SSO integration using AWS Cognito

🗎 360 Palwinder Singh April 12, 2023 Blog 5231 0

AWS Cognito is a managed authentication and authorization service that provides seamless **Single Sign-On (SSO)** integration for your web and mobile applications. Here's a high-level overview of setting up SSO integration using **AWS Cognito**:

1. Create an AWS Cognito user pool:

Sign in to the AWS Management Console, navigate to the Cognito dashboard, and click on "Manage User Pools."
Click "Create a user pool," provide a name, and click "Review defaults" or "Step through settings" to configure the user pool settings based on your requirements.
In the "App clients" section, create a new app client, provide a name, and configure the settings as needed.

2. Set up identity providers (optional):

If you want to use external identity providers (e.g., Google, Facebook, or an enterprise SSO provider), navigate to the "Identity providers" section in your user pool settings and configure the providers you want to use.

3. Configure an Amazon Cognito domain (or use your custom domain):

In the "Domain name" section of your user pool settings, either choose an Amazon Cognito domain or set up your custom domain.

4. Configure the Cognito User Pool as an OAuth2.0/OpenID Connect provider:

In the "App integration" section, click "App client settings."
Select the app client you created earlier, enable the identity providers you want to use, and configure the callback URLs for your application.
Select the allowed OAuth2.0 flows and scopes, and click "Save changes."

5. Implement Cognito in your application:

Install the appropriate AWS SDK or Cognito SDK for your application's programming language or framework (e.g., AWS Amplify for JavaScript-based applications).
Configure your application to use the Cognito User Pool, App Client, and Identity Providers you set up earlier.
Implement sign-in, sign-up, and other user authentication and management features in your application using the SDK.

6. Secure your application using AWS Cognito:

After successful authentication, AWS Cognito will return an ID token, an access token, and a refresh token.
Use the ID token to get user information and the access token to authorize access to your application's resources.
Secure your backend services (e.g., AWS API Gateway, AWS Lambda) using AWS Cognito Authorizers or other mechanisms to ensure that only authenticated users can access your resources.

With these steps, you can integrate AWS Cognito into your application and provide seamless SSO capabilities. Note that the specific implementation details may vary depending on your application's programming language, framework, and architecture.

Online URL: https://www.phpkb.com/kb/article/sso-integration-using-aws-cognito-360.html