AiVRIC

# Admin & RBAC Guide

## Purpose

This guide explains how administrators are created, how admin access is established, and how **role-based access control (RBAC)** is managed within AiVRIC.

It is intended for **account administrators and security owners** responsible for controlling access, enforcing least-privilege policies, and managing visibility across cloud accounts.

---

## Admin Account Creation

The first user to create an AiVRIC account is automatically assigned **administrative access**.

### Creating the Initial Admin Account

1. Navigate to the **AiVRIC Sign Up** page
2. Click **Sign up**

**Sign Up Using Email and Password**

3. Enter **Name**
4. Enter **Company Name**
5. Enter **Email Address**
6. Create and confirm a **Password**
7. Click **Sign up**

**Optional: Sign Up Using SSO**

- Click **Continue with Google**
- Click **Continue with GitHub**

After authentication, the AiVRIC tenant is automatically created and the user is granted **full admin permissions**.

---

### Initial Admin Sign In

1. Navigate to the **AiVRIC Sign In** page
2. Enter **Email** and **Password**
3. Click **Log in**

**OR**

- Sign in using **Google**, **GitHub**, or **SAML SSO** (if configured)

Once signed in, the admin can begin configuring users, roles, and access controls.

---

## Default Admin Access

The initial admin has full access to:

- User and role management
- Account configuration
- Cloud provider connections
- Integrations
- Scan management
- Full visibility across cloud accounts

It is recommended to designate **at least two administrative users**.

---

## Role Management

### Creating a New Role

1. Navigate to **Configuration → Roles**
2. Click **Add Role**
3. Enter a **Role Name**
4. Select applicable permissions
5. Configure visibility and groups
6. Click **Add Role**

Roles can be edited at any time.

## Admin Permissions

When creating or editing a role, the following permissions are available:

❐ Grant all admin permissions
❐ Invite and Manage Users
❐ Manage Account
❐ Unlimited Visibility
❐ Manage Cloud Providers
❐ Manage Integrations
❐ Manage Scans

### Permission Descriptions

- **Invite and Manage Users**
  Manage invitations, role assignment, and access removal.
- **Manage Account**
  Modify account-level settings.
- **Manage Cloud Providers**
  Add, update, or remove cloud provider connections.
- **Manage Integrations**
  Configure third-party integrations.
- **Manage Scans**
  Create, schedule, and manage scans.
- **Unlimited Visibility**
  Access all cloud accounts and provider groups.

## Groups and Account Visibility

Roles control visibility using **provider groups**.

- Unlimited Visibility = full access
- Group-based selection = scoped access
- No visibility options selected = no access to accounts

This supports environment segmentation (Production, Staging, Non-Prod).

# User Invitation & Onboarding

### Send a User Invitation

1. Navigate to **Organization → Invitations**.
2. Select **Send Invitation**.
3. Enter the user's **Email Address**.
4. Select a **Role** for the user.
5. Select **Send Invitation**.

---

### Review Invitation Details

- Invitations appear in the Invitations table.
- View invitation state (e.g., Pending).
- Review assigned role.
- Invitations display creation time and expiration.

The invited user receives an email with instructions to complete account setup.

---

# SSO and RBAC

AiVRIC supports:

- Google SSO
- GitHub SSO
- SAML SSO

Authentication is handled by the identity provider. Authorization is enforced by AiVRIC RBAC.

---

# Offboarding Users

- Remove or disable users in AiVRIC
- For SSO users, removal from the identity provider also revokes access

---

## RBAC Best Practices

- Follow least-privilege principles
- Limit Unlimited Visibility usage
- Use provider groups for segmentation
- Perform periodic access reviews

---

## Support

For access or RBAC assistance, contact **AiVRIC Support**.