Substrate Access

Document Level Classification

100

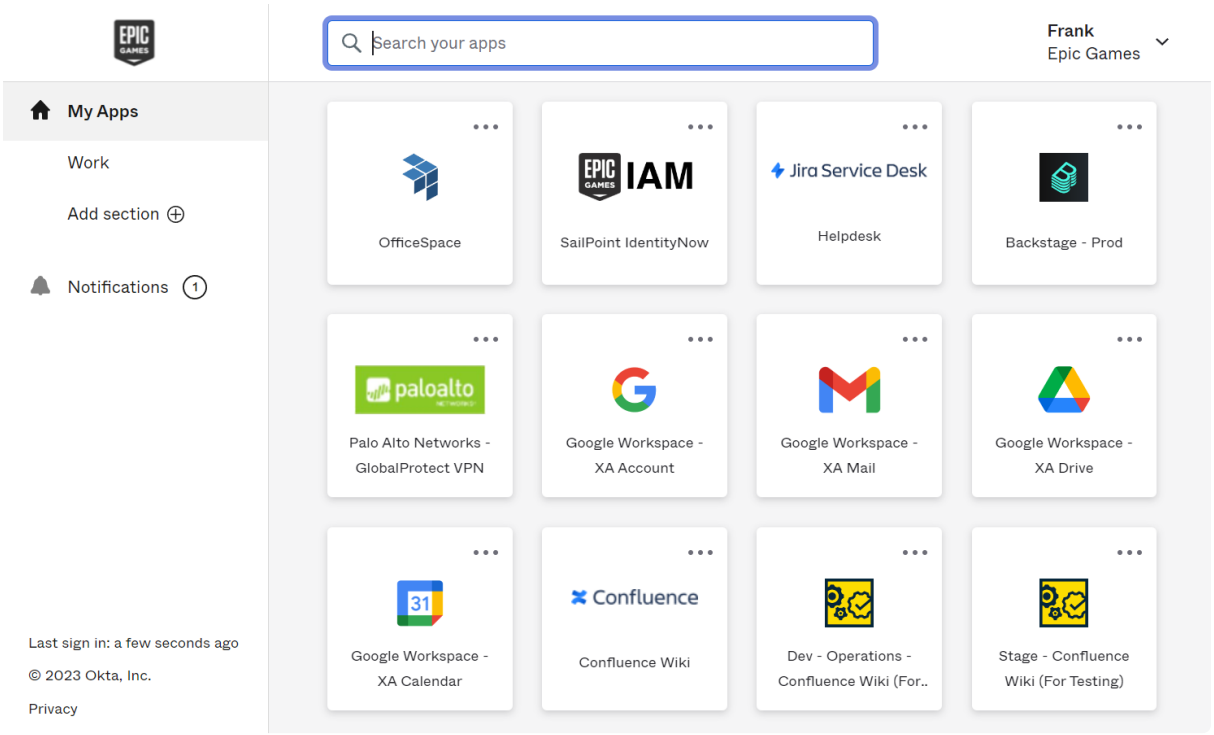
Introduction

As a developer at Epic games using Substrate, you will require access to many systems to perform your day to day tasks. At times it may be a challenge trying to figure out what system you need to use to request access to these systems. This document will cover the systems and or

mechanisms you will interact with when you run into a challenge with system access.

Okta

Okta is cloud-based identity and access management software that helps companies manage and secure user authentication for applications, web services, and devices. For the developer, Okta is where all of the applications you have access to reside. It provides a dashboard with applications represented as clickable tiles. This will also be the first system you will interact with when logging in at Epic and will authenticate with daily. When you log into the Okta Dashboard, you will see all of the applications you have access to. Below is screenshot of the Okta Dashboard.



Okta Support Documentation

Support documentation for Okta can be access in the IT Service Center space in Confluence at Okta Support.

SailPoint IdentityNow

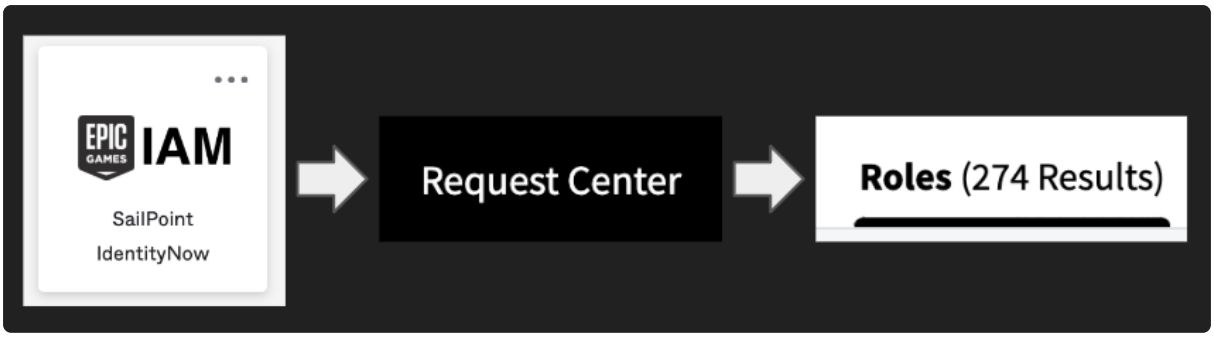
SailPoint IdentityNow is an Identity Governance platform that securely manages user identities and access to applications. In a nutshell, SailPoint is where you request access to various systems. Entry to SailPoint can be found in your Okta Dashboard as illustrated in the screenshot above, by clicking on the **EPIC IAM SailPoint IdentityNow** tile. SailPoint is also integrated with Okta, so when a request is submitted for a system in SailPoint and subsequently approved, the application's tile will show up in the dashboard. Examples of these tiles can also be seen in the screenshot in the Okta section above.

SailPoint Job Roles

SailPoint Job Roles are a collection of Access Profiles. When job roles are requested and subsequently applied to your user profile in SailPoint, they should provide you with all of the access needed to perform the day to day tasks based on your job. For example, if you requested the role called **Cloud Engineering FTE- Engineer**, this would profile you with all the access required for that job. If you are unsure of what Job Role you need speak to your lead or engineering manager.

How to Request a SailPoint Job Role

1. Ask your lead or engineering manager what Role you need.
2. Click on the SailPoint tile in the Okta Dashboard.
3. Click **Request Center** and then **Roles.**
4. Search for the Role using the **Search Roles** field and click **Request.**
5. A dialog titled **Requesting For** will appear.
    1. If it is for you own ID select **Myself**.
    2. If you are requesting for another engineer select **Others** and specify the name or email address.
6. Click **Submit.**
7. MegaBot will keep you updated in Slack.

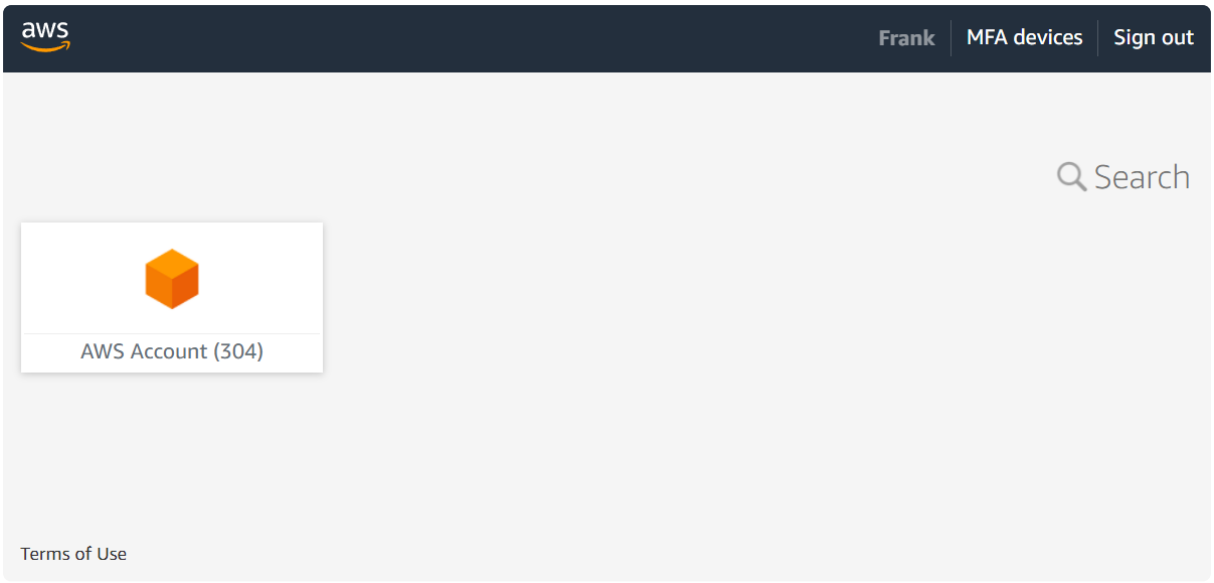


SailPoint Support Documentation

Support documentation for SailPoint IdentityNow can be accessed in the IT Service Center space in Confluence at SailPoint IdentityNow Support.

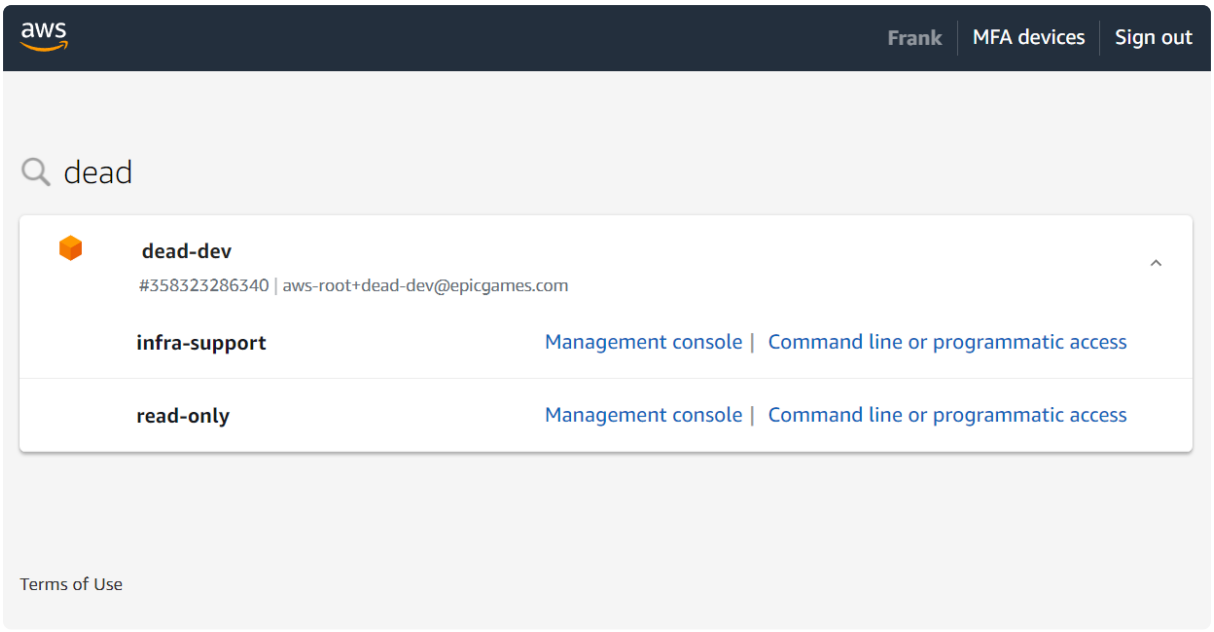
AWS SSO and IAM Roles

AWS SSO is the Identity and Access Management system for AWS. It is the mechanism used to authenticate with AWS. If you already have a Job Role applied to your user ID in SailPoint, you may already have noticed the AWS SSO tile in your Okta Dashboard. If you do have this in your dashboard, clicking on this tile will bring you to the AWS SSO dashboard. In the dashboard you will see a tile called **AWS Account (#)**, where the # represents the number of AWS accounts you have access to. Clicking on the tile will show you all of the AWS accounts you have access to and expanding the selection for the account will show you which IAM roles you can assume when accessing the account.



IAM Roles

When you select an account in the AWS SSO dashboard and expand the selection, you may notice a few different sub sections such as **infra-suppor**t, **read-only**, or **devops**. These represent IAM roles that you can assume when accessing the account. Most likely the role you will select if you are an engineer would be the **devops** role. Clicking on Management console will open the account and assume the role based on which entry you clicked. For example if you clicked the read-only role's Management console link, you will only have read only permissions to the account. If you clicked **devops** you would assume the permissions of the **devops** role.



From the AWS SSO dashboard you would most likely be interested in using the Management console link as accessing AWS from the command line or via programmatic access is covered in Accessing Substrate Infrastructure Using a Terminal Session(CLI).

Requesting Access to Substrate Accounts and Kubernetes Clusters

There are 2 ways of going about requesting access to a Substrate Account or Kubernetes Cluster.

1. Requesting access for a team by having permissions added to the SailPoint Job Role. This pattern can be handled by following the instructions in Requesting Access to a Substrate Account and or Clusters For Teams.
2. Requesting one off access for an individual who does not have access to a Substrate Account or Kubernetes cluster. This pattern can be handled by following the instructions in Requesting Access to a Substrate Account and or Cluster For Individuals.

K8s SSO

While AWS SSO is the authentication mechanism used to authenticate with AWS, K8s SSO is the authentication mechanism used to authenticate with the EKS Kubernetes clusters within substrate accounts. The 2 patterns for requesting access are the same as requesting AWS SSO access and can be requested by following 1 of the 2 patterns below. Also similar to AWS SSO, the access roles that a Substrate developer would most likely be using would be a **devops** role.

1. Requesting access for a team by having permissions added to the SailPoint Job Role. This pattern can be handled by following the instructions in Requesting Access to a Substrate Account and or Clusters For Teams.
2. Requesting one off access for an individual who does not have access to a Substrate Account or Kubernetes cluster. This pattern can be handled by following the instructions in Requesting Access to a Substrate Account and or Cluster For Individuals.

Network Access

From time to time you may encounter issues with not being able to access a resource, application, or system over the Epic network or while connected to VPN. For example, you have been granted access to a specific application and you can see that application in your Okta Dashboard. You click on the application tile but you are unable to get to the application in your browser and receive a timeout. This may be related to not having the correct network access profile as part of the SailPoint Job Role applied to your user ID. In these cases it may be necessary to have a network access profile assigned to you. These scenarios may be tricky and you cannot request individual Access Roles or Entitlements that are bundled with them. In these cases you should contact the #cloud-ops-support-ext to identify what network access you need and contact the IT Help Desk to assist in getting that applied to your user ID.

- Requesting Access to a Substrate Account and or Clusters For Teams
- Requesting Access to a Substrate Account and or Cluster For Individuals
- Substrate AWS Account Stewards
- TONUAM Groups
