aws

Administrator Guide

Amazon Connect Talent

Amazon Connect Talent: Administrator Guide

Table of Contents

What is Amazon Connect Talent?

Amazon Connect Talent is an agentic AI hiring solution built for talent acquisition leaders managing scaled hiring. It delivers AI-led interviews, science-backed assessments, and consistent evaluation, helping recruiters hire high quality candidates faster while providing applicants with a flexible interview experience that reduces human preconceptions.

This guide is for administrators. It describes how to set up and manage Amazon Connect Talent. For tasks that recruiters perform day to day, such as creating evaluations and reviewing candidate results, see the Amazon Connect Talent User Guide.

Topics

Features of Amazon Connect Talent

Amazon Connect Talent provides the following features that you administer:

- **AI-generated candidate evaluations** – Recruiters create evaluations that use assessments, an AI-led interview, or both to measure candidates against a job's competencies.
- **Applicant tracking system (ATS) integration** – Connect your ATS to synchronize jobs and candidates and to return evaluation results.
- **SAML-based single sign-on** – Use your existing identity provider to give users single sign-on access to Amazon Connect Talent.
- **User management and security profiles** – Add users and control what they can do with role-based security profiles.
- **Knowledge bases** – Add your company values and information to personalize candidate evaluations.

- **Candidate-facing branding** – Personalize the candidate experience with your organization's name, logo, and color.
- **Data governance** – Review encryption, data residency, and data retention policies, and request changes to meet your compliance requirements.

Evaluations

An evaluation is how Amazon Connect Talent measures a candidate for a job. An evaluation can include an AI-led interview, assessments, or both. A recruiter builds an evaluation with a step-by-step builder: they select or describe a job, and Amazon Connect Talent generates a draft evaluation. The draft is organized into three parts:

- **Overview** – The job, the key competencies to measure, and the evaluation language.
- **Assessments** – A set of digital tests selected for the job's competencies.
- **AI-led interview** – A set of behavioral questions grouped by competency.

Recruiters review and adjust the draft, then publish it. A published evaluation can be sent to candidates. For how Amazon Connect Talent generates evaluation scoring and criteria, see Managing evaluations.

AI-led interviews

The AI-led interview is a set of behavioral questions that Amazon Connect Talent generates for each competency a job requires. During the interview, Amazon Connect Talent will ask dynamic follow-up questions to explore a candidate's answer. Every question is tagged with the competency it measures and includes a short rationale. Amazon Connect Talent writes questions to be clear, fair, and focused on a single competency, and it can generate them in multiple languages.

Assessments

Assessments measure candidates against a job's competencies. Amazon Connect Talent reports assessment results on a four-level scale: Low, Moderate, High, and Very High. Amazon Connect Talent offers the following assessment types:

- **Work approach** – Measures how a candidate approaches their work.
- **Problem solving** – Measures how a candidate works through problems.

For Work approach and Problem solving, recruiters see a per-competency breakdown and an overall fit summary. When a candidate does not provide enough signal on a competency, Amazon Connect Talent excludes it rather than guessing.

Supported Regions and endpoints

Amazon Connect Talent is available in the following AWS Regions. You create and manage your instance in a supported AWS Region, and your data resides in that AWS Region.

Region name	Region code
US East (N. Virginia)	us-east-1
US West (Oregon)	us-west-2

For the service endpoints and quotas that apply to Amazon Connect Talent, see Endpoints and quotas for Amazon Connect Talent.

Supported languages

Amazon Connect Talent localizes two separate experiences: the recruiter experience and the candidate experience. The recruiter experience is the application that recruiters and administrators use. The candidate experience is the evaluation that candidates complete. These two experiences support different sets of languages. The candidate experience supports a different set of languages than the recruiter experience. Use the following tables separately, and do not assume the two sets match.

Recruiter experience languages

The recruiter experience supports the following languages.

Language	English name
English	English
Deutsch	German

Language	English name
Español	Spanish
Français	French
Italiano	Italian
日本語	Japanese
한국어	Korean
Português (BR)	Portuguese (Brazil)
中文 (简体)	Chinese (Simplified)
中文 (繁体)	Chinese (Traditional)

Candidate experience languages

The candidate experience supports a different set of languages than the recruiter experience. An evaluation can be delivered to a candidate in the following languages.

Language	Locale
English (United States)	`en-US`
English (Australia)	`en-AU`
English (United Kingdom)	`en-GB`
Portuguese (Brazil)	`pt-BR`
French (France)	`fr-FR`
Italian (Italy)	`it-IT`
German (Germany)	`de-DE`
Spanish (United States)	`es-US`

Accessibility

Amazon Connect Talent supports screen readers and keyboard navigation across the recruiter and candidate experiences. The AI-led interview, however, is not optimized for screen readers. Candidates who use a screen reader or other assistive technology incompatible with the AI-led interview can opt out and complete the remaining parts of the evaluation. Opting out keeps the candidate's application Active and preserves their place in your pipeline. For more information, see How a candidate opts out.

Prerequisites for Amazon Connect Talent

Before you set up Amazon Connect Talent, review the following requirements.

Topics

AWS account requirements

To create an Amazon Connect Talent instance, you need the following:

- An active AWS account.
- Access to a supported AWS Region. For more information, see Supported Regions and endpoints.
- A valid email address for the first administrator of the instance.

Avoid using your AWS account root user for everyday tasks. Instead, create an administrative user in IAM and use it to set up and manage Amazon Connect Talent.

IAM permissions and managed policies

For details about how Amazon Connect Talent works with IAM, the AWS managed policies that are available, and example policies, see Identity and access management for Amazon Connect Talent.

Managing your Amazon Connect Talent instance

The following sections describe the IAM permissions required to create and delete an Amazon Connect Talent instance.

Create an instance

The IAM identity (user or role) that creates an Amazon Connect Talent instance needs permissions across several AWS services, because the setup process provisions resources in Connect Customer,

Amazon Lex, Connect Customer Cases, Connect Customer Customer Profiles, Amazon Q in Connect, and Amazon SES.

As a recommended approach, grant the creating identity the following permissions:

- `AmazonConnect_FullAccess`
- `AmazonLexFullAccess`
- Full access to Connect Customer Cases, Connect Customer Customer Profiles, Amazon Q in Connect, and Amazon SES
- `iam:CreateServiceLinkedRole`, `iam:PassRole`, and AWS KMS grant permissions

For a least-privilege alternative, use action-level policies scoped to only the actions the setup process requires.

An identity with the `AdministratorAccess` managed policy can also create instances. Use the scoped approach when possible to follow the principle of least privilege.

When you create an instance, Amazon Connect Talent also provisions the IAM roles it needs to operate on your behalf.

Delete an instance

To delete an Amazon Connect Talent instance, the identity performing the deletion needs permissions to remove resources across the same services that were provisioned during creation.

The following permissions are required, grouped by service:

- **Connect Customer** – `connect:DeleteInstance`, `connect:DeleteIntegrationAssociation`, `connect:DisassociateBot`
- **Amazon Lex** – `lex:ListBots`, `lex:ListBotAliases`, `lex:DeleteBotAlias`, `lex:DeleteBot`
- **Connect Customer Customer Profiles** – `profile:DeleteDomain`, `profile:DeleteIntegration`, `profile:DeleteProfileObjectType`
- **Connect Customer Cases** – `cases:DeleteDomain`
- **Amazon Q in Connect** – `wisdom:DeleteAssistant`
- **Amazon SES** – `ses:DeleteEmailIdentity`

An identity with the `AdministratorAccess` managed policy can also delete instances.

Clean up resources after deleting an instance

After you delete an Amazon Connect Talent instance, some resources provisioned during instance creation might not be removed automatically. You need to manually delete these resources from your AWS account in the same AWS Region as the instance.

The following resources might need manual cleanup:

Resource	Name pattern	How to delete
Amazon Lex bots (up to 3)	*instance-alias* -hiring-interview-lex-bot , *instance-alias* -hiring-chat-lex-bot , *instance-alias* -hiring-assessment-lex-bot	First disassociate the bot from the Connect Customer instance, then delete the bot in the Amazon Lex console.
Connect Customer Customer Profiles domain	amazon-connect-hiring- *instance-alias*	Delete in the Connect Customer Customer Profiles console.
Connect Customer Cases domain	Uses the instance alias	Delete in the Connect Customer Cases console.
Amazon Q in Connect assistant	Hiring Interview Assistant	Delete in the Amazon Q in Connect console.

If you're unable to identify which resources were left behind, contact AWS Support.

Amazon SES requirements

Amazon Connect Talent uses Amazon SES to send email to candidates, such as invitations to complete an evaluation. New Amazon SES accounts start in the Amazon SES sandbox. While your

account is in the sandbox, you can send email only to verified addresses, and daily and per-second sending limits apply.

To send email to candidates who are not verified addresses, request production access to move your account out of the sandbox. For instructions, see Move Amazon SES out of sandbox mode.

Getting started with Amazon Connect Talent

To start using Amazon Connect Talent, you create a Talent instance from the AWS console. The instance creation wizard walks you through identity management, administrator setup, permissions, and resource provisioning. You can also configure SAML 2.0-based authentication for single sign-on access, prepare Amazon SES for candidate email, and set up your instance for recruiters.

Topics

Create your Amazon Connect Talent instance

Start using Amazon Connect Talent

Complete the following high-level steps to start using Amazon Connect Talent:

1. Complete the prerequisites. For more information, see Prerequisites for Amazon Connect Talent.
2. Create an Amazon Connect Talent instance.
3. (Optional) Configure SAML with IAM for single sign-on.
4. Move Amazon SES out of sandbox mode so that you can send email to candidates.
5. Set up your instance for your recruiting team. For more information, see Set up your instance.

Create an Amazon Connect Talent instance

The instance creation wizard walks you through identity management, administrator setup, permissions, and resource provisioning. The process takes a few minutes.

Prerequisites

Before you create an Amazon Connect Talent instance, verify that you have the following:

- An AWS account with an identity that has permissions to create Amazon Connect Talent resources. Instance creation provisions resources across Connect Customer, Amazon Lex, Connect

Customer Cases, Connect Customer Customer Profiles, Amazon Q in Connect, and Amazon SES. For the full list of required permissions, see IAM permissions and managed policies.

- A valid email address for the administrator account

To navigate to Amazon Connect Talent

You can open Amazon Connect Talent in the AWS Management Console in any of the following ways:

- Open the Amazon Connect Talent console directly.
- In the AWS Management Console, enter **Talent** in the search bar, and then choose **Amazon Connect Talent** from the results.
- In the AWS Management Console, open the All services page, and then choose **Amazon Connect Talent** under **Business applications**.

The Amazon Connect Talent instances page shows your instances. The page includes the following columns:

- Instance alias
- Access URL
- Create date
- Status

Choose **Add an instance** to start the creation wizard.

Step 1: Set identity

Choose your identity management option:

- **Store users in Amazon Connect Talent** – Create and manage users directly in Amazon Connect Talent. This is the default option.
- **SAML 2.0-based authentication** – Use identity federation with SAML 2.0 for single sign-on (SSO).

For **Access URL**, enter a unique alias for your instance. The alias must use lowercase letters, numbers, and hyphens. It must be 1–45 characters and end with `-hiring`.

Note

If you select SAML, users sign in through your organization's identity provider. You must configure SAML integration separately after instance creation.

Step 2: Add administrator

Add at least one administrator to your instance.

If you chose **Store users in Amazon Connect Talent**, provide the username, first name, last name, email, and a password (entered twice to verify).

If you chose **SAML 2.0-based authentication**, provide the username, first name, last name, and email.

You can add multiple administrators.

Step 3: Permissions

Review the IAM roles that Amazon Connect Talent creates automatically. These roles allow Amazon Connect Talent to manage its resources and to send email on your behalf. For more information about how Amazon Connect Talent uses IAM, see Identity and access management for Amazon Connect Talent.

Step 4: Review and create

Review your configuration. The review page shows your identity settings, administrator details, and the AWS resources that Amazon Connect Talent provisions for your instance, such as IAM roles, data storage, and email.

Choose **Create instance** to start provisioning.

Important

A progress banner shows the provisioning status. Don't close your browser during instance creation.

View instance details

After creation completes, choose the instance alias to view details, including the access information for your instance, distribution settings such as the instance ARN, and the AWS resources that Amazon Connect Talent manages for the instance.

Configure SAML with IAM for Amazon Connect Talent

Amazon Connect Talent supports identity federation with SAML 2.0 through AWS IAM. This enables web-based single sign-on (SSO) from your organization's identity provider to your talent instance.

Important

Consider the following when you configure SAML for Amazon Connect Talent:

- Choosing SAML requires IAM federation configuration.
- The username must match the `RoleSessionName` SAML attribute.
- Amazon Connect Talent doesn't support reverse federation. Authentication must happen from the identity provider (IdP).
- Most IdPs use the global AWS sign-in endpoint by default. You must override this to the regional endpoint.
- All usernames are case sensitive.
- SAML for Amazon Connect Talent is available in supported Regions. For more information, see Supported Regions and endpoints.

Overview of the SAML authentication flow

The following steps describe the SAML authentication flow for Amazon Connect Talent:

1. The user browses to an internal portal that contains a link to Amazon Connect Talent.
2. The federation service requests authentication from the identity store.
3. The identity store authenticates the user and returns the authentication response.
4. The federation service posts the SAML assertion to the browser.
5. The browser posts the assertion to the AWS sign-in SAML endpoint. AWS authenticates the user and redirects to Amazon Connect Talent.
6. Amazon Connect Talent authorizes the user and opens the instance.

To enable SAML-based authentication

Complete the following high-level steps to enable SAML-based authentication:

1. Create an Amazon Connect Talent instance with SAML 2.0 identity management.
2. Enable SAML federation between your IdP and AWS.
3. Add users to your instance. Usernames must match exactly between your IdP and Amazon Connect Talent.
4. Configure your IdP for SAML assertions, authentication response, and relay state.

To enable SAML federation between your IdP and AWS

1. Create a SAML provider in AWS.
2. Create an IAM role for SAML 2.0 federation. Add a permissions policy that uses the `connect:GetFederationToken` action.
3. Configure your network as a SAML provider for AWS.
4. Configure SAML assertions for the authentication response. Leave the **Application Start URL** blank.
5. Override the Assertion Consumer Service (ACS) URL to the regional endpoint.
6. Configure the relay state URL for your Region and instance.

IAM policy examples

The following example shows an IAM policy that allows all users in a specific instance to federate into Amazon Connect Talent.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "connect:GetFederationToken",
            "Resource": "arn:aws:connect:region:123456789012:instance/instance-id/user/
${aws:userid}"
        }
    ]
}
```

The following example uses an instance ID condition instead of a resource ARN.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "connect:GetFederationToken",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "connect:InstanceId": "instance-id"
                }
            }
        }
    ]
}
```

Configure regional SAML endpoints

1. Update the ACS URL to the regional endpoint. For example: `https://us-west-2.signin.aws.amazon.com/saml`
2. Update the role trust policy to include the regional endpoint in the `SAML:aud` condition.
3. Configure the relay state for the region-specific console.

The session duration is 12 hours. We recommend that users log out of both Amazon Connect Talent and the identity provider when they finish their session.

Move Amazon SES out of sandbox mode

Amazon Connect Talent uses Amazon SES to send evaluation invitations to candidates by email. New Amazon SES accounts start in the sandbox, where you can send email only to verified addresses and lower sending limits apply. To send invitations to candidates who are not verified addresses, request production access for Amazon SES.

> **Important**
>
> Until you move Amazon SES out of sandbox mode, Amazon Connect Talent can't send evaluations to candidates by email or support internal testing.

To request production access:

1. Open the Amazon SES Get set up page.
2. In the **Request production access** card, choose **Request production access**.
3. For **Mail type**, choose **Transactional**.
4. For **Website URL**, enter your organization's website URL.
5. (Optional) For **Additional contacts**, enter up to four email addresses, separated by commas, where you want to receive communications about your request.
6. For **Preferred contact language**, choose **English** or **Japanese**.
7. Under **Acknowledgement**, select the box to agree to the AWS Service Terms and Acceptable Use Policy.
8. Choose **Submit request**.

After you submit, you can't edit your details until the review is complete. The AWS Support team provides an initial response within 24 hours. For more information, see Request production access (moving out of the Amazon SES sandbox) in the *Amazon Simple Email Service Developer Guide*.

After you create your instance, see Set up your instance to configure it for your recruiting team.

Set up your instance

After you create your Amazon Connect Talent instance, configure it for your recruiting team. Complete the following steps to get your instance ready for use.

> **Important**
>
> Before you can send evaluations to candidates or test internally, your Amazon Simple Email Service (Amazon SES) account must be moved out of sandbox mode. If you haven't done this yet, see Move Amazon SES out of sandbox mode.

1. **Set up your security profile** – The default `TechAdmin` profile does not include permissions for hiring setup or candidate review. If you need full access to all Amazon Connect Talent features during setup, edit the `TechAdmin` profile to enable all permission categories, or create a new security profile with all permissions. For more information, see Manage security profiles and roles.

2. **Add users** – Add your recruiting team members and assign each user a security profile that matches their role. You can add users individually or import them in bulk from a CSV file. For more information, see Manage users.
3. **Upload your knowledge base** – Upload your company values, principles, and mission to a knowledge base before you create evaluations. Amazon Connect Talent draws on your knowledge base when selecting competencies for evaluations. For more information, see Manage knowledge bases.
4. **Configure branding** – Personalize the candidate experience with your organization's name, logo, and colors. For more information, see Configure branding.
5. **Configure disclosures** – Add any legal disclosures that candidates see before they start an evaluation. Consult your legal counsel to determine what disclosures are required for your organization. For more information, see Configure disclosures.
6. **Create your first evaluation** – You're ready to create an evaluation. For step-by-step instructions, see Managing evaluations in the *Amazon Connect Talent User Guide*.
7. **Test your evaluation** – Before sending evaluations to candidates, test the evaluation by sending it to yourself or your team. For more information, see Testing Amazon Connect Talent in the *Amazon Connect Talent User Guide*.
8. **Connect your ATS (coming soon)** – When available, connect your applicant tracking system to sync jobs and candidates automatically.

> **Note**
>
> ATS integrations are not available at launch. Support for ATS integrations is coming soon. For more information, see Add your ATS integration.

Managing evaluations

An evaluation is how Amazon Connect Talent measures a candidate for a job. Recruiters create, configure, publish, and manage evaluations. Each evaluation measures a candidate against the competencies for the job using assessments, an AI-led interview, or both.

As an administrator, you set up the knowledge base, settings, and access that support recruiters. Recruiters then build and publish the evaluations that candidates complete. For how to set up these resources, see Settings.

For how evaluations are structured, how scoring and criteria work, and how to create, publish, and review evaluations, see the Amazon Connect Talent User Guide.

Add your ATS integration

> **Note**
>
> ATS integrations are not available at launch. Support for ATS integrations is coming soon.

Amazon Connect Talent integrates with your applicant tracking system (ATS) so that your hiring data stays in sync. When you connect an ATS, Amazon Connect Talent synchronizes jobs and candidates from your ATS, and returns evaluation results to your ATS. This lets recruiters work from the tools they already use.

What ATS integration enables

Connecting your ATS will enable the following:

- **Job synchronization** – Jobs from your ATS become available in Amazon Connect Talent so that recruiters can create evaluations for them.
- **Candidate synchronization** – Candidate records from your ATS become available in Amazon Connect Talent.
- **Automated evaluation invitations** – You link evaluations to a specific application stage from your ATS. When a candidate reaches that stage, Amazon Connect Talent automatically sends them an evaluation invitation by email.
- **Results sync** – When a candidate completes their evaluation, Amazon Connect Talent writes a completion event back to your ATS with a link to review the candidate's results.

You will not be charged for adding your ATS integration.

Using Amazon Connect Talent without an ATS integration

Amazon Connect Talent works in full without an ATS integration. You can:

- Create evaluations by manually uploading or describing your job. For more information, see Add a job.
- Send evaluations to candidates manually by email. For more information, see Sending evaluations to candidates.

- Test Amazon Connect Talent end-to-end by sending evaluations to yourself or your team. For more information, see Testing Amazon Connect Talent.

Settings

Use the Amazon Connect Talent settings to manage users and security profiles, configure instance settings such as knowledge bases, branding, and disclosures, and review your data governance policies.

For information about charges for candidate evaluations, see Billing.

Topics

Manage users

Add users to Amazon Connect Talent and configure them with information and permissions. Each user receives a security profile that determines what they can access and do.

View users

To view users, navigate to **Settings** > **Admin** > **User management**. The page displays a table of all users in your instance. From this page, you can search for users, add users, delete users, refresh the list, and choose a user name to edit that user.

To add a user individually

1. Choose **Add user**.
2. Choose **Add a user manually**.
3. Enter the first name, last name, email address, username, and security profile. For user pool directory instances, also enter a password of 8–64 characters.
4. Choose **Save**.

> **Note**
>
> For SAML-based instances, the **Password** field does not appear. The username must match the identity configured in your identity provider (IdP).

To add users in bulk from a CSV file

1. Choose **Add user**.
2. Choose **Import users using a .csv template**.
3. Download the template, fill in user data, and upload the completed file.
4. Review the validation results. The system displays errors by row if any exist.
5. Choose **Save**.

To delete a user

1. Select the checkbox next to one or more users.
2. Choose **Delete user**.
3. Confirm the deletion.

You can select multiple users to delete them in bulk.

Manage security profiles and roles

Security profiles control what users can see and do in Amazon Connect Talent. Each user must have a security profile assigned. Follow the principle of least privilege when you assign permissions.

Default security profiles

Amazon Connect Talent provides the following default security profiles:

Security profile	Description	Default permissions
`HiringManager`	Intended for hiring managers. By default, can view the hiring setup and candidate results.	• Hiring setup – View • Candidate review – View
`Recruiter`	Intended for recruiters. By default, can view the hiring setup and fully manage candidate review.	• Hiring setup – View • Candidate review – All (View, Edit, Create)
`RecruitingLead`	Intended for recruiting leads. By default, can do everything a recruiter can, plus manage the hiring setup, customize the experience, and view integrations.	• Hiring setup – All (View, Edit, Create) • Candidate review – All (View, Edit, Create) • Experience customization – All (View, Edit) • Integrations – View
`ResearchScientist`	Intended for research scientists. By default, can manage the hiring setup and knowledge base, and view candidate results.	• Hiring setup – All (View, Edit, Create) • Candidate review – View • Knowledge – All (View, Edit, Create, Delete)
`TechAdmin`	Intended for technical admins. By default, can manage users, security profiles, integrations, and knowledge.	• Users – All (View, Edit, Create, Delete) • Security profiles – All (View, Edit, Create) • Knowledge – All (View, Edit, Create, Delete) • Integrations – All (View, Edit, Create, Delete) • Experience customization – All (View, Edit)

Security profile	Description	Default permissions
`ComplianceAdmin`	Intended for compliance owners. By default, can manage compliance settings, and view integrations and candidate results.	• Compliance – All (View, Edit, Create) • Candidate review – View • Integrations – View

The default security profiles are a starting point. A user who can manage security profiles (for example, the `TechAdmin` profile) can adjust the permissions on the default profiles as well as create new ones.

Tip

The default `TechAdmin` profile does not include permissions for hiring setup or candidate review. If you need a single profile with full access to all Amazon Connect Talent features — for example, for the person who sets up and configures the instance — you have two options:

- **Add permissions to the TechAdmin profile** – Edit the `TechAdmin` profile and enable all permission categories, including hiring setup and candidate review.
- **Create a new profile with all permissions** – Create a new security profile (for example, "Admin") and select all permission categories. Assign this profile to users who need full access.

To create a security profile

1. Navigate to **Settings** > **Admin** > **Security profiles**.
2. Choose **Create security profile**.
3. Enter a name and description for the profile.
4. Select the permissions to assign to the profile.
5. Choose **Save**.

To edit a security profile

1. Navigate to **Settings** > **Admin** > **Security profiles**.
2. Choose the security profile you want to edit. This can be a default profile or one you created.
3. Adjust the selected permissions.
4. Choose **Save**.

Your changes take effect for all users assigned that profile.

Security profile permissions

A security profile grants permissions across the following categories.

Permission category	Description
Hiring setup	Manage the steps that happen before a candidate applies, such as jobs, requisitions, and evaluations. Includes viewing aggregate hiring metrics.
Candidate review	Send evaluations to candidates and review their results, transcripts, and recordings. Covers the steps after a candidate applies.
Knowledge	Manage the files in the knowledge base.
Integrations	Manage third-party integrations that connect Amazon Connect Talent to external systems such as applicant tracking systems, HR information systems, and job boards.
Users	Manage users and their permissions.
Security profiles	Manage the security profiles available to be assigned to users.
Experience customization	Manage branding and visual customization.
Compliance	Manage compliance-related settings such as disclosures and data governance.

Tip

Use the `TechAdmin` profile during initial setup, and then switch to a more restrictive profile for daily use. Create security profiles before you add users to your instance.

Manage knowledge bases

A knowledge base stores your company values, principles, and mission. Amazon Connect Talent uses this information to personalize competencies and interview questions for candidates.

To upload files to a knowledge base

1. Navigate to **Settings** > **Admin** > **Knowledge**.
2. Choose **Upload**.
3. Choose the files to upload.
4. Choose **Upload**.
5. Wait for the status to change to **Complete**.

Deleting knowledge base files does not affect existing evaluations that used those files.

Tip

Upload documents that describe your company values, leadership principles, and mission statement. If a file shows a **Failed** status, retry the upload.

Configure branding

Customize the candidate-facing experience with your company branding. You can configure your company name, logo, and brand color.

To update branding

To update branding, navigate to **Settings** > **Recruiting** > **Branding**. Configure the following fields:

- **Company name** (required) – The name that candidates see on the landing screen.
- **Logo** (optional) – Maximum 200 KB. Dimensions must be between 50x50 and 500x200 pixels. Supported formats: PNG, SVG, JPG.
- **Color** (optional) – A hex color value (for example, #ff6b22). This color appears on buttons and accent elements.

The previews update as you make changes. Choose **Save changes** to apply your updates.

Configure disclosures

Configure legal notices that candidates see before they start an evaluation. Use the rich text editor to format your disclosure content.

To edit disclosures

To edit disclosures, navigate to **Settings** > **Data Management** > **Disclosures**. Use the rich text editor to write and format your disclosure, and then choose **Save**. To see how candidates view the disclosure, choose **Preview candidate disclosure**.

> **Tip**
>
> Use plain language in your disclosures. We recommend checking with your legal team before you publish disclosures.

View data governance

The data governance page is a read-only page that displays your data retention and data residency settings. To view it, navigate to **Settings** > **Data Management** > **Data governance**.

Data retention

By default, Amazon Connect Talent deletes interview transcripts, candidate assessment results, and application materials after one year. To request custom retention periods, see Requesting custom data retention periods.

Data residency and encryption

Your data resides in the AWS Region where your instance is hosted, and all data at rest is encrypted. For more information, see Data protection in Amazon Connect Talent.

Billing

Amazon Connect Talent charges a single flat price for each completed candidate evaluation. Track your usage and charges through your AWS account in the AWS Billing and Cost Management console.

Topics

What you are charged for

Amazon Connect Talent charges a single flat price for each completed candidate evaluation. For current pricing, see the Amazon Connect Talent pricing page.

Flat per-evaluation charge

You pay one charge for each billable evaluation. There is no separate price for each assessment or AI-led interview. When a candidate opts out of some parts of an evaluation, you still pay the full price. There is no reduction.

When an evaluation is billable

An evaluation is billable when any of the following are true:

- The candidate completes the evaluation.
- The candidate completes a portion of the evaluation and opts out of the rest.

An assessment or AI-led interview is billable even when the candidate scored poorly. A low score does not change whether the evaluation is billed.

When an evaluation is not billable

An evaluation is not billable in the following cases:

- The candidate opted out of the entire evaluation and completed nothing. Amazon Connect Talent treats this as though the candidate was never invited.
- A part of the evaluation could not be delivered because of a system or technical issue, or it timed out. This does not mean that the candidate scored poorly or closed their browser.
- The evaluation has not finished. Amazon Connect Talent assesses charges only after every assessment and AI-led interview in the evaluation reaches a final outcome. When a candidate stops partway through and never returns, the evaluation is never charged.

Each evaluation is charged independently

Each evaluation is a separate charge. When a recruiter sends a new evaluation and the candidate completes it, for example to re-evaluate a candidate after a weak result, that is a separate billable evaluation and a separate charge. Amazon Connect Talent charges the earlier completed evaluation and the new one separately.

Billing scenarios

The following table shows common outcomes and whether Amazon Connect Talent charges for each one.

Outcome	Charged?	Why
The candidate completed all parts of the evaluation.	Yes	The candidate completed the evaluation.
The candidate completed some parts and opted out of the rest.	Yes, full price	The candidate completed at least one part and opted out of every remaining part. There is no reduction.
One part could not be delivered because of a technical failure.	No	A part could not be delivered because of a system or technical issue.

Outcome	Charged?	Why
The candidate opted out of the entire evaluation.	No	The candidate completed nothing. Amazon Connect Talent treats this as though the candidate was never invited.
The recruiter re-sent the evaluation, and the candidate completed a second evaluatio n.	Yes, twice	Each completed evaluation is charged independently.
The candidate stopped partway through and never returned.	No	The evaluation never reached a final outcome.

Other AWS service charges

In addition to the per-evaluation charge, the following AWS services might appear on your bill when you use Amazon Connect Talent:

- **Amazon Simple Email Service (Amazon SES)** – Amazon Connect Talent uses Amazon SES to send evaluation invitation emails to candidates. Amazon SES charges apply at standard Amazon SES rates. For more information, see Amazon SES pricing.
- **Amazon Simple Storage Service (Amazon S3)** – Amazon Connect Talent uses Amazon S3 to store interview recordings and transcripts. Amazon S3 charges apply at standard Amazon S3 rates, consistent with Amazon Connect storage charges. For more information, see Amazon S3 pricing.

Security in Amazon Connect Talent

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

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

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

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

Topics

Security best practices for Amazon Connect Talent

Amazon Connect Talent provides a number of security features to consider as you develop and implement your own security policies. The following best practices are general guidelines and don't

represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions.

Topics

Detective

Use the following detective controls to monitor activity and detect potential security issues in Amazon Connect Talent.

- Use CloudTrail to log and review administrative and evaluation actions in your account. For more information, see Logging Amazon Connect Talent API calls using AWS CloudTrail.
- Use the AWS Security Hub CSPM integration to review security findings for Amazon Connect Talent alongside findings from your other AWS resources. For more information, see Integration with AWS Security Hub CSPM.

Preventative

Use the following preventative controls to reduce security risk in Amazon Connect Talent.

- Apply least-privilege security profiles, and restrict who can review candidate results and interview transcripts. For more information, see Identity and access management for Amazon Connect Talent.
- If your organization requires it, opt out of the use of your content to improve Amazon Connect Talent and other AWS AI services. For more information, see Opting out of data use for service improvement.

Data protection in Amazon Connect Talent

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

information about data protection in Europe, see the General Data Protection Regulation (GDPR) Center.

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

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail. For information about using CloudTrail trails to capture AWS activities, see Working with CloudTrail trails in the *AWS CloudTrail User Guide*.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-3 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-3.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with Amazon Connect Talent or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Data encryption

Amazon Connect Talent encrypts your data at rest and in transit.

Encryption at rest

Amazon Connect Talent encrypts all data at rest, including interview transcripts, assessment results, and application materials. You can view your encryption settings on the data governance page. For more information, see View data governance.

Encryption in transit

Amazon Connect Talent encrypts data in transit using Transport Layer Security (TLS).

Key management

Amazon Connect Talent manages the encryption keys that protect your data.

Internetwork traffic privacy

Amazon Connect Talent protects traffic between the service and your network, and between the service and other AWS services.

Data retention

Amazon Connect Talent applies default retention periods to your data and deletes it when those periods end. To request custom data retention periods, see Requesting custom data retention periods.

Opting out of data use for service improvement

You can opt out of the use of certain content to improve Amazon Connect Talent and other AWS AI services. For more information, see Opting out of data use for service improvement.

Opting out of data use for service improvement

AWS might use certain content that you process with Amazon Connect Talent to improve the service. This includes fixing operational issues, evaluating service performance, and debugging. Your content is not used for model training. You can choose to opt out of this use.

Only Amazon employees have access to this data. Your trust, privacy, and the security of Your Content are our highest priority, and our use complies with our commitments to you.

For Amazon Connect Talent, the content in scope for this use includes the following:

- AI-led interview transcripts
- Amazon Connect Talent Teammate chat transcripts

You control this choice with an AI services opt-out policy in AWS Organizations. An AI services opt-out policy applies to the accounts in your organization that you specify. When you opt out, AWS

does not use the in-scope content to develop or improve the covered services, and AWS deletes content that is stored for that purpose.

To opt out using an AI services opt-out policy

1. Sign in as a user in your organization's management account.
2. In AWS Organizations, enable the AI services opt-out policy type.
3. Create an AI services opt-out policy that opts out of data use for Amazon Connect Talent.
4. Attach the policy to the root, organizational units (OUs), or accounts that you want it to apply to.

For more information about AI services opt-out policies, see AI services opt-out policies in the *AWS Organizations User Guide*.

To check your opt-out status

To check your opt-out status, review the opt-out policy configured by your organization. For more information, see AI services opt-out policy syntax and examples in the *AWS Organizations User Guide*.

> **Note**
>
> To use the opt-out policy, your AWS accounts must be centrally managed by AWS Organizations. If you have not already created an organization for your AWS accounts, see Creating and managing an organization in the *AWS Organizations User Guide*.

Requesting custom data retention periods

By default, Amazon Connect Talent deletes the following data one year after it is created:

- Interview transcripts
- Candidate assessment results
- Application materials

You can't change the default retention periods on the data governance page. If your organization requires different retention periods to meet your compliance requirements, you can request custom retention periods.

To request custom retention periods

To request custom retention periods for your Amazon Connect Talent instance, contact AWS Support.

Identity and access management for Amazon Connect Talent

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

Topics

Audience

How you use AWS Identity and Access Management (IAM) differs based on your role:

- **Service user** - request permissions from your administrator if you cannot access features (see Troubleshooting Amazon Connect Talent identity and access)
- **Service administrator** - determine user access and submit permission requests (see How Amazon Connect Talent works with IAM)
- **IAM administrator** - write policies to manage access (see Identity-based policy examples for Amazon Connect Talent)

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be authenticated as the AWS account root user, an IAM user, or by assuming an IAM role.

You can sign in as a federated identity using credentials from an identity source like AWS IAM Identity Center (IAM Identity Center), single sign-on authentication, or Google/Facebook credentials. For more information about signing in, see How to sign in to your AWS account in the *AWS Sign-In User Guide*.

For programmatic access, AWS provides an SDK and CLI to cryptographically sign requests. For more information, see AWS Signature Version 4 for API requests in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity called the AWS account *root user* that has complete access to all AWS services and resources. We strongly recommend that you don't use the root user for everyday tasks. For tasks that require root user credentials, see Tasks that require root user credentials in the *IAM User Guide*.

Federated identity

As a best practice, require human users to use federation with an identity provider to access AWS services using temporary credentials.

A *federated identity* is a user from your enterprise directory, web identity provider, or Directory Service that accesses AWS services using credentials from an identity source. Federated identities assume roles that provide temporary credentials.

For centralized access management, we recommend AWS IAM Identity Center. For more information, see What is IAM Identity Center? in the *AWS IAM Identity Center User Guide*.

IAM users and groups

An *IAM user* is an identity with specific permissions for a single person or application. We recommend using temporary credentials instead of IAM users with long-term credentials. For more information, see Require human users to use federation with an identity provider to access AWS using temporary credentials in the *IAM User Guide*.

An *IAM group* specifies a collection of IAM users and makes permissions easier to manage for large sets of users. For more information, see Use cases for IAM users in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity with specific permissions that provides temporary credentials. You can assume a role by switching from a user to an IAM role (console) or by calling an AWS CLI or AWS API operation. For more information, see Methods to assume a role in the *IAM User Guide*.

IAM roles are useful for federated user access, temporary IAM user permissions, cross-account access, cross-service access, and applications running on Amazon EC2. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy defines permissions when associated with an identity or resource. AWS evaluates these policies when a principal makes a request. Most policies are stored in AWS as JSON documents. For more information about JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Using policies, administrators specify who has access to what by defining which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. An IAM administrator creates IAM policies and adds them to roles, which users can then assume. IAM policies define permissions regardless of the method used to perform the operation.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you attach to an identity (user, group, or role). These policies control what actions identities can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

Identity-based policies can be *inline policies* (embedded directly into a single identity) or *managed policies* (standalone policies attached to multiple identities). To learn how to choose between managed and inline policies, see Choose between managed policies and inline policies in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples include IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-

based policies, service administrators can use them to control access to a specific resource. You must specify a principal in a resource-based policy.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Other policy types

AWS supports additional policy types that can set the maximum permissions granted by more common policy types:

- **Permissions boundaries** – Set the maximum permissions that an identity-based policy can grant to an IAM entity. For more information, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – Specify the maximum permissions for an organization or organizational unit in AWS Organizations. For more information, see Service control policies in the *AWS Organizations User Guide*.
- **Resource control policies (RCPs)** – Set the maximum available permissions for resources in your accounts. For more information, see Resource control policies (RCPs) in the *AWS Organizations User Guide*.
- **Session policies** – Advanced policies passed as a parameter when creating a temporary session for a role or federated user. For more information, see Session policies in the *IAM User Guide*.

Multiple policy types

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

How Amazon Connect Talent works with IAM

Before you use IAM to manage access to Amazon Connect Talent, learn what IAM features are available to use with Amazon Connect Talent.

IAM feature	Amazon Connect Talent support
Identity-based policies	Yes

IAM feature	Amazon Connect Talent support
Resource-based policies	No
Policy actions	Yes
Policy resources	Yes
Policy condition keys	Yes
ACLs	No
ABAC (tags in policies)	Partial
Temporary credentials	Yes
Principal permissions	Yes
Service roles	Yes
Service-linked roles	No

To get a high-level view of how Amazon Connect Talent and other AWS services work with most IAM features, see AWS services that work with IAM in the *IAM User Guide*.

Identity-based policies for Amazon Connect Talent

Supports identity-based policies: Yes

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

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. To learn about all of the elements that you can use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

Identity-based policy examples for Amazon Connect Talent

To view examples of Amazon Connect Talent identity-based policies, see Identity-based policy examples for Amazon Connect Talent.

Resource-based policies within Amazon Connect Talent

Supports resource-based policies: No

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Policy actions for Amazon Connect Talent

Supports policy actions: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Include actions in a policy to grant permissions to perform the associated operation.

To see a list of Amazon Connect Talent actions, see Actions Defined by Amazon Connect Talent in the *Service Authorization Reference*.

Policy actions in Amazon Connect Talent use the following prefix before the action:

```
connect
```

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [
      "connect:action1",
      "connect:action2"
         ]
```

To view examples of Amazon Connect Talent identity-based policies, see Identity-based policy examples for Amazon Connect Talent.

Policy resources for Amazon Connect Talent

Supports policy resources: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. As a best practice, specify a resource using its Amazon Resource Name (ARN). For actions that don't support resource-level permissions, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

To see a list of Amazon Connect Talent resource types and their ARNs, see Resources Defined by Amazon Connect Talent in the *Service Authorization Reference*. To learn with which actions you can specify the ARN of each resource, see Actions Defined by Amazon Connect Talent.

To view examples of Amazon Connect Talent identity-based policies, see Identity-based policy examples for Amazon Connect Talent.

Policy condition keys for Amazon Connect Talent

Supports service-specific policy condition keys: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element specifies when statements execute based on defined criteria. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

To see a list of Amazon Connect Talent condition keys, see Condition Keys for Amazon Connect Talent in the *Service Authorization Reference*. To learn with which actions and resources you can use a condition key, see Actions Defined by Amazon Connect Talent.

To view examples of Amazon Connect Talent identity-based policies, see Identity-based policy examples for Amazon Connect Talent.

ACLs in Amazon Connect Talent

Supports ACLs: No

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

ABAC with Amazon Connect Talent

Supports ABAC (tags in policies): Partial

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes called tags. You can attach tags to IAM entities and AWS resources, then design ABAC policies to allow operations when the principal's tag matches the tag on the resource.

To control access based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see Define permissions with ABAC authorization in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see Use attribute-based access control (ABAC) in the *IAM User Guide*.

Using temporary credentials with Amazon Connect Talent

Supports temporary credentials: Yes

Temporary credentials provide short-term access to AWS resources and are automatically created when you use federation or switch roles. AWS recommends that you dynamically generate

temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM and AWS services that work with IAM in the *IAM User Guide*.

Cross-service principal permissions for Amazon Connect Talent

Supports forward access sessions (FAS): Yes

Forward access sessions (FAS) use the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. For policy details when making FAS requests, see Forward access sessions.

Service roles for Amazon Connect Talent

Supports service roles: Yes

A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Create a role to delegate permissions to an AWS service in the *IAM User Guide*.

> **Warning**
>
> Changing the permissions for a service role might break Amazon Connect Talent functionality. Edit service roles only when Amazon Connect Talent provides guidance to do so.

Identity-based policy examples for Amazon Connect Talent

By default, users and roles don't have permission to create or modify Amazon Connect Talent resources. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies.

To learn how to create an IAM identity-based policy by using these example JSON policy documents, see Create IAM policies (console) in the *IAM User Guide*.

For details about actions and resource types defined by Amazon Connect Talent, including the format of the ARNs for each of the resource types, see Actions, Resources, and Condition Keys for Amazon Connect Talent in the *Service Authorization Reference*.

Topics

- Policy best practices
- Using the Amazon Connect Talent console
- Allow users to view their own permissions

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Amazon Connect Talent resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see AWS managed policies or AWS managed policies for job functions in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as CloudFormation. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see Validate policies with IAM Access Analyzer in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Secure API access with MFA in the *IAM User Guide*.

For more information about best practices in IAM, see Security best practices in IAM in the *IAM User Guide*.

Using the Amazon Connect Talent console

To access the Amazon Connect Talent console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the Amazon Connect Talent resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (users or roles) with that policy.

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that they're trying to perform.

To ensure that users and roles can still use the Amazon Connect Talent console, also attach an Amazon Connect Talent AWS managed policy to the entities. For more information, see Adding permissions to a user in the *IAM User Guide*.

Allow users to view their own permissions

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
```

```
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Troubleshooting Amazon Connect Talent identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Amazon Connect Talent and IAM.

Topics

- I am not authorized to perform an action in Amazon Connect Talent
- I am not authorized to perform iam:PassRole
- I want to allow people outside of my AWS account to access my Amazon Connect Talent resources

I am not authorized to perform an action in Amazon Connect Talent

If you receive an error that you're not authorized to perform an action, your policies must be updated to allow you to perform the action.

The following example error occurs when the `mateojackson` IAM user tries to use the console to view details about a fictional *`my-example-widget`* resource but doesn't have the fictional `connect:`*`GetWidget`* permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 connect:GetWidget on resource: my-example-widget
```

In this case, the policy for the `mateojackson` user must be updated to allow access to the *`my-example-widget`* resource by using the `connect:GetWidget` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to Amazon Connect Talent.

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

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

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

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I want to allow people outside of my AWS account to access my Amazon Connect Talent resources

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

To learn more, consult the following:

- To learn whether Amazon Connect Talent supports these features, see How Amazon Connect Talent works with IAM.

- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.

Compliance validation for Amazon Connect Talent

Our new AWS sign-up experience is not designed for regulated workloads. If you're using our new AWS sign-up experience, but you want to use AWS for regulated workloads, you can sign up for AWS (advanced) or activate advanced features for your AWS environment.

To learn whether an AWS service is within the scope of specific compliance programs, see AWS services in Scope by Compliance Program and choose the compliance program that you are interested in. For general information, see AWS Compliance Programs.

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

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. For more information about your compliance responsibility when using AWS services, see AWS Security Documentation.

Configuration and vulnerability analysis in Amazon Connect Talent

Configuration and IT controls are a shared responsibility between AWS and you, our customer. For more information, see the AWS shared responsibility model.

Because Amazon Connect Talent is a fully managed service, AWS handles patching and maintenance of the underlying infrastructure, and there is no guest operating system for you to manage.

Monitoring Amazon Connect Talent

Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon Connect Talent and your other AWS solutions. AWS provides the following monitoring tools to watch Amazon Connect Talent, report when something is wrong, and take automatic actions when appropriate:

- *Amazon CloudWatch* monitors your AWS resources and the applications you run on AWS in real time. You can collect and track metrics, create customized dashboards, and set alarms that notify you or take actions when a specified metric reaches a threshold that you specify. For more information, see the Amazon CloudWatch User Guide.
- *Amazon CloudWatch Logs* enables you to monitor, store, and access your log files from CloudTrail and other sources. CloudWatch Logs can monitor information in the log files and notify you when certain thresholds are met. You can also archive your log data in highly durable storage. For more information, see the Amazon CloudWatch Logs User Guide.
- *Amazon EventBridge* can be used to automate your AWS services and respond automatically to system events, such as application availability issues or resource changes. Events from AWS services are delivered to EventBridge in near real time. You can write simple rules to indicate which events are of interest to you and which automated actions to take when an event matches a rule. For more information, see Amazon EventBridge User Guide.
- *AWS CloudTrail* captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the AWS CloudTrail User Guide.

Monitoring Amazon Connect Talent with Amazon CloudWatch

You can monitor Amazon Connect Talent using CloudWatch, which collects raw data and processes it into readable, near real-time metrics. These statistics are kept for 15 months, so that you can access historical information and gain a better perspective on how your web application or service is performing. You can also set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see the Amazon CloudWatch User Guide.

Monitoring Amazon Connect Talent events in Amazon EventBridge

You can monitor Amazon Connect Talent events in EventBridge, which delivers a stream of real-time data from your own applications, software-as-a-service (SaaS) applications, and AWS services. EventBridge routes that data to targets such as AWS Lambda and Amazon Simple Notification Service. These events are the same as those that appear in Amazon CloudWatch Events, which delivers a near real-time stream of system events that describe changes in AWS resources.

Logging Amazon Connect Talent API calls using AWS CloudTrail

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

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

Amazon Connect Talent information in CloudTrail

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

The event source for Amazon Connect Talent in CloudTrail is `connect-talent.amazonaws.com`. Use this value to filter CloudTrail logs for Amazon Connect Talent events.

For an ongoing record of events in your AWS account, including events for Amazon Connect Talent, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you

specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for creating a trail
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple regions and Receiving CloudTrail log files from multiple accounts

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

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity element.

Understanding Amazon Connect Talent log file entries

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

Integration with AWS Security Hub CSPM

AWS Security Hub CSPM provides you with a comprehensive view of your security state in AWS and helps you to check your environment against security industry standards and best practices. Security Hub CSPM collects security data from across AWS accounts, services, and supported third-party partner products and helps you to analyze your security trends and identify the highest priority security issues.

The Amazon Connect Talent integration with Security Hub CSPM enables you to send findings from Amazon Connect Talent to Security Hub CSPM. Security Hub CSPM can then include those findings in its analysis of your security posture.

Contents

How Amazon Connect Talent sends findings to Security Hub CSPM

In Security Hub CSPM, security issues are tracked as findings. Some findings come from issues that are detected by other AWS services or by third-party partners. Security Hub CSPM also has a set of rules that it uses to detect security issues and generate findings.

Security Hub CSPM provides tools to manage findings from across all of these sources. You can view and filter lists of findings and view details for a finding. See Viewing findings in the *AWS Security Hub User Guide*. You can also track the status of an investigation into a finding. See Taking action on findings in the *AWS Security Hub User Guide*.

All findings in Security Hub CSPM use a standard JSON format called the AWS Security Finding Format (ASFF). The ASFF includes details about the source of the issue, the affected resources, and the current status of the finding. See AWS Security Finding Format (ASFF) in the *AWS Security Hub User Guide*.

Amazon Connect Talent is one of the AWS services that sends findings to Security Hub CSPM.

Types of findings that Amazon Connect Talent sends

Amazon Connect Talent sends the findings to Security Hub CSPM using the AWS Security Finding Format (ASFF). In ASFF, the `Types` field provides the finding type.

Latency for sending findings

When Amazon Connect Talent creates a new finding, it sends the finding to Security Hub CSPM in near real time.

Typical finding from Amazon Connect Talent

Amazon Connect Talent sends findings to Security Hub CSPM using the AWS Security Finding Format (ASFF).

Enabling and configuring the integration with AWS Security Hub CSPM

To use the integration with AWS Security Hub CSPM, you must enable Security Hub CSPM. For information on how to enable Security Hub CSPM, see Setting up Security Hub in the *AWS Security Hub User Guide*.

How to stop sending findings to AWS Security Hub CSPM

To stop sending findings to Security Hub CSPM, you can use either the Security Hub CSPM console or the API.

See Disabling and enabling the flow of findings from an integration (console) or Disabling the flow of findings from an integration (Security Hub API, AWS CLI) in the *AWS Security Hub User Guide*.

Endpoints and quotas for Amazon Connect Talent

The following sections describe the service endpoints and the service quotas for Amazon Connect Talent.

Topics

Service endpoints

A service endpoint is the URL of the entry point for an AWS service. Amazon Connect Talent is available in specific AWS Regions, and you connect to the endpoint for the Region where your instance is hosted. For more information about the Regions where Amazon Connect Talent is available, see Supported Regions and endpoints.

Service quotas

Your AWS account has default quotas, formerly referred to as limits, for each AWS service. Unless otherwise noted, each quota is Region-specific. You can request increases for some quotas, and other quotas cannot be increased.

To view the quotas for Amazon Connect Talent, open the Service Quotas console. In the navigation pane, choose **AWS services** and select **Amazon Connect Talent**.

To request a quota increase, see Requesting a Quota Increase in the *Service Quotas User Guide*. If the quota is not yet available in Service Quotas, use the limit increase form.

Document history for the Amazon Connect Talent Administrator Guide

The following table describes the documentation releases for the Amazon Connect Talent Administrator Guide.

Change	Description	Date
Initial release	Initial release of the Amazon Connect Talent Administrator Guide.	September 1, 2026