Okta SSO Configuration Guide

This guide explains how to integrate **AiVRIC** with **Okta** to provide Single Sign-On (SSO) using SAML 2.0 and optional automated user provisioning. It is intended for Okta administrators and security teams responsible for identity and access management.

Purpose

Integrating AiVRIC with Okta enables:

- Centralized authentication through Okta
- Enforcement of existing MFA and sign-on policies
- Simplified user onboarding and offboarding
- Alignment with enterprise identity and zero-trust strategies

Okta acts as the **identity provider (IdP)**, while AiVRIC manages authorization via its internal RBAC model.

Supported Capabilities

AiVRIC supports the following Okta integration features:

- **SAML 2.0 Single Sign-On**
- **Just-In-Time (JIT) user provisioning**
- **Optional SCIM-based provisioning** (if enabled for your tenant)
- **AiVRIC-native role assignment (RBAC)**

Prerequisites

Before beginning, ensure:

- Admin access to the **Okta Admin Console**

- Organization Admin privileges in **AiVRIC**
- Defined user and role access strategy
- Approved SSO rollout plan (test vs production)

SAML SSO Configuration

Step 1: Create a New SAML Application in Okta

1. Log in to the **Okta Admin Console**
2. Navigate to **Applications → Applications**
3. Select **Create App Integration**
4. Choose **SAML 2.0** as the sign-in method
5. Click **Next**

Step 2: Configure SAML Settings

Configure the following fields using values provided by AiVRIC:

- **Single sign on URL (ACS URL):** Provided by AiVRIC
- **Audience URI (SP Entity ID):** Provided by AiVRIC
- **Name ID format:** EmailAddress
- **Application username:** Email

Attribute Statements

Ensure the following attributes are sent:

Name	Value
email	user.email
firstName	user.firstName
lastName	user.lastName

Step 3: Assign Users or Groups

1. In the application settings, navigate to **Assignments**
2. Assign users or Okta groups authorized to access AiVRIC
3. Save changes

Only assigned users will be able to authenticate.

Enable Okta SSO in AiVRIC

1. Sign in to AiVRIC as an administrator
2. Navigate to **Configuration → Integrations → SSO**
3. Select **Okta** as the identity provider
4. Upload the Okta **IdP metadata XML** or provide SSO details manually
5. Verify attribute mappings
6. Enable SSO for the organization

User Provisioning Options

Just-In-Time (JIT) Provisioning (Default)

When JIT is enabled:

- Users are created in AiVRIC upon first successful SSO login
- No advance provisioning is required
- User access is removed when Okta assignment is revoked

This is the recommended provisioning method for most organizations.

SCIM Provisioning (Optional)

If SCIM is enabled in your AiVRIC tenant:

1. Enable SCIM provisioning in AiVRIC
2. Copy the **SCIM endpoint URL** and **access token**
3. In Okta, navigate to **Provisioning → Integration**
4. Configure SCIM settings using AiVRIC values
5. Enable Create, Update, and Deactivate actions as needed

SCIM enables full lifecycle management without requiring user login events.

Role Assignment & RBAC

AiVRIC roles are managed **within the platform** and are independent of Okta group membership.

Best practice:

- Use Okta to control **who can access AiVRIC**
- Use AiVRIC RBAC to control **what users can do**

After provisioning, administrators assign roles such as:

- Organization Admin
- Security Admin
- Analyst
- Viewer (Read-Only)

Security & Policy Controls

Okta security policies apply to AiVRIC logins, including:

- MFA enforcement
- Network zone restrictions
- Device trust policies
- Session duration limits

AiVRIC recommends enforcing MFA for all privileged roles.

Validation & Testing

After configuration:

1. Test SSO with a pilot user
2. Confirm successful login via Okta
3. Validate user provisioning behavior
4. Review authentication logs in Okta

Troubleshooting

Issue	Common Cause
SSO fails	Incorrect ACS URL or Entity ID
User not created	Missing email attribute or JIT disabled
Access denied	User not assigned to Okta app

Audit & Compliance Notes

This integration supports:

- Centralized identity management
- Strong authentication and MFA controls
- Consistent access revocation

Authentication logs in Okta combined with AiVRIC access logs support audit evidence collection.

Summary

Okta SSO integration allows AiVRIC to seamlessly integrate into existing enterprise identity workflows while maintaining clear separation of authentication and authorization.

For advanced configurations or troubleshooting assistance, contact AiVRIC support.