AWS Console Mobile Application

User Guide

AWS Console Mobile Application: User Guide

Table of Contents

What is the AWS Console Mobile Application?

The Console Mobile Application lets you view and manage a set of resources so that you can support incident response while you are away from your computer.

With the Console Mobile Application, you can monitor resources and view configuration details, metrics, and alarms for a select subset of AWS services. You can see an overview of the account status with real-time data on Amazon CloudWatch, AWS Personal Health Dashboard, and AWS Billing and Cost Management. You can view ongoing issues and follow through to the relevant CloudWatch alarm screens for a detailed view with graphs and configuration options. In addition, you can check on the status of specific AWS services, view detailed resource screens, and perform some actions.

The Console Mobile Application requires an existing AWS account. After you sign in with a root user, IAM user, access keys, or a federated role, the Console Mobile Application stores your credentials so that you can easily switch between identities.

Default service quotas for the AWS Console Mobile Application

There are no quotas imposed by the Console Mobile Application, but there may be limitations imposed by the other AWS services that you use on the app. For more information, see AWS Quotas.

Setting up for the AWS Console Mobile Application

Complete the tasks in this section to get set up to use the Console Mobile Application.

Steps

When you’re finished, you will be ready for the Getting started with AWS Console Mobile Application (p. 3) tutorial.

Step 1: Sign up for AWS

If you do not have an AWS account, complete the following steps to create one. Note that this step must be done from the AWS Management Console on your desktop.

To sign up for an AWS account

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

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

Step 2: Check system requirements

Mobile devices

We support iOS 12.0 and above, and Android 8.0 and above.

Tablets

The Console Mobile Application is optimized for iOS and Android mobile devices with a screen size smaller than 7 inches, but it works on larger screen sizes as well.

Step 3: Download the app

Download the Console Mobile Application from the iOS App Store, Google Play, or Amazon Appstore.

Getting started with the AWS Console Mobile Application

Use this tutorial to get started with the Console Mobile Application. You'll learn about required IAM permissions, how to authenticate through the app, and how to view your AWS resources through the app.

Prerequisites

> **Important**
> As of August 16th, 2021 the AWS Console Mobile Application doesn't offer customer authentication through access keys. We recommend using either IAM user credentials or a federated role to log in to the Console Mobile Application.

Before you begin, be sure that you've completed the steps in Setting up for the AWS Console Mobile Application (p. 2).

To log in to the Console Mobile Application, we recommend using either IAM user credentials or a federated role, rather than a root account. The root account should only be used to create your first IAM user. For more information, see AWS account root user in the *IAM User Guide*.

To sign in with an IAM user, you need to use either the account number or the account alias, which can be found at the top of the Management Console sign-in screen.

To sign in with a federated role, you need the federation link from your administrator.

To sign in with an access key, you need an access key ID and a secret key. Then you enter an identity name and PIN of your choosing. For more information, see Managing access keys for IAM users in the *IAM User Guide*.

If you use AWS Multi-factor Authentication (MFA), we recommend using either a hardware key fob MFA device, a hardware display card MFA device, or a virtual MFA device for the greatest level of account protection. For a list of MFA devices that you can use, see Multi-factor Authentication.

The Console Mobile Application does not currently support using U2F security keys for MFA. For more information, see Supported configurations for using U2F security keys in the *IAM User Guide*.

You can set up biometric authentication on supported iOS and Android devices running the Console Mobile Application version 2.0 and newer.

Step 1: Verify your permissions

To use the Console Mobile Application, you need the same permissions you use to access the AWS Management Console on your desktop. This means you need some basic AWS permissions, in addition to permissions for the AWS services you want to access from the Console Mobile Application.

> **Note**
> To use AWS Billing and Cost Management in the Console Mobile Application, you need to have permissions for the AWS Cost Explorer API, rather than for the AWS Billing and Cost Management console.

The following example shows a JSON policy that allows the user to use the AWS Cost Explorer API:

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

Step 2: Sign in

Choose an identity type. Enter your identity information and, optionally, enable biometric authentication. Then choose **Sign in**. After you sign in, the **Dashboard** will appear.

Step 3: View your dashboard

From the **Dashboard**, you can view information about CloudWatch alarms, AWS Health, and Cost Management.

View and modify CloudWatch alarms

Under **CloudWatch alarms** you can see the status of your alarms. To see more information about your alarms, you can choose the red number of those in alarm or with insufficient data. This shows you a list of those alarms, which you can search or filter. Choose **View all** to see a list of all your CloudWatch alarms, including those with a status of **OK**.

You can filter your alarms by choosing **Filter**, then choosing one of the following options:

- In alarm
- OK
- Insufficient data

To view more information about an alarm, choose the alarm you want to view. The alarm detail screen will appear. You can see more information about the alarm status, threshold, and more.

To modify an alarm threshold, choose **Modify**.

View AWS Health details

On the **Dashboard**, under **AWS Health**, you can see your open issues past 7 days, your scheduled changes, and other notifications past 7 days. Choose any of these numbers to view more information about these events. To view all of your events, choose **View all**. You can browse and search your event log.

View Cost Management details

To view your Cost Management details, from the **Dashboard**, under **Cost Management**, choose your month-to-date costs or **View details**. You can explore your month-to-date costs and more.

Step 4: View information about other AWS services

At the bottom of the screen, choose the **Services** tab. You will see a list of all of AWS services that are supported in the application.

If any of your services are in alarm, you will see the number of alarms in red.

Choose any service to view more information about that service.

For a list of supported services, see Supported AWS Regions and services (p. 6).

Supported AWS Regions and services

In this section, you'll learn which AWS Regions and services are supported by the Console Mobile Application.

Supported Regions

The Console Mobile Application supports the following Regions:

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- EU (Frankfurt)
- EU (Ireland)
- EU (London)
- EU (Paris)
- EU (Stockholm)
- South America (Sao Paulo)

Opt in Regions

Opt in Regions are not enabled by default. You must choose to enable them in the console before they can be used in the Console Mobile Application. The following opt in Regions are supported:

- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Europe (Milan)
- Middle East (Bahrain)

Note
If your sign in identity uses access keys, you will not be able to use opt-in Regions in the Console Mobile Application.

Supported services

The Console Mobile Application supports the following AWS services:

- Amazon API Gateway
- AWS Billing and Cost Management
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Compute Cloud (Amazon EC2)
- Elastic Load Balancing
- AWS Identity and Access Management (IAM)
- AWS Lambda
- AWS OpsWorks
- AWS Personal Health Dashboard
- Amazon Relational Database Service (Amazon RDS)
- Amazon Route 53
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (Amazon VPC)

> **Note**
> The Console Mobile Application supports a select subset of features for the AWS services listed above. If you don't see a feature you want to use on the app, you can contact us. You can also leave feedback in the app by choosing the menu icon in the upper left, then choosing **Feedback**. Add your comments, optionally include logs, and then choose **Submit**.

If you use AWS Billing and Cost Management, note that you need to have API permissions to use that service on the mobile application. See the example IAM policy in Getting started with AWS Console Mobile Application (p. 3).

Security

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

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

Security of the cloud – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to AWS Console Mobile Application, see AWS Services in Scope by Compliance Program.

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

This documentation helps you understand how to apply the shared responsibility model when using Console Mobile Application. The following topics show you how to configure Console Mobile Application to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Console Mobile Application resources.

Topics

Data protection

The AWS shared responsibility model applies to data protection in the Console Mobile Application. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ.

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

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. The Console Mobile Application does this for you, ensuring a secure connection between the application and your AWS resources.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.

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

Resilience in AWS Console Mobile Application

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

For specific information about AWS Regions supported by the Console Mobile Application, see Supported regions (p. 6).

Compliance validation for AWS Console Mobile Application

Third-party auditors assess the security and compliance of AWS Console Mobile Application as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

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

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- Architecting for HIPAA Security and Compliance Whitepaper – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.

  Note
  Not all services are compliant with HIPAA.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- Evaluating Resources with Rules in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Security best practices for AWS Console Mobile Application

We recommend taking some basic security precautions when using the Console Mobile Application on your device. These measures will help protect your AWS account in the event that your device is lost or stolen.

- Make sure your device is protected by biometrics or a PIN code if your device allows.
- Enable biometrics on the Console Mobile Application.
- If your device is lost or stolen, perform a remote wipe by logging into your Apple or Google account on another device. This option should be available for most iOS and Android devices.

Troubleshooting

In this section, you'll find answers to some common questions and concerns.

I lost my device, what should I do?

If you lose your device, we recommend deactivating the IAM user you used to sign into the Console Mobile Application. We also recommend performing a remote wipe on your device.

Can I create resources within the app?

No. You can view and sometimes modify resources within the app, but you cannot create resources.

Why am I being asked to log in again?

A session in the Console Mobile Application lasts 12 hours. After your session expires, you may need to log in again.

Can I leave feedback?

Yes. To leave feedback, open the app and choose the menu icon in the upper left, then choose **Feedback**. Add your comments, optionally include logs, and then choose **Submit**.

You can also provide feedback by contacting us.

Document history for AWS Console Mobile Application User Guide

The following table describes the document history for the AWS Console Mobile Application User Guide.

Change	Description	Date
Region added	Support for the AWS Asia Pacific (Osaka) Region has been added.	April 9, 2021
Opt in Regions added	Four additional Regions are now supported. You must choose to enable them in the console before they can be used.	February 02, 2021
Public release	This is the initial public release of the AWS Console Mobile Application User Guide.	September 30, 2020

AWS glossary

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