

Requesting Access to a Substrate Account and or Cluster For Individuals

Downloaded from Epic Games Confluence

Date: 2025-07-12 04:06:30

Original URL: <https://confluence-epicgames.atlassian.net/wiki/spaces/CDE/pages/81068708>

Document Level Classification

100

- [Introduction](#)
- [Steps for Requesting Access to Substrate Account](#)
 - [01 - Navigate to the SailPoint Request Center, and click on the Access Profiles on the left.](#)
 - [02 - Type AWS and the Substrate account name on the search bar. You can also search for your Substrate account using the account number.](#)
 - [03 - Select the access profile / role you would like to request.](#)
 - [04 - Review and submit the request, click on Review Request and then Submit Request](#)
 - [05 - Once the request is submitted, the AWS account stewards will receive a DM from MegaBot showing your request.](#)

- [06 - After an AWS steward approves or denies the request, you will receive a DM from Megabot.](#)
- [07 - Shortly after your access is approved, you should see the AWS SSO tile in Okta. This should happen within 10 minutes of approval.](#)
- [Steps for Requesting Access to Kubernetes Cluster in a Substrate Account](#)
 - [01 - Navigate to the SailPoint Request Center, and click on the Access Profiles on the left.](#)
 - [02 - Type K8S and the Kubernetes cluster name on the search bar.](#)
 - [03 - Select the access profile / role you would like to request.](#)
 - [04 - Review and submit the request, click on Review Request and then Submit Request](#)
 - [05 - Once the request is submitted, the AWS account stewards will receive a DM from MegaBot showing your request.](#)
 - [06 - After an AWS steward approves or denies the request, you will receive an email from Sailpoint.](#)
- [Verifying Access Using IAMbot](#)

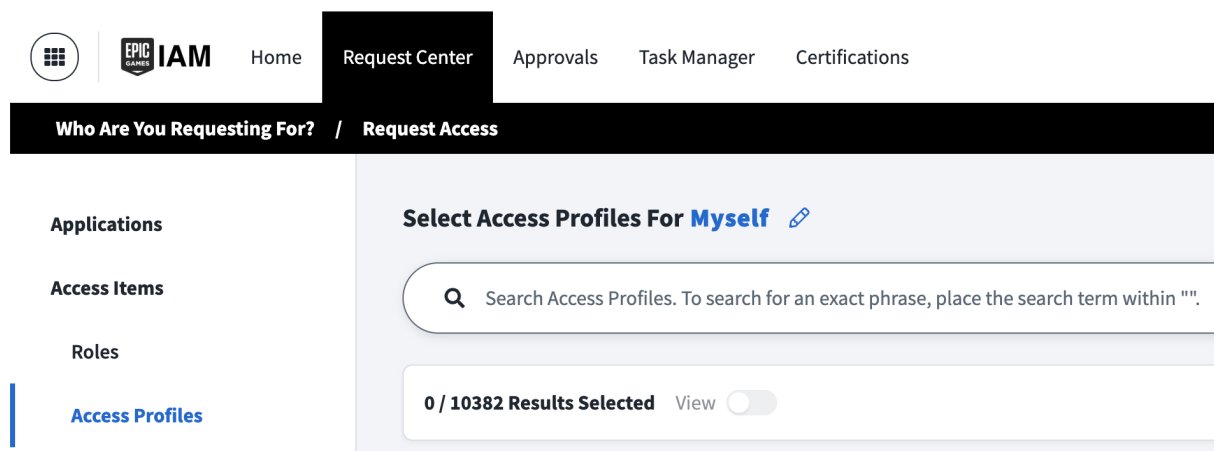
Introduction

If you need to request access to an existing Substrate account for an individual, or if you lost access to a Substrate account, access to Substrate infrastructure is managed by *Okta groups*. If you are a new team member, you can use [SailPoint](#) to request access to your team's Substrate accounts using the *AWS SSO* access profiles. If you requested new Substrate infrastructure, you should have received the role name(s) when the request was completed. If you need access to a K8s cluster in a Substrate account, you also need to request access to the cluster using the *K8S SSO* access profiles in [Sailpoint](#).

Note: These are considered one off requests for individuals in instances where you need access to an AWS SSO account or K8s cluster but it does not need to be added to the Job Role of an entire team. If you request access using AWS SSO, a new tile will appear in Okta as shown in Step 06 below. However, if the request is made via the K8S SSO, a new tile will not appear in Okta. In order to access both the Substrate AWS Account and the K8s Cluster within the account, you must request access to both. Meaning you have to request AWS SSO access and K8S SSO access. If you have only requested AWS SSO access to an account you will not be able to access the K8s cluster within the account until you have requested access to the specific cluster.

Steps for Requesting Access to Substrate Account

01 - Navigate to the [SailPoint Request Center](#), and click on the *Access Profiles* on the left.



02 - Type AWS and the Substrate account name on the search bar. You can also search for your Substrate account using the account number.

The screenshot displays the IAM Request Center interface. The top navigation bar includes the Epic Games logo, the IAM logo, and links to Home, Request Center (which is highlighted), Approvals, Task Manager, and Certifications. Below the navigation bar, a black header reads "Who Are You Requesting For? / Request Access". The left sidebar contains a list of options: Applications, Access Items, Roles, Access Profiles (which is highlighted with a blue bar), and My Requests (with a count of 34). The main content area is titled "Select Access Profiles For **Myself**". It features a search bar with the text "aws dead-dev". Below the search bar, it shows "0 / 22 Results Selected" and a "View" toggle switch. A single result is displayed: "AWS-SSO dead-dev devops [358323286340]". This result includes the text "Grants Access To: AWS SSO", "Access Profile : Grants devops to dead-dev [358323286340]", and "Source: Okta".

All AWS access profiles are named as *AWS-SSO account-name role [account-number]*. You may use this to narrow down the search results.

03 - Select the access profile / role you would like to request.

Select the access profile by clicking **Select** on the right side of the access profile. Add a comment describing the reason for the request and click **Save**.

Leave a comment



Add Comments *

Why is this access needed?

Cancel

Save



04 - Review and submit the request, click on Review Request and then Submit Request

Review Your Request



You are requesting 1 item for yourself

Submit Request 1

AWS-SSO dead-dev infra-support [358323286340]

Details

Grants Access To: AWS SSO

Access Profile: Grants infra-support to dead-dev [358323286340]

1 Comment Set Expiration Remove

1 Identity

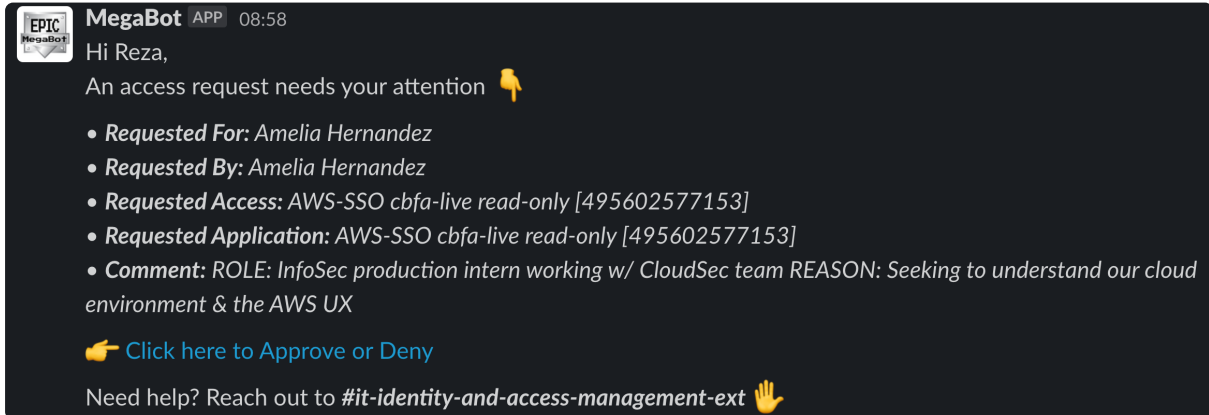
Sarhel Makarau

Select Identities

Rows per page 50 1 - 1 of 1

Page 1 of 1

05 - Once the request is submitted, the AWS account stewards will receive a DM from *MegaBot* showing your request.



The screenshot shows a direct message from 'MegaBot' (labeled as an APP) at 08:58. The message starts with 'Hi Reza,' followed by 'An access request needs your attention' with a pointing hand emoji. A bulleted list contains the following details: 'Requested For: Amelia Hernandez', 'Requested By: Amelia Hernandez', 'Requested Access: AWS-SSO cbfa-live read-only [495602577153]', 'Requested Application: AWS-SSO cbfa-live read-only [495602577153]', and 'Comment: ROLE: InfoSec production intern working w/ CloudSec team REASON: Seeking to understand our cloud environment & the AWS UX'. Below the list is a link 'Click here to Approve or Deny' with a pointing hand emoji. At the bottom, it says 'Need help? Reach out to #it-identity-and-access-management-ext' with a hand emoji.

MegaBot APP 08:58

Hi Reza,

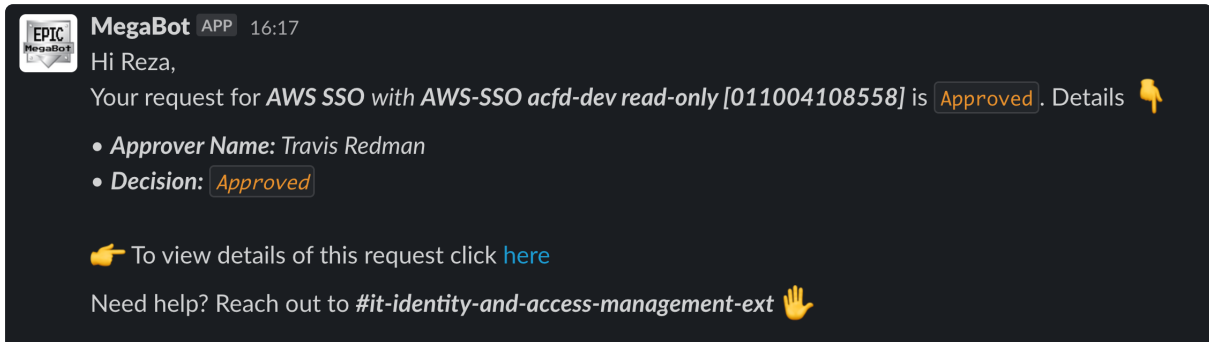
An access request needs your attention 📌

- **Requested For:** Amelia Hernandez
- **Requested By:** Amelia Hernandez
- **Requested Access:** AWS-SSO cbfa-live read-only [495602577153]
- **Requested Application:** AWS-SSO cbfa-live read-only [495602577153]
- **Comment:** ROLE: InfoSec production intern working w/ CloudSec team REASON: Seeking to understand our cloud environment & the AWS UX

👉 [Click here to Approve or Deny](#)

Need help? Reach out to #it-identity-and-access-management-ext 🙋

06 - After an AWS steward approves or denies the request, you will receive a DM from *Megabot*.



The screenshot shows a direct message from 'MegaBot' (labeled as an APP) at 16:17. The message starts with 'Hi Reza,' followed by 'Your request for AWS SSO with AWS-SSO acfd-dev read-only [011004108558] is Approved.' with a 'Details' link and a pointing hand emoji. A bulleted list contains: 'Approver Name: Travis Redman' and 'Decision: Approved'. Below the list is a link 'To view details of this request click here' with a pointing hand emoji. At the bottom, it says 'Need help? Reach out to #it-identity-and-access-management-ext' with a hand emoji.

MegaBot APP 16:17

Hi Reza,

Your request for AWS SSO with AWS-SSO acfd-dev read-only [011004108558] is **Approved**. Details 📌

- **Approver Name:** Travis Redman
- **Decision:** **Approved**

👉 To view details of this request click [here](#)

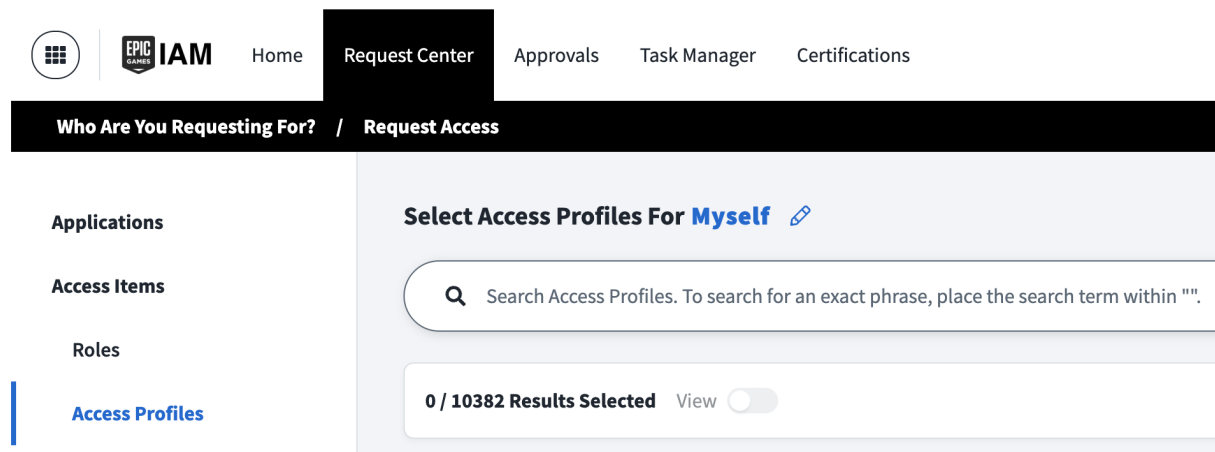
Need help? Reach out to #it-identity-and-access-management-ext 🙋

07 - Shortly after your access is approved, you should see the AWS SSO tile in Okta. This should happen within 10 minutes of approval.

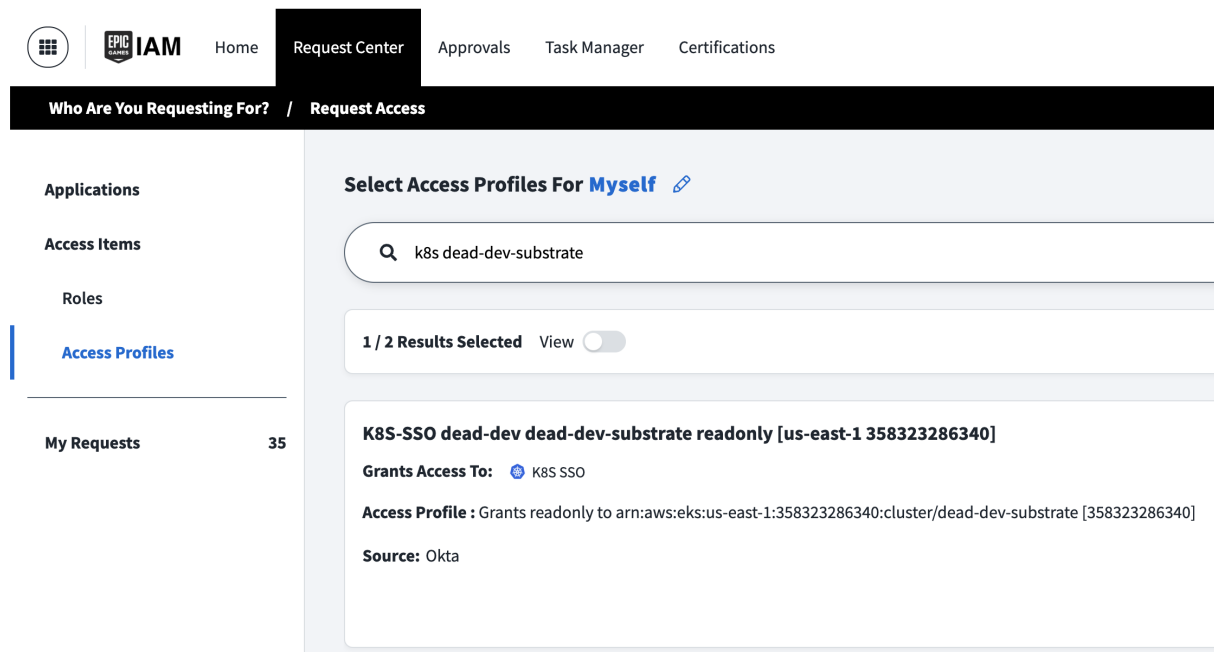
Note: If you have been granted a new role, you need to click the Okta tile for the role to be visible in the UI.

Steps for Requesting Access to Kubernetes Cluster in a Substrate Account

01 - Navigate to the [SailPoint Request Center](#), and click on the *Access Profiles* on the left.



02 - Type *K8S* and the Kubernetes cluster name on the search bar.



The screenshot shows the AWS IAM console interface. The top navigation bar includes 'Home', 'Request Center', 'Approvals', 'Task Manager', and 'Certifications'. The 'Request Center' tab is active. Below the navigation bar, the breadcrumb 'Who Are You Requesting For? / Request Access' is displayed. The left sidebar contains a list of options: 'Applications', 'Access Items', 'Roles', 'Access Profiles' (highlighted with a blue bar), and 'My Requests' (with a count of 35). The main content area is titled 'Select Access Profiles For **Myself**'. It features a search bar with the text 'k8s dead-dev-substrate'. Below the search bar, it indicates '1 / 2 Results Selected' and a 'View' toggle. A single result is shown in a card format: 'K8S-SSO dead-dev dead-dev-substrate readonly [us-east-1 358323286340]'. The card details include 'Grants Access To: K8S SSO', 'Access Profile : Grants readonly to arn:aws:eks:us-east-1:358323286340:cluster/dead-dev-substrate [358323286340]', and 'Source: Okta'.

All K8s access profiles are named as *K8S-SSO account-name cluster-name role [region account-number]*. You may use this to narrow down the search results.

03 - Select the access profile / role you would like to request.

Select the access profile by clicking **Select** on the right side of the access profile. Add a comment describing the reason for the request and click **Save**.

Leave a comment



Add Comments *

Why is this access needed?

Cancel

Save



04 - Review and submit the request, click on *Review Request* and then *Submit Request*

Review Your Request



You are requesting 1 item for yourself

Submit Request 1

K8S-SSO dead-dev dead-dev-substrate user [us-east-1 358323286340]

[Details](#)

Grants Access To: K8S SSO

Access Profile : Grants user to arn:aws:eks:us-east-1:358323286340:cluster/dead-dev-substrate [358323286340]

1 Comment

Set Expiration

[Remove](#)

1 Identity

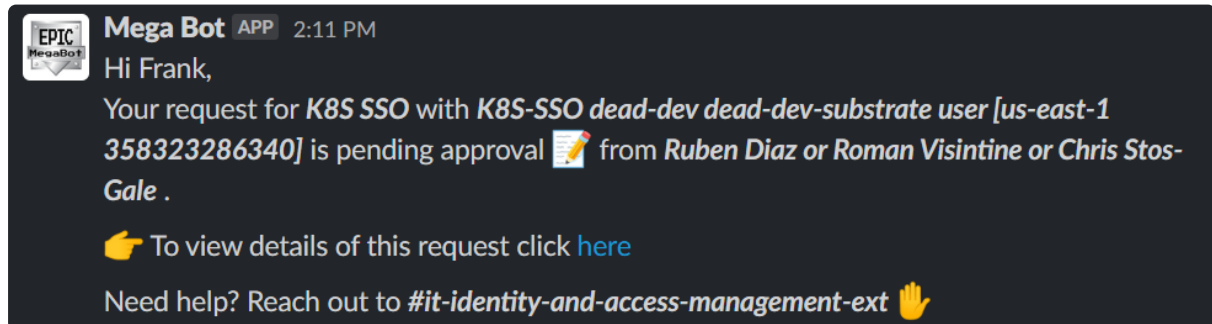
Starhei Makarau

[Select Identities](#)

Rows per page 50 1 - 1 of 1

Page of 1

05 - Once the request is submitted, the AWS account stewards will receive a DM from *MegaBot* showing your request.



06 - After an AWS steward approves or denies the request, you will receive an email from Sailpoint.

Verifying Access Using IAMbot

After you have submitted a request, you will likely want to verify you indeed have the access profiles that you requested. A quick way to verify your access is to use [IAMBot](#) in Slack. To use IAMBot to see a list of access profiles you have, do the following:

1. Open Slack
2. Click on your own name under **Direct messages**.
3. Type `/okta-groups @Your_Name`
4. Press **Enter**

5. You will be presented with a list of all of your Okta groups.

1. AWS SSO Okta profiles will be in the format **aws-sso|**
<account_number>|<aws_profile_name> (example: aws-
sso|244820892670|substrate-labs-user)
2. K8s SSO Okta profiles will be in the format **k8s-sso|**
aws:eks:<region>:<account>:cluster/<cluster_name>|
<profile_name> (example: k8s-sso|arn:aws:eks:us-
east-1:358323286340:cluster/dead-dev-substrate|user)

Page Information:

Page ID: 81068708

Space: Cloud Developer Platform

Downloaded: 2025-07-12 04:06:30