AI SIEM — SSO Configuration Guide

Version: 26h4c | **Product:** AI SIEM | Perfware.cloud

This guide covers configuring Single Sign-On (SSO) for the AI SIEM Editor UI using SAML 2.0 with Okta, Azure AD, or other SAML identity providers.

1. Prerequisites

- AI SIEM deployed at Enterprise tier (SSO is enterprise-only)
- Access to your identity provider admin console (Okta, Azure AD, etc.)
- AI SIEM's Cognito User Pool ID and domain, from the stack's CloudFormation outputs (CognitoUserPoolId and the editor URL). These identify AI SIEM's OWN pool.

2. Cognito Federation Setup

AI SIEM runs its OWN Cognito User Pool (created by the AI SIEM stack); it does not use Log Processor's. SSO is configured on AI SIEM's pool, identified by the CognitoUserPoolId stack output. Configuring SSO on Log Processor does NOT apply to AI SIEM.

Use the sso helper script (scripts/sso.cmd or sso.sh) to register a SAML or OIDC provider on AI SIEM's pool, or configure it in the Cognito console against that pool. Then follow the provider-specific steps below.

3. Okta Configuration

3.1 Create SAML Application in Okta

- Log in to Okta Admin Console
- Navigate to Applications > Create App Integration
- Select SAML 2.0
- App name: Perfware Cloud (or your preferred name)

3.2 SAML Settings

- Single Sign-On URL: https://<cognito-domain>.auth.<region>.amazoncognito.com/saml2/idpresponse
- Audience URI (SP Entity ID): urn:amazon:cognito:sp:<user-pool-id>
- Name ID format: EmailAddress
- Attribute Statements: email -> user.email

3.3 Cognito Identity Provider

- In AWS Console > Cognito > User Pools > Federation > Identity Providers
- Add SAML provider, upload Okta metadata XML
- Map attributes: email -> email

AI SIEM — SSO Configuration Guide

Version: 26h4c | **Product:** AI SIEM | Perfware.cloud

This guide covers configuring Single Sign-On (SSO) for the AI SIEM Editor UI using SAML 2.0 with Okta, Azure AD, or other SAML identity providers.

- Enable the provider in App Client settings

4. Azure AD Configuration

4.1 Enterprise Application

- Azure Portal > Enterprise Applications > New Application
- Create non-gallery application: Perfware Cloud
- Single sign-on > SAML

4.2 SAML Configuration

- Identifier: urn:amazon:cognito:sp:<user-pool-id>
- Reply URL: https://<cognito-domain>.auth.<region>.amazoncognito.com/saml2/idpresponse
- User Attributes: email -> user.mail

4.3 Cognito Setup

Same as Okta section 3.3 — add SAML provider using Azure AD federation metadata URL.

AI SIEM — SSO Configuration Guide

Version: 26h4c | **Product:** AI SIEM | Perfware.cloud

This guide covers configuring Single Sign-On (SSO) for the AI SIEM Editor UI using SAML 2.0 with Okta, Azure AD, or other SAML identity providers.

5. RBAC (Role-Based Access Control)

With Enterprise tier, users can be assigned roles via Cognito groups:

- admin — full access (create/edit/delete threats, execute remediation)
- analyst — view threats, acknowledge, generate playbooks (no remediation)
- viewer — read-only access to dashboard and threat list

Create groups in Cognito User Pool and assign users. The editor checks group membership on each request.

6. Troubleshooting

- SAML assertion errors: verify Audience URI matches exactly
- Attribute mapping: ensure email claim is passed correctly
- Redirect loops: check App Client callback URLs include the editor domain
- Group not recognized: ensure Cognito group name is exactly 'admin', 'analyst', or 'viewer'