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

What Is Alexa for Business? ............................................................................................................................... 1
  How to Get Started with Alexa for Business ................................................................................................. 1
Related Services ................................................................................................................................................. 1
Accessing Alexa for Business .......................................................................................................................... 1
Concepts ............................................................................................................................................................ 1
Resources ............................................................................................................................................................ 2
Prerequisites ...................................................................................................................................................... 4
  Sign Up for AWS ........................................................................................................................................ 4
  Create IAM Users and Policies ....................................................................................................................... 4
  Firewall and Network Requirements ................................................................................................................ 5
  WPA2 Enterprise Prerequisite ......................................................................................................................... 5
  AVS Permissions ........................................................................................................................................... 5
Getting Started with Shared Devices ................................................................................................................ 7
  Get Recommended Hardware .......................................................................................................................... 7
  Prepare Your Devices .................................................................................................................................. 7
  Create Network Profile ................................................................................................................................. 8
  Import Your Devices ................................................................................................................................... 8
  Create an IAM User for Device Setup Tool ................................................................................................... 9
  Run the Device Setup Tool ............................................................................................................................ 10
  Create Room Profile, Skill Group, and Room ............................................................................................... 10
Managing Your Shared Devices ....................................................................................................................... 12
  Managing Rooms ....................................................................................................................................... 12
  Managing Room Profiles .............................................................................................................................. 13
  Managing Devices ...................................................................................................................................... 14
  Managing Network Profiles .......................................................................................................................... 17
  Managing Skills .......................................................................................................................................... 18
    Private Skills ............................................................................................................................................. 20
      Alexa for Business Blueprints ................................................................................................................ 22
  Managing Skill Groups ................................................................................................................................. 22
  Sending Announcements ................................................................................................................................ 23
Managing Alexa in Meeting Rooms .................................................................................................................. 25
  Available Alexa commands in Meeting Rooms ........................................................................................... 25
  Link Alexa for Business to Your Calendar System ....................................................................................... 27
    Link Alexa for Business to Office 365 ......................................................................................................... 27
    Link Alexa for Business to Google G Suite ............................................................................................... 29
    Link Alexa for Business to Microsoft Exchange ...................................................................................... 30
  Control Conferencing Systems .................................................................................................................... 32
    Supported Conferencing Systems ............................................................................................................... 32
    Understanding Alexa-enabled Conferencing ............................................................................................... 33
    Manage Conferencing Providers ................................................................................................................ 35
    Use Zoom Rooms with Alexa for Business ................................................................................................. 36
    Use Cisco Webex Room Devices with Alexa for Business ...................................................................... 38
    Use Poly Group Series with Alexa for Business .......................................................................................... 41
    Use Poly Trio with Alexa for Business ...................................................................................................... 43
    Use Lifesize room systems with Alexa for Business .................................................................................. 45
    Use the Alexa for Business Gateway ........................................................................................................ 47
  Configure Meeting Room Settings ............................................................................................................... 55
  View Room Utilization Metrics .................................................................................................................... 56
Managing Calling ............................................................................................................................................... 57
  Managing Address Books .............................................................................................................................. 57
  Managing Contacts ..................................................................................................................................... 58
Managing Users ............................................................................................................................................... 59
  Set up Enrollment ........................................................................................................................................ 59
  Invite and Remove Users .............................................................................................................................. 60
What Is Alexa for Business?

Alexa for Business makes it easy for you to use Alexa in your organization. Alexa for Business gives you the tools you need to manage Alexa devices, enroll your users, and assign skills, at scale. You can build your own context-aware voice skills using the Alexa Skills Kit, and the Alexa for Business APIs, and you can make these available as private skills for your organization. Alexa for Business also makes it easy to voice-enable your products and services, providing context-aware voice experiences for your customers.

How to Get Started with Alexa for Business

After you set up your shared devices, you organize them by creating rooms and assigning devices to these rooms. You manage skills and settings centrally with skill groups and room profiles. You can configure the rooms to be linked to your corporate calendar and configure them to automatically join meetings.

Related Services

The Alexa Skills Kit is a collection of self-service API actions, tools, documentation, and code examples. You can create your own skill and add it to the Alexa for Business console. All of the code runs in the cloud and nothing is stored on devices. For more information, see the Alexa Skills Kit details page and Managing Skills (p. 18).

Accessing Alexa for Business

Alexa for Business is accessed through the AWS Management Console or the Alexa for Business API.

Concepts

To help you get started with Alexa for Business, review the following concepts:

Alexa

The cloud-based voice service that powers devices such as the Amazon Echo and Amazon Echo Dot. You can give Alexa new abilities by creating your own cloud-based service that accepts requests from Alexa and returns responses.

Alexa device

A device that provides access to the Alexa service. Examples include Amazon Echo, Amazon Echo Dot, and devices that use the Alexa Voice Service.

Device Setup Tool

A Windows-based application you can use to connect Amazon Echo devices to your Wi-Fi network and register them with Alexa for Business.
enrolled user

Employees can join an organization by enrolling their personal Amazon account. When users join their employer’s Alexa for Business organization, they can use all of the Alexa for Business features on an unlimited number of Alexa endpoints registered to the Amazon account used when they join.

master account

Some skills require account linking. If you enable a skill and link your account, this becomes the master account and is shared by default for all devices with that skill enabled. You can override this master account and link a different account inside an individual room.

room

The physical location that contains your device. Examples include conference rooms, lobbies, and hotel rooms.

room profile

A room profile is associated with a room and contains all of the settings for your devices. This enables Alexa to provide weather, time, and other location-based information. You can create a room profile that applies the same settings to all rooms in the same building. You can modify the settings in a room profile, including the default room profile, at any time.

private skill

An Alexa skill that is only available for the users and Alexa devices in your organization. A private skill never shows up in the Alexa Skills store.

skill

A stand-alone capability that an Alexa customer can discover, enable, use, and disable to add new functionality to their Alexa experience.

skill group

A skill group is a collection of one or more skills that can be added to a room. The only way to enable skills on an Alexa for Business-managed device is to add a skill group that contains the skills to enable in a room. After enabling a room, any device in that room has access to those skills.

shared device

An Alexa device placed in a shared location, such as a conference room, lobby, or hotel room.

smart home device

Smart home lights, thermostats, and drapes. Not to be confused with device, which is an Alexa device such as the Amazon Echo.

Resources

The following related resources can help you as you work with this service.

- **Classes & Workshops** – Links to role-based and specialty courses as well as self-paced labs to help sharpen your AWS skills and gain practical experience.
- **AWS Developer Tools** – Links to developer tools, SDKs, IDE toolkits, and command line tools for developing and managing AWS applications.
- **AWS Whitepapers** – Links to a comprehensive list of technical AWS whitepapers, covering topics such as architecture, security, and economics and authored by AWS Solutions Architects or other technical experts.
- **AWS Support Center** – The hub for creating and managing your AWS Support cases. Also includes links to other helpful resources, such as forums, technical FAQs, service health status, and AWS Trusted Advisor.
- **AWS Support** – The primary web page for information about AWS Support, a one-on-one, fast-response support channel to help you build and run applications in the cloud.
- **Contact Us** – A central contact point for inquiries concerning AWS billing, account, events, abuse, and other issues.
- **AWS Site Terms** – Detailed information about our copyright and trademark; your account, license, and site access; and other topics.
Prerequisites

Before you can get started with Alexa for Business, complete the following tasks:

Tasks
- Sign Up for AWS (p. 4)
- Create IAM Users and Policies (p. 4)
- Firewall and Network Requirements (p. 5)
- WPA2 Enterprise Prerequisite (p. 5)
- AVS Permissions (p. 5)

Sign Up for AWS

Your AWS account gives you access to all services, but you are charged only for the resources that you use.

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

To sign up for an AWS account
2. Follow the online instructions.
   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

Create IAM Users and Policies

The Alexa for Business console requires a user name and password so that the service can determine whether you have permission to access its resources. We recommend that you avoid using AWS account credentials for general access because those credentials cannot be revoked or limited in any way. For more information, see AWS Security Credentials in the AWS General Reference.

Instead, use AWS Identity and Access Management (IAM) to create an IAM user and add the user to an IAM group with administrative permissions. You can then access the Alexa for Business console using the credentials for the IAM user. If you signed up for AWS but have not created an IAM user for yourself, you can create one using the IAM console. For more information, see Creating an IAM User in Your AWS Account in the IAM User Guide.

By default, IAM users don't have permissions to manage Alexa for Business resources. You must use a customer managed policy that explicitly grants IAM users those permissions, and attach the policy to the specific IAM users or groups that require those permissions. For more information, see the following topics in the IAM User Guide:
- Managed Policies and Inline Policies
- Access Management

In alignment with standard security guidelines, we recommend that you create another IAM user for the Device Setup Tool. We recommend a separate user with only the necessary permissions for Alexa for Business. For more information, see Create an IAM User for Device Setup Tool (p. 9).
Firewall and Network Requirements

To join meetings and make calls from your Echo devices, you must have the following ports and protocols:

<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol</th>
<th>Destination Port</th>
<th>Transport</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signaling</td>
<td>HTTPS</td>
<td>443</td>
<td>TCP</td>
</tr>
<tr>
<td>Media port/connectivity negotiation</td>
<td>ICE/STUN/TURN</td>
<td>3478</td>
<td>TCP/UDP</td>
</tr>
</tbody>
</table>

**Note**

UDP is preferred. Only open TCP 3478 if UDP 3478 isn't allowed.

| Conference or PSTN calling audio | SRTP              | 49152 - 65535    | UDP       |

**Note**

G.711 audio codec

WPA2 Enterprise Prerequisite

If you plan to use WPA2 Enterprise Wi-Fi to set up your shared devices, you will specify this network security type later in the Device Setup Tool. For more information, see the section called “Run the Device Setup Tool” (p. 10). However, you must create a Private Certificate Authority (PCA) in AWS Certificate Manager (ACM). To do this, follow these steps:

1. Create a Private Certificate Authority and tag the CA with the following: Key=a4b, Value=enabled.
4. Import Your Private CA Certificate into ACM PCA.

AVS Permissions

To register an Alexa Voice Service (AVS) device with Alexa for Business, you must first give access to the Alexa built-in device maker. To do this, use the following steps to create an IAM role in the Alexa for Business console that allows the AVS device maker to register and manage devices with Alexa for Business on your behalf.

**To grant AVS permissions**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Settings, AVS permissions**.
3. From the **AVS device** maker drop-down menu, choose the device maker or **Other**.
4. Enter the **AVS device maker AWS account ID** and **Amazon ID** provided by the device maker.
5. Choose **Create IAM role**.
6. Make note of the **Role ARN** and **External ID** that are displayed. These must be entered in the device maker’s management tool. (The experience might be different across device makers.)
Getting Started with Shared Devices

After setting your IAM permissions, you can now get started with your shared devices. The following devices can be set up as shared devices:

- Echo (1st, 2nd, and 3rd generation)
- Echo Dot (2nd, 3rd, and 3rd generation with clock)
- Echo Plus (1st and 2nd generation)
- Polycom Trio 8500 and 8800
- Lifesize Icon 300, 500, and 700
- Amazon Chime on Dolby Voice Room

Tasks
- Get Recommended Hardware (p. 7)
- Prepare Your Devices (p. 7)
- Create Network Profile (p. 8)
- Import Your Devices (p. 8)
- Create an IAM User for Device Setup Tool (p. 9)
- Run the Device Setup Tool (p. 10)
- Create Room Profile, Skill Group, and Room (p. 10)

Get Recommended Hardware

We recommend that you obtain the following hardware to simplify the setup process:

- Label printer or other equipment to print asset or identification tags for your devices
- Power strips appropriately spaced for Echo or Echo Dot power adapters
- Extra power adapters
- Windows laptop or desktop with Wi-Fi controller

Note
The Device Setup Tool requires a Windows laptop. It doesn't work on any virtual desktop running in the cloud or on Apple hardware.

Prepare Your Devices

There are several tips for preparing your devices before setup:

- After you unpack a brand new device, keep the device connected for at least 15 minutes to download the latest firmware. If your device doesn't have the latest firmware, assigning the device to a room fails.
• As you unpack your devices, label them with the last three characters of the device serial numbers (DSN), printed on the box. DSNs are not printed on some devices, and clearly labeling them helps you track them during setup. You can also create asset tags that have the full DSNs and barcode on the label.

• You need to be within a certain distance of your devices, so we recommend that you use power strips and set them up on one or two long tables.

• If it’s the first time they’re turned on, the devices automatically enter setup mode. If the devices have been turned on previously, hold the action button on the top of the devices for 8 seconds until the light ring turns orange.

• If you are setting up hundreds of devices, leave the power cord for each Echo or Echo Dot plugged into the power strips and move the devices without power cords through your setup station.

Create Network Profile

To create, assign, and manage network settings for your shared Echo devices, see the section called “Managing Network Profiles” (p. 17). Network profiles enable you to manage wireless password rotations and enterprise certificate rotations.

Note
We recommend setting up your shared Echo devices on a dedicated network created for IoT devices.

Import Your Devices

Use the Alexa Companion app to set up your devices using your Amazon.com or Amazon Business account, then import your devices into Alexa for Business. Alternatively, you can create an IAM user for the Device Setup Tool provided by Alexa for Business, then use the Device Setup Tool to set up your devices. For more information, see Create an IAM User for Device Setup Tool (p. 9) and Run the Device Setup Tool (p. 10).

Note
If you need your devices to connect to WPA2 Enterprise Wi-Fi, you must use the Device Setup Tool.

Follow these steps to import your devices into Alexa for Business using the Alexa Companion app.

To import your devices

1. Sign in to the Alexa Companion app using your Amazon.com or Amazon Business account credentials.
2. Set up your devices by following the instructions in the Alexa Companion app.
3. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
5. Choose Import devices.
6. Sign in with the same Amazon.com or Amazon Business credentials that you used to sign in to the Alexa Companion app.
7. For Choose device(s), select the Echo devices to be imported in Alexa for Business, and choose Import.

We recommend associating the network profile with your corporate network credentials to the devices you just imported. For more information, see the section called “Managing Network Profiles” (p. 17).
After your devices are set up, they are listed on the Shared devices page of the Alexa for Business console.

Create an IAM User for Device Setup Tool

Before you can use the Device Setup Tool, you must create an IAM user for it.

To create an IAM user for the Device Setup Tool

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. Choose Users, Create new users.
3. Enter a user name (for example, DeviceSetupTool), and choose Programmatic access, Next.
4. Choose Attach existing policy directly, AlexaforBusinessDeviceSetup from the list, and Next.
5. (Optional) If you plan to use WPA2 Enterprise for the Network security type in the Device Setup Tool, attach the following custom policy for additional ACM PCA permissions:

   Note
   We recommend that you use scoped down permissions for specific CAs.

   ```json
   {
   "Version": "2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
   "Action": [
   "acm-pca:ListCertificateAuthorities"
   ],
   "Resource": "*"
   },
   {
   "Effect": "Allow",
   "Action": [
   "acm-pca:IssueCertificate",
   "acm-pca:GetCertificate"
   ],
   }
   ]
   }
   ```

   If you want don't want to be restricted to a specific PCA CA, attach the following policy:

   ```json
   {
   "Version": "2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
   "Action": [
   "acm-pca:ListCertificateAuthorities",
   "acm-pca:IssueCertificate",
   "acm-pca:GetCertificate"
   ],
   "Resource": "*"
   }
   ]
   }
   ```

6. Choose Create user.
7. Download and save the IAM access key and secret key. You need them later when you configure the Device Setup Tool.

Run the Device Setup Tool

After you create an IAM user for the Device Setup Tool, you can run the Device Setup Tool to set up your devices.

Follow these steps to run the Device Setup Tool on a Windows computer enabled with Wi-Fi.

To run the Device Setup Tool

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Shared devices.
3. Choose Set up devices.
4. On the Set up your Alexa devices page, choose the first button, Download and run Device Setup Tool.
5. Install and open the Device Setup Tool.
6. On the home page of the application, choose Get started.
7. Enter the Access key ID and Secret access key that you created for the Device Setup Tool user, and choose Next.
8. Select the network profile to associate with your devices, and choose Save.
   • For information about how to create a network profile, see Create Network Profile (p. 8).
9. After selecting the network profile and verifying the network configuration is accurate, choose Next.
10. Put your Alexa devices into setup mode by powering them on for the first time, or by holding the action button on the top of the Echo device.
11. From the Device setup home page, choose Start setup to scan for all Alexa devices in setup mode nearby and register them to your Alexa for Business organization.
   
   Note
   If you don't want to set up all Alexa devices in setup mode near your computer, choose Select devices and select from the list the devices to set up. To download a .csv file with the MAC address for your selected devices, choose Download MAC info.
12. Wait for the tool to complete. You can monitor progress in the tool to see which device is being set up, as well as the status of each device (Successful or Failed).
   
   Note
   After the status for a device changes to Successful, you can unplug the device even if the light ring is still orange. If all devices show as Failed, make sure that you have a strong connection to the network and that the Wi-Fi information is entered correctly.

After all of your devices have been set up, they are listed on the Shared devices page of the Alexa for Business console. To set up more devices, repeat steps 1–12 for the additional devices.

Create Room Profile, Skill Group, and Room

After you set up your devices with the Device Setup Tool, you are ready to create the following resources:

• A room (p. 12)
• A room profile (p. 13)
• A skill group (p. 22)
Managing Your Shared Devices

After you set up Alexa for Business, you can add, edit, or delete rooms, room profiles, shared devices, skills, and skill groups.

Tasks

• Managing Rooms (p. 12)
• Managing Room Profiles (p. 13)
• Managing Devices (p. 14)
• Managing Network Profiles (p. 17)
• Managing Skills (p. 18)
• Managing Skill Groups (p. 22)
• Sending Announcements (p. 23)

Managing Rooms

A room is a physical location where you can put your Alexa devices. Examples of rooms include conference rooms, lobbies, or hotel rooms.

We recommend naming your rooms with unique and meaningful identifiers that can be logically parsed by a third party. Instead of “Room 12” or “Suite 104,” pick a name like “ORD_01_0201” or “SEA_38_0021.” The ResolveRoom API action exposes the room name to third-party skill developers, including any skills that you develop privately for your organization.

To create a room

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Rooms, Create room.
3. For Name, enter a unique name.
4. For Profile name, select a room profile or choose Create room profile and choose Next.
5. (Optional) To add a skill group, select the check box next to the skill group to add and choose Next.
   Note
   You can assign a skill group to multiple rooms at once from the Skill group detail page.
6. (Optional) To add devices, select the check box next to the devices.
   Note
   You can also assign devices to a room from the Shared devices list view.
7. Choose Create room.

You can edit the name, description, and room profile of your room in the Rooms tab. You can also assign or unassign devices and skill groups in the same tab.

To edit a room

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Rooms and select the name of the room to edit.
3. Edit the Name, Description, or Room profile and choose Save.
4. Under Devices or Skill groups, choose Assign or Unassign.
If you no longer need a room, you can delete it. This stops the Alexa device in the room from responding to voice requests.

**To delete a room**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Rooms** and select the check box next to the room to delete.
3. Choose **Delete room, Delete**.

After your room is deleted, your Alexa devices are automatically unassigned and can be assigned to a different room. For more information, see Managing Devices (p. 14).

Echo, Echo Dot, and Echo Plus devices use on-device keyword spotting to detect a wake word. When they detect a wake word, the light ring around the top of the device turns blue to indicate that Alexa is streaming audio to the cloud. These voice recordings are anonymously stored in the cloud. You can’t view or listen to the interactions that users have with the Alexa devices in a room. You can choose to delete voice recordings from all of the devices in a specific room. If you delete these recordings, it might degrade your experience using voice features.

**To delete voice recordings**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Rooms** and select a room.
3. Choose **Delete voice recordings, Delete**.

   **Note**
   You can also ask Alexa to delete voice recordings for a particular device by saying “Alexa, delete what I just said” or “Alexa, delete what I said today”.

---

**Managing Room Profiles**

To simplify the process of creating and managing rooms, first define room profiles. A room profile contains the settings for your Alexa devices, so that they can provide you with weather, time, and other location-based information. For example, you can create a room profile that contains the Alexa settings that apply to all rooms in the same building.

If you want to offer room booking to your users, Alexa searches all rooms in a room profile when receiving requests like “Alexa, find a room.” To optimize room searching, you can create a room profile that contains all rooms in the same building, or on the same floor (depending on your office size).

When you create a room, you must select a room profile. If you have not created one, a default room profile is provided. You can modify the settings, including the default room profile, at any time.

**To create a room profile**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Room profiles, Create room profile**.
3. Fill in the following fields:
   - **Profile name** – Enter a unique name for the room profile. (Required)
   - **Location** – Enter the physical address of the building. (Required)
   - **Time zone** – Select the time zone for the room profile. (Required)
   - **Wake word** – Select the voice command that turns on the device.
   - **Temperature units** – Choose Fahrenheit or Celsius.
 Managing Devices

You can set up your Alexa devices (Amazon Echo, Echo Dot, or Echo Plus) using the Device Setup Tool. This connects your device to your Wi-Fi network and registers it with Alexa for Business. You can also use the Alexa Companion app to set up your devices using your Amazon.com or Amazon Business account, then import your devices into Alexa for Business. For more information, see Import Your Devices (p. 8).

After you set up your devices, you can assign them to your rooms.

Note
You need a Windows computer to use the Device Setup Tool. You cannot run the Device Setup Tool on any cloud-based, Windows streaming tool, such as Amazon WorkSpaces, or any imaged driver such as Boot Camp.

To set up your devices using the Device Setup Tool
1. If you haven't already, install the Device Setup Tool. For more information, see Run the Device Setup Tool (p. 10).
2. Note the last three characters of the device service number (DSN), printed on the box. These characters are included in the Wi-Fi network that the device broadcasts while you are setting it up. They are required when you assign your device to a room.
3. Plug your device into a power outlet, and press and hold the **Action** button (white dot) for five seconds. Wait until the device tells you that it is ready and the light ring turns orange.

   **Note**
   If the device has already been set up before, you can manually enter setup mode by pressing and holding the **Action** button for 7 seconds.

4. Open the Device Setup Tool, which discovers your device.

   **Note**
   If the Device Setup Tool doesn’t discover your devices, choose **Start setup**.

5. Select the network profile to associate with your devices, and choose **Save**.
   - For information about how to create a network profile, see the section called "Managing Network Profiles" (p. 17).
   - After selecting the network profile and verifying the network configuration is accurate, choose **Next**.

6. Put your Alexa devices into setup mode by powering them on for the first time, or by holding the action button on the top of the Echo device.

7. From the Device setup home page, choose **Start setup** to scan for all Alexa devices in setup mode nearby and register them to your Alexa for Business organization.

   **Note**
   If you don’t want to set up all Alexa devices in setup mode near your computer, choose **Select devices** and select from the list the devices to set up. To download a .csv file with the MAC address for your selected devices, choose **Download MAC info**.

9. Wait for the tool to complete. You can monitor progress in the tool to see which device is being set up, as well as the status of each device (Successful or Failed).

   **Note**
   After the status for a device changes to Successful, you can unplug the device even if the light ring is still orange. If all devices show as Failed, make sure that you have a strong connection to the network and that the Wi-Fi information is entered correctly.

The Device Setup Tool connects your devices to your Wi-Fi network and registers them with Alexa for Business. For information about how to create a network profile, see Managing Network Profiles (p. 17).

**To assign devices to a room**

1. Open the Alexa for Business console at [https://console.aws.amazon.com/a4b/](https://console.aws.amazon.com/a4b/).
2. Choose **Shared devices** and select the check box next to the devices to assign to a room.
3. Choose **Assign to room**, and choose the room to which to assign the devices.
4. Unplug the device and plug it back in to restart it.

   We recommend that you label the devices with the room to help ensure that the device remains in the correct room. To move devices from one room to another, unassign and then re-assign the devices.

**To view device information**

1. Open the Alexa for Business console at [https://console.aws.amazon.com/a4b/](https://console.aws.amazon.com/a4b/).
2. Choose **Shared devices** to see a list of your registered devices and the following information for each device:
   - **Serial number** – The serial number of the device.
   - **Type** – The type of device.
   - **Device name** – The name of the device.
• **Assigned room** – The room to which the device is assigned.
• **Status** – The status of the device, including the network connection status of the skills and settings being applied to the device.
  - **Synced** – All skills and settings are applied to the device.
  - **In progress** – The device is connected to the network, and Alexa for Business is applying skills and settings to the device.
  - **Failed** – The device could not be sync. For more information, check the **Failure** column.
  - **Deregistered** – This device has been factory reset, or put into device setup mode and not set up properly. Please set up this device again using the **Device Setup Tool**.

Alexa for Business publishes the number of your shared devices online, offline, and deregistered to Amazon CloudWatch as metrics. These metrics are inside the namespace **AWS/A4B**. The metric names are **OnlineSharedDevices**, **OfflineSharedDevices**, and **DeregisteredSharedDevices**. All of these metrics can be grouped by the metric dimensions **Room Profile** or **Organization**.

**Note**
Viewing **AWS/A4B** metrics by **Room Profile** filters out devices in your organization that aren't assigned to a room. It also allows you to filter results for a specific building with offline devices.

**To monitor devices using CloudWatch**
1. Follow the steps in View Available Metrics in the **Amazon CloudWatch User Guide**. Instead of choosing the namespace **EC2**, choose the namespace **AWS/A4B**, and then choose a metric dimension (**Organization** or **Room Profile**).
2. To set up alarms from CloudWatch when a critical number of devices go offline, follow these steps:
   1. Graph the metric. For more information, see Graph a Metric.
   2. Create an alarm. For more information, see Create an Alarm from a Metric on a Graph.

**To delete a device**
1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Shared devices** and select the check box next to the device to deregister.
3. Choose **Actions, Delete Devices**.

   **Note**
   This action removes the device from the console.

You can reset a device to clear all timers, alarms, to-do lists, shopping lists, and Bluetooth-connected phones for a device. This also sets the volume to 5 for a shared device.

**To reset a device**
1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Shared devices** and select the devices to reset.
3. Choose **Actions, Reset device**.

Alexa for Business manages device accounts and settings through rooms and room profiles. When you add devices to a room, change the room of a device, update specific settings in a room profile (including the wake word, volume limit, and device setup mode), or when you reset a device, the device must be connected to the internet for the update to complete successfully. Alexa for Business retries these calls for one hour, and then the device is placed into a **Sync needed** status. To implement your changes, plug in the Alexa device, ensure that it's connected to Wi-Fi, and sync the device.
Managing Network Profiles

To simplify the process of creating and managing network configurations, you can define network profiles. Network profiles are associated with devices and consist of network configuration settings, including the SSID, network security type, network credentials, and description. When you make a change to the network profile, the changes are applied to all shared devices associated with that profile. If your shared devices are set up on a closed network, you can use network profiles for password rotation. If your shared devices are set up on a WPA2 enterprise network, you can also use enterprise certificate rotation.

When you set up a device using the device setup tool, you must first select a network profile to associate devices to. If the device was set up using Import Devices, you can associate the existing device to a network profile.

To create a network profile

1. Make sure that you have the AlexaForBusinessFullAccess policy attached to your IAM user account. For more information, see Adding IAM Identity Permissions (Console).
2. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
3. Choose Network profiles, Create network profile.
4. Fill in the following fields:
   - **Network SSID** – The name of the network SSID. (Required)
   - **Description** – The description of your network profile. This information helps you identify your network configuration if you have multiple network profiles.
   - **Network security type** – The type of security that is used for your network. From the drop-down menu, choose from one of the following options:
     - Open
     - WEP
     - WPA Personal
     - WPA2 Personal
     - WPA2 Enterprise
   - For password-based networks (WEP, WPA Personal, and WPA2 Personal):
     - **Current password** – The current password of the network. (Required)
     - **Next password** – The next password of the network.

   **Note**
   When you create a network profile for a password-based Wi-Fi network, Alexa for Business stores your passwords in AWS Secrets Manager and asynchronously transmits the network profile details to associated devices. To rotate the wireless password for the network associated with your shared Echo devices, use and update the Next password field. After the passwords are successfully transmitted to the device, the sync status for those devices changes to Synced. You can then change the password of your network, and devices will continue to work with the new password.
5. If you chose WPA2 Enterprise, complete the following steps. Otherwise, skip these steps.
1. From the drop-down menus, select the EAP method and AWS certificate authority that you created earlier, and choose Next.

   **Note**
   Certificate changes for the WPA2_Enterprise network profile, including CA ARN and root certificate changes, are transmitted asynchronously to the devices.

2. On the Add root certificate page to set up the Authentication Server Trust, provide the root certificate of your authentication server (RADIUS). This certificate is installed on your devices and used to trust your authentication server during EAP negotiation. Select the certificate from a file on disk or paste it from your clipboard. The certificate must be in PEM format. When you're done, choose Save.

6. Select devices to associate with the network profile (optional), and then choose Create.

You can edit the room's name, description, and profile in **Network profile**.

**To edit a network profile**

1. Open the Alexa for Business console at [https://console.aws.amazon.com/a4b/](https://console.aws.amazon.com/a4b/).
2. Choose Network profiles and choose the name of the network profile to edit.
3. Edit any of the fields and choose Save.

**To assign devices to a network profile**

1. Open the Alexa for Business console at [https://console.aws.amazon.com/a4b/](https://console.aws.amazon.com/a4b/).
2. Choose Network profiles and choose the name of the network profile to associate devices to.
3. Review the network profile details. Choose Associate a device, and choose the devices to associate the network profile to.

**To delete a network profile**

1. Open the Alexa for Business console at [https://console.aws.amazon.com/a4b/](https://console.aws.amazon.com/a4b/).
2. Choose Network profiles.
3. Select the check box next to the network profile to delete.
4. Choose Delete network profile, Delete.

   **Note**
   You can delete a network profile only if no devices are associated to it.

---

**Managing Skills**

Skills are voice-driven capabilities that enhance the functionality of your Alexa device. Alexa for Business gives you access to all Alexa skills. To enable skills for your devices, you must first enable it for your organization and then add it to one or more skill groups that are assigned to your rooms. For more information, see Managing Skill Groups (p. 22).

**To enable a skill**

1. Open the Alexa for Business console at [https://console.aws.amazon.com/a4b/](https://console.aws.amazon.com/a4b/).
2. Choose Skills, Alexa Skills store.
3. Find the skill to add by browsing the list of available skills, filtering by category, or searching by keyword. You can get more details about the skill and how to add it in the skill details.
4. Choose **Enable skill**.
5. If the skill requires it, link your master account by following the account linking steps. When you are done, you receive a success message in the console.
6. If the skill supports it, optionally enable permissions by choosing **Allow** next to each permission and choose **Save**.
7. Choose **Enabled skills**, select the check box next to the skill that you just added, and choose **Add to skill group**.
8. Select the check box next to the skill group to which to add the skill, and choose **Add**.

The skill is enabled on all Alexa devices associated with the skill group.

**Note**
If there are a large number of rooms associated with the same skill group, this step might take up to five minutes.

**To change permissions for a skill**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Skills** and select the skill name.
3. In the upper-right corner, choose **Change permissions**.
4. Choose **Allow** next to each permission to enable it, and then choose **Save**.

**Note**
The permission given is at the skill level. It applies to all shared devices with that skill enabled in your organization. The permission setting doesn’t impact the permissions of your enrolled users. Users must select the permission for themselves in the Alexa companion app. For more information, see **Enable Alexa Skills**.

**To remove a skill**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Skills**.
3. Choose **Disable** next to the skill that you want to remove, then choose **Disable**.

**To link a master account to a skill**

Some skills require the ability to connect with a user in another system. This is called account linking, which links an Alexa for Business account to a user account in another system.

When you add a skill that requires account linking, you are prompted to open the sign-in page of the skill provider and sign in with your user account. After you successfully sign in, Alexa obtains an access token that uniquely identifies the user within the system. Alexa for Business applies this token to all devices that receive your skill by default, making this your master account. Alexa stores this token and includes it in requests sent to the skill provider when the skill is invoked.

If you want to link a unique account for the devices in a specific room, you can override the linked account. For example, to use some smart home skill to control the lights in your conference room, you must link to the user account for that room in the smart home system.

**To link a skill to a room**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Rooms** and select a room.
3. In the **Skills** table, choose **Link account to this room, Link**.
4. Follow the skill account linking steps.

On the **Room details** page, there are optional and required actions available in the **Skill configuration** column, depending on skill type and account linking status:

<table>
<thead>
<tr>
<th>Account linking status/skill type</th>
<th>Master account linked</th>
<th>Account linked to room</th>
<th>No account linking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom skill</td>
<td>Link account to this room</td>
<td>Revert to master account</td>
<td>No action</td>
</tr>
<tr>
<td>Smart home skill</td>
<td>Require scope or link account to this room</td>
<td>Revert to master account and require scope</td>
<td>N/A</td>
</tr>
<tr>
<td>Private skill</td>
<td>Optional skill parameters</td>
<td>Optional skill parameters</td>
<td>Optional skill parameters</td>
</tr>
<tr>
<td></td>
<td>Link account to this room</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**To configure the scope of a smart home skill**

*Note*
Not all smart home skills use scope. Check with the skill developer to see if they do, and if so, what the value should be.

1. Open the Alexa for Business console at [https://console.aws.amazon.com/a4b/](https://console.aws.amazon.com/a4b/).
2. Choose **Rooms** and select a room.
3. In the **Skills** table, choose the edit icon next to the text field and enter the scope for a smart home with a master account skill linked.
4. Choose **Save**.

**To configure a skill parameter of a private skill**

*Note*
Not all private skills call into Alexa for Business to use the scope. Check with the skill developer to determine if this value is needed, and if so, what it should be.

1. Open the Alexa for Business console at [https://console.aws.amazon.com/a4b/](https://console.aws.amazon.com/a4b/).
2. Choose **Rooms** and select a room.
3. In the **Skills** table, choose the edit icon next to the text field and enter the skill parameter value.
4. Choose **Save**.

**Private Skills**

In addition to public Alexa skills, developers can use the Alexa Skills Kit to create and publish skills privately to Alexa for Business organizations. This way, developers do not need to certify or have the skill available with all other Alexa skills.

Public and private skills share many of the same features. They are both developed in the same way using the Alexa Skills Kit, and they can both use account linking to map users to a back-end system.
There are, however, areas where private skills are different from public skills. When considering whether to make a skill public or private, refer to the list below.

A private skill has the following characteristics:

- The skill isn’t discoverable in the public Alexa Skills Store.
- The skill developer can whitelist which organizations can review the skill, including its description and functionality, as well as enable it.
- The skill developer can control which organizations can enable the private skill and therefore limit attempts to authenticate against back-end systems for account linking.
- The skill does not need to go through Amazon’s certification process for public skill publishing and for every skill change. For more information on public skill certification, see Certification Requirements for Custom Skills.
- The IT admin has additional control to review and enable the skill for the organization through the AWS console.
- The IT admin can use Alexa for Business to control whether enrolled users can view and enable a private skill.

If the skill is intended for a limited audience, such as your organization or partner organizations, it’s a good candidate for a private skill.

To create private skills with the Alexa Skills Kit

- For information about how to create private skills with the Alexa Skills Kit, see Build Skills with the Alexa Skills Kit.

  Note
  If you are building a private skill and want to use any information from a shared device that requires permission, follow the instructions in the Alexa Skills Kit. For more information, see Permissions.

To publish private skills created with the Alexa Skills Kit

- There are two ways you can publish private skills created with the Alexa Skills Kit:
  - If you are publishing a single skill, we recommend that you use the developer console beta. For more information, see Create and Publish Private Skills (Developer Console Beta).
  - If you want to automate the creation of private skills, you can use the ASK CLI. For more information, see Create and Publish Private Skills (ASK CLI).

To manage private skills created with the Alexa Skills Kit

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Skills, Private skills.
3. In the list, select the skill that was published to your account and choose Review.

  Note
  It takes about 20 minutes after publishing for a skill to appear in this list.
4. To enable the skill for your Alexa for Business organization, choose Enable.
5. To enable the skill for your Alexa devices, choose Enabled skills, select the check box next to the skill that you added, and choose Add to skill group.
6. To make the skill available for end users to discover and enable, choose Private skills and select the Available to users check box.
Alexa for Business Blueprints

Any member of an Alexa for Business organization can publish private business skills to your organization within minutes using Alexa for Business Blueprints. After a user builds a blueprint, you can review and publish the skill to use across your company with any Alexa-enabled device. There are two blueprints designed specifically for business use. The **Business Q&A** blueprint is a template that users can customize with their own questions and answers related to your organization. The **Onboard Guide** blueprint helps new employees get up to speed in their new roles with specialized how-to questions about the team and the office. For more information about how to use Alexa for Business Blueprints, see Create Alexa Experiences for Your Organization.

**To create and publish private skills with Alexa for Business Blueprints**

1. Invite your employees to create blueprint skills:
   1. Open the Alexa for Business console at [https://console.aws.amazon.com/a4b/](https://console.aws.amazon.com/a4b/).
   2. From the dashboard, under **Create Alexa Skills**, choose **send an email**.
   3. Edit the email as needed and send it to your employees.
2. A member of your organization creates and publishes a blueprint skill for your review. For more information about to do this, go to the Blueprints website, and choose **Help Center**, Publish to Alexa for Business.
3. Review and enable the blueprint skill:
   1. Open the Alexa for Business console at [https://console.aws.amazon.com/a4b/](https://console.aws.amazon.com/a4b/).
   2. Choose **Skills**, Private skills, and find the skill submitted by the user.
   3. Choose **Review** to review the skill, and then choose **Enable** to enable it. You can add the skill to skill groups to enable it in the desired rooms. Optionally, you can select the check-box to make the skill available to your organization’s enrolled users, who can then use the Alexa app to enable the skill in their account.

As an administrator, you can also create and publish skills with blueprints. Follow the previous steps in this section.

**Managing Skill Groups**

Skill groups are collections of skills that Alexa for Business uses to enable skills on the Alexa devices in your rooms. For example, you can define a skill group with all the skills for your conference rooms. When you assign an Alexa device to a room, Alexa for Business enables the skills in the skill groups assigned to the room.

You can add skills to your skill groups at any time, and Alexa for Business automatically enables them on the Alexa devices. To enable skills for a device in a room, you must first add them to a skill group, then assign that skill group to a room or group of rooms.

You can also remove a skill group from one or more rooms, or delete it.

**To create a skill group**

1. Open the Alexa for Business console at [https://console.aws.amazon.com/a4b/](https://console.aws.amazon.com/a4b/).
2. Choose **Skill groups**, Create skill group.
3. For **Name and Description**, enter unique values and choose Create.
4. To add skills, select the group, choose **Add skills to group**, and then select the skills to add.
You can now assign the skill group to your rooms.

**To add or remove skills for an existing skill group**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Skill groups**.
3. In the **Name** column, choose the name of the skill group to edit.
4. Under **Skills**, select the check box next to the skill to edit, and choose **Add skills** or **Remove skills**.

**To assign a skill group to one or more rooms**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Skill groups**.
3. In the **Name** column, choose the name of the skill group to assign.
4. Under **Assigned rooms**, select the check boxes next to the rooms to which to assign the skill group, and choose **Assign to room**, **Assign**.

**To unassign a skill group from one or more rooms**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Skill groups**.
3. In the **Name** column, choose the name of the skill group to unassign.
4. Under **Assigned rooms**, select the check boxes next to the rooms from which to unassign the skill group, and choose **Unassign from room**, **Unassign**.

**To delete a skill group**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Skill groups**.
3. Select the check box next to the skill group to delete, and choose **Delete skill group**, **Delete**.

---

**Sending Announcements**

You can send Alexa announcements to one or more rooms in your Alexa for Business organization. When you do this, Alexa wakes and speaks the announcement that you enter, for the rooms that you select.

You can create an announcement from the Alexa for Business console, or with the SendAnnouncement API. For more information, see the [Alexa for Business API Reference](https://docs.aws.amazon.com/alexaforbusiness/latest/DeveloperGuide/). The API allows developers to trigger a text or audio announcement on Alexa for Business-managed endpoints from any app. For example, when a threshold is reached on an IoT sensor, send an alert to the shared devices in an operations team area. Or, you can turn your Alexa for Business deployment into a PA system.

**Note**

Systems using the API need IAM permissions.

Use the following steps to create an announcement from the console. Also use these steps with the API, to test how the announcement sounds, or to make sure it reaches the correct rooms.

**To send or test an announcement from the console**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Announcements**, **Create announcement**.

---
3. On the **Write message** page, next to **Message text**, enter a message for Alexa to announce. Choose **Next**.

   **Note**
   There is a maximum of 250 characters.

4. On the **Select rooms** page, choose one of the following options from the **Room selection** drop-down menu:
   - **Manual selection** - Select one room from a list of all your rooms. You can filter by **Room name** and **Profile**. This option is good for testing an announcement. You can send it to one room while sitting in that room, to hear how it sounds.
   - **Room ARN** - Enter the ARN of the room or rooms, separated by commas or line breaks. You can call an API to retrieve room ARNs.
   - **Room profile** - Select the name of the room profile and review the list of rooms.
   - **Room name filter** - Enter an exact room name, or the prefix of multiple rooms. For example, enter **Room** to see Room1 and Room2.
   - **All rooms** - Select all the rooms in your organization.

5. Choose **Send announcement**.

   **Note**
   Alexa doesn't proactively listen for requests after making the announcement. After hearing an announcement, users must say the wake word to make Alexa requests.
Managing Alexa in Meeting Rooms

Alexa for Business simplifies meeting room experiences for your employees. Alexa enables you to simplify day-to-day tasks, build a smarter workplace, and offer a differentiated employee experience. You can control conferencing systems, check room availability, and book rooms with just your voice. For example, say “Alexa, join my meeting” and Alexa finds the upcoming meeting from the calendar, turns on the display, and connects you to the meeting. Alexa for Business integrates with popular video conferencing devices, room control systems, meeting room scheduling solutions, and calendar systems. You can also use Alexa for Business in your meeting rooms to offer your employees a natural interface to report service and equipment issues, answer frequently asked questions, and provide a company news briefing by building private skills.

Tasks
- Available Alexa commands in Meeting Rooms (p. 25)
- Link Alexa for Business to Your Calendar System (p. 27)
- Control Conferencing Systems (p. 32)
- Configure Meeting Room Settings (p. 55)
- View Room Utilization Metrics (p. 56)

Available Alexa commands in Meeting Rooms

Alexa for Business simplifies meeting room experiences and lets your users interact with meeting rooms by using their voice.

The following table shows an overview of commands that you can ask Alexa in meeting rooms.

<p>|</p>
<table>
<thead>
<tr>
<th>You can say...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Alexa, is this room available?”</td>
<td>Check room availability</td>
</tr>
<tr>
<td>“Alexa, is this room free?”</td>
<td></td>
</tr>
<tr>
<td>“Alexa, is the room booked at 4 PM?”</td>
<td></td>
</tr>
<tr>
<td>“Alexa, is this room free for 30 minutes?”</td>
<td>Check room availability for a specific duration</td>
</tr>
<tr>
<td>“Alexa, is this room free at 10 AM?”</td>
<td>Check room availability for a specific time</td>
</tr>
<tr>
<td>“Alexa, who booked this room?”</td>
<td>Find out who reserved room</td>
</tr>
<tr>
<td>“Alexa, who booked this room at 2 PM?”</td>
<td></td>
</tr>
<tr>
<td>“Alexa, book this room for 30 minutes”</td>
<td>Make an instant booking</td>
</tr>
<tr>
<td>“Alexa, book this room at 2 PM for 60 minutes”</td>
<td></td>
</tr>
<tr>
<td>“Alexa, reserve this room until 1 PM”</td>
<td></td>
</tr>
<tr>
<td>“Alexa, extend the meeting”</td>
<td>Extend a room reservation</td>
</tr>
<tr>
<td>“Alexa, extend the meeting by half an hour”</td>
<td></td>
</tr>
<tr>
<td>“Alexa, extend the meeting for 15 minutes”</td>
<td></td>
</tr>
<tr>
<td>“Alexa, when is the next meeting?”</td>
<td>Find the next reservation</td>
</tr>
<tr>
<td>“Alexa, find me a room”</td>
<td>Find an available room</td>
</tr>
<tr>
<td>Available Alexa commands in Meeting Rooms</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>

**You can say...** | **To do this...** |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>“Alexa, find a room for an hour”  “Alexa, find a room at noon”</td>
<td></td>
</tr>
<tr>
<td>“Alexa, join my meeting”  “Alexa, start my meeting”</td>
<td>Join your unscheduled or scheduled meeting</td>
</tr>
<tr>
<td>“Alexa, end the meeting”  “Alexa, hang up”</td>
<td>Leave a meeting</td>
</tr>
<tr>
<td>“Alexa, call 855-255-8888”  “Alexa, call 88000”</td>
<td>Dial phone numbers</td>
</tr>
<tr>
<td>“Alexa, call [contact name]”</td>
<td>Call contacts</td>
</tr>
<tr>
<td>“Alexa, redial”</td>
<td>Redial</td>
</tr>
<tr>
<td>“Alexa, answer”  “Alexa, decline”</td>
<td>Answer or decline an incoming call</td>
</tr>
<tr>
<td><strong>Note</strong> This is only available on third-party conferencing devices that have implemented Alexa Voice Service.</td>
<td></td>
</tr>
<tr>
<td>“Alexa, end the call”</td>
<td>End a call</td>
</tr>
<tr>
<td>“Alexa, press 123#”  “Alexa, enter *7”</td>
<td>Send digits</td>
</tr>
<tr>
<td>“Alexa, increase volume”  “Alexa, lower volume”</td>
<td>Control the volume</td>
</tr>
<tr>
<td>“Alexa, turn on lights”  “Alexa, turn off lights”  “Alexa, dim the lights”</td>
<td>Control smart devices</td>
</tr>
<tr>
<td>“Alexa, ask &lt;company&gt; for the Wi-Fi password?”</td>
<td>Access company FAQs using Blueprints or private skills</td>
</tr>
<tr>
<td>“Alexa, ask &lt;company&gt; to report an issue.”</td>
<td>Report service issues</td>
</tr>
<tr>
<td>“Alexa, ask &lt;company&gt; for latest news.”</td>
<td>Hear company flash briefings</td>
</tr>
</tbody>
</table>

**Available commands during active calls**

| “Alexa, end the call” | End a call |
| “Alexa, hang up”  “Alexa, end the meeting” | |
| “Alexa, press 123#”  “Alexa, enter *7” | Send digits |
You can say... | To do this...
---|---
“Alexa, increase volume” | Control the volume
“Alexa, lower volume” | 
"Alexa, check in" | Check into a meeting reservation

### Link Alexa for Business to Your Calendar System

You can link Alexa for Business to your Microsoft Exchange, Office 365, or Google G-Suite calendar system and associate a calendar resource to the room you created in Alexa for Business. The calendar integration enables users to join meetings in the room, check whether the room is available, and book the room for an ad hoc meeting by asking Alexa.

#### Tasks
- Link Alexa for Business to Office 365 (p. 27)
- Link Alexa for Business to Google G Suite (p. 29)
- Link Alexa for Business to Microsoft Exchange (p. 30)

### Link Alexa for Business to Office 365

There are two methods to link Alexa for Business to your Office 365 account.

Use Method 1 to link your Office 365 account by using a service account that has permissions to read and write to your room calendars. This method provides you with more control over the calendar resources that Alexa for Business can access.

Use Method 2 to use application permissions and set up the calendar only once. Then you won't need to update permissions when you add Alexa to more rooms. You must sign in as a global administrator user to link your Office 365 account to Alexa for Business.

**Note**

If your organization has set up Microsoft Azure AD conditional access policies, you might need to allow the Alexa for Business client app to access data in your Microsoft Office tenant. For more information about managing conditional access policies, see What are conditions in Azure Active Directory conditional access?

#### Method 1: Link with Delegate Permissions (Recommended)

**To link with delegate permissions**

1. Create a service account for Alexa for Business in your Office 365 tenant:
   1. Sign into Office 365 as an administrator.
   2. Add a user in your Office 365 account that will use a service account. For more information, see Add users individually or in bulk to Office 365.

      For example, if your domain is "mycompany.com" and you add a user with the user name of "alexaforbusiness," the email address is "alexaforbusiness@mycompany.com".

2. Open PowerShell and connect to Exchange Online. For more information, see Connect to Exchange Online PowerShell.
3. Run the following PowerShell command to create a service account with access to the calendars in your organization:
New-Mailbox -UserPrincipalName alexaforbusiness@<your_domain> -Alias "AlexaforBusiness" -Name alexaforbusiness -FirstName Alexa -LastName "Service Account" -DisplayName "Alexa for Business Service Account"

**Note**
Make sure that "your_domain" is the domain of your organization, and enter your password when prompted.

4. To look up meeting dial-in information from your resource mailboxes, configure them to include descriptions. Run one of the following commands to keep the descriptions in the meeting invites of your resource mailboxes:

For a single room mailbox:

```powershell
Set-CalendarProcessing "<room name>" -DeleteComments $FALSE
```

For all room mailboxes:

```powershell
Get-Mailbox -ResultSize unlimited -RecipientTypeDetails "RoomMailbox" | Set-CalendarProcessing -DeleteComments $FALSE
```

5. Run one of the following commands to give the service account permissions to access the room calendars in your organization:

For a single room mailbox:

```powershell
Add-MailboxFolderPermission <room name>:\Calendar -User alexaforbusiness -AccessRights Editor
```

For all room mailboxes:

```powershell
Get-Mailbox -ResultSize unlimited -RecipientTypeDetails "RoomMailbox" | ForEach-Object {Add-MailboxFolderPermission $_":\calendar" -user alexaforbusiness -AccessRights Editor}
```

6. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.

7. Choose **Calendar, Office 365**.

8. Choose **Service account using delegate access** and **Link account**, sign in with the service account you created in step 4, and accept the user consent.

Now you can associate the email address of your resource mailboxes with your rooms in Alexa for Business.

**To complete room setup**

1. Associate the email address of your resource mailboxes in Office 365 to your Alexa for Business rooms.

   1. In the Alexa for Business console, choose **Rooms** and choose the room to which to add the email address.
   2. Choose **Edit** and enter the email address of your resource mailbox to associate to the Alexa for Business room.
   3. Choose **Save**.

2. Test the calendar integration.

   1. Create a new meeting invite in your Microsoft Outlook client.
   2. Add the room as the resource, add meeting dial-in information to your meeting invite, and send the invite to book the room.
3. Say “Alexa, start my meeting” to the Echo device assigned to the room. Your Echo device automatically dials into your meeting without prompting you for a meeting ID.
4. To test room booking, say “Alexa, is this room free?” to the Echo device in the room.

### Method 2: Link with Application Permissions

#### To link with application permissions

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Calendar, Office 365.
3. Choose Application permissions and Link account, then sign in with the Office 365 account that belongs to the Global Administrators group.
4. Give consent that Alexa for Business has read and write access to the calendars in your Office 365 organization.

#### To complete room setup

1. Associate the email address of your resource mailboxes in Office 365 to your Alexa for Business rooms.
   1. In the Alexa for Business console, choose Rooms and choose the room to which to add the email address.
   2. Choose Edit and enter the email address of your resource mailbox to associate to the Alexa for Business room.
   3. Choose Save.
2. Test the calendar integration.
   1. Create a new meeting invite in your Microsoft Outlook client.
   2. Add the room as the resource, add meeting dial-in information to your meeting invite, and send the invite to book the room.
   3. Say “Alexa, start my meeting” to the Echo device assigned to the room.

Your Echo device automatically dials into your meeting without prompting you for a meeting ID.

### Link Alexa for Business to Google G Suite

The following versions of G Suite are supported:

- G Suite Basic
- G Suite Business
- G Suite Enterprise
- G Suite for Education

**Note**

If you already linked your account and want to enable room booking, you must re-link it.

#### To link Alexa for Business to Google G Suite

1. Make sure that you have a super administrator account and have enabled API access in the Google Admin console. For more information, see Enable API access in the Admin console.
2. Link Alexa for Business to Google G Suite using your administrator account.
a. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
b. Choose Calendar, G Suite.
c. Choose Link account and sign in with an account that has super administrator privileges.
d. Give consent that Alexa for Business has manage permissions to the calendars in your G Suite organization.

3. Create a new meeting invite in your G Suite client.
4. Add the room as the resource, add meeting dial-in information to your meeting invite, and send the invite to book the room.
5. Associate the email address of your resource mailboxes in G Suite to your Alexa for Business rooms.
   1. In the Alexa for Business console, choose Rooms and choose the room to which to add the email address.
   2. Choose Edit and enter the email address of your resource mailbox to associate to the Alexa for Business room.
   3. Choose Save.
6. Say "Alexa, start the meeting" to the Echo device assigned to the room. Your Echo device automatically dials into your meeting without prompting you for a meeting ID.
7. To test room booking, say "Alexa, is this room free?" to the Echo device in the room. Your Echo device returns that the room is booked.

**Link Alexa for Business to Microsoft Exchange**

To link Alexa for Business to Microsoft Exchange

1. Before you proceed, confirm that you meet the following requirements:
   • You have an administrator account within your Microsoft Exchange server.
   • Microsoft Exchange is version 2013.
   • You have a valid Exchange Web Services (EWS) endpoint with a valid digital certificate purchased from a trusted public certificate authority (CA).
   • You have basic authentication enabled on your Exchange Web Servers (EWS) endpoint.
2. Verify that basic authentication is enabled:
   1. Open Microsoft Exchange Management Shell.
   2. Type `Get-WebServicesVirtualDirectory | fl`.  
   3. Verify that the parameter `BasicAuthentication` is set to `True`.
3. If basic authentication isn't enabled, run the following command to enable it:

   ```powershell
   Set-WebServicesVirtualDirectory -Identity "Contoso\EWS(Default Web Site)" -BasicAuthentication $true
   ```

   **Note**
   Contoso\EWS(Default Web Site) is the identity of the Microsoft Exchange Web Services virtual directory.
4. Create a service account with access to the calendars in your organization.
   a. Open the Exchange Management Shell.
   b. Run the following command to create the service account.

   ```powershell
   New-Mailbox -UserPrincipalName alexaforbusiness@your_domain -Alias Alexa for Business -Name alexaforbusiness -OrganizationalUnit Users -FirstName"
Alexa -LastName Service Account -DisplayName "Alexa for Business Service Account"

**Note**
Make sure that your_domain is the domain of your organization. You are prompted to enter a password.

5. To look up meeting dial-in information from your resource mailboxes, configure them to include descriptions:
   - Run one of the following commands to keep the descriptions in the meeting invites of your resource mailboxes:
     - For a single room mailbox:
       ```powershell
       Set-CalendarProcessing <room name> -DeleteComments $FALSE
       ```
     - For all room mailboxes:
       ```powershell
       Get-Mailbox -ResultSize unlimited -RecipientTypeDetails 'RoomMailbox' | Set-CalendarProcessing -DeleteComments $FALSE
       ```

6. Set up permissions. The service account must have permissions to access the room calendars in your organization. Run one of the following commands to give the service account access to your room resource mailboxes:
   - For a single room mailbox:
     ```powershell
     Add-MailboxFolderPermission <room name>:\Calendar -User alexaforbusiness -AccessRights Editor
     ```
   - For all room mailboxes:
     ```powershell
     Get-Mailbox -ResultSize unlimited -RecipientTypeDetails 'RoomMailbox' | ForEach-Object {Add-MailboxFolderPermission $_":\calendar" -user alexaforbusiness -AccessRights Editor}
     ```

7. Link the service account to Alexa for Business.
   - Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
   - Choose Calendar, Microsoft Exchange.
   - Enter the user principal name (UPN) of your service account.
   - Enter the service account password.
   - Enter the URL of your EWS endpoint. The default URL for EWS is usually in the following format: https://mail.domain.com/EWS/Exchange.asmx.
   - For Access method, select Delegation.
   - Choose Link account.

8. Associate the email address of your resource mailboxes in Microsoft Exchange to your Alexa for Business rooms.
   - Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
   - Choose Rooms and choose the room to which to add the email address.
   - Choose Edit.
   - Enter the email address of your resource mailbox that you want to associate to the Alexa for Business room.
   - Choose Save.

9. Test the integration.
   - Create a new meeting invite in your Microsoft Outlook client.
b. Add the room as the resource.

c. Add meeting dial-in information to your meeting invite.

d. Send the invite to book the room.

e. Say “Alexa, start my meeting” to the Echo device assigned to the room. Your Echo device prompts you to join the scheduled meeting without asking you for the meeting ID.

f. Say, “Alexa, is this room free?” to the Echo device assigned to the room. Your Echo device returns that the room is booked.

Control Conferencing Systems

Alexa for Business integrates with popular video conferencing devices and in-room control systems to seamlessly control your conferencing system.

Tasks

- Supported Conferencing Systems (p. 32)
- Understanding Alexa-enabled Conferencing (p. 33)
- Manage Conferencing Providers (p. 35)
- Use Zoom Rooms with Alexa for Business (p. 36)
- Use Cisco Webex Room Devices with Alexa for Business (p. 38)
- Use Poly Group Series with Alexa for Business (p. 41)
- Use Poly Trio with Alexa for Business (p. 43)
- Use Lifesize room systems with Alexa for Business (p. 45)
- Use the Alexa for Business Gateway (p. 47)

Supported Conferencing Systems

Alexa for Business supports the following video conferencing systems and in-room control systems:

<table>
<thead>
<tr>
<th>Device model</th>
<th>Requirements</th>
<th>Alexa built-in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco/Tandberg SX, EX, DX, MX, C</td>
<td>Firmware must be TC7.3 or CE8.0+</td>
<td>No</td>
</tr>
<tr>
<td>Cisco Webex Room Kit</td>
<td>Firmware must be CE8.0+</td>
<td>No</td>
</tr>
<tr>
<td>Zoom Rooms</td>
<td>Zoom Rooms for Mac version 4.1.20278.0206 or higher</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Zoom Rooms for PC version 4.1.22620.0319 or higher</td>
<td></td>
</tr>
<tr>
<td>Crestron 3-Series</td>
<td>Please contact a Crestron-certified installer</td>
<td>No</td>
</tr>
<tr>
<td>Poly Group Series 310, 500, 700</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Poly Trio 8500 and 8000</td>
<td>Firmware must be 5.9.0 or higher</td>
<td>Yes</td>
</tr>
<tr>
<td>Amazon Chime on Dolby Voice Room</td>
<td>For more information, see Setting Up Amazon Chime on Dolby Voice Room.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Alexa for Business Administration Guide
Understanding Alexa-enabled Conferencing

<table>
<thead>
<tr>
<th>Device model</th>
<th>Requirements</th>
<th>Alexa built-in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifesize Icon 300, 500, and 700</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

When the room doesn’t contain any of the supported video conferencing or in-room control systems, you can use the Echo device as a speaker phone to dial into meetings. In this case, the Echo device uses Alexa Calling and Messaging, and makes a PSTN call to the phone number specified in your conference provider settings. Currently, the Echo device can call phone numbers in the US, Canada, and Mexico.

The following diagram shows how Alexa for Business controls your conference devices.

For more information, see Getting Started with Shared Devices (p. 7) or the documentation provided by the device manufacturer.

Understanding Alexa-enabled Conferencing

Alexa for Business lets you bring Alexa to your meeting rooms. Use Alexa to start meetings and control your conference room systems by using your voice. You can say things like “Alexa, join my meeting” and Alexa prompts you to join the scheduled meeting on the calendar. If there is no scheduled meeting or you want to join a different meeting, say your meeting ID and, if required, the PIN.

You can use Alexa for Business to control the conference device in your meeting room. First, enable and set up the Alexa skill for your compatible conference devices, then set up your conferencing provider, and finally, you can link a calendar system.

Tasks
- Conference Providers (p. 33)
- PSTN Settings (p. 34)
- SIP/H323 Settings (p. 35)
- Calendar Integration (p. 35)

Conference Providers

To use Alexa for Business to join meetings from the conference devices in your meeting rooms, set up your conference provider. Alexa for Business offers a list of built-in conference providers, including...
Amazon Chime, Cisco WebEx, and Zoom. If your conference provider isn’t listed, choose Custom conference provider and specify the details.

The conference provider contains the following settings:

- Provider name and meeting
- PSTN dial-in
- SIP/H323 dial-in

When you ask Alexa to join a meeting, Alexa searches for a scheduled meeting on the calendar that you can join. If there’s no meeting on the calendar or the user declines to join it, Alexa asks the user for dial-in information to join a one-time meeting. The provider name and meeting settings are used during this exchange. The following table provides examples of what you can say to Alexa to start meetings.

### Example Dialogues

<table>
<thead>
<tr>
<th>Description</th>
<th>Dialogue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Chime is set up as the conference provider and no meeting PIN is required.</td>
<td>User: “Alexa, start my meeting”&lt;br&gt;Alexa: “There is no meeting on the calendar. What is your &lt;Amazon Chime&gt; meeting ID?”</td>
</tr>
<tr>
<td>A meeting PIN is optional.</td>
<td>User: “Alexa, start my meeting.”&lt;br&gt;Alexa: “There is no meeting on the calendar. What is your &lt;provider name&gt; meeting ID?”&lt;br&gt;User: “123456789.”&lt;br&gt;Alexa: “Do you have a meeting PIN?”&lt;br&gt;User: “Yes.”&lt;br&gt;Alexa: “What is your meeting PIN?”&lt;br&gt;User: “5678.”&lt;br&gt;Alexa: “OK, joining your meeting.”</td>
</tr>
<tr>
<td>A meeting PIN is required.</td>
<td>User: “Alexa, start my meeting.”&lt;br&gt;Alexa: “There is no meeting on the calendar. What is your &lt;provider name&gt; meeting ID?”&lt;br&gt;User: “123456789.”&lt;br&gt;Alexa: “What is your meeting PIN?”&lt;br&gt;User: “5678.”&lt;br&gt;Alexa: “OK, joining your meeting.”</td>
</tr>
</tbody>
</table>

### PSTN Settings

When you use your Echo device as a speaker phone to dial into meetings, you must configure the PSTN settings. Alexa for Business uses PSTN settings, and the meeting ID and PIN from the scheduled meeting, to create a dial sequence.
Alexa for Business uses this dial sequence to join the audio conference in the background and send the meeting ID and PIN as dual-tone multi-frequency signaling (DTMF) tones. The specified delays provide pauses before Alexa for Business enters the information. For example, there is a wait, the welcome announcement completes, and the user can enter the meeting ID.

**SIP/H323 Settings**

When you use Alexa to control your existing conference devices, such as Cisco Webex, you must specify the SIP or H323 endpoint that gets called when you ask Alexa to join a meeting.

Alexa for Business uses these endpoints, and the meeting ID and PIN from the scheduled meeting to create a dial string. This dial string is sent to the Alexa skill you enabled to control your conference device.

*Note*
SIP/H323 settings are used only when using Alexa to control third-party conference devices. They aren't used when using an Echo device as a speaker phone.

**Calendar Integration**

You can connect Alexa for Business to your calendar system. This allows users to join scheduled meetings without knowing the dial-in details. When Alexa for Business is connected to your calendar system and a user asks Alexa to join a meeting, Alexa for Business reads the meeting on the associated room calendar and gets the dial-in information.

Alexa for Business can get meeting dial-in information from the following conference providers:

- Amazon Chime
- BlueJeans
- Zoom
- RingCentral Meetings
- Skype for Business
- Fuze
- Cisco WebEx

*Note*
Cisco WebEx meeting invites that include TSP audio bridge are currently not supported.

- Google Hangouts Meet

*Note*
Google Hangouts Meet is only supported on shared devices.

If there are issues with one of the conference providers, send an email to a4b-conferencing@amazon.com and include an example of your meeting invite.

*Note*
Connecting Alexa for Business to your calendar system is required only when your third-party Alexa skill doesn’t natively support joining scheduled meetings.

**Manage Conferencing Providers**

For more information about conference providers, PSTN settings, and SIP/H323 settings, see the section called “Control Conferencing Systems” (p. 32).

**To add a conferencing provider**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Conference settings, Add provider.
3. Choose one of the available conferencing providers, which automatically fills in the Provider pane.  
   **Note**  
   If the conference provider used by your organization is not available, choose Other.
4. Review the following settings and edit them as necessary:
   - **Meeting settings** – Specify whether a meeting PIN is required to join the meeting. (Required)
   - **PSTN dial-in number** – Specify the phone number of your conferencing provider. This must be a US phone number.
   - **PSTN dial-in delays** – Specify the delays before the meeting ID and PIN are sent using DTMF.
   - **SIP/H323 dial-in** – SIP/H323 dial-in settings are used to dial into meetings using your existing video conferencing equipment. (Required)
5. Choose Add.

You can edit the meeting settings and dial-in information for a provider at any time.

To remove a conferencing provider
1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. In the navigation bar, choose Conference settings.
   **Note**  
   You can’t remove a provider that is set as the default.

To edit a conferencing provider
1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Conference settings and choose the name of the provider to edit.
3. Edit the following settings as necessary:
   - **Meeting settings** – Specify whether a meeting PIN is required to join the meeting. (Required)
   - **PSTN dial-in number** – Specify the phone number of your conferencing provider. This must be a US phone number.
   - **PSTN dial-in delays** – Specify the delays before the meeting ID and PIN are sent using DTMF.
   - **SIP/H323 dial-in** – SIP/H323 dial-in settings are used to dial into meetings using your existing video conferencing equipment. (Required)
4. Choose Save.

To set a conferencing provider as default
When a user joins a meeting and there is no scheduled meeting, the user is prompted for the meeting ID and PIN of the default provider. You can only have one default provider for your account.
1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Conference settings.
3. Select the name of the provider to set as default.
4. Choose Set as default.

### Use Zoom Rooms with Alexa for Business

You can connect Alexa for Business to your Zoom Rooms system to control meetings using your voice.
To use the integration, make sure you're using:

- Zoom Rooms for macOS: Version 4.1.20278.0206 or higher
- Zoom Rooms for PC: Version 4.1.22620.0319 or higher

**To integrate Alexa for Business with your Zoom Rooms system**

1. **Prepare for integration:**
   1. Set up your Echo device. For more information, see Getting Started with Shared Devices (p. 7).
   2. Create a new skill group for the Zoom Alexa skill. For more information, see Managing Skill Groups (p. 22).
   3. Create a room in Alexa for Business, add the skill group, and assign the Echo device to the room. For more information, see Managing Rooms (p. 12).
   4. If you're using Office 365 or Microsoft Exchange as your calendar system, link your calendar to Alexa for Business. For more information, see the section called “Link Alexa for Business to Your Calendar System” (p. 27).

2. **Set up Zoom as a conferencing provider:**
   1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
   2. Choose **Conferencing**, **Add provider**, **Zoom** and save the settings.
   3. Enable the Zoom for Alexa skill:
      1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
      2. Choose **Conference settings**, **Zoom for Alexa** in the list of conference equipment, and **Enable**.
      3. When you're prompted to link an account, sign in with the Zoom account where you registered your Zoom Rooms, and choose **Authorize** to complete the account linking.
      4. Choose **Skills**, **Enabled skills**, and then select the skill.
      5. Choose **Assign to skill group**, and choose the skill group associated with the rooms where you want to use Zoom.

4. **Configure the skill for your room:**
   1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
   2. Choose **Rooms**, open the room where you want to use Zoom integration, and choose **Skills**.
   3. Choose the pencil icon to edit the skill configuration.
   4. For the **Scope value**, type the name of a Zoom room that already exists or will be created in the Zoom web portal.

5. **Discover your Zoom Room device:**
   1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
   2. Choose **Rooms**, open the room, and in the **Alexa Devices** section, verify that the status is **Synced**.
   3. Choose **Smart Home devices**, **Discover devices**.
   4. If your Zoom Rooms configuration is successfully set up, your Zoom Rooms system displays in the list.

You can now control your Zoom Rooms by talking to Alexa. For example, say “Alexa, start my meeting” or “Alexa, join my meeting.”

When a scheduled meeting associated with your Zoom Room is found on the calendar, you are prompted to join this meeting. If you don't want to join the scheduled meeting, you can either start an instant meeting by using the meeting ID 123, or join your personal meeting room by speaking your personal, 10-digit meeting ID.
If you encounter any of the following issues, try these resolutions:

- Alexa says that the Zoom room isn’t found:
  Make sure that the account used for account linking is the same as the account that you used to sign into your Zoom room.
- Alexa can’t find an upcoming event on your calendar:
  Make sure that the meeting on your calendar was scheduled as a Zoom meeting.
- Alexa says "It looks like the conference provider is invalid":
  Make sure that you have the latest version of the Zoom Rooms software.

Use Cisco Webex Room Devices with Alexa for Business

Use Alexa for Business to control your Cisco Webex room systems and join meetings by using your voice. Alexa for Business supports the following Cisco video conferencing endpoints:

- Cisco Webex DX, EX, MX, and SX series
- Cisco Webex Room Kit

To have Alexa control your Cisco video conferencing endpoints, run the Alexa for Business gateway within your local network. The Alexa for Business gateway receives control events from Alexa for Business and issues commands to the Cisco video conferencing endpoints in your meeting rooms. For example, when a user asks Alexa to join a meeting, an event is sent to the gateway. The gateway processes this event, connects to the Cisco video conferencing endpoint in the room, and then initiates the dial-in to the meeting. The following diagram shows the setup and network boundaries.

For more information, see the section called “Use the Alexa for Business Gateway” (p. 47).

To use Alexa for Business to control your Cisco video conferencing endpoints, you must meet the following requirements:

- You have a Cisco Webex system with firmware version TC7.3.12 or CE8 or higher.
You have Windows Server 2008 or later, Windows 7 desktop or later, or a Linux server or choice to run the Alexa for Business gateway. This can be a virtual or physical machine.

Your locally deployed Alexa for Business gateway is allowed to make outbound HTTPS connections and has local network access to control your Cisco Webex system. Incoming external communication or inbound ports aren't required.

To use Cisco Webex with Alexa for Business

1. Set up your conferencing provider in Alexa for Business.
   a. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
   b. Choose Conference settings and then choose the name of your default conferencing provider.
   c. Enter the H323/SIP endpoint if it isn't filled in. Alexa for Business sends these settings with the meeting ID/PIN to create a dial-in string that's called on in the Cisco Webex system.

2. Enable the skill.
   a. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
   b. Choose Conference settings and Alexa for Cisco Webex in the list of conference equipment.
   c. Choose Enable.
   d. You receive a prompt to link an account. Sign in or create an Amazon.com account (for example, marymajor@example.com).
   e. Choose Skills, Enabled skills, and then select the skill.
   f. Choose Assign to skill group and choose the skill group associated with the rooms where you want to make the skill available.

3. Install the Alexa for Business gateway. For more information, see Use the Alexa for Business Gateway (p. 47).

4. Add your Cisco Webex system to Alexa for Business and add it to a room.
   a. Choose Endpoint, Add endpoint.
   b. Specify the Cisco Webex system name.
   c. Enter a friendly name, which can be used to control the Cisco endpoint using your voice. For example, "Alexa, turn on <friendly name>.
   d. (Optional) Enter a description.
   e. Choose the Cisco Webex model.
   f. Specify the endpoint URL of your Cisco Webex endpoint. For example, "http://10.0.1.42".

   Note
   If you don't specify a protocol, "http" is used.

   g. Choose the Alexa for Business room where the Cisco Webex endpoint is located.
   h. Choose Add.
   i. Choose Rooms and the name of the room where you just assigned the Cisco Webex endpoint.
   j. Choose the gateway group to control your Cisco endpoint.
   k. Choose Discover devices to have the endpoint available in your room.
   l. Test the integration by saying "Alexa, start my meeting," and say the meeting ID and PIN for your meeting when prompted.

To add a Cisco Webex endpoint

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Conferencing settings, Alexa for Cisco Webex.
3. In the endpoint section, choose Add endpoint. For System name, enter Cisco Webex.
4. Enter a friendly name, which can be used to control the Cisco endpoint using your voice. For example, "Alexa, turn on <friendly name>." Enter an optional description.

5. Choose Cisco Webex model and specify the endpoint URL of your Cisco Webex endpoint. For example, "http://10.0.1.42".

   **Note**
   If you don't specify a protocol, "http" is used.

6. Choose the Alexa for Business room where the Cisco Webex endpoint is located and choose **Add**.

7. Choose **Rooms** and the name of the room where you just assigned the Cisco Webex endpoint.

8. Choose the gateway group to control your endpoint.

9. To have the endpoint available in your room, go to the **Smart Home devices** section and choose **Discover devices**.

You can now use Alexa to control your Cisco Webex endpoint using voice.

**To remove an endpoint**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.

2. Choose **Conferencing settings, Alexa for Cisco Webex**.

3. Go to the endpoint section and select the check box next to the device to deregister.

4. Choose **Remove**.

**To use HTTPS to connect to your Cisco Webex endpoints**

1. Choose one of the following options:

   1. To connect Alexa for Business to your Cisco Webex systems over Transport Layer Security (TLS), the gateway must be able to verify the signature of the certificates. To enable this capability, install the root CA and other intermediate CAs that signed the certificate on the host where you run the gateway. If the Cisco system can't be authenticated, the connection isn't established.

   You can either install the root CA and other intermediate CAs in the certificate store of your gateway host. You can also specify the path to the certificates in the gateway config file; for example.

   "rootCAsFile": "path\to\certs\custom-certs.pem"

   2. (Not secure and not recommended) If your Cisco endpoints are configured with a self-signed certificate, you can also disable the certificate validation to allow the gateway to connect regardless of the certificate in use. To do this, open the gateway configuration file and change the following configuration value:

   "skipSslVerification": true

   2. To apply the change, restart the gateway.

   3. Verify the gateway log file to confirm that the certificate validation works correctly. If the certificate validation fails, you see the following message in the log file:

   handler-cisco: failed executing request: Get https://<ip-address>/getxml?location=/Status: x509: certificate signed by unknown authority

**To debug log files**

1. Go to one of the following locations to see the log files written by the Alexa for Business gateway:

   - On Windows: C:\ProgramData\Amazon\AlexaForBusinessGateway\Logs

40
• On Linux: /var/log/a4b-gateway/gateway.log

2. In the log files, verify that the gateway is listening to the queue for control commands. Find control requests in the log file by searching for “inbound: worker received request.” By default, the log shows all the different control commands the gateway is performing. Looks for errors to determine why the gateway can’t control your Cisco endpoint.

### Use Poly Group Series with Alexa for Business

Use Alexa for Business to control your Poly Group Series systems and join meetings by using your voice.

To have Alexa control your Poly Group Series video conferencing endpoints, run the Alexa for Business gateway within your local network. The Alexa for Business gateway receives control events from Alexa for Business and issues commands to the Cisco video conferencing endpoints in your meeting rooms. For example, when a user asks Alexa to join a meeting, an event is sent to the gateway. The gateway processes this event, connects to the Cisco video conferencing endpoint in the room, and then initiates the dial-in to the meeting.

To use Alexa for Business to control your Poly Group Series video conferencing endpoints, you must meet the following requirements:

• You have Poly Group Series 310, 500, or 700.
• You enabled SSH on your Poly Group Series endpoint.
• You have Windows Server 2008 or later, Windows 7 desktop or later, or a Linux server or choice to run the Alexa for Business gateway. This can be a virtual or physical machine.
• Your locally deployed Alexa for Business gateway is allowed to make outbound HTTPS connections and has local network access to control your Poly Group Series system. Incoming external communication or inbound ports aren't required.

To use Poly Group Series with Alexa for Business

1. Set up your Alexa-enabled devices. For more information, see Getting Started with Shared Devices (p. 7).
2. Link your calendar system to Alexa for Business. For more information, see the section called “Link Alexa for Business to Your Calendar System” (p. 27).
3. Enable the Alexa for Cisco Webex/Poly Group skill.
   a. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
   b. Choose Skill groups, Create skill group, and then enter a name for your skill group (for example, Conferencing skills).
   c. Choose Conference settings, and then in the list of conference equipment, choose Alexa for Cisco Webex/Poly Group Series.
   d. Choose Enable.
   e. You receive a prompt to link an account. Sign in or create an Amazon.com account (for example, marymajor@example.com).
   f. Choose Skills, Enabled skills, and then select the skill.
   g. Choose Assign to skill group, and then choose the skill group that you just created.
4. Install the Alexa for Business gateway. For more information, see Use the Alexa for Business Gateway (p. 47).
5. Set up your conferencing provider in Alexa for Business.
   a. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
   b. Choose Conference settings, and then choose the name of your conferencing provider.
c. If you're using Poly Group Series for Skype for Business, choose Skype for Business and make sure the following SIP URI is specified as SIP endpoint:

   sip:{{USERNAME}}@{{DOMAIN}};gruu;opaque=app:conf:focus:id:{{VIDEOID}}

d. For other conferencing providers, enter the H323/SIP endpoint if the field is empty. Alexa for Business sends these settings with the meeting ID/PIN to create a dial-in string that's called in the Poly Group Series system.

6. Create your meeting rooms in Alexa for Business. For more information, see the section called "Managing Rooms" (p. 12).

7. Add your Poly Group Series endpoint to Alexa for Business, and then add it to a room.

   a. Choose Endpoint, Add endpoint.
   b. Specify the system name.
   c. Enter a friendly name, which can be used to control the endpoint using your voice. For example, "Alexa, turn on <friendly name>.
   d. (Optional) Enter a description.
   e. Choose the Poly Group Series model.
   f. If your Poly Group Series endpoint is running Skype for Business mode, choose Skype for Business mode.
   g. Specify the IP address or host name of your Poly Group Series endpoint. For example, "10.0.1.42."
   h. Choose the Alexa for Business room where the Poly Group Series endpoint is located.
   i. Choose Add.
   j. Choose Rooms and the name of the room where you just assigned the Poly Group Series endpoint.
   k. Choose the gateway group to control your Poly endpoint.
   l. To have the endpoint available in your room, in the Smart Home devices section, choose Discover devices.
   m. To test the integration, schedule a meeting on the room calendar, say "Alexa, start my meeting," and confirm the scheduled meeting when prompted.

To add another Poly Group Series endpoint

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Conferencing settings, Alexa for Cisco Webex/Poly Group Series.
3. Choose Endpoint, Add endpoint.
4. Enter the System name.
5. Enter a friendly name, which can be used to control the endpoint using your voice. For example, "Alexa, turn on <friendly name>."
6. (Optional) Enter a description.
7. Choose the Poly Group Series model.
8. If your Poly Group Series endpoint is running Skype for Business mode, choose Skype for Business mode.
9. Enter the IP address or host name of your Poly Group Series endpoint. For example, "10.0.1.42."
10. Choose the Alexa for Business room where the Poly Group Series endpoint is located, and then choose Add.
11. Choose Rooms and the name of the room where you just assigned the Poly Group Series endpoint.
12. Choose the gateway group to control your endpoint.
13. To have the endpoint available in your room, go to the Smart Home devices section and choose Discover devices.
14. When the Poly Group Series endpoint is listed under **Smart Home device**, setup is complete.
15. To test the integration, schedule a meeting on the room calendar, say “Alexa, start my meeting,” and confirm the scheduled meeting when prompted.

You can now use Alexa to control your Poly Group Series endpoint using voice.

**To remove an endpoint**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Conferencing settings, Alexa for Cisco Webex/Poly Group Series**.
3. Go to the endpoint section and select the check box next to the device to de-register.
4. Choose **Remove**.

**Use Poly Trio with Alexa for Business**

The latest firmware for Poly Trio has integrated natively with Alexa Voice Service and lets you use Alexa in your meeting rooms. With Alexa on Poly Trio, you can make hands-free phone calls, join meetings, check meeting room availability, book or find a meeting room for your meeting, and access private skills, such a company briefing or company FAQs. For more information, see [Poly Trio Systems with Alexa for Business Deployment Guide](#).

To use Alexa on Poly Trio devices, you must meet the following requirements:

- Firmware 5.9.0 or higher must be installed on your Poly Trio devices.
- Your Poly Trio must be registered with the Poly Cloud Service. To get your Poly Cloud Service tenant created, contact your Poly sales representative, or go to [https://www.polycom.com/forms/pdms-e-trial.html](https://www.polycom.com/forms/pdms-e-trial.html).

**To use Poly Trio with Alexa for Business**

1. **Set up AVS permissions.**
   
   To grant Poly permissions to register your Trio devices into your AWS account and assign them to a room, you must create an IAM service role.

   If your IAM user account, group, or role is assigned administrator or PowerUserAccess permissions, then you have all the permissions to set up Alexa for Business. If you don't have administrator permissions, then an AWS account administrator must update your IAM user account, group, or role to include PowerUserAccess permissions or perform the following steps for you.

   1. Open the Alexa for Business console at [https://console.aws.amazon.com/a4b/](https://console.aws.amazon.com/a4b/).
   2. Choose **Settings, AVS permissions**.
   3. Choose **Poly** from the drop-down menu and choose **Create IAM role**.
   4. Download the CSV file. You’ll need to upload this file in the Poly Cloud Service in a future step.

2. **Set up your conferencing provider.**

   To have Alexa for Business join your meetings, you must set up your conferencing provider. Alexa for Business offers a list of built-in conference providers, including Amazon Chime, BlueJeans, Cisco Webex, Skype for Business, and Zoom. Alexa for Business uses the conference provider settings to build the dial sequence when joining a meeting. For more information, see the section called “Manage Conferencing Providers” (p. 35).

   1. Open the Alexa for Business console at [https://console.aws.amazon.com/a4b/](https://console.aws.amazon.com/a4b/).
   2. Choose **Conferencing** and **Add provider**.
3. Choose the conferencing provider that you are using in your organization, and enter the PTSN dial-in number and SIP endpoint.

3. Link your calendar.

To join scheduled meetings, check room availability, and book a room for a meeting by asking Alexa, you must link your calendar to Alexa for Business.

Alexa for Business supports Microsoft Exchange, Microsoft Office365, and Google G-Suite. For more information, see the section called “Link Alexa for Business to Your Calendar System” (p. 27).

Note
Although your Poly Trio might be connected to your calendar system to provide one-touch join, the locally linked calendar won’t be used by Alexa.

4. Enable skills and add them to a skill group.

Skills are voice-driven capabilities that enhance the functionality of your Alexa device. Alexa for Business gives you access to all skills in the Alexa Skills store. You can also build skill specifically for your organization by using Blueprints or developing a private skill.

To enable skills for your devices, you must first enable the skill for your organization and then add it to one or more skill groups that are assigned to your rooms. For more information, see the section called “Managing Skill Groups” (p. 22) and the section called “Managing Skills” (p. 18).

5. Create a room profile.

To simplify the process of creating and managing rooms, first define room profiles. A room profile contains the settings for your Alexa devices, so that they can provide you with weather, time, and other location-based information. For example, you can create a room profile that contains the Alexa settings that apply to all rooms in the same building.

6. Prepare your Poly Trio device.

To use Alexa for Business on your Poly Trio, you must register your Poly Trio through PDMS-E with Alexa for Business. Before you can register your Poly Trio, first Enable the Universal Agent (formerly known as Poly Cloud Connector or PCC). The Universal Agent must onboard your Poly Trio to PDMS-E, even if you’re onboarding Poly Trio using the MAC address.

Before you begin using the following steps, make sure that you have configured your Network Time Protocol server with Poly Trio.

a. Copy the following XML information into a text file and save it as a .cfg file (for example, pcc.cfg).

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<UPLOAD>
<ALL>
<feature.pcc.enabled="1"/>
<feature.da.enabled="1"/>
</ALL>
</UPLOAD>
```

b. Log in to the Poly Trio Web Interface as an administrator.

c. Choose Utilities, Import & Export Configuration, Choose File, and select the .cfg file generated (for example, pcc.cfg) to enable Universal Agent.

d. To enable Alexa for Business for your Poly Trio, copy the following XML information into a text file and save it as a .cfg file (for example, alexa.cfg).

Note
You can also enable these settings using your existing management and provisioning solution, such as Poly Resource Manager.
Use Lifesize room systems with Alexa for Business

You can use Alexa for Business with Lifesize room systems. Alexa is supported on Lifesize Phone HD when connected to a Lifesize Icon 300, 500, or 700 device. With Alexa on Lifesize room systems, you...
To set up Lifesize room systems with Alexa for Business

1. **Set up Alexa Voice Service (AVS) permissions.**

   To grant Lifesize permissions to register your Lifesize room systems into your AWS account and assign them to a room, you must create an AWS Identity and Access Management (IAM) service role.

   If your IAM user account, group, or role is assigned administrator or PowerUserAccess permissions, then you have all the permissions necessary to set up Alexa for Business. If you don’t have administrator permissions, then an AWS account administrator must update your IAM user account, group, or role to include PowerUserAccess permissions or perform the following steps for you.

   1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
   2. Choose **Settings**, **AVS permissions**.
   3. Choose **Lifesize** from the drop-down menu and **Create IAM role**.
   4. Download the CSV file. You will upload this file in the Lifesize admin portal in a later step.

2. **Create a room profile.**

   To simplify the process of creating and managing rooms, define room profiles. A room profile contains the settings for your Alexa devices, so that they can provide you with weather, time, and other location-based information. For example, you can create a room profile that contains the Alexa settings that apply to all rooms in the same building. For more information, see the section called “Managing Room Profiles” (p. 13).

3. **Link your calendar.**

   To join scheduled meetings, check room availability, and book a room for a meeting by asking Alexa, you must link your calendar to Alexa for Business.

   Alexa for Business supports Microsoft Exchange, Microsoft Office 365, and Google G Suite. For more information, see the section called “Link Alexa for Business to Your Calendar System” (p. 27).

4. **Link your AWS account to your Lifesize account.**

   To register a Lifesize room system with Alexa for Business, you must first grant access through your Lifesize account.

   1. Sign into the **Lifesize admin console**.
   2. Choose **Account Settings** and **Device Settings**.
   3. In the **Alexa for Business** section, enter the **Role ARN** and **External ID** from the CSV file you downloaded in step 1.
   4. Choose **Authenticate**.
   5. Lifesize is now set as a conferencing provider in your Alexa for Business account. If you are using another meeting service with Lifesize room systems, set up the conferencing provider. For more information, see **Conferencing Providers**.

5. **Register your Lifesize room system device with Alexa for Business to enable Alexa on the device.**

   1. In the **Lifesize admin console**, choose **Room Systems**.
   2. Select a room system that you want to register with Alexa for Business.
   3. On the room system page, choose **Settings** and go to the Alexa for Business section.
   4. Choose **Register**.
   5. Select the **Room Profile** that you want to register the device to.
Use the Alexa for Business Gateway

The Alexa for Business gateway enables you to connect Alexa for Business to your Cisco Webex and Poly Group Series endpoints to control meetings with your voice. The gateway software runs on your on-premises hardware and securely proxies conferencing directives from Alexa for Business to your Cisco endpoint. The gateway is available for both Windows and Linux.

The gateway needs two pairs of AWS credentials to communicate with Alexa for Business. We recommend that you create two limited-access IAM users for your Alexa for Business gateways, one for installing the gateway and one for operating the gateway.

To create new IAM users

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. Choose Users, Add user.
3. Enter a user name (for example, AlexaforBusinessGatewayInstaller).
4. For Access type, choose Programmatic access.
5. Choose Next, Attach existing policies directly, AlexaForBusinessFullAccess in the list of policies, and then choose Next.
6. Choose Create user.
7. Download and save the IAM access key and secret key. You need them later when you configure the Alexa for Business gateway.
8. To create a second user that is used to run the Alexa for Business gateway, repeat steps 2-7. Enter a user name (for example, AlexaforBusinessGateway) and choose AlexaForBusinessGatewayExecution in the list of policies.

Tasks

- Install the Gateway (p. 48)
- Run Multiple Gateways (p. 49)
- Maintain the Gateway (p. 51)
Install the Gateway

The gateway is available on the Alexa for Business console.

To install the Alexa for Business gateway, you need the following:

- One of the following virtual or physical machines to run the Alexa for Business gateway:
  - Windows Server 2008 or later
  - Windows 7 desktop or later
  - Linux server
- A minimum of 1 GB available disk space.
- A minimum of 2 GB of RAM.
- Your locally deployed Alexa for Business gateway is allowed to make outbound HTTPS connections. It also has local network access to control your Cisco Webex or Poly Group Series endpoints. (Incoming external communication or inbound ports aren't required.)

To prepare for installation

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Conferencing, Conferencing equipment skills, Alexa for Cisco Webex, and Download gateway.
3. Select the package for your operating system and choose Download.

To install and configure the gateway on Windows

1. Run the installer on your Windows server as an administrator: right-click on the downloaded file and choose Run as administrator.
2. When prompted, enter the user credentials to sign into your Cisco Webex or Poly Group Series endpoints.
3. Register your gateway. If it's enabled, the Alexa for Business registration tool starts automatically. You can also manually run the registration tool as an administrator at C:\Program Files\Amazon\AlexaForBusinessGateway\register.exe.
4. Open the Alexa for Business console again, refresh Alexa for Business Gateways, and confirm that your gateway is listed.
5. In the Services window, verify that the service (Alexa for Business gateway) is installed and running.

To install and configure the gateway on Amazon Linux

1. Install the gateway:
   - On Amazon Linux, Red Hat, or CentOS, run the following command:
     
     ```
     sudo yum install -y a4b_gateway_<architecture>.rpm
     ```
   - For Ubuntu Server, run the following command:

     ```
     sudo dpkg -i a4b_gateway_<architecture>.deb
     ```
   - On other Distros, run the following commands:

     ```
     sudo tar zxvf a4b_gateway_<architecture>.tar.gz
     sudo cp bin/* /usr/bin/
     ```
sudo mkdir /etc/alexaforbusinessgateway

sudo cp config/* /etc/alexaforbusinessgateway

(sysvinit): sudo cp service/sysvinit/alexaforbusinessgateway /etc/init.d/alexaforbusinessgateway

(Upstart): sudo cp service/upstart/alexaforbusinessgateway.conf /etc/init/alexaforbusinessgateway.conf

(Systemd): sudo cp service/systemd/alexaforbusinessgateway.service /usr/lib/systemd/system/alexaforbusinessgateway.service

2. Set the credentials of your Cisco Webex or Poly Group Series endpoints:

sudo nano /etc/alexaforbusinessgateway/secrets.cfg

3. Verify that the system manager is set to the correct value (valid values are sysvinit, upstart, or systemd):

sudo cat /etc/alexaforbusinessgateway/gateway.cfg.template | grep serviceManager

4. Register the gateway to your Alexa for Business setup:

1. Run the following command:

   sudo /usr/bin/alexaforbusinessgateway-register

2. When prompted, enter the IAM access keys and secret keys of the IAM users that you created previously.

3. For more advanced scenarios, run the following command to see additional help documentation:

   sudo /usr/bin/alexaforbusinessgateway-register --help

5. Start the Alexa for Business gateway service:

   • sysvinit: sudo service alexaforbusinessgateway start
   • Upstart: sudo initctl start alexaforbusinessgateway
   • Systemd: sudo systemctl start alexaforbusinessgateway

6. (Optional) Check the logs for errors logged when starting the service:

   sudo tail /var/log/alexaforbusinessgateway/gateway.log

Run Multiple Gateways

You can run multiple gateways to eliminate a single point of failure. You can also run a gateway in each of your locations to lower the latency between the gateway and your Cisco or Poly endpoints. This is also an option if you want to run the gateway on different network subnets.

The following are two examples of how to set up multiple gateways:
High Availability setup

Gateway group

Gateway 1

Gateway 2

High Availability setup in multiple locations

Gateway group

Gateway 1

Gateway 2

New York

Gateway group

Gateway 1

Gateway 2

Seattle
When you register a gateway to your AWS account, the gateway is added to a gateway group. When you add video conferencing endpoints, you must also assign a gateway group. The gateways registered to this gateway group will control your endpoint when you ask Alexa to start your meeting.

**Note**
You can add a gateway group to run a gateway in a different location, and choose this group when you register new gateway.

**To add a gateway group**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Conferencing settings**, Alexa for Cisco Webex/Poly Group Series, **Add gateway group**.
3. Enter the **Name** and an optional description, and choose **Add gateway group**.
4. To add a gateway to your group, follow the steps to install and register the gateway. (When prompted, select the gateway group that you just created.)

If you need to add a gateway to a different group, first remove the gateway, then register it again.

**To remove a gateway group**

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Conferencing settings**, Alexa for Cisco Webex/Poly Group Series, **Remove gateway group**, and **Remove**.
3. Alexa for Business can no longer control the conferencing endpoints that were controlled with this group.

**Maintain the Gateway**

By default, the gateway automatically updates every day during predefined maintenance windows. These windows are defined in the gateway.cfg file that the gateway accesses at startup. To change these maintenance windows, edit the gateway.cfg file and restart the gateway service. To manually update the gateway, run the updater binary installed with the gateway as the administrator (for Windows) or as the root (for Linux).

If your Cisco Webex or AWS credentials change, use the following steps to update your Alexa for Business gateways to use the new credentials.

**To update Cisco Webex Credentials for Windows**

1. Stop the **AlexaForBusinessGateway** service.
2. Choose **Start** and type **Command Prompt**.
3. From the search results, right-click **Command Prompt** and choose **Run as administrator**.
4. Run the following command:

   ```
   del <path_to_secrets.cfg_file> (for example: del “C:\Program Files\Amazon \AlexaForBusinessGateway\secrets.cfg”)
   ```
5. Create a new secrets.cfg file with the following structure:

   ```
   {
   "CISCO": {
   "USERNAME": "your cisco appliance username here",
   "PASSWORD": "your cisco appliance password here"
   }
   ```
6. Start the `AlexaForBusinessGateway` service.

**To update Cisco Webex Credentials for Linux**

1. Update the credentials in `/etc/alexaforbusinessgateway/secrets.cfg`.
2. Restart the `AlexaForBusinessGateway` service:
   
   - Sysvinit: `sudo service alexaforbusinessgateway restart`
   - Upstart: `sudo initctl restart alexaforbusinessgateway`
   - Systemd: `sudo systemctl restart alexaforbusinessgateway`

**To update AWS Credentials for Windows**

1. Stop the `AlexaForBusinessGateway` service.
2. Choose **Start** and type **Command Prompt**.
3. From the search results, right-click **Command Prompt** and choose **Run as administrator**.
4. Run the following command:
   
   ```
   del <path_to_credentials_file> (for example: del “C:\Program Files\Amazon
   \AlexaForBusinessGateway\credentials”)  
   ```
5. Create a new credentials file with the following structure:

   ```
   [default]
   aws_access_key_id = YOUR ACCESS KEY ID HERE
   aws_secret_access_key = YOUR SECRET ACCESS KEY HERE
   ```
6. Start the `AlexaForBusinessGateway` service.

**To update AWS Credentials for Linux**

1. Update the credentials in `/etc/alexaforbusinessgateway/credentials.cfg`.
2. Restart the `AlexaForBusinessGateway` service:
   
   - Sysvinit: `sudo service alexaforbusinessgateway restart`
   - Upstart: `sudo initctl restart alexaforbusinessgateway`
   - Systemd: `sudo systemctl restart alexaforbusinessgateway`

**Gateway Configuration Options**

The following configuration parameters are available in the gateway.cfg file.

**Main Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>a4b</td>
<td>A4B</td>
<td></td>
<td>Object</td>
</tr>
<tr>
<td>skipSslVerification</td>
<td>Set to true to ignore SSL validation errors when the gateway is connecting to your</td>
<td>false</td>
<td>Boolean</td>
</tr>
</tbody>
</table>
## Parameter

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
<th><strong>Default Value</strong></th>
<th><strong>Type</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>video conferencing endpoints</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>credentials</td>
<td>Defines which AWS credentials to use</td>
<td>Null or object</td>
<td></td>
</tr>
<tr>
<td>localLog</td>
<td>Settings to have gateway log to a local file</td>
<td>Object</td>
<td></td>
</tr>
<tr>
<td>remoteLog</td>
<td>Settings to have gateway log to Amazon CloudWatch</td>
<td>Object</td>
<td></td>
</tr>
<tr>
<td>maintenance</td>
<td>Maintenance settings for the gateway, such as the update window and service manager</td>
<td>/path/to/root-ca/cert.pem</td>
<td>Object</td>
</tr>
<tr>
<td>rootCAasFile</td>
<td>Maintenance settings for the gateway, such as the update window and service manager</td>
<td></td>
<td>String</td>
</tr>
<tr>
<td>metrics</td>
<td></td>
<td></td>
<td>Object</td>
</tr>
</tbody>
</table>

### A4B Object

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
<th><strong>Default Value</strong></th>
<th><strong>Type</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>region</td>
<td>AWS Region where the gateway connects with the Alexa for Business endpoint</td>
<td>us-east-1</td>
<td>String</td>
</tr>
<tr>
<td>endpoint</td>
<td>The Alexa for Business endpoint the gateway connects to</td>
<td><a href="https://a4b.us-east-1.amazonaws.com">https://a4b.us-east-1.amazonaws.com</a></td>
<td>String</td>
</tr>
<tr>
<td>gatewayARN</td>
<td>The ARN of the gateway after it is registered with your Alexa for Business setup</td>
<td></td>
<td>String</td>
</tr>
</tbody>
</table>

### Shared Credentials

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
<th><strong>Default Value</strong></th>
<th><strong>Type</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>filename</td>
<td>Path to your AWS credentials</td>
<td>/path/to/.aws/credentials/file</td>
<td>String</td>
</tr>
<tr>
<td>profile</td>
<td>The profile to use in your AWS credentials file</td>
<td></td>
<td>String</td>
</tr>
</tbody>
</table>
### Static Credentials

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>accessKeyId</td>
<td>AWS access key</td>
<td></td>
<td>String</td>
</tr>
<tr>
<td>secretAccessKey</td>
<td>AWS secret key</td>
<td></td>
<td>String</td>
</tr>
<tr>
<td>sessionToken</td>
<td>AWS session token. This is required only if you use temporary security credentials</td>
<td></td>
<td>String</td>
</tr>
</tbody>
</table>

### LocalLog Object

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Boolean to enable logging to a local file</td>
<td>True</td>
<td>Boolean</td>
</tr>
<tr>
<td>logDir</td>
<td>Path to the log location</td>
<td></td>
<td>String</td>
</tr>
</tbody>
</table>

### RemoteLog Object

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Boolean to enable logging to Amazon CloudWatch</td>
<td>False</td>
<td>Boolean</td>
</tr>
<tr>
<td>failureDir</td>
<td>Path to the directory for backup when logging to CloudWatch fails</td>
<td></td>
<td>String</td>
</tr>
</tbody>
</table>

### Maintenance Object

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>serviceName</td>
<td>The service name of the gateway</td>
<td>alexaforbusiness</td>
<td>String</td>
</tr>
<tr>
<td>serviceManager</td>
<td>The service manager used on your Linux systems. Valid values are sysvinit, upstart, or systemd</td>
<td>systemd</td>
<td>String</td>
</tr>
<tr>
<td>updateFrequency</td>
<td>Defines how often to check for an update inside a maintenance window</td>
<td>15m</td>
<td>String</td>
</tr>
<tr>
<td>updateBranch</td>
<td>Defines which branch to update from</td>
<td>stable</td>
<td>String</td>
</tr>
</tbody>
</table>
Configure Meeting Room Settings

Meeting room settings help you measure and improve your meeting room utilization. You can enable end of meeting reminders, room utilization metrics, and intelligent room release.

**Note**
These settings are supported only when Alexa for Business is linked to an Office 365 or G Suite calendar system.

**To configure meeting room settings**
1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Room profiles, Create room profile.
3. Fill in the following fields under Meeting room settings:
   - **Room utilization metrics** - See how your meeting rooms are being used. Learn how many meetings are booked in every room, and the amount of time that your rooms are reserved. Enable Intelligent room release, described in the following item, to access additional metrics. These

---

### Windows Object

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>windows</td>
<td>Defines the time windows of the gateway checking for updates</td>
<td></td>
<td>Object</td>
</tr>
</tbody>
</table>

### HealthCheckPeriod Object

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>healthCheckPeriod</td>
<td>How long to wait after an update for the service to regain health, before the update is considered a failure</td>
<td>5m</td>
<td>String</td>
</tr>
</tbody>
</table>

### Maintenance Window Object

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>day</td>
<td>Day of the week when the gateway checks for updates</td>
<td></td>
<td>String</td>
</tr>
<tr>
<td>time</td>
<td>Time of day when the gateway checks for updates</td>
<td></td>
<td>String</td>
</tr>
<tr>
<td>width</td>
<td>Maximum length of the maintenance window</td>
<td></td>
<td>String</td>
</tr>
</tbody>
</table>

### Metrics Object

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Boolean to enable logging to CloudWatch</td>
<td>When this option is enabled, metrics are pushed to CloudWatch</td>
<td>String</td>
</tr>
</tbody>
</table>

---
metrics include attendance rate, freed up meeting room hours, and recovered meetings. All metrics are available on the Reports tab in the console. You can also schedule daily, weekly, or monthly delivery of room utilization metrics. For information about how to schedule reports, see the section called “Create a Scheduled Report” (p. 69).

- **Intelligent room release** - Release meeting room reservations when no one has checked into a reservation. You can select a time window within which a check-in must occur. Alexa reminds you when the room is within a few minutes of release, and when the room is actually released. If a device is offline, no release occurs. Users are checked in when they interact with Alexa verbally, or are in an active conference call on a device with Alexa built in. Users can also check in by saying “Alexa, check in.” When a room is released, the organizer will be notified via email from the address “no-reply@a4b.amazonaws.com.”

- **End of meeting reminder** - Alexa can remind the room when their meeting reservation is ending. You can choose the timing of the reminder, and the reminder behavior. Choose from the following audio and announcement options:
  - Gentle chime
  - Knock
  - Alexa Announcement #1: “Time check”
  - Alexa Announcement #2: “5 minutes left”

- **Instant booking** - When an employee says “Alexa, join the meeting” and the room is free, Alexa automatically books the room for the selected duration.

### View Room Utilization Metrics

Alexa for Business can help you gain visibility into, your meeting room utilization, and improve it. You can create usage reports to access the following room metrics. For more information, see *Creating Usage Reports* (p. 67).

- **Metrics for all rooms**
  - **Total meetings** - The total number of meetings on a calendar assigned to a room in Alexa for Business.
  - **Total minutes** - The total number of minutes associated with the total number of meetings on a calendar assigned to a room in Alexa for Business.

- **Metrics available if intelligent room release is enabled**
  - **Attended meetings** - An attended meeting is one that was checked into within your selected window. Alexa automatically checks in users if they interact with Alexa verbally or are in an active conference call using an Alexa built-in conferencing device. Users can also check in by saying “Alexa, check in.”
  - **Released meetings** - A released meeting occurs when Alexa releases a room reservation because there was no check-in within the selected window. Released meetings that are part of a recurring series are also included in their own table in these metrics.
  - **Attendance rate** - Attendance rate is a percentage that is calculated by dividing the number of attended meetings by the sum of attended meetings and released meetings.
  - **Released minutes** - The total number of minutes associated to released meetings for a room.
  - **Recovered meetings** - A recovered meeting occurs when an employee reserves a meeting room over a previously released time slot in that room.
Managing Calling

You can make calls from your shared devices with Alexa for Business. You can call a contact that you defined in the Alexa for Business console by saying the name out loud. Likewise, you can call a contact's number by saying the number out loud. For example, say “Alexa, call helpdesk” or “Alexa, call 206-555-0126.”

Note
The following types of calls are currently not supported when using an Echo device:

- Emergency services numbers (for example, “911”)
- Premium-rate numbers (for example, “1-900” numbers or toll numbers)
- N-1-1 numbers or abbreviated dial codes (for example, “211” or “411”)
- International numbers (numbers outside of the US, Canada, or Mexico)
- Dial-by-letter numbers (for example, “1-800-FLOWERS”)

To configure Alexa for Business to make calls from your shared devices

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Room profiles, select the name of the room profile associated with your rooms, and enable Outbound calling.

Tasks
- Managing Address Books (p. 57)
- Managing Contacts (p. 58)

Managing Address Books

To call contacts from your shared devices, you must first create an address book and assign it to the room profile associated with the rooms where the devices are assigned. You can create multiple address books, but you can only assign one address book to a room profile.

To create an address book

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Directory, Create address book, and enter a unique name for the address book.

To assign an address book to a room profile

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Rooms profiles and select the name of the room profile to edit.
3. Under Outbound calling, select the address book to assign, and then choose Save.

To edit an address book

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Directory and select the name of the address book to edit.
Managing Contacts

To call people using Alexa, add contacts to Alexa for Business. After you create contacts, you can add them to address books. Edit or delete a contact at any time.

Contacts can contain multiple phone numbers and one SIP address. When asking Alexa to call someone, you can add the words “at home,” “work,” or “mobile.” Say something like: “Alexa, call John Stile’s mobile.” If a contact has both a work phone number and SIP address, Alexa always calls the work phone number.

To bulk import contacts into Alexa for Business, use the AWS CLI or AWS SDK. For more information, see Alexa for Business API Reference.

To create a contact
1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Directory, Contacts.
3. Choose Create contacts, and enter a name, the phone numbers, SIP address, and description.
4. To add more contacts, choose Add another contact.
5. Choose Add contacts.

To add contacts to address books
1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Directory, Contacts.
3. Select the names of the contacts to add to your address book and choose Add to address books.
4. Select the check boxes next to the address book to which to add the contacts and choose Add.

To edit a contact
1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Directory, Contacts, and select the contacts to edit.
3. Edit the values for Name, Phone number, SIP address, and Description, and then choose Save.

To delete a contact
1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Directory, Contacts, and select the check box next to the contacts to delete.
3. Choose Delete contacts, Delete.
Managing Users

You can invite users to connect their personal Alexa account with your organization. When you send an invitation to a user, they receive an email with a temporary URL that allows them to join your organization after logging in with their Amazon account. When they join your organization, they gain access to the following features on their Alexa devices, both at home and at work:

- Discovering and enabling all the private skills that you make available to users.
- Discovering and enabling the private skills that you made available to them in their companion app.
- Joining meetings on Amazon Echo-family devices (Echo Show, Echo Plus, Echo, Echo Dot, and Echo Spot) managed by the account they used when joining your organization, and using the default conferencing provider.
- Linking their Microsoft Exchange calendar, if you issued the invitation to an email address that is part of the Exchange service account you linked in the Alexa for Business console.

In addition to the benefits available to users after joining your organization, you can require that users restrict any calendar accounts that they have linked and that match the domain of your service account configured in the Calendar section of the Alexa for Business console.

Tasks

- Set up Enrollment (p. 59)
- Invite and Remove Users (p. 60)
- Set up Microsoft Exchange Access for Users (p. 60)
- Require Users to Restrict Calendars to Voice (p. 63)
- Instruct Users to Use the Alexa Smart Scheduling Assistant (p. 64)

Set up Enrollment

Before you can invite users, you must first set up user enrollment.

To set up user enrollment

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Settings, User enrollment, Edit.
3. For Company Name, enter the name of your company.
4. For Company contact email address, enter the full email address that your invited users can contact if they have any questions while going through the enrollment process.
5. Choose Save.

You can edit the company name, company contact email, featured private skills, and featured public skills at any time.

Note

Any invitations that have been sent before you make edits displays old information in both the email and the online webpage that a user navigates to during enrollment.

To edit the user enrollment email

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose User Enrollment, Edit.
3. Edit the values for Company name, Company contact email address, Featured private skills, or Featured public skills.
4. Choose Save.

Invite and Remove Users

After you configure user enrollment for your organization, you can invite users.

To invite a user
1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Users and select Invite new user.
3. Enter the First name, Last name, and Email address of the user to enroll.
   **Note**
   Typically, this is a corporate email address that can be mapped to a corporate identity in your system. When connecting to a Microsoft Exchange account, this must be the same email address as the one on the corporate Exchange server. Make sure that the email addresses you enter when inviting users are correct. Whoever receives the email with the unique URL can log in with their Amazon account and be a part of your organization.
4. (Optional) Choose Add another user and add the information from step 3. Repeat this step until you have entered all the information for the users to invite.
5. Choose Send invite to send an invitation to each user for whom you provided information.

To remove a user
1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Users and select the check box next to the user to delete.
3. Choose Remove user, Remove.

After you remove a user, they can no longer access any of the benefits of being enrolled in your organization. If you remove a user who has not completed enrollment, the token is not valid.

A user might fail to enroll while the URL token is valid. In this case, you can resend the invitation.

To resend an expired invitation
1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Users and select the check box next to the user.
3. Choose Resend invitation.

Set up Microsoft Exchange Access for Users

You can link Alexa for Business to your Microsoft Exchange server. This enables enrolled users to ask Alexa about their scheduled events or add new events to their Microsoft Exchange calendar.

To give enrolled users access to their Microsoft Exchange calendar, set up a service account on your Microsoft Exchange server to access the users' calendars. After the service account is set up, users can link Alexa to their Microsoft Exchange using the Alexa app.

If you already set up a service account to access your room calendars, skip to step 3 and give the service account permissions to your users' calendars.
Before your proceed, confirm that you meet the following requirements:

- You have an administrator account within your Microsoft Exchange server.
- Microsoft Exchange is version 2013 or higher.
- You have a valid Exchange Web Services (EWS) endpoint with a valid digital certificate purchased from a trusted public certificate authority (CA).
- Basic authentication is enabled on both your EWS endpoint.

**To verify that basic authentication is enabled**

1. Open the Exchange Management Shell.
2. Type `Get-WebServicesVirtualDirectory | fl`.
3. Verify that the parameter `BasicAuthentication` is set to `True`.
4. If basic authentication isn't enabled, run the following command to enable it:

   ```powershell
   Set-WebServicesVirtualDirectory -Identity "Contoso\EWS(Default Web Site)" -BasicAuthentication $true
   ```

   **Note**
   - Contoso\EWS(Default Web Site) is the identity of the EWS virtual directory.

**To create a service account with access to the calendars in your organization**

1. Open the Exchange Management Shell.
2. Run the following command to create the service account:

   ```powershell
   New-Mailbox -UserPrincipalName alexaforbusiness@your_domain -Alias Alexa for Business -Name alexaforbusiness -OrganizationalUnit Users -FirstName Alexa -LastName Service Account -DisplayName "Alexa for Business Service Account"
   ```

   **Note**
   - Make sure that "your_domain" is the domain of your organization. You are prompted to enter a password.

The service account must have permissions to access the calendars in your organization. You can enable service account access to the calendars in your organization by using one of the following two methods:

- Set up impersonation, which enables the service account to impersonate a given account so that it can perform all operations using the permissions associated with the given account.
- Add the service account as full access and send as permissions for each of your user mailboxes.

**To set up impersonation**

1. Open the Exchange Management Shell and run the following command:

   ```powershell
   New-ManagementRoleAssignment -name:impersonationAssignmentName -Role:ApplicationImpersonation -User: alexaforbusiness
   ```

2. To limit the service account, define the scope. For example, to only give the service account permissions to the room mailboxes in the organization, run the following command in Exchange Management Shell:

   ```powershell
   New-ManagementScope -Name "UserMailboxes" -RecipientRestrictionFilter {RecipientTypeDetails -eq "UserMailbox"}
   ```

3. To apply permissions to the service account, run the following command:
New-ManagementRoleAssignment -Name "ResourceImpersonation" -Role ApplicationImpersonation -User alexaforbusiness -CustomRecipientWriteScope "UserMailboxes"

To add the service account as full access

- Run one of the following commands to give the service account access to all user mailboxes:

  For a single user:

  Add-MailboxFolderPermission <username>:\Calendar -user alexaforbusiness -accessrights Editor

  Add-ADPermission -Identity <username> -User alexaforbusiness -Extendedrights "Send As"

  **Note**
  Replace <username> with the alias of your user.

  For all user mailboxes:

  $users = Get-Mailbox -ResultSize unlimited -RecipientTypeDetails UserMailbox | Select -ExpandProperty Name ForEach ($user in $users) { Add-MailboxFolderPermission -Identity $user:\Calendar -user alexaforbusiness -accessrights Editor Add-ADPermission -Identity $user –User alexaforbusiness -Extendedrights "Send As" }

To link the service account to Alexa for Business

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Calendar, Microsoft Exchange.
3. Enter the user principal name (UPN) of your service account and service account password.
4. Enter the URL of your EWS endpoint. The default URL for EWS is usually in the following format: https://mail.domain.com/EWS/Exchange.asmx.
5. Select the access method that you have set up and choose Link account.

To test integration to access the calendar of an enrolled user

1. Open the Alexa app as an enrolled user.
2. Choose Settings, Calendar.
3. Choose Microsoft Exchange and complete the required steps.

Alexa can now read back the upcoming events on the calendar.

To troubleshoot Microsoft Exchange access

- If you experience one of the following issues, follow these steps:

  - If account linking fails in the Alexa app, verify that the email address you invited the user with matches the email address in your Microsoft Exchange server. Also, make sure that basic authentication is enabled for your EWS endpoint.

  - If setting up the Microsoft Exchange account fails in Alexa for Business and you see the error message "The calendar account could not be linked. If the issue persists, contact AWS Support. Invalid parameter provided.", validate that your EWS endpoint is valid and remotely accessible.
To test the EWS endpoint connection and service account credentials

1. Open the Microsoft Remote Connectivity Analyzer.
2. On the Exchange Server tab, choose Service account access.
3. Follow the prompts, fill in the required information, and verify that the service is working correctly.
4. If you receive one of the following results, follow these steps:
   - If the tool fails, the issue is probably your setup. Verify the following:
     - You’re using the EWS endpoint instead of the OWA endpoint. EWS endpoints are usually formatted as: https://mail.domain.com/EWS/Exchange.asmx
     - The service account and password are correct.
     - You’re using Microsoft Exchange 2013 or higher.
     - Your EWS endpoint is reachable from the internet.
   - If the tool succeeds, but associating the account still fails in the Alexa for Business console, verify that you have entered the right credentials in the console.
   - If the issue persists, contact AWS Support.

To manage expiring service account passwords

1. Create a new user principal name (UPN) service account and password.
2. Ensure that the new UPN service account has access to calendars, impersonation, and full access.
3. Validate that the new account works by testing the EWS endpoint and UPN.
4. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
5. Choose Calendar, Microsoft Exchange.
6. Enter the new user principal name (UPN) of the service account that you just created.
7. Enter the service account password for the new UPN, and choose Link account.

Expiring password notifications

Alexa for Business sends warning emails to the service account holder at 14 days, 7 days, 3 days, and 1 day before their password expires. After the password expires, the user receives a daily reminder email. Users can also see these alerts in their AWS Personal Health Dashboard.

Require Users to Restrict Calendars to Voice

After users link their work calendars to Alexa, they can restrict their calendars to respond to their voices only. You have the option in the Alexa for Business console to make this a requirement for all users by registering domains for voice restriction. The domains must match the email addresses of the linked calendars.

To add domains for calendar voice restriction

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Calendars, and in the Calendar voice restriction section, choose Add domain.
3. Follow the steps to add your email domain (for example, example.com).

To remove domains from calendar voice restriction

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Calendars, and in the Calendar voice restriction section, select the check box next to the domain you want to remove.
3. Choose Remove domain and follow the steps.

Enrolled users can set a voice restriction for their linked calendar accounts in the Alexa app. When users set a voice restriction, Alexa uses voice profiles to determine who is speaking, and when to provide information from their calendar.

Note
To set a voice restriction for their calendar, users must first create a voice profile. If they don't have one already, they are prompted to create one in the Voice Restriction section in their calendar settings. For more information, see Create a Voice Profile.

To set a voice restriction for a calendar
1. Open the Alexa app, and on the menu, choose Settings and Calendar.
2. Choose the linked calendar from the list.
3. In the Voice Restriction section, on the menu, choose one of the following options:
   - Only My Voice – Alexa reads calendar events only after recognizing your voice.
   - All Enrolled Voices – Alexa reads calendar events for any recognized speakers in your home with a voice profile.
   - No Voice Restriction – Alexa doesn't restrict access to the calendar.

The voice restriction selected applies to all of the devices registered to the user's account.

If there are other adult users in the user's home, users can personalize calendar access across their shared Alexa devices by creating an Amazon Household. Users can link their calendar accounts to Alexa individually in the Alexa app, then set the Only My Voice voice restriction so that Alexa provides information from that calendar only when recognizing each of their voices. For more information, see Using Household Profiles on Alexa Devices.

Instruct Users to Use the Alexa Smart Scheduling Assistant

Alexa for Business allows enrolled users to connect their work calendar to Alexa. They can then use the Alexa Smart Scheduling Assistant to add, move, or cancel meetings or ask Alexa about what meetings are on their calendar. They can also invite other users to join conference calls scheduled on their calendar.

The following calendars are supported:

- Google G Suite
- Microsoft Office 365
- Microsoft Exchange 2013 or later

Enrolled users can perform any of the following procedures.

To link a work calendar account to Alexa
1. Open the Alexa app, and on the menu, choose Settings, Calendar.
2. Choose your calendar from the list of supported providers, choose Link, and follow the steps.
   
   **Note**
   You may need to provide sign-in information for your calendar account and verify that you want to give Alexa access to it. To link your Exchange calendar to Alexa, your IT administrator must set up Exchange. For more information, see the section called “Set up Microsoft Exchange Access for Users” (p. 60).

3. Set your work calendar as the default calendar for new events.

**Enable Alexa calling and messaging**

- To join a conference call scheduled on your calendar, see Sign Up for Alexa Calling and Messaging.

**To manage contacts to use for scheduling or calling**

- To manage work or personal contacts for your Alexa app, see Add and Edit Your Contacts to the Alexa App.

**Use utterances to talk to Alexa**

- You can ask Alexa any of the following questions:
  
  - To browse events on your calendar:
    - Alexa, what's on my calendar?
    - Alexa, what's on my calendar tomorrow?
    - Alexa, what's on my calendar on [any day]?
  
  - To schedule a meeting:
    - Alexa, schedule a meeting today at 3PM.
    - Alexa, schedule a one hour meeting with John.
    - Alexa, schedule a meeting with John tomorrow.
  
  - To move a meeting:
    - Alexa, move my meeting.
    - Alexa, move my meeting at 2PM today to 4PM today.
    - Alexa, move my meeting called [meeting title] to 5PM tomorrow.
  
  - To cancel a meeting:
    - Alexa, cancel my meeting at 2PM today.
    - Alexa, cancel [meeting title] from my calendar.
  
  - To join a conference call:
    - Alexa, join my meeting.
  
  - To call a contact:
    - Alexa, call John.
    - Alexa, call 222-555-0126.

   **Note**
   Emergency services, such as 911, are not supported. For more information, see Alexa Calling and Messaging FAQs.

**Troubleshooting**

If you experience any of the following issues with the Alexa Smart Scheduling Assistant, try these steps:
• **I can't schedule a meeting with a contact, but I can schedule an event.**

  Choose **Contacts** in your Alexa companion app and see if the contact is displayed. If the contact is not in the Alexa app but in your phone contacts, log out of the app and log in again.

• **I can't get availability information when scheduling a meeting.**

  Open your calendar and check that you have access to the contact's availability information. Next, verify that there is an email address associated with your contact in your Alexa companion app. Then try again - Alexa may not have recognized the name you spoke. If you’re still having issues, try scheduling a different contact. If that doesn’t work, contact support through the **AWS Forum**.

• **I can't get availability for the full day.**

  For Microsoft Office 365 and Microsoft Exchange, Alexa follows the work hours set on the calendar. Work hours are set in your provider and can be changed using your calendar client. To learn more, contact your IT administrator.

• **I show as available on my calendar, but Alexa doesn't offer that time in its suggestion.**

  Alexa checks availability information across all linked calendars. For example, if you have Microsoft Office 365 and Gmail linked, then Alexa looks at the availability across both calendars for you as the organizer. Note that Alexa does check all calendars of the recipient.

• **I see "Created with Alexa <https://aws.amazon.com/alexaforbusiness>" in the invite email.**

  Meeting invites created with Alexa for Business include this text in the invite by default.
Creating Usage Reports

See how Alexa for Business helps your organization by creating usage reports. These reports include the following informative metrics:

- Invocations on shared devices
- Meetings joined using Alexa
- Private skill invocations
- Active enrolled users
- Alexa invocations on shared devices
- Meetings joined
- Private skill invocations
- Daily active enrolled users of Alexa for Business
- Meetings joined on shared devices
- Meetings auto-joined and joined by PIN
- Total utilization by room name on shared devices
- Meetings joined by room name on shared devices
- Private skill invocations on shared devices
- Top five invocation types on shared devices
- Top 25 invocation types on shared devices
- Total number of private skill invocations
- 30 day room utilization report

**Note**
For more information about these metrics, see the section called "View Room Utilization Metrics" (p. 56).

- Total meetings
- Total minutes
- Attended meetings
- Released meetings
- Attendance rate
- Released minutes
- Recovered meetings

The reports consist of .csv files that you can view in BI tools. You can use them for further analysis by using ETL processes. A visual HTML report is generated alongside the .csv files. It gives you a comprehensive view of Alexa for Business use in your organization. You can create a report to deliver immediately to your S3 bucket, or create a scheduled report that gets delivered automatically to your S3 bucket daily or weekly. The .csv files contain 1-day or 7-day aggregate metrics based on your selection. The HTML report shows a summary of the last 30 days of use.

**Tasks**
- Usage Report Prerequisites (p. 68)
- Create a Report (p. 68)
• Create a Scheduled Report (p. 69)

Usage Report Prerequisites

Before you can export your usage reports to S3, complete the following steps.

To prepare for report creation

1. If you don't have one already, create an S3 bucket.

2. Open the S3 console and create an S3 bucket.

3. Enter a bucket name. (For example, my-s3-bucket-name.)

4. Set the S3 bucket policy.

   1. Select the S3 bucket you created, choose Permissions, and then choose Bucket Policy.

   2. In the Bucket policy editor, copy and paste the following S3 bucket policy. Replace "<my-s3-bucket-name>" with your bucket name, and choose Save.

      ```json
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Sid": "Stmt1530229847751",
            "Effect": "Allow",
            "Principal": {
              "AWS": "arn:aws:iam::994698236012:root"
            },
            "Action": [
              "s3:PutObject",
              "s3:PutObjectAcl",
              "s3:GetBucketAcl"
            ],
            "Resource": [
              "arn:aws:s3::<my-s3-bucket-name>",
              "arn:aws:s3::<my-s3-bucket-name>/**
            ]
          }
        ]
      }
      ```

3. Verify that you have permissions to write to the S3 bucket location. Also make sure that the AWS IAM user, which you logged into the Alexa for Business console with, has the same permissions.

   Note
   
   If your IAM user can't write to the S3 bucket, you can't configure it as an export location.

Create a Report

You can create an individual report to immediately deliver to your S3 bucket.

To create a report

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.

2. Choose Reports, and then choose the Create report button on the Create report tab.
Create a Scheduled Report

You can create a scheduled report that gets delivered automatically to your S3 bucket every day or every week.

To create a scheduled report

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose Reports, and then choose the Schedule report button on the Scheduled reports tab.
3. Enter a Name for the report, then choose the Frequency, Delivery day, Format, S3 bucket name, and Path prefix.

   Note
   Using a zip file format containing individual .csv files is usually better for archive use cases, and using an unpacked structure is easier for automated processing of data or ETL. The file name for zip files and partition for unpacked files include the date range associated with the data. The file/partition name or the date column in the spreadsheet corresponds to the last day of the date range. For example, for a 7-day aggregate, the date column is the final day of the date range.

4. When you’re done, choose Create.

   You can view your scheduled reports at any time on the Schedule reports tab or from the Alexa for Business Dashboard. On the Dashboard, under the Usage Reports section, choose the button to view your daily or weekly reports and open the S3 location associated with those reports.

   To stop the delivery of scheduled reports, choose Remove schedule reports on the Schedule reports tab.
Security in Alexa for Business

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is 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, as follows:

- **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. For more information about the compliance programs that apply to Alexa for Business, 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 Alexa for Business. The following topics show you how to configure Alexa for Business to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Alexa for Business resources.

Topics
- Data Protection in Alexa for Business (p. 70)
- Identity and Access Management for Alexa for Business (p. 71)
- Logging and Monitoring in Alexa for Business (p. 80)
- Compliance Validation for Alexa for Business (p. 82)
- Resilience in Alexa for Business (p. 82)
- Infrastructure Security in Alexa for Business (p. 82)
- Configuration and Vulnerability Analysis in Alexa for Business (p. 83)
- Security Best Practices for Alexa for Business (p. 83)

Data Protection in Alexa for Business

The Alexa for Business console collects data necessary to set up, configure, and manage Alexa devices being operated by Alexa for Business. Specifically, Alexa for Business collects emails that are used to invite employees or others to link their personal accounts to their corporate Alexa for Business account. In addition, the Alexa system collects and stores voice data used to interact with Alexa, as well as responses, in order to improve Alexa features, such as speech recognition and natural language understanding.

To secure your content, Alexa for Business and Alexa provides multiple methods to clear voice and transcript data from the Alexa system, including the Alexa for Business console, APIs, and voice commands. You can also choose not to have your data annotated by humans, so it will only be used for machine learning.

All customer-specific data within Alexa for Business and Alexa is encrypted at rest and in transit. Alexa for Business secures content by default.
Data Encryption

All customer-specific data within Alexa for Business and Alexa is encrypted at rest and in transit. Alexa for Business data is encrypted at rest using a CMK owned by AWS, and Alexa data is encrypted using a KMS owned by the Alexa team.

Encryption at Rest

Encryption at rest is configured by default.

Encryption in Transit

Encryption in transit is configured by default. Alexa for Business offers secure connections between Alexa/Echo devices and the Alexa cloud with HTTPS using TLS 1.2.

Key Management

There are currently no options for customers to manage encryption keys.

Interwork Traffic Privacy

This section does not apply to Alexa for Business.

Identity and Access Management for Alexa for Business

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be authenticated (signed in) and authorized (have permissions) to use Alexa for Business resources. IAM is an AWS service that you can use with no additional charge.

Topics

• Audience (p. 71)
• Authenticating With Identities (p. 72)
• Managing Access Using Policies (p. 73)
• How Alexa for Business Works with IAM (p. 75)
• Alexa for Business Identity-Based Policy Examples (p. 77)
• Troubleshooting Alexa for Business Identity and Access (p. 79)

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work you do in Alexa for Business.

Service user – If you use the Alexa for Business service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Alexa for Business features to do your work, you might need additional permissions. Understanding how access is managed can help
you request the right permissions from your administrator. If you cannot access a feature in Alexa for Business, see Troubleshooting Alexa for Business Identity and Access (p. 79).

**Service administrator** – If you're in charge of Alexa for Business resources at your company, you probably have full access to Alexa for Business. It's your job to determine which Alexa for Business features and resources your employees should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Alexa for Business, see How Alexa for Business Works with IAM (p. 75).

**IAM administrator** – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Alexa for Business. To view example Alexa for Business identity-based policies that you can use in IAM, see Alexa for Business Identity-Based Policy Examples (p. 77).

## Authenticating With Identities

Authentication is how you sign in to AWS using your identity credentials. For more information about signing in using the AWS Management Console, see The IAM Console and Sign-in Page in the IAM User Guide.

You must be authenticated (signed in to AWS) as the AWS account root user, an IAM user, or by assuming an IAM role. You can also use your company's single sign-on authentication, or even sign in using Google or Facebook. In these cases, your administrator previously set up identity federation using IAM roles. When you access AWS using credentials from another company, you are assuming a role indirectly.

To sign in directly to the AWS Management Console, use your password with your root user email or your IAM user name. You can access AWS programmatically using your root user or IAM user access keys. AWS provides SDK and command line tools to cryptographically sign your request using your credentials. If you don't use AWS tools, you must sign the request yourself. Do this using Signature Version 4, a protocol for authenticating inbound API requests. For more information about authenticating requests, see Signature Version 4 Signing Process in the AWS General Reference.

Regardless of the authentication method that you use, you might also be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Using Multi-Factor Authentication (MFA) in AWS in the IAM User Guide.

### AWS Account Root User

When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

### IAM Users and Groups

An **IAM user** is an identity within your AWS account that has specific permissions for a single person or application. An IAM user can have long-term credentials such as a user name and password or a set of access keys. To learn how to generate access keys, see Managing Access Keys for IAM Users in the IAM User Guide. When you generate access keys for an IAM user, make sure you view and securely save the key pair. You cannot recover the secret access key in the future. Instead, you must generate a new access key pair.

An **IAM group** is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to
manage for large sets of users. For example, you could have a group named IAMAdmins and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see When to Create an IAM User (Instead of a Role) in the IAM User Guide.

IAM Roles

An IAM role is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by switching roles. You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Using IAM Roles in the IAM User Guide.

IAM roles with temporary credentials are useful in the following situations:

- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.
- **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as federated users. AWS assigns a role to a federated user when access is requested through an identity provider. For more information about federated users, see Federated Users and Roles in the IAM User Guide.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see How IAM Roles Differ from Resource-based Policies in the IAM User Guide.
- **AWS service access** – A service role is an IAM role that a service assumes to perform actions in your account on your behalf. When you set up some AWS service environments, you must define a role for the service to assume. This service role must include all the permissions that are required for the service to access the AWS resources that it needs. Service roles vary from service to service, but many allow you to choose your permissions as long as you meet the documented requirements for that service. Service roles provide access only within your account and cannot be used to grant access to services in other accounts. You can create, modify, and delete a service role from within IAM. For example, you can create a role that allows Amazon Redshift to access an Amazon S3 bucket on your behalf and then load data from that bucket into an Amazon Redshift cluster. For more information, see Creating a Role to Delegate Permissions to an AWS Service in the IAM User Guide.
- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see Using an IAM Role to Grant Permissions to Applications Running on Amazon EC2 Instances in the IAM User Guide.

To learn whether to use IAM roles, see When to Create an IAM Role (Instead of a User) in the IAM User Guide.

Managing Access Using Policies

You control access in AWS by creating policies and attaching them to IAM identities or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions.
AWS evaluates these policies when an entity (root user, IAM user, or IAM role) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see Overview of JSON Policies in the IAM User Guide.

An IAM administrator can use policies to specify who has access to AWS resources, and what actions they can perform on those resources. Every IAM entity (user or role) starts with no permissions. In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

### Identity-Based Policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, role, or group. These policies control what actions that identity can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM Policies in the IAM User Guide.

Identity-based policies can be further categorized as inline policies or managed policies. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see Choosing Between Managed Policies and Inline Policies in the IAM User Guide.

### Resource-Based Policies

Resource-based policies are JSON policy documents that you attach to a resource such as an Amazon S3 bucket. Service administrators can use these policies to define what actions a specified principal (account member, user, or role) can perform on that resource and under what conditions. Resource-based policies are inline policies. There are no managed resource-based policies.

### Access Control Lists (ACLs)

Access control lists (ACLs) are a type of policy that controls which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format. Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see Access Control List (ACL) Overview in the Amazon Simple Storage Service Developer Guide.

### Other Policy Types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of entity’s identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the Principal field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions Boundaries for IAM Entities in the IAM User Guide.
• **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see How SCPs Work in the AWS Organizations User Guide.

• **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see Session Policies in the IAM User Guide.

### Multiple Policy Types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy Evaluation Logic in the IAM User Guide.

### How Alexa for Business Works with IAM

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

#### Topics

- Alexa for Business Identity-Based Policies (p. 75)
- Alexa for Business Resource-Based Policies (p. 77)
- Access Control Lists (ACLs) (p. 77)
- Authorization Based on Alexa for Business Tags (p. 77)
- Alexa for Business IAM Roles (p. 77)

### Alexa for Business Identity-Based Policies

With IAM identity-based policies, you can specify allowed or denied actions and resources, and also the conditions under which actions are allowed or denied. Alexa for Business supports specific actions, resources, and condition keys. For more information about all of the elements that you use in a JSON policy, see IAM JSON Policy Elements Reference in the IAM User Guide.

#### Actions

The **Action** element of an IAM identity-based policy describes the specific action or actions that will be allowed or denied by the policy. Policy actions usually have the same name as the associated AWS API operation. The action is used in a policy to grant permissions to perform the associated operation.

Policy actions in Alexa for Business use the following prefix before the action: `a4b:`. For example, to grant someone permission to run an Amazon EC2 instance with the Amazon EC2 RunInstances API operation, you include the `ec2:RunInstances` action in their policy. Policy statements must include either an **Action** or **NotAction** element. Alexa for Business defines its own set of actions that describe tasks that you can perform with this service.

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

```json
"Action": [ "a4b:GetTranscript", "a4b:PutTranscript" ]
```
Alexa for Business Administration Guide
How Alexa for Business Works with IAM

"ec2:action1",
"ec2:action2"

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

"Action": "ec2:Describe*"

To see a list of Alexa for Business actions, see Actions Defined by Alexa for Business in the IAM User Guide.

Resources

The Resource element specifies the object or objects to which the action applies. Statements must include either a Resource or a NotResource element. You specify a resource using an ARN or using the wildcard (*) to indicate that the statement applies to all resources.

The Amazon EC2 instance resource has the following ARN:

`arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}`

For more information about the format of ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces.

For example, to specify the i-1234567890abcdef0 instance in your statement, use the following ARN:

"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"

To specify all instances that belong to a specific account, use the wildcard (*):

"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/"*

Some Alexa for Business actions, such as those for creating resources, cannot be performed on a specific resource. In those cases, you must use the wildcard (*).

"Resource": "*"

Many Amazon EC2 API actions involve multiple resources. For example, AttachVolume attaches an Amazon EBS volume to an instance, so an IAM user must have permissions to use the volume and the instance. To specify multiple resources in a single statement, separate the ARNs with commas.

"Resource": [
   "resource1",
   "resource2"
]

To see a list of Alexa for Business resource types and their ARNs, see Resources Defined by Alexa for Business in the IAM User Guide. To learn with which actions you can specify the ARN of each resource, see Actions Defined by Alexa for Business.

Condition Keys

Alexa for Business does not support any global condition keys.
Examples

To view examples of Alexa for Business identity-based policies, see Alexa for Business Identity-Based Policy Examples (p. 77).

Alexa for Business Resource-Based Policies

Alexa for Business does not support resource-based policies.

Access Control Lists (ACLs)

Alexa for Business does not support Access Control Lists (ACLs).

Authorization Based on Alexa for Business Tags

Alexa for Business does not support tagging resources or controlling access based on tags.

Alexa for Business IAM Roles

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

Using Temporary Credentials with Alexa for Business

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

Alexa for Business supports using temporary credentials.

Service-Linked Roles

Alexa for Business does not support service-linked roles.

Service Roles

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

Alexa for Business supports service roles.

Alexa for Business Identity-Based Policy Examples

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

For more information about how to create an IAM identity-based policy using these example JSON policy documents, see Creating Policies on the JSON Tab in the IAM User Guide.

Topics

- Policy Best Practices (p. 78)
- Allow Users to View Their Own Permissions (p. 78)
Policy Best Practices

Identity-based policies are very powerful. They determine whether someone can create, access, or delete Alexa for Business resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get Started Using AWS Managed Policies** – To start using Alexa for Business quickly, use AWS managed policies to give your employees the permissions they need. These policies are already available in your account and are maintained and updated by AWS. For more information, see Get Started Using Permissions With AWS Managed Policies in the IAM User Guide.

- **Grant Least Privilege** – When you create custom policies, grant only the permissions required to perform a task. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. For more information, see Grant Least Privilege in the IAM User Guide.

- **Enable MFA for Sensitive Operations** – For extra security, require IAM users to use multi-factor authentication (MFA) to access sensitive resources or API operations. For more information, see Using Multi-Factor Authentication (MFA) in AWS in the IAM User Guide.

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

Allow Users to View Their Own Permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```
Troubleshooting Alexa for Business Identity and Access

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

Topics
- I Am Not Authorized to Perform iam:PassRole (p. 79)
- I Want to View My Access Keys (p. 79)
- I'm an Administrator and Want to Allow Others to Access Alexa for Business (p. 80)
- I Want to Allow People Outside of My AWS Account to Access My Alexa for Business Resources (p. 80)

I Am Not Authorized to Perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password. Ask that person to update your policies to allow you to pass a role to Alexa for Business.

Some AWS services allow you to pass an existing role to that service, instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Alexa for Business. However, the action requires the service to have permissions granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

In this case, Mary asks her administrator to update her policies to allow her to perform the `iam:PassRole` action.

I Want to View My Access Keys

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

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

**Important**

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

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

To allow others to access Alexa for Business, you must create an IAM entity (user or role) for the person or application that needs access. They will use the credentials for that entity to access AWS. You must then attach a policy to the entity that grants them the correct permissions in Alexa for Business.

To get started right away, see Creating Your First IAM Delegated User and Group in the IAM User Guide.

I Want to Allow People Outside of My AWS Account to Access My Alexa for Business Resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

• To learn whether Alexa for Business supports these features, see How Alexa for Business Works with IAM (p. 75).
• To learn how to provide access to your resources across AWS accounts that you own, see Providing Access to an IAM User in Another AWS Account That You Own in the IAM User Guide.
• To learn how to provide access to your resources to third-party AWS accounts, see Providing Access to AWS Accounts Owned by Third Parties in the IAM User Guide.
• To learn how to provide access through identity federation, see Providing Access to Externally Authenticated Users (Identity Federation) in the IAM User Guide.
• To learn the difference between using roles and resource-based policies for cross-account access, see How IAM Roles Differ from Resource-based Policies in the IAM User Guide.

Loggging and Monitoring in Alexa for Business

Alexa for Business is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Alexa for Business. CloudTrail captures all API calls for Alexa for Business as events. The calls captured include calls from the Alexa for Business console and code calls to the Alexa for Business API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Alexa for Business. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail, you can determine the request that was made to Alexa for Business, the IP address from which the request was made, who made the request, when it was made, and additional details.

For more information about CloudTrail, see the AWS CloudTrail User Guide.

Alexa for Business Information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Alexa for Business, that activity is recorded in a CloudTrail event along with other AWS service events in Event history. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for Alexa for Business, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create
a trail in the console, the trail applies to all AWS Regions. Currently, events for Alexa for Business appear only in US East (N. Virginia), which is the only available Region. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

All Alexa for Business actions are logged by CloudTrail and are documented in the Alexa for Business API Reference. For example, CreateRoom, AssociateSkillGroupWithRoom, and DeleteRoom all generate entries in CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine whether the request was made:

- With root or AWS Identity and Access Management (IAM) user credentials.
- With temporary security credentials for a role or federated user.
- By another AWS service.

For more information, see the CloudTrail userIdentity Element.

Understanding Alexa for Business Log File Entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following is an example of a CloudTrail log entry for Alexa for Business:

```json
{
    "Records": [{
        "eventVersion": "1.05",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Jane",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Jane"
        },
        "eventTime": "2017-11-13T10:00:02Z",
        "eventSource": "a4b.amazonaws.com",
        "eventName": "CreateRoom",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.2.0.1",
        "userAgent": "AWS Internal",
        "requestParameters": null,
        "responseElements": {
            "roomArn": "arn:aws:a4b:us-east-1:123456789012:room/8eed09c4eae340d2ba08b8c6c3e40970/66afda686e75c5b62fcef60ac00e7a6"
        }
    }
}
```
Compliance Validation for Alexa for Business

Alexa for Business is not in scope of any AWS compliance programs.

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 Alexa for Business 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.
- **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.

Resilience in Alexa for Business

This section does not apply to Alexa for Business.

Infrastructure Security in Alexa for Business

This section does not apply to Alexa for Business.
Configuration and Vulnerability Analysis in Alexa for Business

Echo devices automatically receive updates from Amazon without any customer interaction.

Security Best Practices for Alexa for Business

This section does not apply to Alexa for Business.
The following table describes important changes to the Alexa for Business Administration Guide, beginning in November 2017. For notifications about updates to this documentation, you can subscribe to an RSS feed.

<table>
<thead>
<tr>
<th>update-history-change</th>
<th>update-history-description</th>
<th>update-history-date</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can use Alexa for Business with Lifesize room systems. (p. 84)</td>
<td>For more information, see Use Lifesize room systems with Alexa for Business.</td>
<td>June 9, 2020</td>
</tr>
<tr>
<td>The max volume range for a room profile has changed to 4-10. (p. 84)</td>
<td>For more information, see Managing Room Profiles.</td>
<td>May 12, 2020</td>
</tr>
<tr>
<td>If intelligent room release is on, users now get an email when their room is released. Also, any interaction with Alexa counts as a check-in, and recurring meeting data is included in room utilization metrics. (p. 84)</td>
<td>For more information, see Configure Meeting Room Settings and View Room Utilization Metrics in the Alexa for Business Administrator’s Guide.</td>
<td>April 8, 2020</td>
</tr>
<tr>
<td>Echo Dot 3rd generation with clock is now supported. (p. 84)</td>
<td>For more information, see Getting Started with Shared Devices in the Alexa for Business Administrator’s Guide.</td>
<td>March 10, 2020</td>
</tr>
<tr>
<td>Configure Alexa for Business to meet your security and compliance objectives, and learn how to use other AWS services that help you to secure your Alexa for Business resources. (p. 84)</td>
<td>For more information, see Security in Alexa for Business in the Alexa for Business Administrator’s Guide.</td>
<td>December 20, 2019</td>
</tr>
<tr>
<td>Meeting room settings help you measure and improve your meeting room utilization (p. 84)</td>
<td>For more information, see Configure Room Settings in the Alexa for Business Administrator’s Guide.</td>
<td>November 25, 2019</td>
</tr>
<tr>
<td>Alexa now supports Amazon Chime on Dolby Voice Room (p. 84)</td>
<td>For more information, see Compatible Conference Devices in the Alexa for Business Administrator’s Guide.</td>
<td>October 29, 2019</td>
</tr>
<tr>
<td>Enable data use policy to help improve our services (p. 84)</td>
<td>For more information, see Managing Room Profiles in the Alexa for Business Administrator’s Guide.</td>
<td>August 13, 2019</td>
</tr>
<tr>
<td>Action</td>
<td>For more information, see</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Contacts can contain multiple phone numbers and one SIP address (p. 84)</td>
<td>Managing Contacts in the Alexa for Business Administrator's Guide.</td>
<td>June 21, 2019</td>
</tr>
<tr>
<td>To simplify the process of creating and managing network configurations, you can define network profiles. (p. 84)</td>
<td>Managing Network Profiles in the Alexa for Business Administrator's Guide.</td>
<td>May 21, 2019</td>
</tr>
<tr>
<td>Send Alexa announcements to one or more rooms. Alexa will wake and speak the announcement that you create. (p. 84)</td>
<td>Sending Announcements in the Alexa for Business Administrator's Guide.</td>
<td>May 2, 2019</td>
</tr>
<tr>
<td>Use Polycom Trio with Alexa for Business (p. 84)</td>
<td>Use Polycom Trio with Alexa for Business in the Alexa for Business Administrator’s Guide.</td>
<td>April 16, 2019</td>
</tr>
<tr>
<td>Users can ask Alexa to find an available meeting room (p. 84)</td>
<td>Managing Conferencing and Room Booking in the Alexa for Business Administrator’s Guide.</td>
<td>April 3, 2019</td>
</tr>
<tr>
<td>Publish private business skills with Alexa Skill Blueprints (p. 84)</td>
<td>Alexa Skill Blueprints in the Alexa for Business Administrator’s Guide.</td>
<td>March 27, 2019</td>
</tr>
<tr>
<td>Run multiple gateways (p. 84)</td>
<td>Running Multiple Gateways in the Alexa for Business Administrator’s Guide.</td>
<td>March 15, 2019</td>
</tr>
<tr>
<td>Import Devices with the Alexa Companion App (p. 84)</td>
<td>Import Your Devices in the Alexa for Business Administrator’s Guide.</td>
<td>January 16, 2019</td>
</tr>
<tr>
<td>Use the Device Setup Tool for WPA2 Enterprise network security type (p. 84)</td>
<td>Run the Device Setup Tool in the Alexa for Business Administrator’s Guide.</td>
<td>December 10, 2018</td>
</tr>
<tr>
<td>See how Alexa for Business helps your organization by creating usage reports (p. 84)</td>
<td>Creating Usage Reports in the Alexa for Business Administrator’s Guide.</td>
<td>December 7, 2018</td>
</tr>
<tr>
<td>Use Alexa for Business to control your Polycom Group Series systems and join meetings by using your voice. (p. 84)</td>
<td>Use Polycom Group Series with Alexa for Business in the Alexa for Business Administrator’s Guide.</td>
<td>December 6, 2018</td>
</tr>
<tr>
<td>Feature</td>
<td>More Information</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Register an Alexa Voice Service (AVS) device with Alexa for Business by giving access to the Alexa built-in device maker. (p. 84)</td>
<td>For more information, see AVS Permissions in the Alexa for Business Administrator's Guide.</td>
<td>October 24, 2018</td>
</tr>
<tr>
<td>Ask Alexa to check whether a room is available, book a room, and tell you who reserved a room (p. 84)</td>
<td>For more information, see Link Alexa for Business to Your Calendar System in the Alexa for Business Administrator’s Guide.</td>
<td>October 9, 2018</td>
</tr>
<tr>
<td>Use the Device Setup Tool - Beta for WPA2 Enterprise network security type (p. 84)</td>
<td>For more information, see Run the Device Setup Tool in the Alexa for Business Administrator’s Guide.</td>
<td>September 24, 2018</td>
</tr>
<tr>
<td>Link Alexa for Business to Office 365 with delegate or application permissions (p. 84)</td>
<td>For more information, see Link Alexa for Business to Office 365 in the Alexa for Business Administrator’s Guide.</td>
<td>August 15, 2018</td>
</tr>
<tr>
<td>New deregistered device status (p. 84)</td>
<td>For more information, see Managing Devices in the Alexa for Business Administrator’s Guide.</td>
<td>August 3, 2018</td>
</tr>
<tr>
<td>Calendar voice restriction and Alexa Smart Scheduling Assistant (p. 84)</td>
<td>For more information, see Require Users to Restrict Calendars to Voice and Instruct Users to Use the Alexa Smart Scheduling Assistant in the Alexa for Business Administrator’s Guide.</td>
<td>May 21, 2018</td>
</tr>
<tr>
<td>Connect Alexa for Business to your Zoom Rooms system (p. 84)</td>
<td>For more information, see Use Zoom Rooms with Alexa for Business in the Alexa for Business Administrator’s Guide.</td>
<td>May 9, 2018</td>
</tr>
<tr>
<td>View the network connection status of a device and monitor devices using CloudWatch (p. 84)</td>
<td>For more information, see Managing Devices in the Alexa for Business Administrator’s Guide.</td>
<td>April 30, 2018</td>
</tr>
<tr>
<td>Password expiration emails (p. 84)</td>
<td>For more information, see Set up Microsoft Exchange Access for Users in the Alexa for Business Administrator’s Guide.</td>
<td>April 26, 2018</td>
</tr>
<tr>
<td>Various conferencing updates (p. 84)</td>
<td>For more information, see Managing Conferencing in the Alexa for Business Administrator’s Guide.</td>
<td>April 10, 2018</td>
</tr>
<tr>
<td>Change permissions for a skill (p. 84)</td>
<td>For more information, see Managing Skills in the Alexa for Business Administrator’s Guide.</td>
<td>April 6, 2018</td>
</tr>
<tr>
<td>Feature</td>
<td>Information</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Make calls from your shared devices with Alexa for Business (p. 84)</td>
<td>For more information, see Managing Calling in the Alexa for Business Administrator’s Guide.</td>
<td>March 28, 2018</td>
</tr>
<tr>
<td>Updates to the Device Setup Tool (p. 84)</td>
<td>For more information, see Run the Device Setup Tool in the Alexa for Business Administrator’s Guide.</td>
<td>March 26, 2018</td>
</tr>
<tr>
<td>Added support for Fuze and Google Hangouts Meet (p. 84)</td>
<td>For more information, see Understanding Alexa-enabled Conferencing in the Alexa for Business Administrator’s Guide.</td>
<td>March 16, 2018</td>
</tr>
<tr>
<td>Use the Alexa for Business gateway to connect Alexa for Business to your Cisco TelePresence systems (p. 84)</td>
<td>For more information, see Use the Alexa for Business Gateway in the Alexa for Business Administrator’s Guide.</td>
<td>February 8, 2018</td>
</tr>
<tr>
<td>Assign multiple devices to a room (p. 84)</td>
<td>For more information, see Managing Devices in the Alexa for Business Administrator’s Guide.</td>
<td>January 26, 2018</td>
</tr>
<tr>
<td>Initial release (p. 84)</td>
<td>Initial release</td>
<td>November 29, 2017</td>
</tr>
</tbody>
</table>