Entra ID (Azure AD) SSO & Provisioning Guide

This guide describes how to integrate **AiVRIC** with **Microsoft Entra ID (formerly Azure Active Directory)** for Single Sign-On (SSO) and optional automated user provisioning. It is intended for identity administrators and security teams responsible for access control and identity governance.

Purpose

Integrating AiVRIC with Entra ID enables:

- Centralized authentication using your existing identity provider
- Consistent enforcement of corporate identity policies (MFA, conditional access)
- Reduced administrative overhead through automated user lifecycle management
- Alignment with zero-trust and least-privilege access models

---

Supported Capabilities

AiVRIC supports the following Entra ID integration features:

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

Entra ID remains the source of authentication, while AiVRIC manages authorization and role-based access.

Prerequisites

Before beginning setup, ensure the following:

- Administrative access to **Microsoft Entra ID**
- Organization Admin or Security Admin role in **AiVRIC**
- Approved SSO rollout plan (production vs pilot)
- Defined role-mapping strategy for AiVRIC users

SAML Single Sign-On Configuration

Step 1: Create an Enterprise Application

1. Sign in to the **Microsoft Entra admin center**
2. Navigate to **Enterprise applications → New application**
3. Select **Create your own application**
4. Name the application (for example, *AiVRIC SSO*)
5. Choose **Integrate any other application you don't find in the gallery (Non-gallery)**

Step 2: Configure SAML Settings

1. Open the newly created application
2. Select **Single sign-on → SAML**
3. Configure the following fields:

- **Identifier (Entity ID):** Provided by AiVRIC
- **Reply URL (Assertion Consumer Service URL):** Provided by AiVRIC
- **Sign-on URL:** Optional (AiVRIC login URL)

4. Ensure the following claims are sent:

Claim	Required
email	Yes
given_name	Recommended
family_name	Recommended
name	Optional

Step 3: Download Metadata

- Download the **Federation Metadata XML** from Entra ID
- Upload this metadata file into AiVRIC under: **Configuration → Integrations → SSO**

Enable SSO in AiVRIC

1. Sign in to AiVRIC as an administrator
2. Navigate to **Configuration → Integrations → SSO**
3. Select **Entra ID / Azure AD**
4. Upload the SAML metadata file
5. Verify attribute mappings
6. Enable SSO for the organization

Once enabled, users will authenticate via Entra ID.

User Provisioning Options

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

When JIT is enabled:

- Users are created in AiVRIC upon first successful SSO login
- No pre-provisioning is required
- Deprovisioning occurs when Entra ID access is removed

This is the recommended approach for most customers.

SCIM Provisioning (Optional)

If SCIM is enabled for your tenant:

- Users and group assignments are synchronized automatically
- Access changes propagate without requiring a login event

Configuration steps:

1. Enable SCIM in AiVRIC
2. Copy the SCIM endpoint and token
3. Configure provisioning in Entra ID
4. Assign users or groups to the application

Role Assignment & RBAC

AiVRIC roles are managed within the platform and are independent of Entra ID roles.

Common practices:

- Use Entra ID for **who can access AiVRIC**
- Use AiVRIC RBAC for **what users can do**

Admins assign roles after initial provisioning:

- Organization Admin
- Security Admin
- Analyst
- Read-Only / Viewer

Conditional Access & Security Controls

Entra ID Conditional Access policies apply to AiVRIC logins, including:

- MFA enforcement
- Device compliance requirements
- IP allow/deny rules
- Risk-based authentication

AiVRIC recommends enforcing MFA for all privileged roles.

Validation & Testing

After configuration:

1. Test SSO using a pilot user
2. Confirm correct role assignment
3. Validate user creation or SCIM sync
4. Review sign-in logs in Entra ID

Troubleshooting

Issue	Common Cause
Login fails	Incorrect Entity ID or Reply URL
User not created	JIT disabled or missing email claim
Access denied	User not assigned to enterprise app

Audit & Compliance Notes

This integration supports requirements for:

- Centralized identity management
- Strong authentication controls
- Access review and revocation

SSO logs from Entra ID and access logs from AiVRIC can be used together to support audits.

Summary

Entra ID integration allows AiVRIC to operate as part of your existing identity and zero-trust architecture, improving security while simplifying access management.

For advanced configurations, SCIM provisioning, or troubleshooting assistance, contact AiVRIC support.