**AWS SAML Single Sign-On (SSO) with Okta**

**Overview**

This guide provides a step-by-step approach to configuring AWS SAML-based Single Sign-On (SSO) using Okta as the Identity Provider (IdP).

**Prerequisites**

* An **Okta Administrator** account.
* Access to the **AWS IAM Console**.
* A **valid AWS IAM Role** for federated access.

**Step 1: Configure Okta as the Identity Provider (IdP)**

**1.1 Create an AWS SAML Application in Okta**

1. Log in to your **Okta Admin Console**.
2. Go to **Applications > Applications**.
3. Click **Create App Integration**.
4. Select **SAML 2.0** and click **Next**.
5. Enter the following details:
   * **App Name**: AWS SSO
   * **App Logo (Optional)**
   * Click **Next**.

**1.2 Configure SAML Settings in Okta**

1. **Single Sign-On URL**: https://signin.aws.amazon.com/saml
2. **Audience URI (SP Entity ID)**: urn:amazon:webservices
3. **Name ID format**: EmailAddress
4. **Application Username**: Okta Username
5. Click **Next** > **Finish**.

**1.3 Assign Users to the Application**

1. Open your AWS SAML application in Okta.
2. Go to **Assignments** > **Assign to People/Groups**.
3. Select users who should have SSO access.
4. Click **Save**.

**1.4 Retrieve IdP Metadata**

1. Navigate to **Sign On** tab.
2. In the **SAML 2.0** section, click **Identity Provider Metadata**.
3. Download and save the XML file. (You will use this in AWS IAM setup.)

**Step 2: Configure AWS IAM for SAML Authentication**

**2.1 Create a SAML Identity Provider in AWS**

1. Log in to the **AWS Management Console**.
2. Navigate to **IAM > Identity Providers**.
3. Click **Add Provider**.
4. Select **Provider Type**: SAML.
5. **Provider Name**: OktaIdP.
6. **Metadata Document**: Upload the metadata XML file downloaded from Okta.
7. Click **Create Provider**.

**2.2 Create an IAM Role for SAML Access**

1. Navigate to **IAM > Roles**.
2. Click **Create Role**.
3. Select **SAML 2.0 federation** as the trusted entity.
4. Choose the Okta IdP created earlier.
5. Select **Allow programmatic and AWS Management Console access**.
6. Attach necessary permissions (e.g., **AdministratorAccess** or **ReadOnlyAccess**).
7. Name the role (e.g., AWS-Okta-SAML-Role) and click **Create Role**.

**Step 3: Configure Attribute Statements in Okta**

1. Open your AWS SAML application in Okta.
2. Go to **Sign On** > **Edit SAML Attributes**.
3. Add the following attributes:
   * **Role**: https://aws.amazon.com/SAML/Attributes/Role  
     Value: arn:aws:iam::AWS-ACCOUNT-ID:role/ROLE-NAME,arn:aws:iam::AWS-ACCOUNT-ID:saml-provider/OktaIdP
   * **RoleSessionName**: https://aws.amazon.com/SAML/Attributes/RoleSessionName  
     Value: user.email
   * **SessionDuration (Optional)**: https://aws.amazon.com/SAML/Attributes/SessionDuration Value: 3600 (1 hour)
4. Click **Save**.

**Step 4: Test the SSO Login**

1. Go to the Okta User Dashboard (https://your-okta-domain.okta.com).
2. Click on the **AWS SAML Application**.
3. You should be redirected to AWS without needing to enter credentials.

**Step 5: Troubleshooting**

**5.1 404 Page Not Found Error**

* Ensure that the **SSO URL is correct** in Okta (https://signin.aws.amazon.com/saml).
* Verify that the **SAML application in Okta is assigned to users**.
* Make sure the **IAM Role and Identity Provider exist in AWS**.

**5.2 Access Denied in AWS**

* Check if the user has been assigned the **correct IAM Role**.
* Ensure that the role’s **trust policy includes the correct SAML provider**.

**Conclusion**

You have now successfully configured **AWS SAML SSO with Okta**. Users can log in to AWS securely without entering credentials manually, improving security and access control.

For advanced configurations, refer to the AWS and Okta documentation.