Cognito user pool configuration

The TEAM Cognito user pool configuration needs to be updated to complete the deployment process and make the TEAM application accessible via the AWS IAM Identity Center sign-in portal.

Update configuration parameters

- Create a new file named **details.json** in the **deployment** directory.
- Copy the contents of the file **details-template.json** to the new file.
- Replace the **MetadataURL** in the **details.json** file with the value of **AWS IAM Identity Center SAML metadata file URL** copied from the previous section.

For example:

```
{
    "MetadataURL": "https://portal.sso.us-east-1.amazonaws.com/saml/metadata/ODQzNTUxMTgwNTcyX2lucy0
}
```

Run Cognito configuration script

The **cognito.sh** bash script in the **deployment** folder performs the following actions within the **TEAM_ACCOUNT**:

- Configures AWS IAM Identity Center as a SAML provider for the TEAM Cognito user pool
- Updates the TEAM application client configuration to make use of the configured AWS IAM Identity Center SAML provider

> **IMPORTANT**
>
> Ensure that the named profile for the **TEAM Deployment account** has sufficient permissions before executing the **cognito.sh** script

Execute the following command in the root directory to deploy the script

```
cd deployment
```

```
./cognito.sh
```

The **cognito.sh** script should be deployed successfully without any errors.

The application deployment, configuration and integration is now complete! The users can log into the TEAM application via the Identity Center access portal, as shown below.

0:00 / 0:14

The TEAM administrators can now configure your organization-specific policies and settings for requesting and granting elevated access.

🚀 Next Step: Set up Eligibility & Approval Policies to start using TEAM.