Single Sign-On Integration Guide

Overview

AI Monitor supports federated authentication via SAML 2.0 and OpenID Connect (OIDC) identity providers. Users authenticate through your corporate identity provider (Okta, Azure AD, Google Workspace, etc.) and are automatically provisioned in Cognito on first login (Just-In-Time provisioning).

Prerequisites

- A deployed AI Monitor stack with Cognito authentication
- AWS CLI configured with appropriate permissions
- The sso.cmd (Windows) or sso.sh (Linux/Mac) script
- Administrator access to your identity provider

Quick Start

Step 1: Get your Cognito configuration

```
sso.cmd <stack-name> info
```

This displays:

- Pool ID – your Cognito User Pool identifier
- Client ID – the app client ID
- Domain – the Cognito hosted UI domain
- ACS URL – SAML Assertion Consumer Service URL
- Entity ID – SAML Service Provider Entity ID
- Redirect URI – OIDC callback URL

Step 2: Configure your identity provider

Provide your IdP with the values from Step 1. See provider-specific sections below.

Step 3: Register the IdP with AI Monitor

For SAML:

```
sso.cmd <stack-name> setup-saml <provider-name> <metadata-url>
```

For OIDC:

```
sso.cmd <stack-name> setup-oidc <provider-name> <issuer> <client-id> <client-secret>
```

Step 4: Test

Navigate to your editor URL. The Cognito login page should show your IdP as a sign-in option.

Okta SAML Setup

In Okta Admin Console:

1. Applications → Create App Integration → SAML 2.0
2. General Settings: enter app name (e.g. "AI Monitor")
3. SAML Settings:
   - Single sign-on URL: <your ACS URL from sso info>
   - Audience URI (SP Entity ID): <your Entity ID from sso info>
   - Name ID format: EmailAddress
   - Application username: Email
4. Assignments tab: Assign users or groups to the app
5. Sign On tab: Copy the "Identity Provider metadata" URL

Then run:

```
sso.cmd AIMonitor setup-saml Okta https://dev-xxx.okta.com/app/yyy/sso/saml/metadata
```

Azure AD (Entra ID) SAML Setup

In Azure Portal:

1. Azure Active Directory → Enterprise Applications → New Application → Create your own
2. Single sign-on → SAML
3. Basic SAML Configuration:
   - Identifier (Entity ID): <your Entity ID from sso info>
   - Reply URL (ACS URL): <your ACS URL from sso info>
4. User Attributes & Claims: Ensure email is mapped
5. Copy the "App Federation Metadata Url"

Then run:

```
sso.cmd AIMonitor setup-saml AzureAD
https://login.microsoftonline.com/<tenant>/federationmetadata/2007-
06/federationmetadata.xml?appid=<app-id>
```

OIDC Setup (Generic)

For OIDC providers (Google Workspace, Auth0, etc.):

1. Create an OAuth/OIDC application in your IdP
2. Set the redirect URI to: <your Redirect URI from sso info>
3. Note the issuer URL, client ID, and client secret

Then run:

```
sso.cmd AIMonitor setup-oidc <name> <issuer-url> <client-id> <client-secret>
```

User Management with SSO

Federated usernames

When a user signs in via SSO for the first time, Cognito creates a federated user with the username format:

```
<ProviderName>_<email>
```

For example: Okta_john@company.com

Assigning groups/roles (RBAC)

To assign roles to federated users, use the federated username:

```
groups.cmd <stack> add-to-group Okta_john@company.com admin
groups.cmd <stack> add-to-group Okta_jane@company.com viewer
```

To find a federated user's exact username:

```
aws cognito-idp list-users --user-pool-id <pool-id> --filter "email = \"john@company.com\"" --query "Users[*].Username" --output text
```

Important: The federated user (Okta_john@company.com) and a native Cognito user (john@company.com) are separate identities. Group membership must be assigned to the federated username.

Just-In-Time (JIT) Provisioning

JIT provisioning is enabled by default. When a user authenticates via SSO for the first time:

- Cognito automatically creates the user account
- Email attribute is mapped from the SAML/OIDC assertion
- No pre-provisioning required in Cognito
- User must be assigned to the app in the IdP

Sign-In Flows

SP-Initiated (most common):

1. User navigates to the editor URL
2. ALB redirects to Cognito hosted UI
3. User clicks the IdP button (e.g. "Okta")
4. Redirected to IdP for authentication
5. IdP sends SAML assertion back to Cognito
6. Cognito issues tokens, redirects to editor

IdP-Initiated:

1. User signs into the IdP portal (e.g. Okta dashboard)
2. User clicks the AI Monitor app tile
3. IdP sends SAML assertion directly to Cognito ACS URL
4. Cognito issues tokens, redirects to editor

Managing Providers

List configured providers:

```
sso.cmd <stack> list
```

Remove a provider:

```
sso.cmd <stack> remove <provider-name>
```

This removes the IdP and reverts the app client to Cognito-only authentication. Existing native Cognito users can still sign in with their email/password.

Show configuration info:

```
sso.cmd <stack> info
```

Switching Back to Cognito-Only

To disable SSO and revert to Cognito email/password only:

```
sso.cmd <stack> remove <provider-name>
```

Existing Cognito users retain their passwords. Federated-only users (created via JIT) will need a password set via:

```
users.cmd <stack> reset-password <email>
```

Troubleshooting

"Unable to sign in" (on Okta side)

- User not assigned to the app in Okta. Go to Assignments tab and assign the user.
- Check Okta System Log (Reports → System Log) for detailed error.

User shows as viewer despite being in admin group

The group was assigned to the native Cognito username (email), not the federated username (Okta_email). Reassign using the federated username:

```
groups.cmd <stack> add-to-group Okta_user@domain.com admin
```

Supported Identity Providers

Any SAML 2.0 or OIDC-compliant provider, including:

- Okta
- Azure AD / Microsoft Entra ID
- Google Workspace
- OneLogin
- PingFederate
- Auth0
- AWS IAM Identity Center (successor to AWS SSO)
- Any SAML 2.0 or OIDC compliant provider

Security Notes

- SAML assertions are validated by Cognito – only trusted IdPs can authenticate users
- All communication uses HTTPS/TLS
- Federated users cannot set a Cognito password (they always authenticate via IdP)
- Removing an IdP immediately prevents SSO login via that provider
- Native Cognito users are unaffected by IdP changes
- Session timeout is configurable on the ALB listener (default: 7 days)