Amazon Honeycode

Administrator's Guide

Amazon Honeycode: Administrator's Guide

Table of Contents

Single Sign-On (SSO) for Honeycode

Amazon Honeycode supports single sign-on (SSO) for organizations with a Plus or Pro plan. Single sign-on works with any identity provider (IdP) that supports Security Assertion Markup Language (SAML) 2.0.

In this section, you'll learn how to set up SSO for Honeycode in the AWS Management Console.

What is SSO?

Single sign-on is a way for users to authenticate and log in to an application using their corporate credentials. SSO allows for central access management of Honeycode SSO teams by AWS account admins.

Get Started

Prerequisites

There are some items you'll need to have in place before you can set up single sign-on for your organization. You must:

- Have an AWS account
- Enable IAM Identity Center for your organization in the region us-west-2 (Oregon). Honeycode will use IAM Identity Center application assignments to perform authentication and access information about users and groups
- Set up groups in AWS IAM Identity Center (successor to AWS SSO)
- Be able to add a TXT record to your domain naming system (DNS)
- Claim all domains that are to be associated with an SSO team from the same AWS account
- Claim any subdomains explicitly

> **Note**
> We do not currently support migration of workbooks and apps created with a standard account to an SSO team. If you need additional help, please reach out to `<honeycode-bd@amazon.com>`.

Required IAM policies

Configure your user, role, or group with at least the following AWS-managed policies:

- `AmazonHoneycodeFullAccess`
- `AWSSSODirectoryReadOnly`
- `AWSSSOMemberAccountAdministrator`
- `AWSSupportAccess`

In addition to the AWS-managed policies listed above, create and attach the following policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "iam:AWSServiceName": "honeycode.amazonaws.com"
        }
      }
    }
  ]
}
```

These policies allow Honeycode connect and interact with your organization’s IAM Identity Center. Once you connect Honeycode to IAM Identity Center, you can detach these policies from your user/role/group.

Setting up SSO

AWS account admins can set up single sign-on for Amazon Honeycode in the AWS Management Console. Here is a brief overview of SSO setup:

- Claim your domain
- Add a TXT record to your DNS and wait for verification
- Create a new SSO team
- Add admin and member groups

Claim your domain
Enter the company domains to be used for single sign-on.

Add TXT record to DNS
We'll provide the TXT record to verify domain ownership.

Create SSO team
Enter team name, Honeycode plan, and domain details.

Add admins & members
Add admin and member groups as they appear in your IdP.

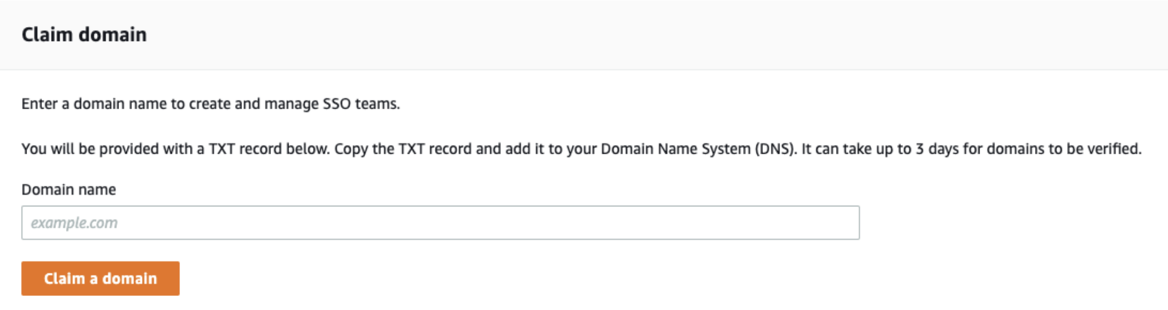
Warning
AWS IAM Identity Center (successor to AWS SSO) is required for successful setup and operation of Honeycode SSO Teams. Deletion of AWS IAM Identity Center (successor to AWS SSO) will render the linked SSO Teams unusable. Affected teams cannot be recovered by re-creating AWS IAM Identity Center application assignments, as AWS IAM Identity Center application assignments manage group and user identities for authentication and authorization.

Note
From the time you add the TXT record to your DNS, verification can take up to three business days. Once your domain is verified, you can complete the SSO setup process.

1a. Claim your domain

In the AWS Management Console, go to **Honeycode > Domains**. In the Claim domain section, enter a domain name.

- *Example: company.com*



Claim domain

Enter a domain name to create and manage SSO teams.

You will be provided with a TXT record below. Copy the TXT record and add it to your Domain Name System (DNS). It can take up to 3 days for domains to be verified.

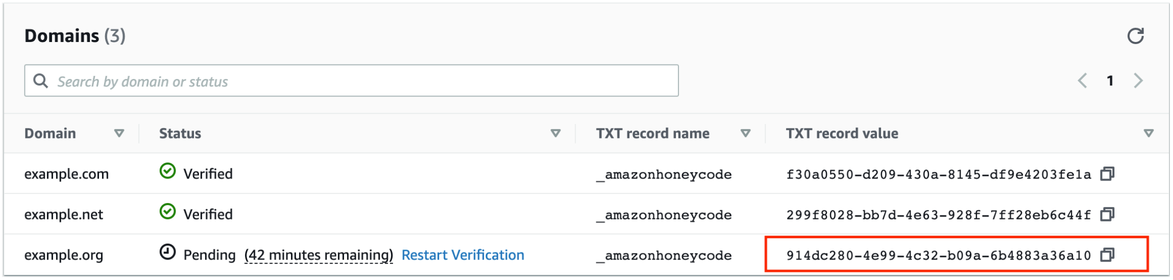
Domain name

Click **Claim a domain**. The domain entered will appear in the Manage domains section with the status Pending.

> **Note**
> All domains that are to be associated with a Honeycode SSO team must be claimed from the same AWS account.

1b. Add the TXT record to your DNS

After claiming your domain, you will find a unique key provided in the TXT record column of the Manage domains section.



Domains (3)

Domain	Status	TXT record name	TXT record value
example.com	Verified	_amazonhoneycode	f30a0550-d209-430a-8145-df9e4203fe1a
example.net	Verified	_amazonhoneycode	299f8028-bb7d-4e63-928f-7ff28eb6c44f
example.org	Pending (42 minutes remaining) Restart Verification	_amazonhoneycode	914dc280-4e99-4c32-b09a-6b4883a36a10

A TXT record provides information about your domain and verifies ownership. **Copy the TXT record** value and add it to your Domain Name System (DNS) settings.

The following shows the available domain verification statuses:

- **PENDING**: Domain is not yet verified. Add the TXT record to your DNS.
- **VERIFIED**: Domain ownership is verified. Honeycode continues re-verifying ownership of the domain.
- **FAILED**: The verification request expired. Restart the verification process.
- **INVALID**: Domain re-verification failed. Re-add the TXT record to your DNS prior to the ending of grace period.
- **REVOKED**: Ownership was not re-verified within the 7 days grace-period. Restart the verification process.

> **Note**
> It might take some time for propagation of the DNS record after re-adding the TXT record. Ensure you add the TXT record well before the grace period expires.

We've included instructions for adding a TXT record to Amazon Route 53, as well as some general instructions for adding a TXT record to other DNS providers.

How to add a TXT record to an Amazon Route 53 domain

1. **Copy the TXT record value** provided in Honeycode > Domains in the AWS console.
2. Open the Route 53 console at https://console.aws.amazon.com/route53/.
3. In the navigation pane, choose **Hosted zones**.
4. Select the domain that you want to add a TXT record to, and then choose **Go to Record sets**.
5. Choose **Create record set**
6. In the **Create Record Set** pane, make the following selections:

    a. For **Name**, type **`_amazonhoneycode`**.
    b. For **Type**, choose **TXT - Text**.
    c. For **TTL (Seconds)**, type **`1800`**.
    d. For **Value**, paste the TXT record value you copied from the communication received.
    e. Choose **Create**.

Note
After the TXT record has been added to your DNS, domain verification can take up to 3 business days.

How to add a TXT record to other DNS providers

1. **Go to your DNS provider** website and sign in to your account. If you aren't sure which DNS provider serves your domain, you can look it up by using a free Whois service.
2. Find the page for updating your domain's DNS records. This page might have a name similar to one of the following examples: **DNS Records**, **DNS Zone File**, or **Advanced DNS**. If you're unsure, consult the provider's documentation.
3. **Add a TXT record** with the name and value provided in Honeycode > Domains in the AWS console.
4. **Save your changes.**

Note
After the TXT record has been added to your DNS, domain verification can take up to 3 business days.

How to check that the TXT record is added correctly

Use the nslookup tool to confirm that the TXT record is added correctly to your DNS service. The nslookup tool is available for Windows and Linux.

1. Open a command prompt to find the name servers for your domain. These servers contain the most up-to-date information for your domain, and can take longer to propagate to other DNS servers.
2. To list all of the name servers that serve your domain, run the following command:

```
nslookup -type=NS example.com
```

3. Next, verify that the TXT record is correctly added. Using your domain and one of the name servers that you found in step 2, run the following command:

```
nslookup -type=TXT _amazonhoneycode.example.com ns1.name-server.net
```

4. In the output of the command, verify that the string that follows text matches the TXT record value in the AWS console under Honeycode > Domains.

Example:

Looking for a TXT record under `_amazonhoneycode.example.com` with a value of `fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk=`.

If the record is correctly added, the command should have the following output:

```
_amazonhoneycode.example.com text = "fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk="
```

> **Warning**
> Please do not remove the TXT record from your DNS while the domain is assigned to Amazon Honeycode.

2. Create an SSO team

The next step is to create your first Honeycode SSO team. Please note that teams created with a standard account cannot be converted to SSO teams.

> **Note**
> After selected domains are associated with an SSO team, users will lose access to any workbooks or apps created with a standard account using the same domain. If you would like more information, reach out to `<honeycode-bd@amazon.com>`.

Go to **Honeycode > Teams** in the AWS console and click **Create SSO team**. You'll be prompted to add the following:

- **Team name**: This is how users in your company will be identified in Amazon Honeycode
- **Team description (optional)**: This will only be seen be team admins with access to the AWS console
- **Email contact**: The email for the primary AWS account admin
- **Honeycode plan**: Select your team's plan. SSO is available for Amazon Honeycode Plus and Pro plans.
- **Domains**: The verified domains you'd like to associate with your SSO team

Amazon Honeycode will automatically create a new service linked role. This role allows Honeycode to interact with your IAM Identity Center. You can learn more about the service linked roles here (p. 13).

After you've filled out the required fields, click **Next**.

3. Add admin and member groups

After you've filled out the required fields, you'll be prompted next to add admin and member groups as they appear in your identity provider (IdP). Single sign-works with any IdP that supports Security Assertion Markup Language (SAML) 2.0.

Teams have two roles, admins and members. Your team can have multiple admins, or just one. Team admins can manage access to workbooks and apps in Honeycode, and make changes to the team's plan.

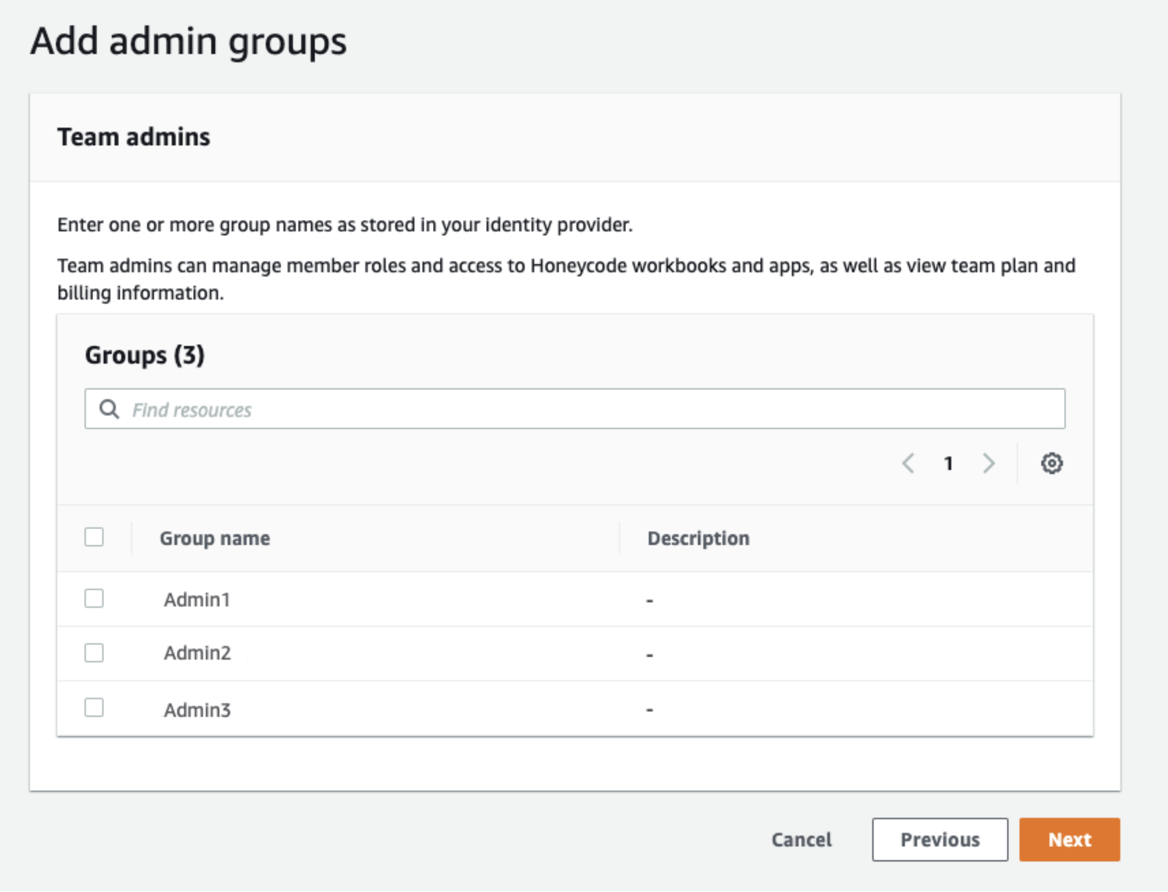
Team members have the ability create workbooks, build apps, and share with SSO team members.

> **Note**
> Each admin or member on a team counts as one user in the current team, regardless if the same user is an admin or member of other teams, or if they are present in multiple groups. If the same group is marked as admin and as a member, they are only considered as admin.

Add admin groups

Team admins can manage access to workbooks and apps in Honeycode, and make changes to the team's plan.

Select one or more group names as stored in your identity provider (IdP). Once you’ve added at least one group name, click **Next**.



Add admin groups

Team admins

Enter one or more group names as stored in your identity provider.

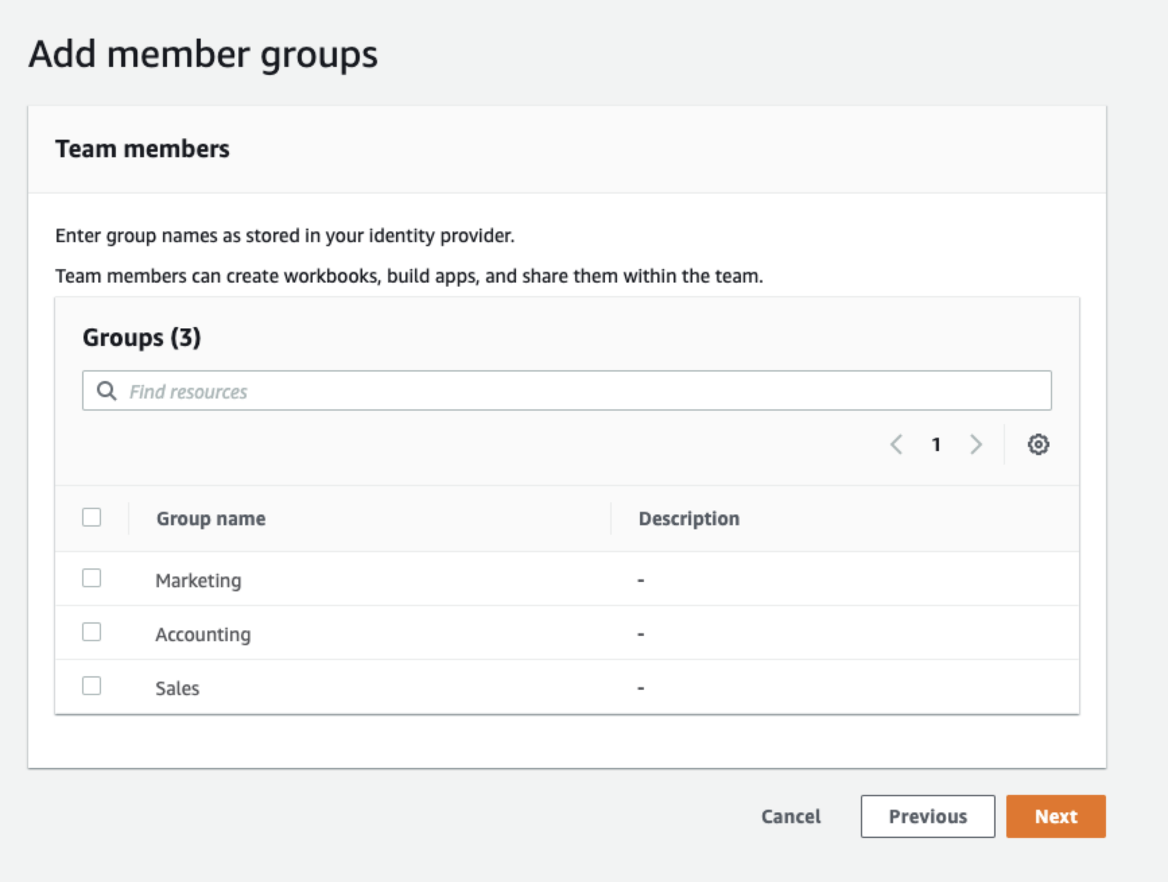
Team admins can manage member roles and access to Honeycode workbooks and apps, as well as view team plan and billing information.

Groups (3)

□	Group name	Description
□	Admin1	-
□	Admin2	-
□	Admin3	-

Add member groups

Team members can create workbooks, build apps, and share with SSO team members. To add member groups, select the group names as stored in your identity provider. Click **Next**.



Add member groups

Team members

Enter group names as stored in your identity provider.

Team members can create workbooks, build apps, and share them within the team.

Groups (3)

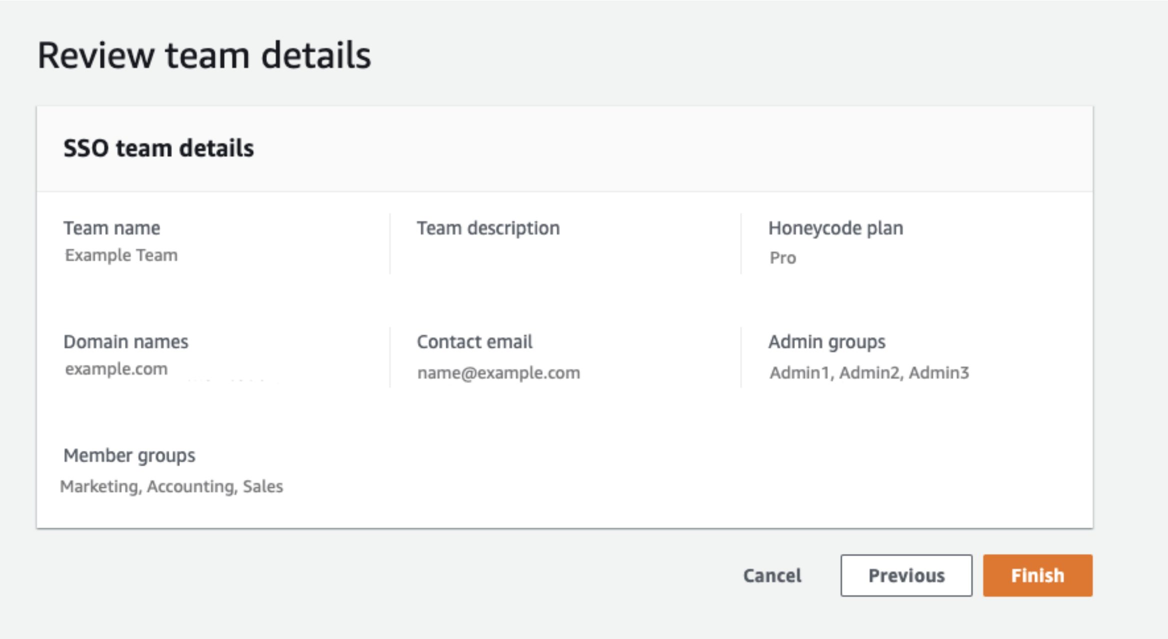
□	Group name	Description
□	Marketing	-
□	Accounting	-
□	Sales	-

Users in your admin and member groups will now be able to sign in to Amazon Honeycode using their corporate credentials. It may take up to 4 hours from initial setup, before the full Honeycode service is available for use.

> **Note**
> Any subsequent changes made to team groups, domains or changes in group membership (in AWS IAM Identity Center (successor to AWS SSO)) may take up to 4 hours to be reflected in Honeycode.

4. Review SSO team details

Verify that your SSO team details are correct and click **Finish**.



Review team details

SSO team details

Team name
Example Team

Team description

Honeycode plan
Pro

Domain names
example.com

Contact email
name@example.com

Admin groups
Admin1, Admin2, Admin3

Member groups
Marketing, Accounting, Sales

Deleting an SSO team

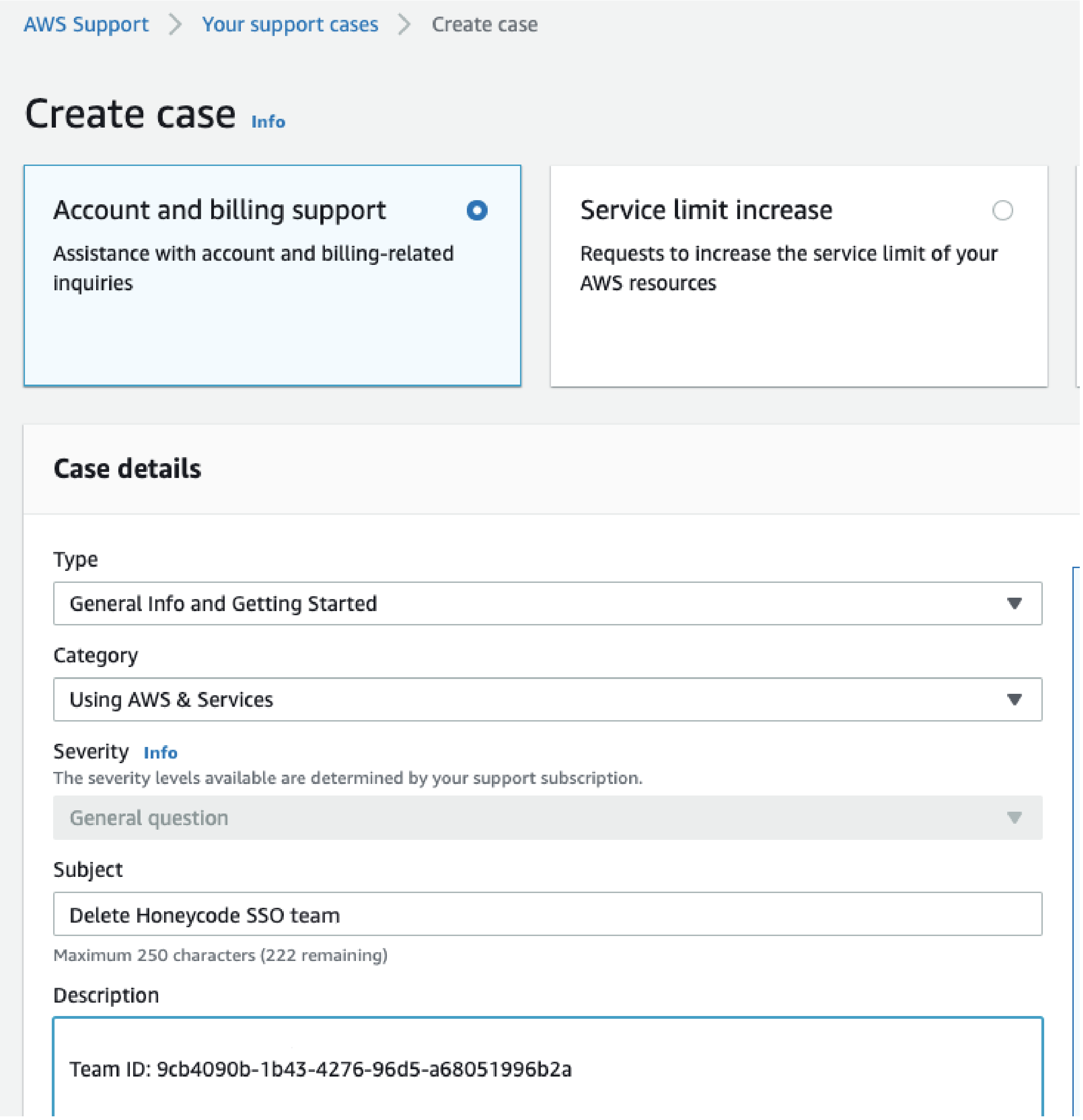
To request deletion of an SSO team, please create an AWS support case.

1. From the top menu of the AWS console, select **Support > Support center**, and then click **Create case**.
2. File the case under: **Account and billing support**
3. Under **Case details**, please make the following selections:

    a. **Type**: General Info and Getting Started

    b. **Category**: Using AWS & Services

    c. **Subject**: Delete Honeycode SSO team
4. Please include the following details in the support ticket:
    - Team ID
5. Click **Submit**



Create case

● Account and billing support
Assistance with account and billing-related inquiries

○ Service limit increase
Requests to increase the service limit of your AWS resources

Case details

Type: General Info and Getting Started

Category: Using AWS & Services

Severity
The severity levels available are determined by your support subscription.
General question

Subject: Delete Honeycode SSO team

Maximum 250 characters (222 remaining)

Description:

Team ID: 9cb4090b-1b43-4276-96d5-a68051996b2a

Note

You will continue to be billed for up to 10 business days after you've requested deletion. We will offer you a refund for this time assuming you've had no new usage.

FAQs

AWS account & Honeycode

Q: What regions do you currently support?

A: We support us-west-2. Support for additional regions is coming soon.

Q: What identity providers (IdP) do you currently support?

A: All IdPs supported by AWS IAM Identity Center (successor to AWS SSO) are supported by Honeycode.

Q: Can I use my on-premises active directory to sign in to Honeycode?

A: Yes, you can use AWS AD Connector to connect to your on-premises AD. Complete the setup with AWS IAM Identity Center (successor to AWS SSO) and use this setup to sign in to Honeycode. Please refer to How to Connect Your On-Premises Active Directory to AWS Using AD Connector.

Q: Does the AWS Directory Service and AWS IAM Identity Center (successor to AWS SSO) need to reside in the same region?

A: Yes, both services need to reside in the same region.

Q: Can I use an external identity provider with AWS IAM Identity Center (successor to AWS SSO)?

A: Yes, you can easily connect to any supported identity provider. Learn more about connecting to an external IdP.

Q: Can I use Google Workspace (formerly known as G Suite) as an external IdP for AWS IAM Identity Center (successor to AWS SSO)?

A: Yes, you can use any SAML-based identity provider. Learn more about connecting Gsuite to AWS IAM Identity Center (successor to AWS SSO).

Q: Why do I need to add IAM policies to set up single sign-on?

A: In the AWS Management Console, your user can take only actions authorized by policies attached to the user. Honeycode integrates with several AWS services, including AWS IAM Identity Center (successor to AWS SSO) and AWS Support, to allow setup of single sign-on. Each AWS service maintains its own AWS-managed policies that grant access to actions of their respective services. See Policies and permissions in IAM for more information.

Q: How long does it take Honeycode to reflect the changes made to users/groups in AWS IAM Identity Center (successor to AWS SSO)?

A: It may take up to four hours for your changes to be reflected in Honeycode.

Q: If I have multiple accounts within AWS Organizations, which AWS account should I use to connect to Honeycode?

A: You can use any member account within AWS Organizations to on-board Honeycode SSO. The AWS account that you use, will be billed and connected to your Amazon Honeycode team.

Domains

Q: Why is my domain status still pending?

A: The status may remain pending if Honeycode couldn’t verify domain ownership due to missing TXT records (p. 3) in the DNS. Please note, DNS propagation to reflect the TXT record may take additional time and result in verification delays.

Q: Why did my domain fail verification?

A: A domain will fail verification if it is already claimed or verified in another AWS account. This can also happen if the claim domain request is outstanding for more than 30 days.

Q: How do I remove a verified domain from my AWS account?

A: Please create an AWS support case and include any domain names you’d like to be removed. The Honeycode team will work with you to have them removed.

Note

Removal of unverified or pending domain names will not have any implications to AWS IAM Identity Center (successor to AWS SSO) or the honeycode service.

Q: What happens to teams associated with a verified domain that is removed from my AWS account?

A: Removal of verified domains associated with teams would mean immediate disassociation from all teams. This means that all users with the domain email addresses will also be removed from associated teams and their workbooks and apps will be deleted.

Q: How do I remove associated domains from my SSO teams?

A: You can remove any domains associated with an SSO team from the AWS console.

1. Go to Honeycode > Teams and select a team.
2. Click **View Details**.
3. From the top right, of the Team details page, click **Edit**.
4. Remove domains from the Select a domain section at the bottom.

Note

Removing a domain from your team will cause Honeycode to remove all users having that domain in their email address. Any workbooks or apps solely owned by these users will be deleted.

Q: How can I contact support for issues with claiming my domain?

A: If you have followed the steps outlined to claim a domain and the status is still pending, please contact `<honeycode-bd@amazon.com>` for support.

Team management

Q: How do I locate my team ID?

A: Your team ID is located in the AWS console on the Team Details page. Go to **Honeycode > Teams** and select a team. Click **View Details**.

Q: After I've created my first SSO team, how do I create more teams?

A: In the AWS console, go to **Honeycode > Teams** and click **Create SSO team**. You'll be prompted to go through the steps as outlined in Create an SSO team (p. 5).

Q: How do I add new admins and team members?

A: In the AWS console, go to **Honeycode > Teams** and select the team you'd like to edit. Click **View details**. You can add more admin and members groups in the fields specified below team details.

Q: How do I delete a team?

A: Currently SSO teams must be manually deleted via an AWS support case. Learn more. (p. 8) Please note you may continue to be billed for 10 days after you delete a team. We will offer you a refund for this time if there is no new usage in your team during this period.

Q: Are there any limits on the number of users and groups that can be added to my Honeycode team?

A: Any restrictions we currently have on users or groups are inherited from AWS IAM Identity Center (successor to AWS SSO) or your IdP. Please refer to AWS IAM Identity Center (successor to AWS SSO) limits for details.

Q: What happens if the alias of a team admin or member changes in the IdP?

A: AWS IAM Identity Center (successor to AWS SSO) defines the uniqueness criteria here. Honeycode currently relies on user emails to define uniqueness. Change of email address may result in a user not being unable to sign in to Honeycode.

Q: What happens when a group is removed from the team?

A: Removal of a group would mean that the users in that group will no longer be able to sign in to Honeycode. Any workbooks and apps solely owned by the removed users will be deleted.

Q: Can I delete the service linked role used for connecting IAM Identity Center to Honeycode?

A: AWS IAM will prevent the deletion of the service role while your Honeycode team or resources are in use. Once off-boarded Honeycode completely, you can then remove the service linked role.

Workbooks and apps

Q: How are workbooks and apps shared with groups?

A: When sharing workbooks and apps in Honeycode, search for group names as identified in the AWS console. You may share with individual email addresses as well.

Q: What happens to workbooks owned by an admin or team member who leaves an SSO team?

A: If an admin or member is no longer part of a team, all workbooks and apps solely owned by the user are deleted. To avoid any loss of data, Honeycode recommends that workbook owners transfer ownership to a new owner prior to leaving the team.

Q: How can a team admin transfer ownership of a workbook to another admin or team member?

A: Team admins and workbook owners can share a workbook via Honeycode and assign owner status.

Q: What happens to workbooks owned by an admin or team member that is no longer in the IdP?

A: Honeycode uses groups as configured in AWS IAM Identity Center (successor to AWS SSO). If an admin or team member is no longer present in AWS IAM Identity Center groups, they will be automatically removed from all teams they are assigned to.

> **Note**
> Removal of a team admin or member in your IdP such as Okta, Azure, or Active Directory will not be identified by Honeycode unless the same changes are reflected in AWS IAM Identity Center (successor to AWS SSO).

APIs and integrations

Q: Can I integrate my Honeycode apps with external systems after I activate IAM Identity Center?

A: Yes, we support the use of Honeycode APIs/SDKs, plus Zapier, Amazon AppFlow, Webhooks, and future integrations if you are using SSO.

Security in Amazon Honeycode

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

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

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

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

Topics

Using Service-Linked Roles for Honeycode

Amazon Honeycode uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Honeycode. Service-linked roles are predefined by Honeycode and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Honeycode easier because you don't have to manually add the necessary permissions. Honeycode defines the permissions of its service-linked roles, and unless defined otherwise, only Honeycode can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting their related resources. This protects your Honeycode resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see AWS Services That Work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-Linked Role Permissions for Honeycode

Honeycode uses the service-linked role named **AWSServiceRoleForAmazonHoneycode** – required for Amazon Honeycode to access your resources.

The AWSServiceRoleForAmazonHoneycode service-linked role trusts the following services to assume the role:

- `honeycode.amazonaws.com`

The role permissions policy allows Honeycode to complete the following actions on the specified resources:

- Action: `sso:GetManagedApplicationInstance` on `all AWS resources`

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

Creating a Service-Linked Role for Honeycode

You don't need to manually create a service-linked role. When you set up Honeycode integration with AWS SSO in the AWS Management Console, the AWS CLI, or the AWS API, Honeycode creates the service-linked role for you.

> **Important**
> This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. Also, if you were using the Honeycode service before November 18, 2020, when it began supporting service-linked roles, then Honeycode created the AWSServiceRoleForAmazonHoneycode role in your account. To learn more, see A New Role Appeared in My IAM Account.

Creating a Service-Linked Role in Honeycode (Console)

You can use the Honeycode console to create a service-linked role.

Follow the Single Sign-On section of this guide to create the service-linked role.

You can also use the IAM console to create a service-linked role with the **Honeycode** use case. In the AWS CLI or the AWS API, create a service-linked role with the `honeycode.amazonaws.com` service name. For more information, see Creating a Service-Linked Role in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

If you delete this service-linked role, you can use the same IAM process to create the role again.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you set up Honeycode integration with AWS SSO, Honeycode creates the service-linked role for you again.

Editing a Service-Linked Role for Honeycode

Honeycode does not allow you to edit the AWSServiceRoleForAmazonHoneycode service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the *IAM User Guide*.

Deleting a Service-Linked Role for Honeycode

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don’t have an unused entity that is not actively monitored or maintained. However, you must clean up your service-linked role before you can manually delete it.

Cleaning Up a Service-Linked Role

Before you can use IAM to delete a service-linked role, you must first delete any resources used by the role.

To ensure that Honeycode is not using any resources in your account, open an AWS Support Case and request deletion of the service-linked role.

Manually Delete the Service-Linked Role

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForAmazonHoneycode service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Supported Regions for Honeycode Service-Linked Roles

Honeycode supports using service-linked roles in all of the regions where the service is available. For more information, see AWS Regions and Endpoints.

Document History for Administrator's Guide

The following table describes the documentation for this release of Amazon Honeycode.

- **API version: latest**
- **Latest documentation update:** Apr 5, 2021

update-history-change	update-history-description	update-history-date

AWS glossary

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