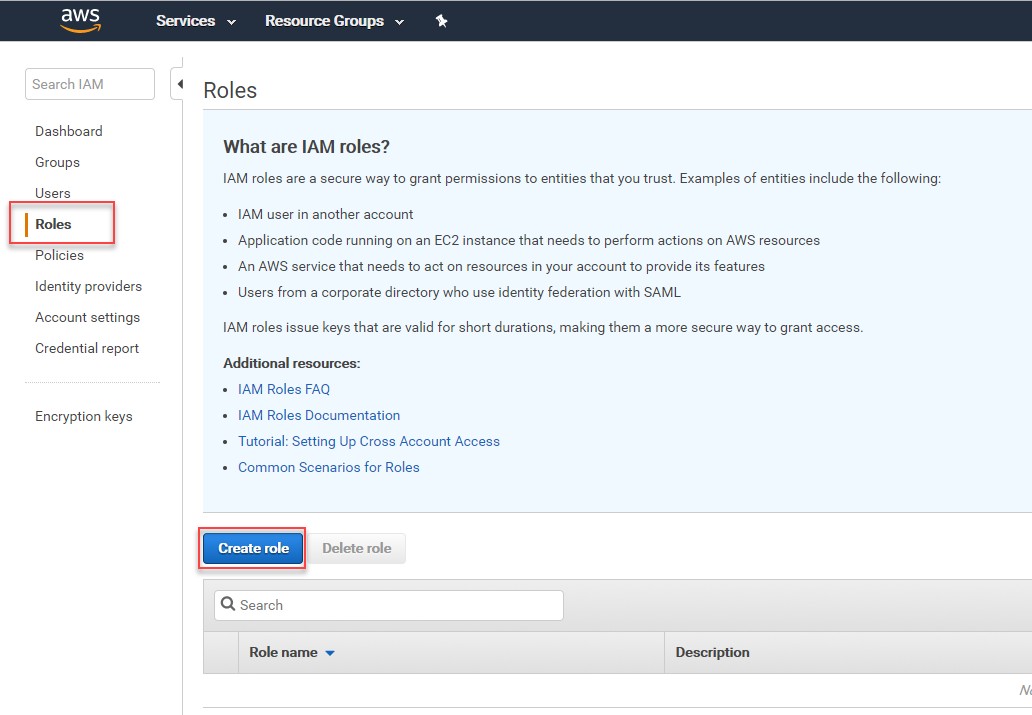
# Skyhigh AWS Integration Notes

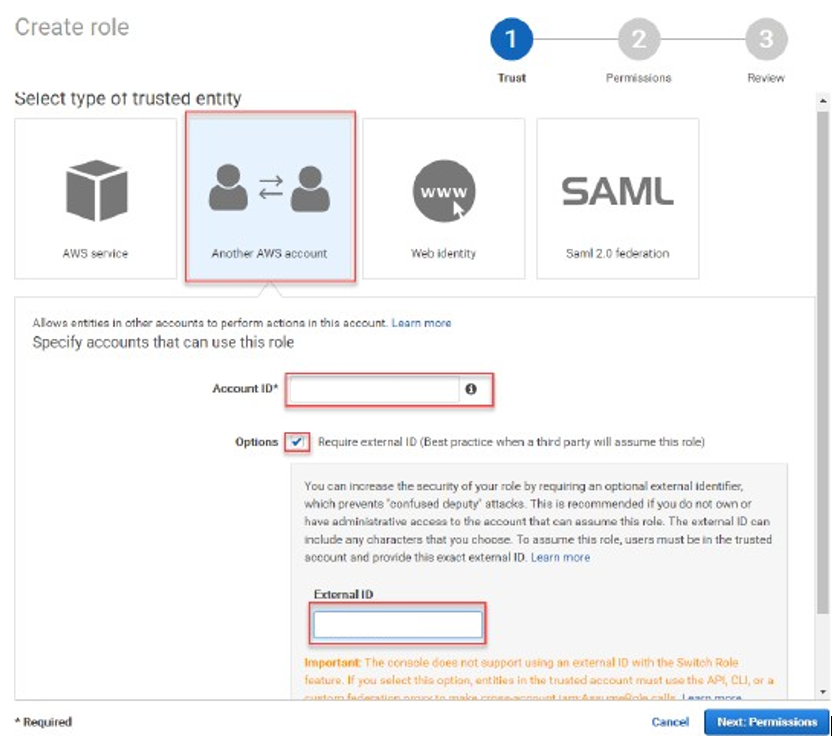
When integrating Skyhigh for AWS, you'll use the Account Settings page to enter your AWS account information; you can also choose to upload a CSV file of all AWS account information. The same page allows you to enable Activity Monitoring and/or Security Configuration Audit.

Before you begin, make sure you've created an IAM role in your AWS account to grant access to Skyhigh. Assign the permission template "ReadOnlyAccess" to this role. Skyhigh's Account ID and External ID are specific to you and will be available on the Skyhigh Dashboard while enabling AWS integration.

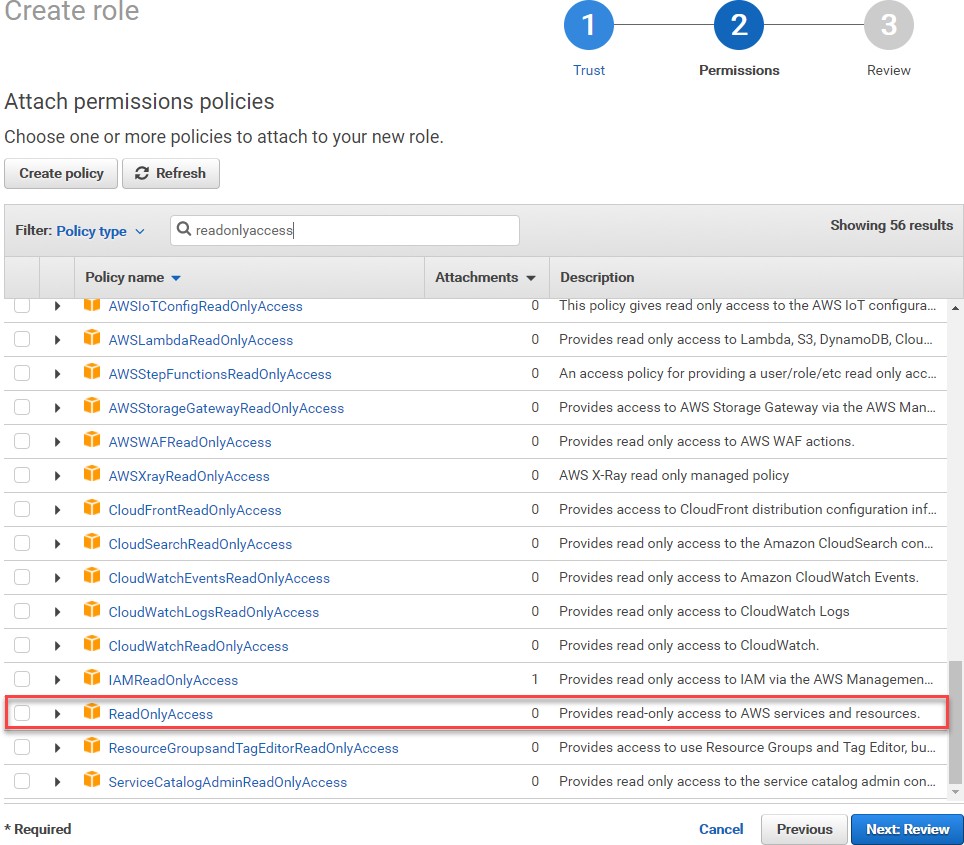
# Create IAM Roles

## To create an IAS Role in AWS with the required permissions:

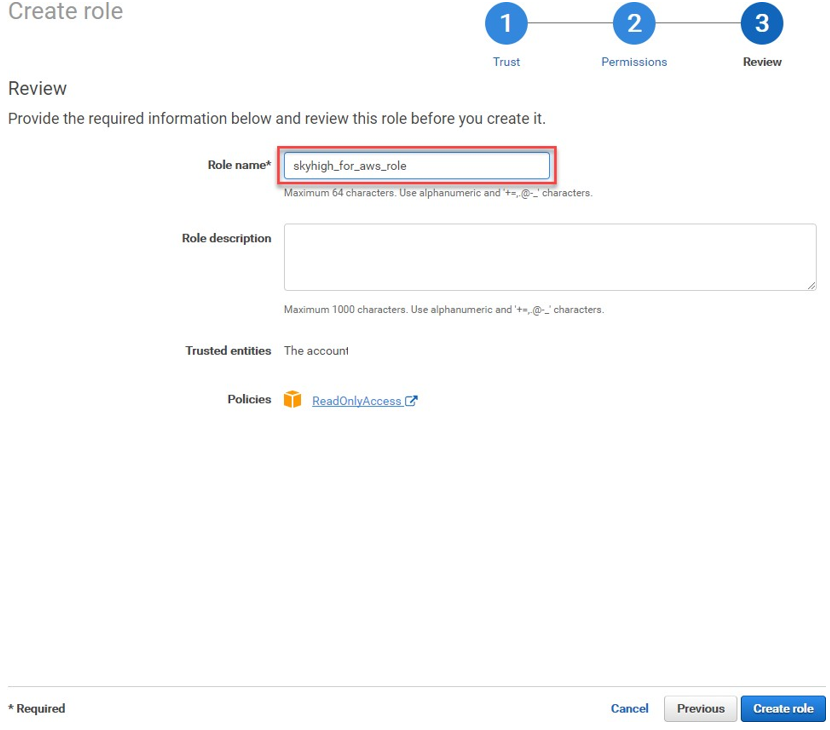
1. Login to your AWS account and select IAM from the services menu.
2. From IAM, navigate to Users > Create role.
3. Select Another AWS account and copy the AWS account ID and external ID from the Skyhigh dashboard into the AWS.



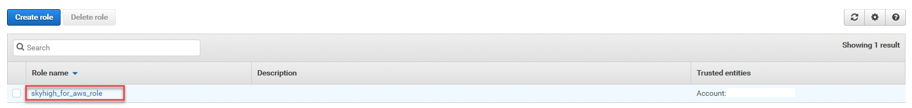
1. Select the ReadOnlyAccess permission.

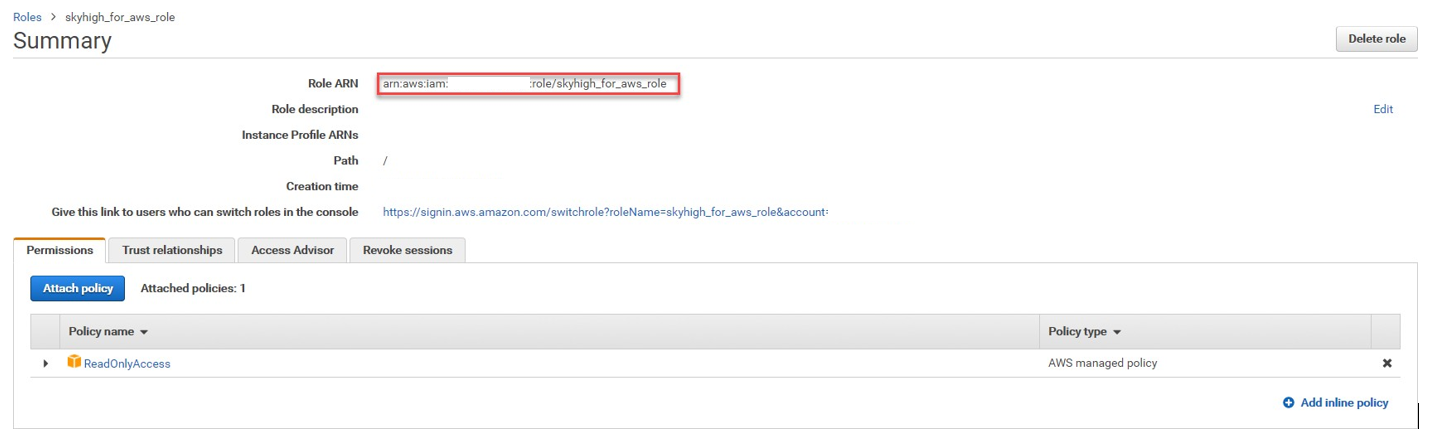


1. Name the role Skyhigh\_for\_AWS\_role (or whatever the you prefer).



1. Click the role name in AWS and copy the ARN.





You'll paste the Role ARN into Skyhigh

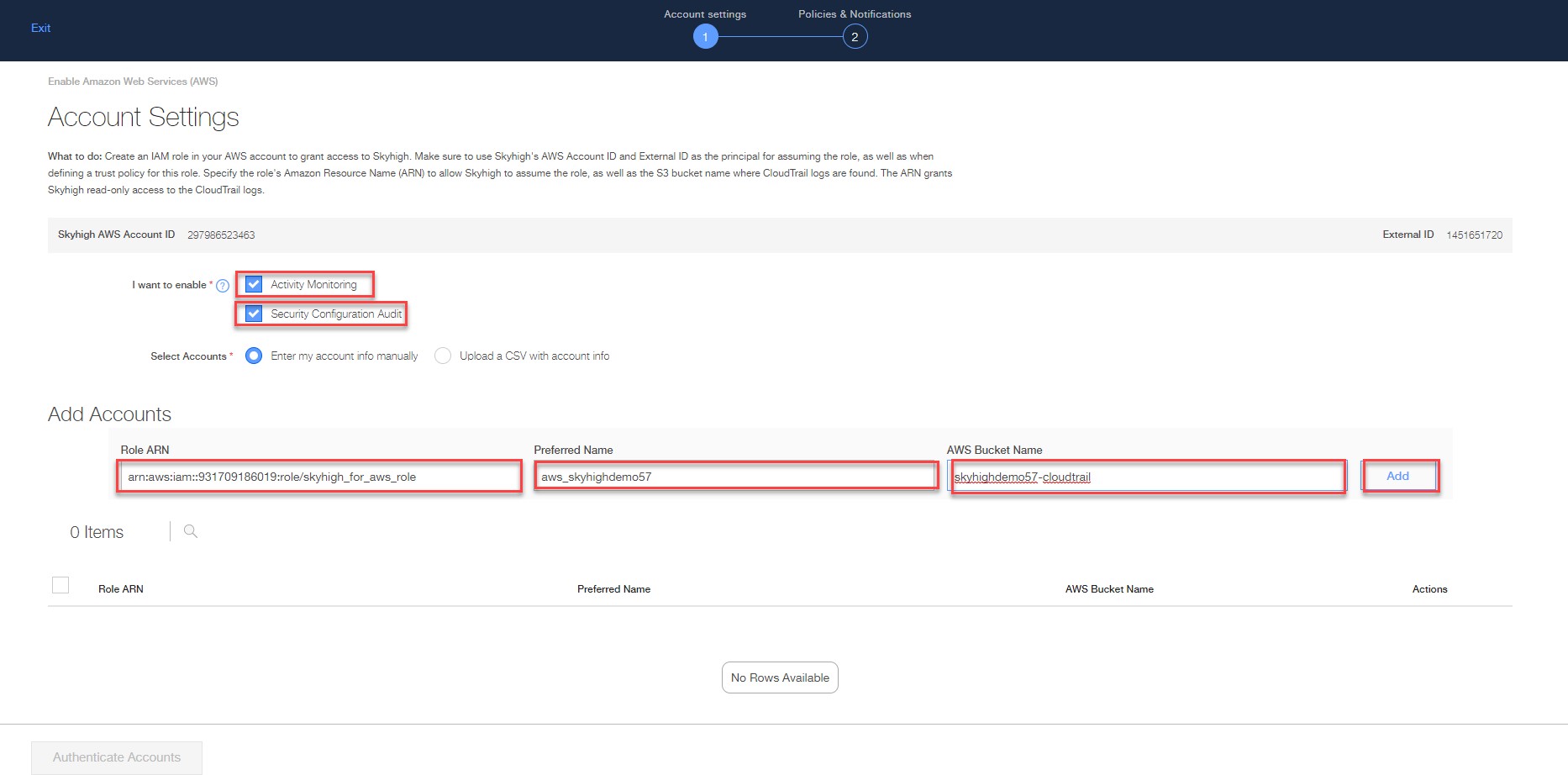
Integrate AWS

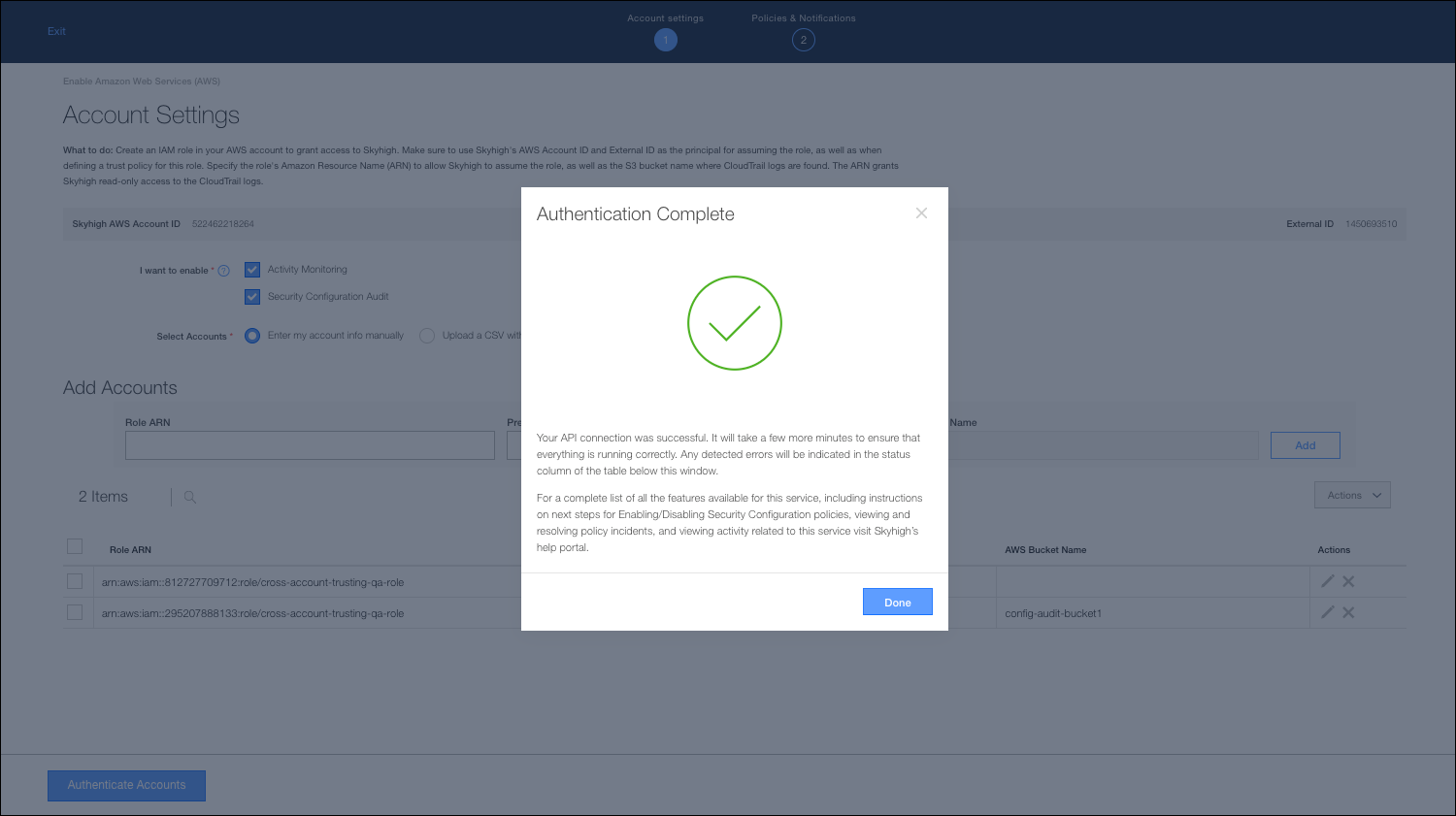
To integrate AWS:

1. Go to Setup & Configuration > Sanctioned Services.
2. Click Enable to the right of Amazon Web Services.
3. In the Account Settings screen, choose options for I want to enable:
   * Activity Monitoring. Select this option to monitor the activity of AWS users and detect risk activity trends for the entire organization over time. If you do not select Activity Monitoring you will not need to provide AWS Bucket names to Skyhigh. [Learn more](https://success.myshn.net/Incident_Management_and_Threat_Protection/Activity_Monitoring)
   * Security Configuration Audit. Select this option to automatically enable the 77 configuration audit policies. [Learn](https://success.myshn.net/Skyhigh_for_IaaS/Security_Configuration_Audit_for_IaaS) [more](https://success.myshn.net/Skyhigh_for_IaaS/Security_Configuration_Audit_for_IaaS)
4. For Select Accounts, choose a method to provide AWS account information to Skyhigh:
   * Enter my account info manually. Choose this option, then type each AWS account's Role ARN, Preferred Name, and AWS Bucket name (if you've enabled Activity Monitoring).
   * Upload a CSV with account info. Choose this option if you have a CSV file in the following format:

role-arn, preferred-name, aws-bucket-name role-arn, preferred-name, aws-bucket-name

Note that if you have not enabled Activity Monitoring, you do not need to provide the Bucket Names. Click Upload to upload the CSV file to Skyhigh.



1. Click Authenticate Accounts to have Skyhigh authenticate each AWS account you entered. If any issues are found, they will display. Otherwise, you'll see an Authentication Complete message. Click Done.
2. In the Policies and Notifications screen, choose the email addresses you'd like to have notified when an incident is generated, and/or type additional emails in the text box. Then click Done to complete the integration.

