Alexa for Business

Administration Guide

Alexa for Business: Administration Guide

Table of Contents

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. 13).

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 a 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)

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, use the following procedure to create one.

To sign up for AWS

1. Open https://aws.amazon.com/ and choose **Create an AWS Account**.
2. Follow the online instructions.

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. 7).

Firewall and Network Requirements

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

Service	Protocol	Destination Port	Transport
Signaling	HTTPS	443	TCP
Media port/connectivity negotiation	ICE/STUN/TURN	3478	TCP/UDP **Note** UDP is preferred. Only open TCP 3478 if UDP 3478 isn't allowed.
Conference or PSTN calling audio **Note** G.711 audio codec	SRTP	49152 - 65535	UDP

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 and 2nd generation)
- Echo Dot (2nd generation)
- Echo Plus

Tasks

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 an IAM User for Device Setup Tool

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. Choose **Create user**.
6. 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

Follow these steps to run the Device Setup Tool.

To run the Device Setup Tool

1. Download, install, and open the Device Setup Tool on a Windows computer enabled with Wi-Fi.

   Note
   By downloading the Device Setup Tool, you agree to the AWS Customer Agreement and AWS Service Terms. If you already have an AWS customer agreement, you agree that the terms of that agreement govern your download and use of this product.
2. From the home page of the application, choose **Get started**.
3. Enter the IAM access key and secret access key that you created for the Device Setup Tool user, and choose **Next**.
4. Enter the Wi-Fi information of the network to connect to your Alexa devices.
5. Enter the Wi-Fi information of the network to connect to your computer during setup, and choose **Next**.

   Note
   To change this information later, choose **Change Wi-Fi** from the **Device setup** home page.
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**.
8. 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 1–8 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. 9)
- A room profile (p. 10)
- A skill group (p. 16)

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

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. If you are planning to enable smart home skills in your room, we recommend naming rooms with only alphanumeric characters and the following special characters (no dots, no spaces): _ - = # ; : ? @ &.

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. 11).

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**.

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 the 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.

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**.
   - **Distance units** – Choose **Feet** or **Meters**.
   - **Max volume** – Choose a value between **6**–**10** to limit the volume output of the device to this value.
   - **Device setup mode** – Choose **On** to allow users to hold the action button for 7 seconds to put the device into setup mode. Otherwise, choose **Off**.
   - **Outbound calling** – Choose **Enable** or **Disable** to specify the ability to make outbound PSTN phone calls from the Echo devices.

- **Address book** – Select the address book you want to assign to the room profile.

4. Choose **Create**.

You can edit the name, description, and room profile of your room in **Room profile**.

To edit a room profile

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Room profiles** and choose the name of the room profile to edit.
3. Edit any of the fields and choose **Save**.

If a room profile is assigned to a room, you can't delete it.

To delete a room profile

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Room profiles**, **Delete room profile**.
3. Select the check box next the room profile to delete.
4. Choose **Delete room profile**, **Delete**.

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. 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 a device

1. If you haven't already, install the Device Setup Tool. For more information, see Run the Device Setup Tool (p. 7).
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 **Discover devices**.

5. Choose the devices to set up and choose **Set up devices**.
6. Enter your Wi-Fi network details and choose **Next**.

The Device Setup Tool connects your devices to your Wi-Fi network and registers them with Alexa for Business.

To assign devices to a room

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 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/.
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.
     - **Online** – The device is connected to the network and all skills and settings have been applied.
     - **Offline** – The device isn't connected to the network. The device might be unplugged or the network might not be working. The time stamp next to the status shows the date and local time when the device was first detected to be offline.
     - **Sync in progress** – The device is connected to the network, and Alexa for Business is applying skills and settings to the device.
     - **Sync needed** –The device is connected to the network, but not all skills and settings have been applied to the device. This usually happens when the device was offline when Alexa for Business tried to apply all skills and settings. To sync the device, choose **Sync**. To sync multiple devices with this status, select all the devices from the table and choose **Sync devices** from the drop-down menu.
     - **Deregistered** –The device is no longer registered with the AWS account. The time stamp next to the status shows the date and local time when the device was first detected to be deregistered. To remove the device, select the device and choose **Actions**, **Delete Devices**.

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**, and 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.

To sync a device

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Shared devices** and select one or more devices with the status **Sync needed**.
3. Choose **Actions**, **Sync devices**.

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. 16).

To enable a skill

1. Open the Alexa for Business console at 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:

Account linking status/ skill type	Master account linked	Account linked to room	No account linking
Custom skill	Link account to this room	Revert to master account	No action
Smart home skill	Require scope or link account to this room	Revert to master account and require scope	N/A
Private skill	Optional skill parameters Link account to this room	Optional skill parameters Revert to master account	Optional skill parameters

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/.
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/.
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 publish skills privately to Alexa for Business organizations without the 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 backend 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 backend 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.

As a general guideline, 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 build private skills

- For information about how to build private skills, 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

- There are two ways you can publish private skills:
  - 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

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 can take up to two hours 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.

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/.
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**.

Managing Conferencing

You can enable Alexa conferencing, as well as link Alexa for Business to your calendar system, to control conferencing with your devices and dial into meetings using your voice.

Tasks

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

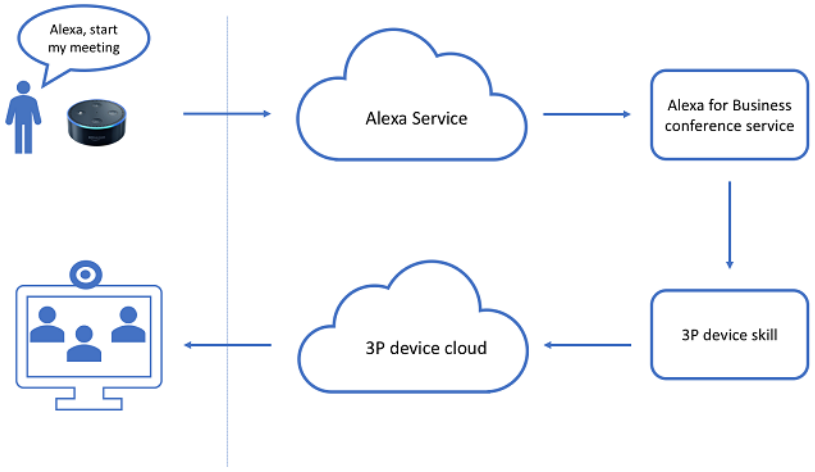
Compatible Conference Devices

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

Device model	Requirements
Cisco/Tandberg SX, EX, DX, MX, C	Firmware must be TC7.3 or CE8.0+
Cisco Spark Room Kit	Firmware must be CE8.0+
Zoom Rooms	Zoom Rooms for Mac version 4.1.20278.0206 or higher Zoom Rooms for PC version 4.1.22620.0319 or higher
Crestron 3-Series	Please contact a Creston-certified installer

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. 6) or the documentation provided by the device manufacturer.

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 you 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

Description	Dialogue
Amazon Chime is set up as the conference provider and no meeting PIN is required.	User: "Alexa, start my meeting" Alexa: "There is no meeting on the calendar. What is your <Amazon Chime> meeting ID?"
A meeting PIN is optional.	User: "Alexa, start my meeting."

Description	Dialogue
	Alexa: “There is no meeting on the calendar. What is your <provider name> meeting ID?” User: “123456789.” Alexa: “Do you have a meeting PIN?” User: “Yes.” Alexa: “What is your meeting PIN?” User: “5678.” Alexa: “OK, joining your meeting.”
A meeting PIN is required.	User: “Alexa, start my meeting.” Alexa: “There is no meeting on the calendar. What is your <provider name> meeting ID?” User: “123456789.” Alexa: “What is your meeting PIN?” User: “5678.” Alexa: “OK, joining your meeting.”

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 Telepresence, 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.

Use Echo Device as Speakerphone

To use an Echo device as a speakerphone

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Room profiles**, choose the name of the room profile associated with your meeting rooms, and enable **Outbound calling**.
3. Choose **Conferencing**, **Add provider**.
4. 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 **Custom conferencing provider**.
5. 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.
6. Choose **Add**.
7. (Optional) To join scheduled meetings, link your calendar to Alexa for Business. For more information, see Link Alexa for Business to Your Calendar System (p. 23).

You can now say "Alexa, join my meeting" and Alexa prompts you to join the scheduled meeting or to provide the ID of the meeting to join.

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. 6).
    2. Create a new skill group for the Zoom Alexa skill. For more information, see Managing Skill Groups (p. 16).
    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. 9).
    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. 23).
2. Set up Zoom as a conferencing provider:
    1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
    2. Choose **Conference settings**, **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.

        Note
        The scope value can only contain letters, numbers, spaces, and the following special characters: _ - = # ; : ? @ &. If your Zoom Room name contains any other characters, update your room name in the Zoom admin 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 the 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.

Link Alexa for Business to Your Calendar System

Alexa can automatically dial into scheduled meetings using your Echo devices or existing video conferencing equipment deployed in meeting rooms. To do this, connect Alexa for Business to Office 365, Google G Suite, or Microsoft Exchange.

Tasks

- Link Alexa for Business to Office 365 (p. 23)
- Link Alexa for Business to Office 365 (Limit Access Option) (p. 24)
- Link Alexa for Business to Google G Suite (p. 25)
- Link Alexa for Business to Microsoft Exchange (p. 25)

Link Alexa for Business to Office 365

By default, linking Alexa for Business to Office 365 gives the Alexa for Business client app read access to your organization’s calendars. Granting full read permissions enables Alexa for Business to default to the organizer’s calendar when the room calendar’s invitation is insufficient to automatically join a meeting. If you want to grant access to specific room calendars, see Link Alexa for Business to Office 365 (Limit Access Option) (p. 24).

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Calendar**, **Office 365**.
3. Choose **Link account** and sign in with the Office 365 account that belongs to the Global Administrators group.
4. Give consent that Alexa for Business has read access to the calendars in your Office 365 organization.
5. 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**.

6. 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 Office 365 (Limit Access Option)

By default, linking Alexa for Business to Office 365 gives the Alexa for Business client app read access to your organization’s calendars. Granting full read permissions enables Alexa for Business to default to the organizer’s calendar when the room calendar’s invitation is insufficient to automatically join a meeting. If you want to grant access to specific room calendars, follow these steps.

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 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, 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:

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

    For all room mailboxes:

    ```
    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:

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

   For all room mailboxes:

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

6. To link the service account to Alexa for Business, follow these steps:

   1. In the Alexa for Business console, choose **Calendar**, **Microsoft Exchange**.
   2. Enter the user principal name (UPN) of the service account you created earlier, service account password, and URL of the Office 365 EWS endpoint (https://outlook.office365.com/EWS/Exchange.asmx).
   3. For **Access method**, select **Delegation**.
   4. Choose **Link account**.

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

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

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 read access to the calendars in your G Suite organization.

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:

   ```
   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.

   ```
   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:

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

     For all room mailboxes:

     ```
     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:

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

   For all room mailboxes:

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

7. Link the service account to Alexa for Business.

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

   b. Choose **Calendar**, **Microsoft Exchange**.

   c. Enter the user principal name (UPN) of your service account.

   d. Enter the service account password.

   e. 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.

   f. For **Access method**, select **Delegation**.

   g. Choose **Link account**.

8. Associate the email address of your resource mailboxes in Microsoft Exchange to your Alexa for Business rooms.

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

   b. Choose **Rooms** and choose the room to which to add the email address.

   c. Choose **Edit**.

   d. Enter the email address of your resource mailbox that you want to associate to the Alexa for Business room.

   e. Choose **Save**.

9. Test the integration.

   a. 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.

   f. Your Echo device prompts you to join the scheduled meeting without asking you for the meeting ID.

If you have any issues linking Alexa for Business to Microsoft Exchange, see Set up Microsoft Exchange Access for Users (p. 42).

Use the Alexa for Business Gateway

The Alexa for Business gateway enables you to connect Alexa for Business to your Cisco TelePresence systems 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 hardware. 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

- Installing the Gateway (p. 28)
- Maintaining the Gateway (p. 29)

Installing the Gateway

The gateway is available on the Alexa for Business console.

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 TelePresence**, 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 IAM access keys and secret keys of the IAM users that you created previously.
3. Enter a unique name for your gateway.
4. (Optional) Enter a description to identify the gateway in the Alexa for Business console.
5. When prompted, enter the user credentials to sign into your Cisco TelePresence appliances.
6. Open the Alexa for Business console again, refresh **Alexa for Business Gateways**, and confirm that your gateway is listed.
7. 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 TelePresence systems:

   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

Maintaining 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 TelePresence or AWS credentials change, use the following steps to update your Alexa for Business gateways to use the new credentials.

To update Cisco TelePresence 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 TelePresence 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

Parameter	Description	Default Value	Type
a4b	A4B		Object
skipSslVerification	Set to true to ignore SSL validation errors when the gateway is connecting to your video conferencing endpoints	false	Boolean
credentials	Defines which AWS credentials to use		Null or object
localLog	Settings to have gateway log to a local file		Object
remoteLog	Settings to have gateway log to AWS Cloudwatch		Object
maintenance	Maintenance settings for the gateway, such as the update window and service manager	/path/to/root-ca/cert.pem	Object
rootCAsFile	Maintenance settings for the gateway, such as the update window and service manager		String
metrics			Object

A4B Object

Parameter	Description	Default Value	Type
region	AWS Region where the gateway connects with the Alexa for Business endpoint	us-east-1	String
endpoint	The Alexa for Business endpoint the gateway connects to	https://a4b.us-east-1.amazonaws.com	String
gatewayARN	The ARN of the gateway after it is registered		String

Parameter	Description	Default Value	Type
	with your Alexa for Business setup		

Shared Credentials

Parameter	Description	Default Value	Type
filename	Path to your AWS credentials	/path/to/.aws/credentials/file	String
profile	The profile to use in your AWS credentials file		String

Static Credentials

Parameter	Description	Default Value	Type
accessKeyId	AWS access key		String
secretAccessKey	AWS secret key		String
sessionToken	AWS session token. This is required only if you use temporary security credentials		String

LocalLog Object

Parameter	Description	Default Value	Type
enable	Boolean to enable logging to a local file	True	Boolean
logDir	Path to the log location		String

RemoteLog Object

Parameter	Description	Default Value	Type
enable	Boolean to enable logging to AWS Cloudwatch	False	Boolean
failureDir	Path to the directory for backup when logging to AWS Cloudwatch fails		String

Maintenance Object

Parameter	Description	Default Value	Type
serviceName	The service name of the gateway	alexaforbusiness	String
serviceManager	The service manager used on your Linux systems. Valid values are sysvinit, upstart, or systemd	systemd	String
updateFrequency	Defines how often to check for an update inside a maintenance window	15m	String
updateBranch	Defines which branch to update from	stable	String
windows	Defines the time windows of the gateway checking for updates		Object
healthCheckPeriod	How long to wait after an update for the service to regain health, before the update is considered a failure	5m	String

Maintenance Window Object

Parameter	Description	Default Value	Type
day	Day of the week when the gateway checks for updates		String
time	Time of day when the gateway checks for updates		String
width	Maximum length of the maintenance window		String

Metrics Object

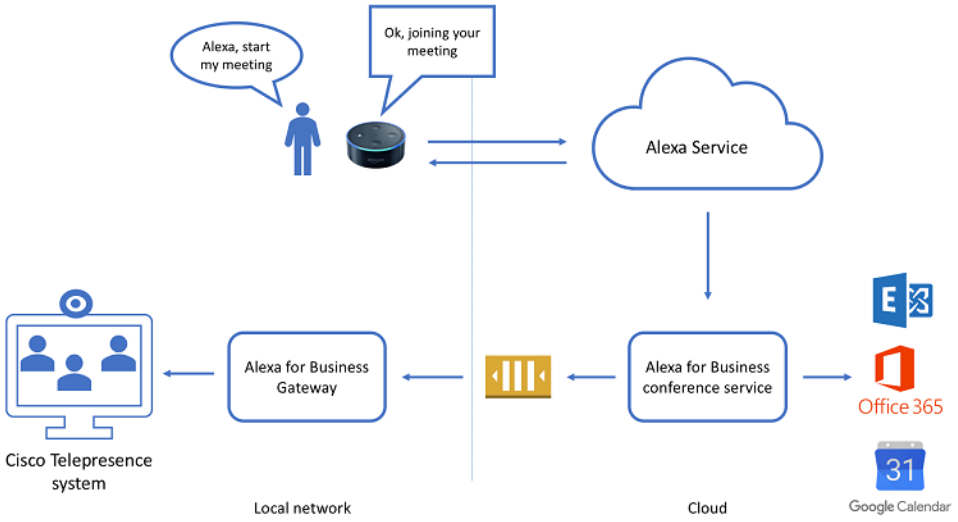
Parameter	Description	Default Value	Type
enable	Boolean to enable logging to AWS Cloudwatch	When this option is enabled, metrics are pushed to AWS Cloudwatch	String

Use Cisco TelePresence with Alexa for Business

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

- Cisco Telepresence DX, EX, MX, and SX series
- Cisco Spark 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. 27).

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

- You have a Cisco TelePresence 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 TelePresence system. Incoming external communication or inbound ports aren't required.
- Cisco video conferencing endpoints registered with Cisco Spark cloud are currently not supported.

To use Cisco TelePresence 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 TelePresence 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 TelePresence** 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. 27).

4. Add your Cisco TelePresence system to Alexa for Business and add it to a room.

   a. Choose **Endpoint**, **Add endpoint**.

   b. Specify the **Cisco TelePresence** 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 TelePresence** model.

   f. Specify the endpoint URL of your Cisco TelePresence 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 TelePresence endpoint is located.

   h. Choose **Add**.

   i. Choose **Rooms** and the name of the room where you just assigned the Cisco TelePresence endpoint.

   j. Choose **Discover devices** to have the endpoint available in your room.

   k. 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 TelePresence endpoint

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Conferencing settings**, **Alexa for Cisco TelePresence**.
3. In the endpoint section, choose **Add endpoint**. For **System name**, enter **Cisco TelePresence**.
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 TelePresence model** and specify the endpoint URL of your Cisco TelePresence 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 TelePresence endpoint is located and choose **Add**.
7. Choose **Rooms** and the name of the room where you just assigned the Cisco TelePresence endpoint.

8. 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 TelePresence 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 TelePresence**.
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 Telepresence endpoints

1. Choose one of the following options:

    1. To connect Alexa for Business to your Cisco Telepresence 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. 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:

        a. 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\
    - 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.

Manage Conferencing Providers

For more information about conference providers, PSTN settings, and SIP/H323 settings, see the section called “Understanding Alexa-enabled Conferencing” (p. 18).

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**.
3. On the **Conference settings** page, choose **Remove**.

   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**.

Managing Calling

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

Note
The following types of calls are currently not supported:

- 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 using an Echo device

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. 39)
- Managing Contacts (p. 40)

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 **Calls**, **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 **Calls** and select the name of the address book to edit.
3. Edit the values for **Name** and **Description**, and then choose **Save**.

To delete an address book

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Calls** and select the name of the address book to delete.
3. Choose **Delete address book**, **Delete**.

Managing Contacts

After you create contacts, you can add them to address books. Edit or delete a contact at any time.

To create a contact

1. Open the Alexa for Business console at https://console.aws.amazon.com/a4b/.
2. Choose **Calls**, **Contacts**.
3. Choose **Create contacts**, and enter a name, phone number, and optional 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 **Calls**, **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 **Calls**, **Contacts**, and select the contacts to edit.
3. Edit the values for **Name**, **Phone number**, 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 **Calls**, **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

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:

   ```
   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: `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:

   ```
   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:

   ```
   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. 42).

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 the 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.

Logging Alexa for Business Administration Calls with AWS CloudTrail

Alexa for Business is integrated with CloudTrail. CloudTrail is a service that captures API calls made by or on behalf of Alexa for Business in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures all API calls from the Alexa for Business console. Using the information collected by CloudTrail, you can determine which requests were made, the source IP address for the request, who made the request, and when it was made. For more information, including how to configure and enable CloudTrail, see the AWS CloudTrail User Guide.

When CloudTrail logging is enabled in your AWS account, API calls made from Alexa for Business on your behalf are tracked in log files. These records are written together with other AWS service records in a log file. CloudTrail determines when to create and write to a new file based on time period and file size.

You can store your log files in your bucket for as long as you want, or you can define Amazon S3 lifecycle rules to archive or delete log files automatically. By default, your log files are encrypted using Amazon S3 server-side encryption (SSE). To take quick action upon log file delivery, you can choose to have CloudTrail publish Amazon SNS notifications when new log files are delivered. For more information, see Configuring Amazon SNS Notifications for CloudTrail.

CloudTrail log files can contain one or more log entries, with each entry comprised of multiple JSON-formatted events. A log entry represents a single request and contains information about the action taken, who generated the request, where they were when they made the request, system information, and information that will vary depending on the type of request. Every log entry also contains information about who generated the request. The user identity information in the log helps you determine whether the request was made with root or IAM user credentials, with temporary security credentials for a role or federated user, or by another AWS service. For more information, see the **userIdentity** field in the CloudTrail Log Event Reference.

Log entries are not in any particular order and are not an ordered stack trace of the public API calls. Entries for Alexa for Business are identified by the **a4b.amazonaws.com** event source. Sensitive information, such as passwords, authentication tokens, file comments, and file contents, are redacted in log entries.

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

```
{
  "Records": [{
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "EX_PRINCIPAL_ID",
      "arn": "arn:aws:iam::123456789012:user/Alice",
      "accountId": "123456789012",
      "accessKeyId": "EXAMPLE_KEY_ID",
      "userName": "Alice"
    },
    "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/8eed09c4eae340d2ba08b8c6c3e40970/66afda686e75c5b62fceaf60ac00e7a6"
    },
    "requestID": "6a875d42-c859-11e7-93bc-f944dc16ba6b",
    "eventID": "2b045b94-82d9-407d-aff3-6c308b40fecb",
    "resources": [{
      "ARN": "arn:aws:a4b:us-
east-1:123456789012:profile/8eed09c4eae340d2ba08b8c6c3e40970/00491b672c651240de09540d2072f660",
      "accountId": "123456789012",
      "type": "AWS::A4B::Profile"
    }, {
      "ARN": "arn:aws:a4b:us-
east-1:123456789012:room/8eed09c4eae340d2ba08b8c6c3e40970/66afda686e75c5b62fceaf60ac00e7a6",
      "accountId": "123456789012",
      "type": "AWS::A4B::Room"
 }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
    }
  ]
```

Document History for Alexa for Business Administration Guide

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.

update-history-change	update-history-description	update-history-date
New deregistered device status	For more information, see Managing Devices in the Alexa for Business Administrator's Guide.	August 3, 2018
Calendar voice restriction and Alexa Smart Scheduling Assistant	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.	May 21, 2018
Connect Alexa for Business to your Zoom Rooms system	For more information, see Use Zoom Rooms with Alexa for Business in the Alexa for Business Administrator's Guide.	May 9, 2018
View the network connection status of a device and monitor devices using CloudWatch	For more information, see Managing Devices in the Alexa for Business Administrator's Guide.	April 30, 2018
Password expiration emails	For more information, see Set up Microsoft Exchange Access for Users in the Alexa for Business Administrator's Guide.	April 26, 2018
Various conferencing updates	For more information, see Managing Conferencing in the Alexa for Business Administrator's Guide.	April 10, 2018
Change permissions for a skill	For more information, see Managing Skills in the Alexa for Business Administrator's Guide.	April 6, 2018
Make calls from your shared devices with Alexa for Business	For more information, see Managing Calling in the Alexa for Business Administrator's Guide.	March 28, 2018

Updates to the Device Setup Tool	For more information, see Run the Device Setup Tool in the Alexa for Business Administrator's Guide.	March 26, 2018
Added support for Fuze and Google Hangouts Meet	For more information, see Understanding Alexa-enabled Conferencing in the Alexa for Business Administrator's Guide.	March 16, 2018
Use the Alexa for Business gateway to connect Alexa for Business to your Cisco TelePresence systems	For more information, see Use the Alexa for Business Gateway in the Alexa for Business Administrator's Guide.	February 8, 2018
Assign multiple devices to a room	For more information, see Managing Devices in the Alexa for Business Administrator's Guide.	January 26, 2018
Initial release	Initial release	November 29, 2017