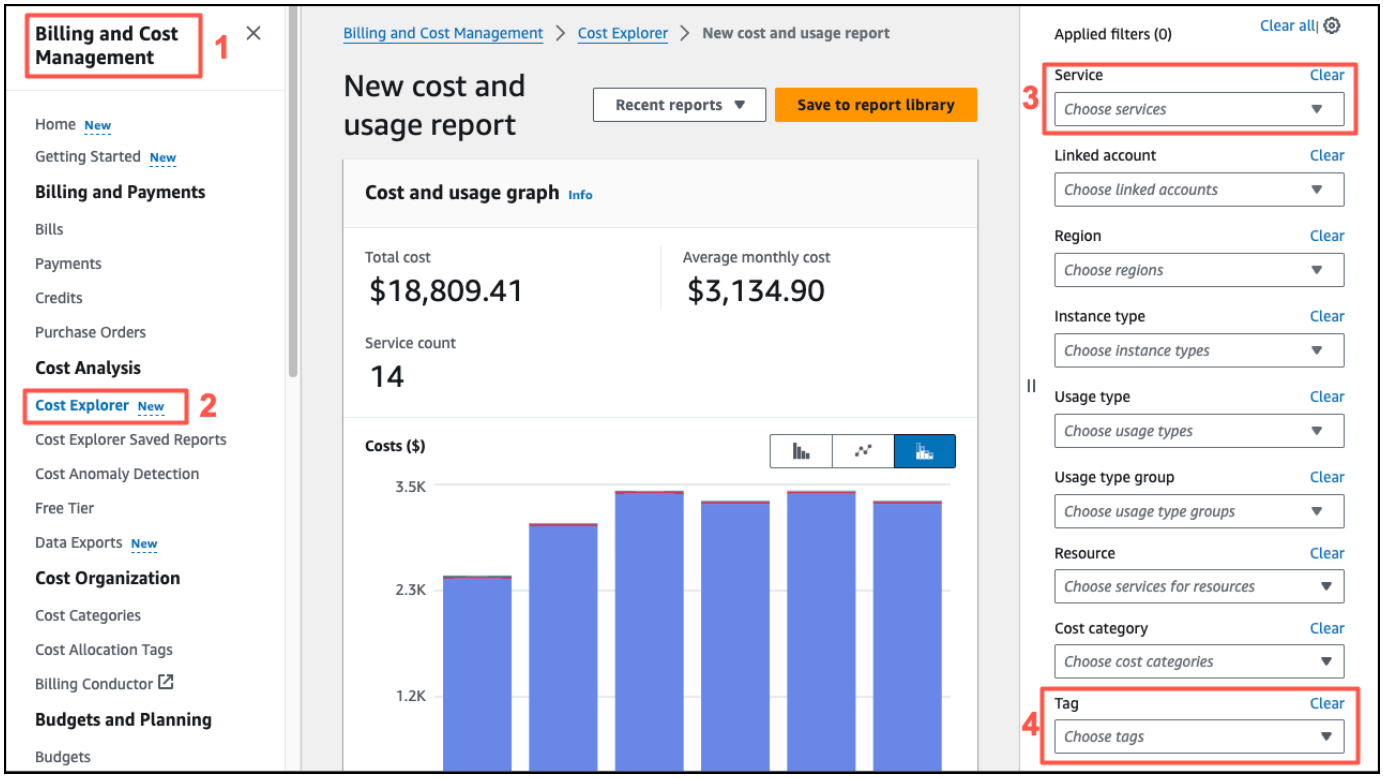
コストレポートを表示する

Amazon Monitron AWS 生成されたタグがアクティブ化され、アクティブになったら、コスト管理コンソールの AWS Cost Explorer を使用して、これらのタグでフィルタリングされた使用状況レポートと AWS コストレポートを表示できます。

タグキーと値のペアを選択することで、使用状況とコスト履歴をフィルタリングできます。たとえば、特定のプロジェクトの使用レポートを表示する場合は、まずタグ値を選択しaws:monitron:project、次に使用可能なオプションからプロジェクト ID 値を選択します。

コストと使用状況レポートを生成するには

1. 「https://https://console.aws.amazon.com/costmanagement.com で AWS コスト管理コンソールを開きます。
2. 左側のナビゲーションペインから、Cost Explorer を選択します。
3. 新しいコストと使用状況レポートページから、右側のナビゲーションメニューからフィルターで、 をサービス Amazon Monitron として選択します。
4. 右側のナビゲーションメニューから、タグ で、ドロップダウンオプションからプロジェクトまたはサイトに割り当てられたタグキーを選択します。
5. 次に、プロジェクトまたはサイトに割り当てられた Amazon Monitron タグ値を選択します。



> **Note**
>
> レポートライブラリに選択したフィルターを使用してレポートを保存し、後で簡単に確認できます。レポートの日付範囲や詳細度など、レポートをさらに調整およびカスタマイズすることもできます。

アプリ設定

このセクションでは、 Amazon Monitron アプリとコンソールの設定を変更する方法について説明します。

トピック

- ローカリゼーション設定

ローカリゼーション設定

Amazon Monitron アプリは、ウェブブラウザまたは電話からデバイスの場所を検出し、この情報を使用してアプリのデフォルト設定を入力します。のデフォルト設定 Amazon Monitron には、言語、日付/時刻形式、数値形式 (カンマと小数点) が含まれます。

現在 でサポートされている言語 Amazon Monitron は次のとおりです。

- 英語
- フランス語
- スペイン語
- ポルトガル語 (BR)

アプリケーションでサポートされている言語はすべて、コンソールでもサポートされています。

特定のエリアで言語を使用できない場合、 Amazon Monitron アプリはデフォルトで英語、および米国の単位/数値形式になります。アプリは現在地を一度検出し、その後は手動で変更するまでこれらのデフォルト値を使用します。

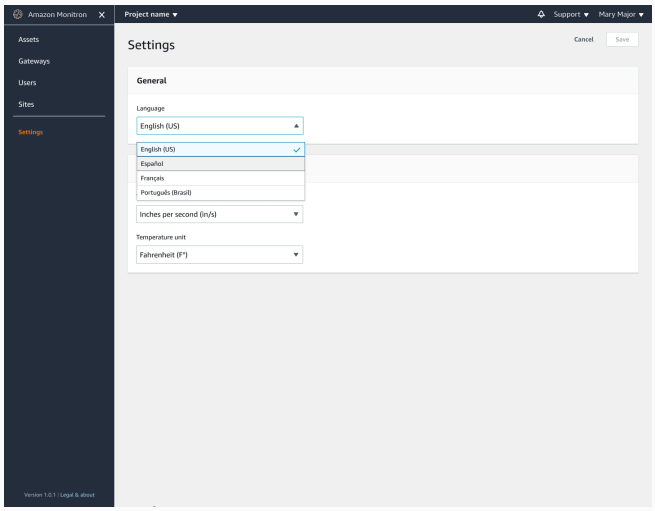
ローカリゼーション設定の変更

ウェブアプリとモバイルアプリの両方、および コンソールの Amazon Monitron 言語設定を変更できます。

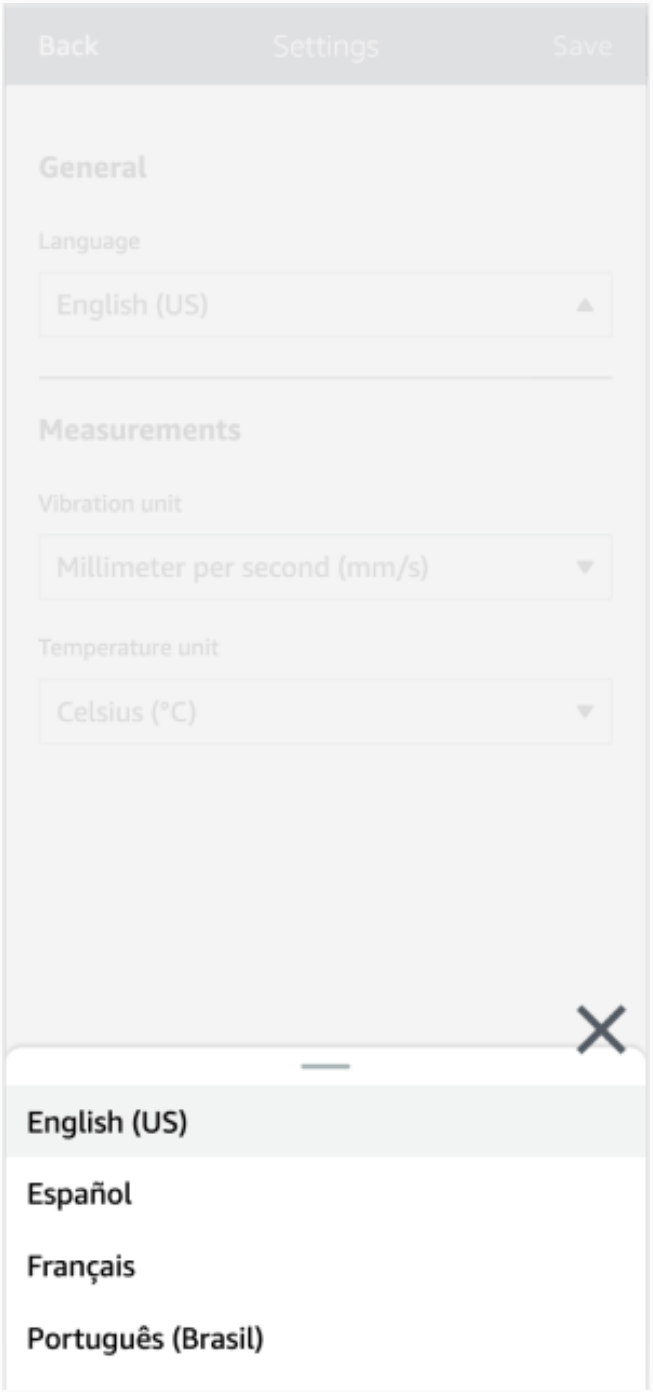
ローカリゼーション設定を変更するには

1. アプリの [設定] メニューで、言語、測定値、温度の設定を更新して保存します。

> **Important**
>
> 言語や単位のへの設定変更はローカルでブラウザに保存され、同じブラウザで開いたすべてのプロジェクトに適用されます。これらの変更はデバイス間で共有されません。

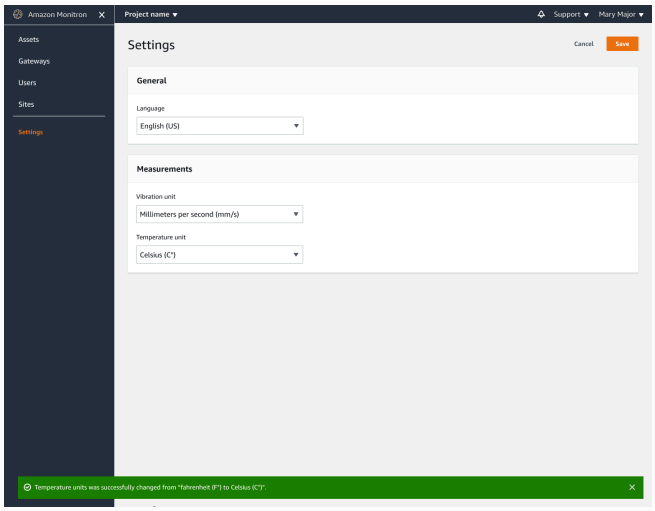


ウェブアプリビュー

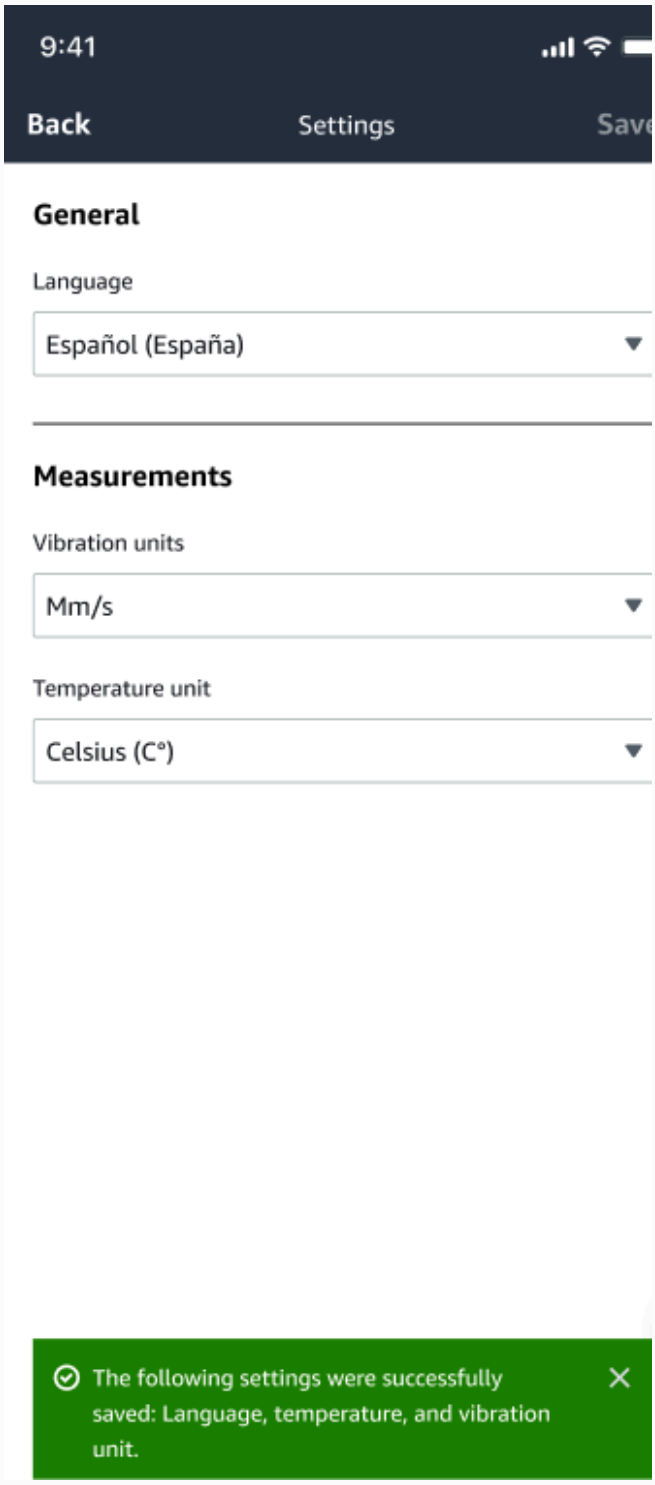


モバイルアプリビュー

2. [保存] を選択します。
3. 2 つ以上の設定を変更すると、次の警告バナーが表示されます。

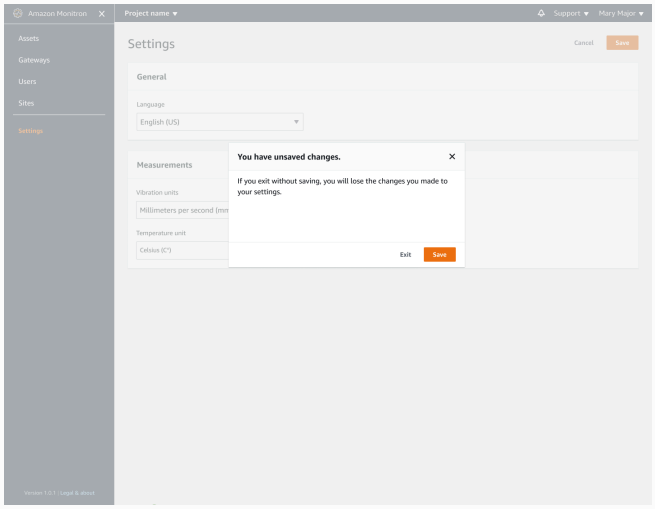


ウェブアプリビュー

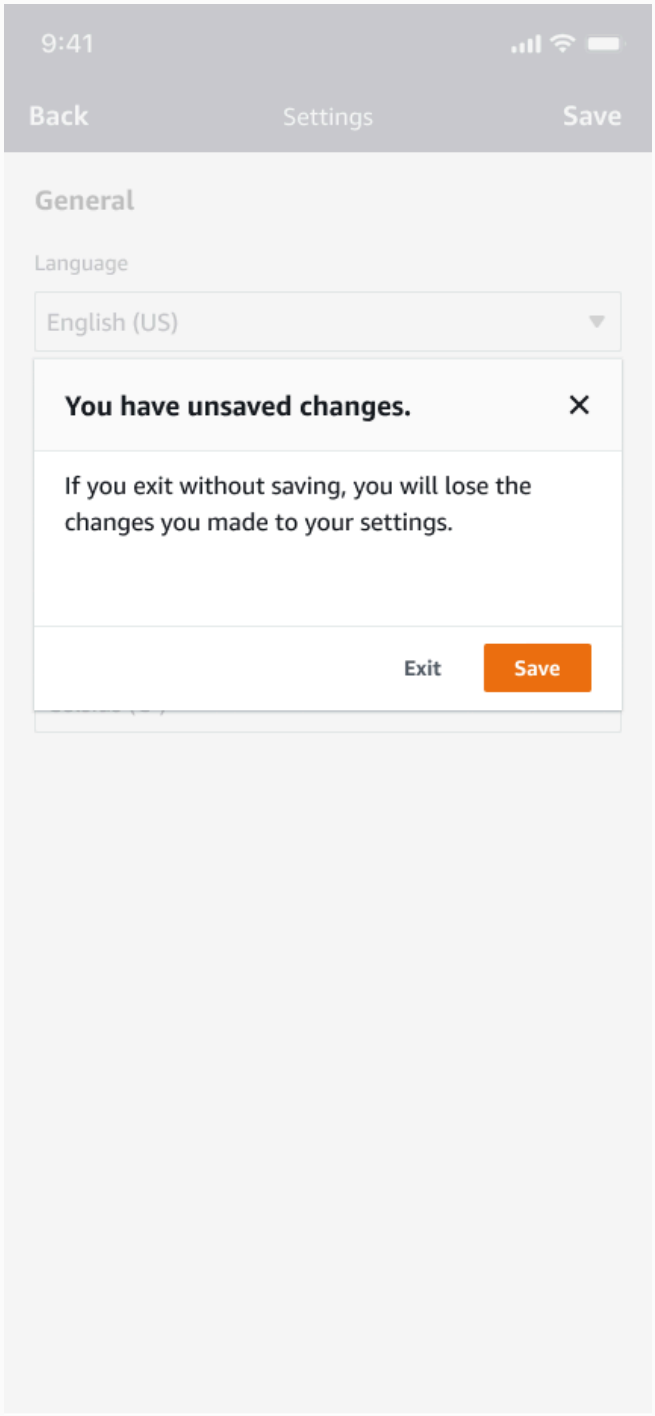


モバイルアプリビュー

4. 保存せずに設定メニューを終了すると、次の警告が表示されます。



ウェブアプリビュー



モバイルアプリビュー

AWS CloudTrailを使用した Amazon Monitron アクションのログ記録

Amazon Monitron は AWS CloudTrail、Amazon Monitron のユーザー、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail は、Amazon Monitron の API コールをイベントとしてキャプチャします。CloudTrail は、Amazon Monitron コンソールと Amazon Monitron モバイルアプリの両方からの呼び出しをキャプチャします。証跡を作成すると、Amazon Monitron に関するイベントを含めた CloudTrail のイベントの Amazon Simple Storage Service (Amazon S3) バケットへの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail が収集した情報を使用することで、Amazon Monitron に対して行われたコンソールないしモバイルアプリのリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエストが行われた日時、および追加の詳細を確認できます。

設定や有効化の方法など、CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

トピック

- CloudTrail 内の Amazon Monitron 情報
- 例: Amazon Monitron ログファイルのエントリ

CloudTrail 内の Amazon Monitron 情報

CloudTrail は、アカウントの作成時に AWS ユーザーに対して有効になります。Amazon Monitron でサポートされているイベントアクティビティが発生すると、そのアクティビティは CloudTrail イベントとイベント履歴の他の AWS サービスイベントに記録されます。 AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「CloudTrailイベント履歴でのイベントの表示」を参照してください。

Amazon Monitron のイベントなど、 AWS アカウントのイベントの継続的な記録については、証跡を作成します。追跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成すると、証跡はすべての AWS リージョンに適用されます。証跡は、 AWS パーティションのすべてのリージョンからのイベントを ログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをさらに分析して処理するように、他の AWS サービスを設定できます。詳細については、次を参照してください:

- 証跡の作成のための概要
- CloudTrail がサポートするサービスと統合
- CloudTrail 用 Amazon SNS 通知の構成
- 「複数のリージョンからCloudTrail口グファイルを受け取る」および「複数のアカウントからCloudTrail口グファイルを受け取る」

Amazon Monitron は、多数のアクションをイベントとして口グ記録することをサポートしています。オペレーションは AWS コンソールまたは Amazon Monitron モバイルアプリからパブリックにアクセスできますが、APIs自体はパブリックではなく、変更される可能性があります。これらは口グ記録のみを目的としており、これらを使ってアプリケーションを構築すべきではありません。

Amazon Monitron は、CloudTrail 口グファイルのイベントとして以下のアクションをサポートします。

- 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

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。これには、リクエストを行った IAM アイデンティティのタイプと、どの認証情報が使用されたかに関する詳細が含まれます。一時的認証情報が使用された場合、エレメントは、認証情報がどのように取得されたかを示します。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか
- リクエストが、ロールとフェデレーティッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか
- リクエストが別の AWS サービスによって行われたかどうか

詳細については、AWS CloudTrail ユーザーガイドの「CloudTrail userIdentity エレメント」を参照してください。

例: Amazon Monitron ログファイルのエントリ

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。CloudTrail ログファイルは、パブリック API 呼び出しの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、プロジェクト削除 (`DeleteProject`) アクションの CloudTrail ログエントリです。

トピック

- DeleteProject アクション成功
- DeleteProject アクション失敗 (認可エラー)
- DeleteProject アクション失敗 (競合の例外エラー)

DeleteProject アクション成功

次の例は、DeleteProject アクション成功時に CloudTrail ログに表示される内容を示しています。

```
{
  "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"
}
```

DeleteProject アクション失敗 (認可エラー)

次の例は、エラーが発生して DeleteProject アクションが失敗した後に CloudTrail ログに表示される内容を示しています。この場合のエラーは認可エラーで、ユーザーには指定されたプロジェクトを削除する権限がありません。

```
{
    "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"
}
```

DeleteProject アクション失敗 (競合の例外エラー)

次の例は、エラーが発生して DeleteProject アクションが失敗した後に CloudTrail ログに表示される内容を示しています。この場合のエラーは競合の例外で、Amazon Monitron がプロジェクトを削除しようとしてもセンサーが残っているというものです。

```
{
  "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"
}
```

Amazon Monitron のセキュリティ

でのクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティの影響を受けやすい組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – クラウドで AWS AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。 AWS また、 では、安全に使用できるサービスも提供しています。サードパーティーの監査者は、AWS コンプライアンスプログラムコンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。Amazon Monitron に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウド内のセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、 お客様のデータの機密性、企業の要件、および適用可能な法律や規制といった他の要因 についても責任を担います。

このドキュメントは、Amazon Monitron 使用時における責任共有モデルの適用法を理解するのに役立ちます。以下のトピックでは、セキュリティとコンプライアンスの目標を達成するように Amazon Monitron を設定する方法について説明します。また、Amazon Monitron リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- Amazon Monitron でのデータ保護
- Amazon Monitron のための Identity and Access Management
- Amazon Monitron でログ記録とモニタリングを実行する
- Amazon Monitron のコンプライアンス検証
- Amazon Monitron のインフラストラクチャセキュリティ
- Amazon Monitron のセキュリティベストプラクティス

Amazon Monitron でのデータ保護

Amazon Monitron は、 AWS 責任共有モデル。 には、データ保護に関する規制とガイドラインが含まれています。 AWS は、すべての AWS サービスを実行するグローバルインフラストラクチャを保護する責任があります。 は、このインフラストラクチャでホストされるデータの制御 AWS を維持します。 これには、お客様のコンテンツと個人データを処理するためのセキュリティ設定コントロールが含まれます。 AWS のお客様と APN パートナー、 データコントローラーまたはデータ処理者として動作する は、 AWS クラウドに保存した個人データに対して責任を負います。

データ保護の目的で、 AWS アカウントの認証情報を保護し、 AWS Identity and Access Management (IAM) を使用して個々のユーザーをセットアップして、各ユーザーに職務を果たすために必要なアクセス許可のみを付与することをお勧めします。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- TLS (Transport Layer Security) を使用して AWS リソースと通信します。

- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 AWS サービス内のすべてのデフォルトのセキュリティコントロールを使用します。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これにより、Amazon S3 に保存される個人データの検出と保護が支援されます。

顧客のアカウント番号などの機密の識別情報は、[名前] フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これは、コンソール、API、 AWS CLIまたは SDK を使用して Amazon Monitron または他の AWS サービスを使用する場合も同様です。 AWS SDKs Amazon Monitron や他のサービスに入力したすべてのデータは、診断ログに取り込まれる可能性があります。外部サーバーへの URL を指定するときは、そのサーバーへのリクエストを検証するための認証情報を URL に含めないでください。

データ保護の詳細については、AWS セキュリティブログ のブログ投稿「AWS の責任共有モデルと GDPR」を参照してください。

トピック

- 保管中のデータ
- 転送中のデータ

- AWS KMS Amazon Monitron での および データ暗号化

保管中のデータ

クラウドに保存されているデータは、 AWS Key Management Service (AWS KMS) を介した 2 種類のキータイプのいずれかを使用して暗号化されます。データは AWS 所有のキーを使用して、Amazon Simple Storage Service (Amazon S3) に暗号化されます。Amazon Monitron は Amazon DynamoDB のテーブルにもデータを格納します。デフォルトでは、これらは AWS 所有の CMK を使用して暗号化されます。ただし、プロジェクトの設定時にお客様が[カスタム暗号化設定]を選択した場合、Amazon Monitron はカスタマー管理の CMK を使用します。

「???」も参照してください。

転送中のデータ

Amazon Monitron は TLS (Transport Layer Security) を使用して、センサーと Amazon Monitron 間で転送されるデータを暗号化します。

AWS KMS Amazon Monitron での および データ暗号化

Amazon Monitron は、 AWS Key Management Service () を通じて 2 種類のキーのいずれかを使用してデータとプロジェクト情報を暗号化しますAWS KMS。次のいずれかを選択できます。

- AWS 所有のキー。これはデフォルトの暗号化キーであり、プロジェクトの設定時に[カスタム暗号化設定]を選択しなかった場合に使用されます。
- カスタマーマネージド CMK。 AWS アカウントの既存のキーを使用するか、 AWS KMS コンソールまたは API を使用してキーを作成できます。既存のキーを使用している場合は、 AWS KMS キーの選択を選択し、キーのリストから AWS KMS キーを選択するか、別のキーの Amazon リソースネーム (ARN) を入力します。新しいキーを作成する場合は、 AWS KMS キーの作成を選択します。詳細については、AWS Key Management Service デベロッパーガイドのキーの作成を参照してください。

AWS KMS を使用してデータを暗号化する場合は、次の点に注意してください。

- Amazon S3 および Amazon DynamoDB のクラウドに保存されているデータは暗号化されます。
- AWS 所有の CMK を使用してデータを暗号化する場合、Amazon Monitron はお客様ごとに個別の CMK を使用します。

- IAM ユーザーには、Amazon Monitron に接続された AWS KMS API オペレーションを呼び出すために必要なアクセス許可が必要です。Amazon Monitron のマネージドポリシーには、コンソールを使用するための以下のアクセス権限が含まれています。

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

  詳細については、デベロッパーガイド AWS KMS の「AWS Key Management Service IAM ポリシーの使用」を参照してください。

- CMK を削除または無効化すると、データにアクセスできなくなります。詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS keysを削除する」を参照してください。

Amazon Monitron のための Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインインを許可) し、誰に Amazon Monitron リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- Amazon Monitron で IAM を使用する方法
- Amazon Monitron のサービスリンクロールの使用

対象者

AWS Identity and Access Management (IAM) の使用方法は、Amazon Monitron で行う作業によって異なります。

サービスユーザー – ジョブを実行するために Amazon Monitron サービスを使用する場合は、管理者から必要なアクセス許可と認証情報が与えられます。さらに多くの Amazon Monitron 機能を使用して作業を行うには、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。Amazon Monitron の機能にアクセスできない場合は、「Amazon Monitron のアイデンティティとアクセスのトラブルシューティング」を参照してください。

サービス管理者 - 社内の Amazon Monitron リソースを担当している場合は、通常、Amazon Monitron へのフルアクセスがあります。サービスのユーザーがどの Amazon Monitron 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社で Amazon Monitron と IAM を併用する方法の詳細については、「Amazon Monitron で IAM を使用する方法」を参照してください。

IAM 管理者 - 管理者は、Amazon Monitron へのアクセス権を管理するポリシーの作成方法について、詳細を確認する場合があります。IAM で使用可能な Amazon Monitron アイデンティティベースのポリシーの例を確認するには、「Amazon Monitron のアイデンティティベースポリシーの例」を参照してください。

アイデンティティを使用した認証

認証は、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けることによって、認証 (にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 AWS サインイン ユーザーガイド」の「 へのサインイン方法 AWS アカウント」を参照してください。

AWS プログラムで にアクセスする場合、 は、ソフトウェア開発キット (SDK) とコマンドライン インターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストを暗号化して署名します。AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 では、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させる AWS ことをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」を参照してください。

トピック

- AWS アカウント ルートユーザー
- IAM ユーザーとグループ
- IAM ロール

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウントのすべての AWS のサービス およびリソースへの完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、IAM ユーザーガイドの「ルートユーザー認証情報が必要なタスク」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内の ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できま

す。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内の ID です。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

- クロスサービスアクセス — 一部の は他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする を使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、IAM ユーザーガイドの JSON ポリシー概要を参照してください。

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

トピック

- アイデンティティベースのポリシー
- その他のポリシータイプ
- 複数のポリシータイプ

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロン

ポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

その他のポリシータイプ

AWS は、一般的でない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所有する複数の をグループ化して一元管理するためのサービス AWS アカウント です。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。
- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースに対するアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID に対する有効なアクセス許可に影響を与える可能性があります。RCP AWS のサービス をサポートする のリストを含む Organizations と RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS Organizations
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もありま

す。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。が複数のポリシータイプが関係する場合にリクエストを許可するかどうか AWS を決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

Amazon Monitron で IAM を使用する方法

IAM を使用して Amazon Monitron へのアクセスを管理する前に、Amazon Monitron で使用できる IAM 機能について理解しておく必要があります。Amazon Monitron およびその他の AWS のサービスが IAM と連携する方法の概要を把握するには、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

トピック

- Amazon Monitron アイデンティティベースのポリシー
- Amazon Monitron リソースベースのポリシー
- Amazon Monitron タグに基づく認可
- Amazon Monitron の IAM ロール
- Amazon Monitron のアイデンティティベースポリシーの例
- Amazon Monitron のアイデンティティとアクセスのトラブルシューティング

Amazon Monitron アイデンティティベースのポリシー

IAM のアイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションが許可または拒否される条件を指定できます。Amazon Monitron は、特定のアクション、リソース、および条件キーをサポートしています。JSON ポリシーで使用するすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素のリファレンス」を参照してください。

トピック

- アクション
- リソース

- 条件キー
- 例

アクション

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

Amazon Monitron のポリシーアクションは、アクションの前にプレフィックス `monitron:` を使用します。例えば、Amazon Monitron `CreateProject` オペレーションを使用してプロジェクトを作成するアクセス許可を付与するには、ポリシーに `monitron:CreateProject` アクションを含めます。ポリシーステートメントには`Action` または `NotAction` 要素を含める必要があります。Amazon Monitron は、このサービスで実行できるタスクを記述する独自のアクションのセットを定義します。

> **Note**
>
> `deleteProject` オペレーションでは、削除するための AWS IAM Identity Center (SSO) 権限が必要です。これらの権限がない場合でも、削除機能でプロジェクトは削除されます。ただし、SSO からリソースは削除されないため、SSO でリソースがぶら下がってしまうことになります。

単一のステートメントに複数のアクションを指定するには次のようにコンマで区切ります。

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

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、List という単語で始まるすべてのアクションを指定するには次のアクションを含めます。

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

リソース

Amazon Monitron では、ポリシーでリソース ARN を指定することはできません。

条件キー

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Monitron では独自の条件キーが定義されており、また一部のグローバル条件キーの使用がサポートされています。すべての AWS グローバル条件キーのリストについては、IAM ユーザーガイドのAWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Monitron の条件キーのリストを確認するには、「IAM ユーザーガイド」の「Amazon Monitron で定義されるアクション」を参照してください。条件キーを使用できるアクションとリソースについては、「Amazon Monitron で定義されるアクション」を参照してください。

例

Amazon Monitron のアイデンティティベースポリシーの例を確認するには、「Amazon Monitron のアイデンティティベースポリシーの例」を参照してください。

Amazon Monitron リソースベースのポリシー

Amazon Monitron では、リソースベースのポリシーはサポートされていません。

Amazon Monitron タグに基づく認可

承認のために、特定のタイプの Amazon Monitron リソースにタグを関連付けることができます。タグに基づいてアクセスを管理するには、`Amazon Monitron:TagResource/${TagKey}`、`aws:RequestTag/${TagKey}`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

Amazon Monitron の IAM ロール

IAM ロールは、特定のアクセス許可を持つ AWS アカウント内のエンティティです。

Amazon Monitron での一時的な認証情報の使用

一時的な認証情報を使用して、フェデレーションでサインインする、IAM ロールを引き受ける、またはクロスアカウントロールを引き受けることができます。一時的なセキュリティ認証情報を取得するには、AssumeRole や GetFederationToken などの AWS STS API オペレーションを呼び出します。

Amazon Monitron は、一時的な認証情報の使用をサポートします。

サービスリンクロール

サービスにリンクされたロールを使用すると、 AWS サービスは他の サービスのリソースにアクセスして、ユーザーに代わってアクションを実行できます。サービスリンクロールは IAM アカウント内に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールの許可を表示できますが、編集することはできません。

Amazon Monitron は、サービスにリンクされたロールをサポートしています。

サービスロール

この機能により、ユーザーに代わってサービスがサービス役割を引き受けることが許可されます。この役割により、サービスがお客様に代わって他のサービスのリソースにアクセスし、アクションを完

了することが許可されます。サービス役割はIAM アカウントに表示され、アカウントによって所有されます。つまり、IAM 管理者はこの役割の権限を変更できます。ただし、それにより、サービスの機能が損なわれる場合があります。

Amazon Monitron は、サービスロールをサポートします。

Amazon Monitron のアイデンティティベースポリシーの例

デフォルトでは、IAM ユーザーとロールには Amazon Monitron リソースを作成または変更する権限がありません。また、 を使用してタスクを実行することはできません AWS Management Console。管理者はアクセス許可が必要な IAM ユーザー、グループ、またはロールにその権限を付与する必要があります。その後、権限を付与されたユーザー、グループ、またはロールは、指定された必要なリソースで特定の操作を実行できます。続いて、管理者はそれらの権限が必要な IAM ユーザーまたはグループにそのポリシーをアタッチする必要があります。

JSON ポリシードキュメントのこれらの例を使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「JSON タブでのポリシーの作成」を参照してください。

トピック

- ポリシーのベストプラクティス
- Amazon Monitron コンソールを使用する
- 例: すべての Amazon Monitron プロジェクトを一覧表示する
- 例: Amazon Monitron プロジェクトをタグに基づいて一覧表示する

ポリシーのベストプラクティス

ID ベースのポリシーでは、ユーザーのアカウント内で誰かが Amazon Monitron リソースの作成、アクセス、または削除ができるかどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行 – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能の AWS マネージドポリシー」を参照してください。

- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を通じてサービスアクションが使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイドの IAM でのセキュリティのベストプラクティスを参照してください。

Amazon Monitron コンソールを使用する

コンソールを使用して Amazon Monitron をセットアップするには、権限の高いユーザー (`AdministratorAccess` マネージドポリシーがアタッチされているユーザーなど) を通して初期設定プロセスを完了してください。

初期設定後、Amazon Monitron コンソールにアクセスして日常的な操作を行うには、最小限のアクセス許可が必要です。これらのアクセス許可により、 AWS アカウントの Amazon Monitron リソースの詳細を一覧表示および表示し、IAM Identity Center に関連する一連のアクセス許可を含めることができます。これらの最小限必要な許可よりも厳しく制限されたアイデンティティベースポリシーを作成すると、そのポリシーを添付したエンティティ (IAM ユーザーまたはロール) に対し

てコンソールが意図したとおりに機能しません。Amazon Monitron コンソールの基本機能については、AmazonMonitronFullAccess マネージドポリシーをアタッチする必要があります。状況によっては、Organizations と SSO サービスに追加の権限が必要になる場合もあります。詳細については、 AWS サポートにお問い合わせください。

例: すべての Amazon Monitron プロジェクトを一覧表示する

このポリシー例では、 AWS アカウントの IAM ユーザーに、アカウント内のすべてのプロジェクトを一覧表示するアクセス許可を付与します。

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

例: Amazon Monitron プロジェクトをタグに基づいて一覧表示する

アイデンティティベースのポリシーの条件を使用して、タグに基づいて Amazon Monitron リソースへのアクセスを制御できます。この例では、プロジェクトを一覧表示できるポリシーを作成する方法について示しています。ただし、プロジェクトタグ location に Seattle の値がある場合のみ、アクセス許可は付与されます。このポリシーでは、このアクションをコンソールで実行するために必要なアクセス許可も付与します。

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

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

```
            }
        }
    ]
}
```

詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素: 条件」を参照してください。

Amazon Monitron のアイデンティティとアクセスのトラブルシューティング

Amazon Monitron と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復には、次の情報を利用してください。

トピック

- Amazon Monitron でアクションを実行する権限がない
- AWS アカウント以外のユーザーに Amazon Monitron リソースへのアクセスを許可したい

Amazon Monitron でアクションを実行する権限がない

アクションを実行する権限がないというエラーが表示された場合は、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なmonitron:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 monitron:GetWidget on resource: my-example-widget
```

この場合、monitron:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

AWS アカウント以外のユーザーに Amazon Monitron リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまた

はアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- Amazon Monitron がこれらの機能をサポートしているかどうかを確認するには、「Amazon Monitron で IAM を使用する方法」を参照してください。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

Amazon Monitron のサービスリンクロールの使用

Amazon Monitron は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、Amazon Monitron に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは Amazon Monitron によって事前定義されており、ユーザーに代わってサービスが他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要な許可を手動で追加する必要がないため、Amazon Monitron のセットアップが簡単になります。サービスリンクロールの許可は Amazon Monitron が定義し、別段の定義がない限り、Amazon Monitron のみがそのロールを引き受けることができます。定義される許可は信頼ポリシーと許可ポリシーに含まれており、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールをサポートする他のサービスについては、「IAM と連動するAWS のサービス」を参照し、[Service-linked role (サービスリンクロール)] の列内で [Yes (はい)] と表記されたサービスを確認してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[Yes] (はい) リンクを選択します。

トピック

- Amazon Monitron のサービスリンクロール許可
- Amazon Monitron のサービスリンクロールの作成
- Amazon Monitron のサービスリンクロールの編集
- Amazon Monitron のサービスリンクロールの削除
- Amazon Monitron サービスリンクロールがサポートされるリージョン
- AWS Amazon Monitron の マネージドポリシー
- Amazon Monitron による AWS マネージドポリシーの更新

Amazon Monitron のサービスリンクロール許可

Amazon Monitron はAWSServiceRoleForMonitron[_{SUFFIX}]という名前のサービスにリンクされたロールを使用します。AWSServiceRoleForMonitron を使用して、Cloudwatch Logs、Kinesis データストリーム、KMS キー、SSO など他の AWS サービスにアクセスします。ポリシーの詳細については、AWS 「 マネージドポリシーリファレンスガイド」のAWSServiceRoleForMonitronPolicy」を参照してください。

AWSServiceRoleForMonitron[_{SUFFIX}] のサービスにリンクされたロールは、以下のサービスを信頼してロールを引き受けます。

- `monitron.amazonaws.com`、または `core.monitron.amazonaws.com`

MonitronServiceRolePolicy という名前のロールのアクセス許可ポリシーは、指定したリソースに対して Amazon Monitron が以下のアクションを実行することを許可します。

- アクション: Amazon CloudWatch Logs `logs:CreateLogGroup`、CloudWatch ロググループ、ログストリーム、および /aws/monitron/* パスにあるログイベント上の `logs:CreateLogStream` および `logs:PutLogEvents`

MonitronServiceDataExport-KinesisDataStreamAccess という名前のロールのアクセス許可ポリシーは、指定したリソースに対して Amazon Monitron が以下のアクションを実行することを許可します。

- アクション: Amazon Kinesis `kinesis:PutRecord`、`kinesis:PutRecords`、およびライブデータエクスポート用に指定された Kinesis データストリーム上の `kinesis:DescribeStream`

- アクション: ライブデータエクスポート用に AWS KMS 指定された Kinesis データストリームで使用されるキーの Amazon AWS KMS `kms:GenerateDataKey`
- アクション: 使用していないサービスにリンクされたロール自体を削除する Amazon IAM `iam:DeleteRole`

AWSServiceRoleForMonitronPolicy という名前のロールのアクセス許可ポリシーは、Amazon Monitron が指定されたリソースで以下のアクションを実行することを許可します。

- アクション: IAM アイデンティティセンター `sso:GetManagedApplicationInstance`、`sso:GetProfile`、`sso:ListProfiles`、`sso:Associa` および `sso:ListProfileAssociations` `sso-directory:DescribeUsers` `sso-directory:SearchUserssso:ListApplicationAssignments`プロジェクトに関連付けられた IAM アイデンティティセンターユーザーにアクセス

> **Note**
>
> Amazon Monitron が Amazon Monitron プロジェクトの基盤となるアプリケーションインスタンスとの関連付けを一覧表示できるようにするために、`sso:ListProfileAssociations` を追加してください。

サービスリンク役割の作成、編集、削除を IAM エンティティ (ユーザー、グループ、役割など) に許可するにはアクセス許可を設定する必要があります。詳細については、「IAM User Guide」(IAM ユーザーガイド) の「Service-linked role permissions」(サービスにリンクされたロールのアクセス権限) を参照してください。

Amazon Monitron のサービスリンクロールの作成

サービスリンクロールを手動で作成する必要はありません。で Amazon Monitron でユーザーに代わって他の AWS サービスを呼び出すアクセス許可を必要とする機能を有効にすると AWS Management Console、Amazon Monitron によってサービスにリンクされたロールが作成されます。

Amazon Monitron のサービスリンクロールの編集

Amazon Monitron では、サービスにリンクされたロール AWSServiceRoleForMonitron[_{SUFFIX}] を編集できません。サービスリンクロールの作成後は、さまざまなエンティティがロールを参照する可能性があるため、ロール名を変更することはできません。ただし、IAM を使用してロールの説明を

編集することはできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

Amazon Monitron のサービスリンクロールの削除

AWSServiceRoleForMonitron[_{SUFFIX}] ロールを手動で削除する必要はありません。で Amazon Monitron を通じて作成した Amazon Monitron プロジェクトを削除すると AWS Management Console、Amazon Monitron はリソースをクリーンアップし、サービスにリンクされたロールを削除します。

IAM コンソール、、 AWS CLI または AWS API を使用して、サービスにリンクされたロールを手動で削除することもできます。そのためにはまず、サービスリンクロールのリソースをクリーンアップする必要があります。その後で、手動で削除できます。

> **Note**
>
> リソースを削除しようとしたときに Amazon Monitron サービスがロールを使用している場合は、削除が失敗する可能性があります。失敗した場合は数分待ってから操作を再試行してください。

AWSServiceRoleForMonitron[_{SUFFIX}] で使用される Amazon Monitron リソースを削除するには

- このサービスリンクロールを使用して Amazon Monitron プロジェクトを削除してください。

サービスリンクロールを IAM で手動削除するには

IAM コンソール、 AWS CLI、または AWS API を使用して、AWSServiceRoleForMonitron[_{SUFFIX}] サービスにリンクされたロールを削除します。詳細については、 IAM ユーザーガイド の「サービスにリンクされたロールの削除」を参照してください。

Amazon Monitron サービスリンクロールがサポートされるリージョン

Amazon Monitron は、このサービスを利用できるすべてのリージョンでサービスリンクロールの使用をサポートします。詳細については、「AWS のリージョンとエンドポイント」を参照してください。

Amazon Monitron は、サービスを利用できるすべてのリージョンで、サービスにリンクされたロールの使用をサポートしているわけではありません。AWSServiceRoleForMonitron[_{SUFFIX}] ロールは、以下のリージョンで使用できます。

リージョン名	リージョン識別子	Amazon Monitron でのサポート
米国東部 (バージニア北部)	us-east-1	はい
米国東部 (オハイオ)	us-east-2	いいえ
米国西部 (北カリフォルニア)	us-west-1	いいえ
米国西部 (オレゴン)	us-west-2	いいえ
アジアパシフィック (ムンバイ)	ap-south-1	いいえ
アジアパシフィック (大阪)	ap-northeast-3	いいえ
アジアパシフィック (ソウル)	ap-northeast-2	いいえ
アジアパシフィック (シンガポール)	ap-southeast-1	いいえ
アジアパシフィック (シドニー)	ap-southeast-2	はい
アジアパシフィック (東京)	ap-northeast-1	いいえ
カナダ (中部)	ca-central-1	いいえ
欧州 (フランクフルト)	eu-central-1	いいえ
欧州 (アイルランド)	eu-west-1	はい
欧州 (ロンドン)	eu-west-2	いいえ
欧州 (パリ)	eu-west-3	いいえ
南米 (サンパウロ)	sa-east-1	いいえ
AWS GovCloud (US)	us-gov-west-1	いいえ

AWS Amazon Monitron の マネージドポリシー

IAM エンティティに AmazonMonitronFullAccess をアタッチできます。このポリシーにより、すべての Amazon Monitron のリソースとオペレーションへのアクセスを許可する管理アクセス許可が付与されます。

```
{
    "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 による AWS マネージドポリシーの更新

Amazon Monitron の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始してから表示します。このページの変更に関する自動通知を入手するには、Amazon Monitron ドキュメントの履歴ページから、RSS フィードを購読してください。

変更	説明	日付
AWSServiceRoleForMonitronPolicy - 既存のポリシーの更新	ロールのアクセス許可ポリシー`sso:ListApplicationAssignments` に `sso:CreateApplicationAssignment` と を追加しました。	2024 年 9 月 30 日
AmazonMonitronFullAccess — 既存ポリシーの更新	Amazon Monitron に、Kinesis データストリームの記述と一覧表示、および CloudWatch のロググループ、ログストリーム、ログイベントを記述、取得、作成できるアクセス許可が追加されました。 Amazon Monitron コンソールを使用して Kinesis データストリームと CloudWatch Logs に関する情報を表示するには、これらの権限を使用する必要があります。	2022 年 6 月 8 日

Amazon Monitron でログ記録とモニタリングを実行する

モニタリングは、Amazon Monitron アプリケーションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。Amazon Monitron コンソールとモバイルアプリのアクションをモニタリングするには、 AWS CloudTrailを使用します。

CloudTrail ログは、Amazon Monitron のユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を提供します。CloudTrail により収集された情報を使用して、Amazon Monitron に対して行われたリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエストが行われた日時、および追加の詳細を特定することができます。詳細については、「AWS CloudTrail を使用した Amazon Monitron アクションのログ記録」を参照してください。

Amazon Monitron のコンプライアンス検証

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、AWS のサービス「コンプライアンスプログラムによる範囲内」を参照して、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「Downloading Reports in AWS Artifact」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供します。

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスの機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべて AWS のサービス HIPAA の対象となるわけではありません。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド – コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) など) にわたるセキュリティコントロールを保護し、そのガイダンスに AWS のサービス マッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セ

キュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、Security Hub のコントロールリファレンスを参照してください。

- Amazon GuardDuty – 環境をモニタリングして AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか調べることで、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

Amazon Monitron のインフラストラクチャセキュリティ

マネージドサービスである Amazon Monitron は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS 公開された API コールを使用して、ネットワーク経由で Amazon Monitron にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードはJava 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。またはAWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

Amazon Monitron のセキュリティベストプラクティス

Amazon Monitron には、独自のセキュリティポリシーを策定および実装する際に考慮が必要なさまざまなセキュリティ機能が用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを説明するものではありません。これらのベストプラク

ティスはお客様の環境に適切ではないか、十分ではない場合があるため、これらは指示ではなく、有用な考慮事項と見なしてください。

以下は、セキュリティ問題の防止に役立つ Amazon Monitron でのベストプラクティスです。

- Amazon Monitron のユーザーの AWS IAM Identity Center (IAM Identity Center) ディレクトリを作成すると、ディレクトリのセキュリティを向上させるために、ディレクトリの多要素認証 (MFA) が有効になります。
- Amazon Monitron モバイルアプリを使用するすべてのプロジェクト管理者およびサイト管理者は、プロジェクト設定時に選択したユーザーディレクトリにリストされている組織内のすべてのユーザーに対して、読み取りアクセス権を持っていることに注意してください。ユーザーの組織情報へのアクセスを制限したい場合は、独立したディレクトリを使用することを強くお勧めします。
- 攻撃者が Amazon Monitron プロジェクトの招待メールを装い、ユーザーに E メールを送信するフィッシング攻撃の危険性があるため、ログイン認証情報を入力する前に、ログイン画面にディレクトリ名が表示されていることを確認するようユーザーに警告してください。
- Amazon Monitron モバイルアプリはスマートフォン上で実行してプロジェクトにアクセスできるため、使用しないときはアクセスを保護するために、すべてのユーザーで画面ロックを有効にしてください。

Amazon Monitron デバイスの問題のトラブルシューティング

いずれかの Amazon Monitron デバイスに問題がある場合は、以下の提案を使用して問題のトラブルシューティングを行います。それでも問題が解消しない場合は、 AWS サポートにお問い合わせください。

> **Note**
>
> iOS ではデフォルトブラウザの Safari、Android ではデフォルトブラウザの Chrome の使用をお勧めします。

トピック

- Amazon Monitron に関する問題のトラブルシューティング
- Amazon Monitron ゲートウェイに関するトラブルシューティング

Amazon Monitron に関する問題のトラブルシューティング

完全に自己完結型のユニットのため、センサーに問題が発生する可能性はほとんどありません。しかし、それでもいくつかの問題が発生する可能性があります。

トピック

- センサーをコミッショニングできない場合
- センサーがオフラインの場合
- センサーが外れた場合

センサーをコミッショニングできない場合

以下の質問について検討してください。

- Amazon Monitron アプリを実行しているスマートフォンのインターネット接続は安定していますか

センサーをコミッショニングするには、 Amazon Monitron アプリを実行している携帯電話にインターネット接続が必要です。

- スマートフォンをセンサーに近づけていますか

コミッショニング時には、スマートフォンはセンサーから 2 cm 以内にある必要があります。センサーのコミッショニング中は、スマートフォンを動かさないでください。

- スマートフォンでは NFC が有効になっていますか

  一部の iOS デバイスでは、コントロールセンターで NFC タグリーダーを手動でオンにする必要があります。お使いのデバイスがそれに該当するかどうかを確認するには、「iPhone ユーザーガイド」を参照してください。

- NFC アンテナをセンサーに近づけていますか

  iPhone の場合、NFC アンテナはデバイスの上部近辺にあります。Android デバイスの場合、アンテナの位置は異なる場合があります。Samsung、Google Pixel、またはデバイスの製造元のドキュメントを確認してください。

- コミッショニングの進行状況バーは表示されていますか (Android のみ)

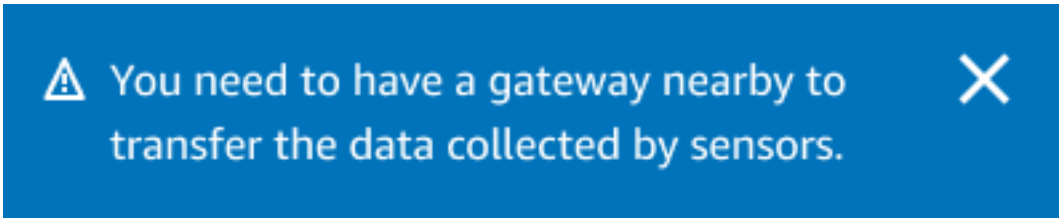
コミッショニングの進行状況バーが表示されない (Android のみ)、または最初にリセットされる場合は、センサーとスマートフォンの間の NFC 通信が弱いか、確立できていません。スマートフォンを動かして NFC 接続の確立を試みます。スマートフォンでは、ブランドによって NFC を送信する部分の位置が異なることがよくあります。スマートフォンのハードウェア仕様を確認し、NFC を送信する部分でセンサーをタップします。NFC がオンになっていて、ブロードキャストされていることを確認します。

- センサーが既に使用中であるというエラーが表示されていますか

  センサーを以前のアセットまたはポジションから削除し、コミッショニングプロセスを再試行します。それでもうまくいかない場合は、現在使用していない別のセンサーでコミッショニングを試してください。

センサーがオフラインの場合

センサーがアセットとペアリングされると、 Amazon Monitron は最初の測定を 2 回 (30 秒間) 試行します。どちらも成功しない場合、以下のようなアラートがアプリに表示されます。



センサーがデータの送信を停止した場合は、以下を試してください。

- 1 回限りの測定を行います。これが正常に実行できれば、センサーは機能しています。これが実行できない場合、センサーは機能しておらず、バッテリーが切れている可能性があります。新しいセンサーと交換してください。
- 使用可能なゲートウェイが範囲内にあることを確認します。 Amazon Monitron のセンサーとゲートウェイは Bluetooth Low Energy (BLE) を使用して通信し、通信範囲は通常 20～30 メートルです。まったく障害物のない空間では、センサーとゲートウェイはより遠い距離でも通信できます。
- 障害物を確認します。コンクリートの壁や金属製の物体は信号を減衰させます。
- 信号干渉がないか確認します。センサーとゲートウェイが通信に使用する Bluetooth 信号は、2.4 GHz ISM (産業、科学、医療) 帯域を占有します。この帯域を使用するその他のデバイスには、ワイヤレスヘッドセットとマウス、ワイヤレスカメラ、電子レンジ、ガレージドアオープナーなどがあります。
- 測定を開始しても (読み込みバーが表示される)、完了しない場合は、測定をやり直してください。同じ問題が再度発生する場合は、センサーを削除して再度コミッショニングを試みます。
- 測定に失敗した場合、またはセンサーをコミッショニングできない場合は、カスタマーサポートにお問い合わせください。

センサーが外れた場合

再度取り付けます。

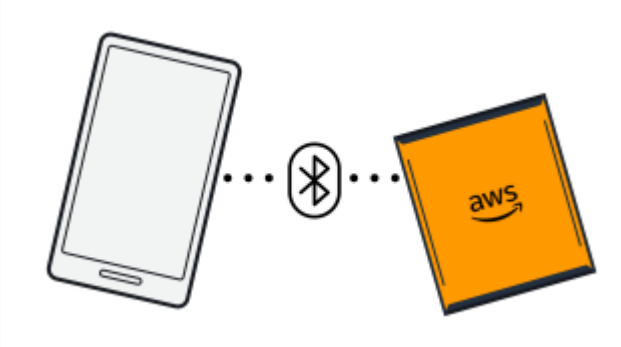
Amazon Monitron ゲートウェイに関するトラブルシューティング

トピック

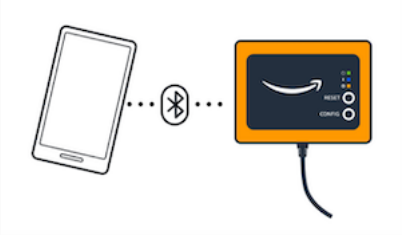
- モバイルアプリをゲートウェイとペアリングできない場合
- ゲートウェイのコミッショニングに失敗した場合
- ゲートウェイがオフラインになった場合

モバイルアプリをゲートウェイとペアリングできない場合

モバイルアプリで [ゲートウェイを追加] を選択しても、アプリがゲートウェイを検出しない場合は、以下を試してください。



Bluetooth pairing with a Wi-Fi gateway



Bluetooth pairing with an Ethernet gateway.

- ゲートウェイの電源がオンになっていることを確認します。

  ゲートウェイの正面のライトを確認します。1 つでも点灯している場合は、ゲートウェイに電力が供給されています。ゲートウェイに電力が供給されていない場合は、以下の点を確認してください。

  - 電源コードはゲートウェイの背面と電源コンセントにしっかりと接続されていますか。
  - 電源コンセントは正しく機能していますか。
  - ゲートウェイの電源ケーブルは機能していますか。ケーブルを別のゲートウェイに接続すると、機能しているかどうかをテストできます。
  - ケーブルをゲートウェイに差し込むコンセントは清潔で、内部にゴミが詰まっていませんか。ゲートウェイのコンセントとケーブルの接続端を必ず確認してください。
- ゲートウェイがコミッショニングモードになっていることを確認してください。

  「Wi-Fi ゲートウェイのコミッショニング」または「イーサネットゲートウェイのコミッショニング」を参照してください。
- スマートフォンの Bluetooth が機能していることを確認します。
  - オフにしてからオンに切り替えてみてください。それでも解決しない場合は、スマートフォンを再起動してもう一度確認してください。
  - スマートフォンの Bluetooth 圏内にいますか。Bluetooth の通信範囲は通常 10 メートル未満です。

- Bluetooth 信号を電子的に妨害している可能性がある障害物はありますか。「センサーがオフラインの場合」を参照してください。

これらのアクションを実行しても問題が解決しない場合は、以下の手順を実行します。

- モバイルアプリからログアウトし、再起動します。
- Wi-Fi ゲートウェイをリセットするか、イーサネットゲートウェイをリセットします。

ゲートウェイのコミッショニングに失敗した場合

Amazon Monitron ゲートウェイのコミッショニングプロセスが失敗した場合は、以下を試してください。

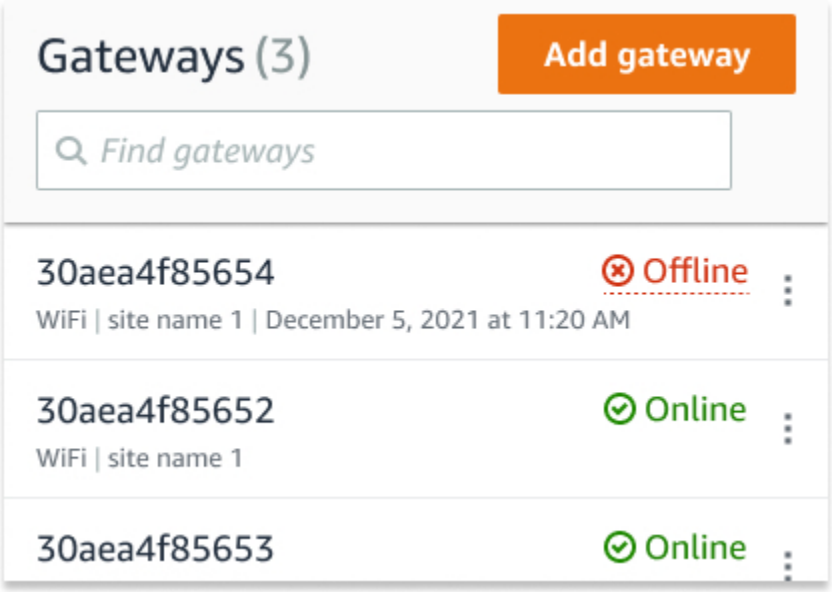
- Amazon Monitron アプリを実行している携帯電話にインターネット接続があることを確認します。
- Wi-Fi ゲートウェイのコミッショニングに失敗した場合は、モバイルデバイスに用意されているモバイルホットスポットを使用して、コミッショニングを実行します。これでコミッショニングに成功した場合、Wi-Fi ネットワークまたはファイアウォール設定に設定上の問題があると考えられます。

ゲートウェイがオフラインになった場合

モバイルアプリまたはウェブアプリで、ゲートウェイがオフラインである、またはネットワークに接続されていないと表示されることがあります。このような場合は、以下を試してください。

- 最近ゲートウェイを設定に追加した場合は、ステータスが更新されるまでお待ちください。新しくコミッショニングされたゲートウェイは、オンラインになるまでに最大 20 秒かかります。
- Wi-Fi ゲートウェイの設定を、静的 IP で試みていないことを確認します。現在、Wi-Fi ゲートウェイは静的 IP をサポートしていません。ただし、同じデバイスに常に同じ IP アドレスを割り当てるようにネットワークを設定できます。
- ファイアウォールがゲートウェイをブロックしていないことを確認します。 Amazon Monitron ゲートウェイは TCP ポート 8883 を使用します。 Amazon Monitron ゲートウェイへのファイアウォールアクセスを提供するには、amazonaws.com://www.com サブドメイン」の TCP ポート 8883 への接続を許可する必要があります。
- 問題がネットワークの混雑ではないことを確認します。ゲートウェイがオフラインであることをから通知 Amazon Monitron される方法は 2 つあります。

- モバイルアプリまたはウェブアプリでゲートウェイに関する情報を確認すると、ゲートウェイにオフラインと表示されていることがわかります。



  オフラインゲートウェイのタイムスタンプは、そのゲートウェイからシグナルを最後に Amazon Monitron 受信した時刻を示します。

  この場合、ゲートウェイのオフラインステータスに関する通知が届いていない可能性があります。 Amazon Monitron は、ゲートウェイがオフラインのように見えるたびに通知を発行しません。新しくコミッショニングされたゲートウェイは、インターネットに接続するまでオフラインとみなされます。輻輳したネットワーク上のゲートウェイは、15 分間そのゲートウェイから Amazon Monitron が聞こえない場合、オフラインと見なされます。

- 扱っているものが新しくコミッショニングされたゲートウェイや新しくペアリングされたセンサーではないことを確認します。新しいものである場合は、1 時間お待ちください。センサーは 1 時間に 1 回データを送信します。待ちたくない場合は、1 回限りの測定を行うことができます。
- ゲートウェイが電源に接続されていることを確認します。接続されている場合は、ゲートウェイを取り外し、再接続します。
- Wi-Fi ゲートウェイの場合は、Wi-Fi 接続を確認します。ゲートウェイを追加した後で Wi-Fi ネットワークのパスワードを変更している場合、接続できなくなります。再接続するには、ゲートウェイを削除してから再度追加し、新しいパスワードを使用して Wi-Fi ネットワークに接続する必要があります。ゲートウェイを追加する方法の詳細については、「Wi-Fi ゲートウェイのコミッショニング」または「イーサネットゲートウェイのコミッショニング」を参照してください。
- イーサネットゲートウェイの場合は、ネットワーク設定を確認します。

- Amazon Monitron モバイルアプリを使用してゲートウェイを削除し、ゲートウェイの工場出荷時設定のリセットを実行してから、ゲートウェイを再度インストールします。詳細については、Wi-Fi ゲートウェイの工場出荷時設定へのリセット または イーサネットゲートウェイの工場出荷時設定へのリセット を参照してください。

これらの提案が Amazon Monitron デバイスを再度動作させるのに役に立たない場合は、 AWS サポートにお問い合わせください。

Amazon Monitron デバイス

Amazon Monitron スターターキット、センサー、ゲートウェイは Amazon.com または Amazon Business で購入できます。Amazon Monitron デバイスは、米国、英国、欧州で購入可能です。

Amazon Monitron のクォータ

アプリケーションが要求する場合、Amazon Monitron のクォータの多くでは引き上げをリクエストすることができます。サービスクォータおよびクォータの引き上げをリクエストする方法に関する詳細については、「AWS サービスクォータ」を参照してください。また、担当の IT マネージャーに連絡して、クォータの引き上げをリクエストすることもできます。

サポート対象の リージョン

現在、Amazon Monitron は次のリージョンでサポートされています。

- 米国東部 (バージニア北部): us-east-1
- 欧州 (アイルランド): eu-west-1
- アジアパシフィック (シドニー): ap-southeast-2

クォータ

Amazon Monitron のすべてのオペレーションには次のクォータがあります。

説明	クォータ
プロジェクトあたりのサイトの最大数	50
サイトあたりのアセットの最大数	100
アセットあたりのポジション (またはセンサー) の最大数	20
サイトあたりのゲートウェイの最大数	200
サイトあたりのユーザーの最大数	20
プロジェクトあたりのカスタムクラスの最大数	25
カスタムクラスあたりの位置の最大数	500

Amazon Monitron ユーザーガイドのドキュメント履歴

- ドキュメントの最終更新日： 2024 年 10 月 31 日

次の表に、 の各リリースにおける重要な変更点を示します Amazon Monitron。このドキュメントの更新に関する通知については、RSS フィードにサブスクライブできます。

変更	説明	日付
Amazon Monitron は、新規顧客に公開されなくなりました。既存のお客様は、通常どおりサービスを引き続き使用できます。Amazon Monitron に似た機能については、ブログ記事を参照してください。	Amazon Monitron は新規お客様に公開されなくなりました。既存のお客様は、通常どおりサービスを引き続き使用できます。Amazon Monitron と同様の機能については、ブログ記事を参照してください。	2024 年 10 月 31 日
Amazon Monitron は、2024 年 10 月 31 日以降、新しいお客様に公開されなくなります。サービスを使用する場合は、その日付より前にサインアップしてください。既存のお客様は、通常どおりサービスを引き続き使用できます。Amazon Monitron と同様の機能については、ブログ記事を参照してください。	Amazon Monitron は、2024 年 10 月 31 日以降、新規のお客様に公開されなくなります。サービスを使用する場合は、その日付より前にサインアップしてください。既存のお客様は、通常どおりサービスを引き続き使用できます。Amazon Monitron に似た機能については、ブログ記事を参照してください。	2024 年 10 月 1 日
サービスにリンクされたロールポリシーの更新	ロールのアクセス許可ポリシー`sso:ListApplicationAssignments` に `sso:CreateApplicationAssignment` と を追加しました。	2024 年 9 月 30 日

ユーザー管理	プロジェクト全体で管理者としてユーザー割り当てとアクセス許可を表示および管理できます。詳細については、「ユーザーの管理」を参照してください。	2024 年 3 月 19 日
サイト間のアセットの移動	Amazon Monitron アセットはサイト間で移動できます。詳細については、「アセットの移動」を参照してください。	2024 年 3 月 19 日
Amazon Monitron ゲートウェイの更新	デバイスの QR コードをスキャンすることで、 Amazon Monitron ゲートウェイ MAC アドレスの詳細を取得できるようになりました。詳細については、「イーサネットゲートウェイの MAC アドレスの詳細の取得」および「Wi-Fi ゲートウェイの MAC アドレスの詳細の取得」を参照してください。	2024 年 2 月 22 日
ISO アラートのミュート解除	ISO アラート (アラームと警告) のミュートを解除できるようになりました。詳細については、「アラートのミュートとミュート解除」を参照してください。	2024 年 1 月 31 日
ゲートウェイの静的 IP アドレス	Amazon Monitron は、ゲートウェイの新しい静的 IP アドレスをサポートするようになりました。詳細については、「ネットワークの保護」を参照してください。	2024 年 1 月 25 日

Amazon Monitron 請求モニタリングの更新	AWSが生成したタグを使用して Amazon Monitron 、請求をモニタリングできるようになりました。詳細については、「コストのモニタリング」を参照してください。	2023 年 12 月 13 日
Amazon Monitron カスタムマシンクラス	Amazon Monitron でカスタムマシンクラスを作成できるようになりました。詳細については、「カスタムクラスの作成」を参照してください。	2023 年 12 月 7 日
Amazon Monitron の安全性の更新	Amazon Monitron センサーの安全性情報を更新しました。	2023 年 11 月 26 日
Amazon Monitron IT マネージャーガイドの廃止	Amazon Monitron IT マネージャーガイドは Amazon Monitron「Amazon Monitron ユーザーガイド」に統合されました。	2023 年 10 月 24 日
Amazon Monitron CloudTrail イベント名の更新	Amazon Monitron CloudTrail イベント名が更新されました。詳細については、「Amazon Monitron information in CloudTrail」を参照してください。	2023 年 10 月 2 日
新しくサポートされるリージョン	Amazon Monitron がアジアパシフィック (シドニー) リージョンで利用可能になりました。サポートされているすべてのリージョンについては、「Supported Regions」を参照してください。	2023 年 8 月 17 日

モバイルアプリでゲートウェイの詳細を表示	モバイルアプリから Amazon Monitron ゲートウェイの詳細を表示できるようになりました。「Viewing Ethernet gateway details」と「Viewing Wi-Fi gateway details」を参照してください。	2023 年 7 月 20 日
プロジェクトの切り替え	AWS アカウント内の Amazon Monitron プロジェクトを切り替えることができるようになりました。詳細については、「Switching between projects」を参照してください。	2023 年 6 月 15 日
ゲートウェイ名の編集	ゲートウェイの Amazon Monitron ゲートウェイ名を編集できるようになりました。詳細については、「Editing ethernet gateway」と「Editing Wi-Fi gateway」を参照してください。	2023 年 6 月 15 日
ウェブアプリからポジションを作成	ウェブアプリから Amazon Monitron センサーの位置を作成できるようになりました。「Adding a sensor position」を参照してください。	2023 年 6 月 15 日
センサーのバッテリー寿命ステータス	Amazon Monitron は、センサーの状態を追跡するのに役立つセンサーバッテリーの状態を表示するようになりました。詳細については、「Sensor battery status」を参照してください。	2023 年 5 月 22 日

センサー測定値の散布図ビュー	センサー Amazon Monitron データを散布図形式で表示できるようになりました。	2023 年 5 月 22 日
マシンクラス更新の編集	各 Amazon Monitron センサーにマシンクラスを割り当てることができるようになりました。	2023 年 5 月 22 日
Kinesis データエクスポートスキーマ v2 の追加	Amazon Monitron Kinesis データエクスポートスキーマ v2 および v1 の廃止手順を追加しました。	2023 年 4 月 4 日
振動 ISO イメージの更新	モバイルおよびウェブ UI の新しい測定機能とフィルタリングツールが表示されるように、いくつかのイメージを更新しました。	2023 年 3 月 16 日
センサーのポジション情報の追加	センサーのポジション詳細を識別する方法の概要	2023 年 1 月 24 日
アプリ内更新	注意事項とアプリ内更新機能に関する更新情報を追加しました。ユーザーはこれらの情報をモニタリングして、Amazon Monitron の機能が最新であることを確認する必要があります。	2022 年 12 月 15 日
ゲートウェイ名の編集	ユーザーは、作成後にゲートウェイ名を編集できます。	2022 年 12 月 15 日
オフラインのデバイス	この更新では、オフラインになったセンサーの動作について説明します。	2022 年 12 月 15 日

Kinesis データエクスポート手順の更新	Kinesis の構成と設定の手順を更新しました。	2022 年 12 月 5 日
サービスにリンクされたロールポリシーの更新	`sso:ListProfileAssociations` をロールのアクセス許可ポリシーに追加しました。	2022 年 9 月 30 日
ネットワーク情報の追加	Amazon Monitron がローカルネットワークに接続する仕組みの詳細を確認できるようになりました。	2022 年 7 月 5 日
ウェブアプリのサポート	Amazon Monitron にウェブアプリが追加されました。	2021 年 11 月 18 日
イーサネットゲートウェイの追加	Amazon Monitron イーサネットゲートウェイを購入して、既存の Amazon Monitron システムと統合できるようになりました。	2021 年 9 月 7 日
新しくサポートされるリージョン	Amazon Monitron が欧州 (アイルランド) リージョンで利用可能になりました。サポートされているすべてのリージョンについては、「Supported Regions」を参照してください。	2021 年 5 月 5 日
1 回限りのダウンロードをサポート	CLI またはコンソールを使用して Amazon S3 にデータをダウンロードできます。	2021 年 1 月 21 日
新しいガイドとサービス	Amazon Monitron ユーザーガイドとサービスが初めてリリースされました。	2020 年 12 月 1 日