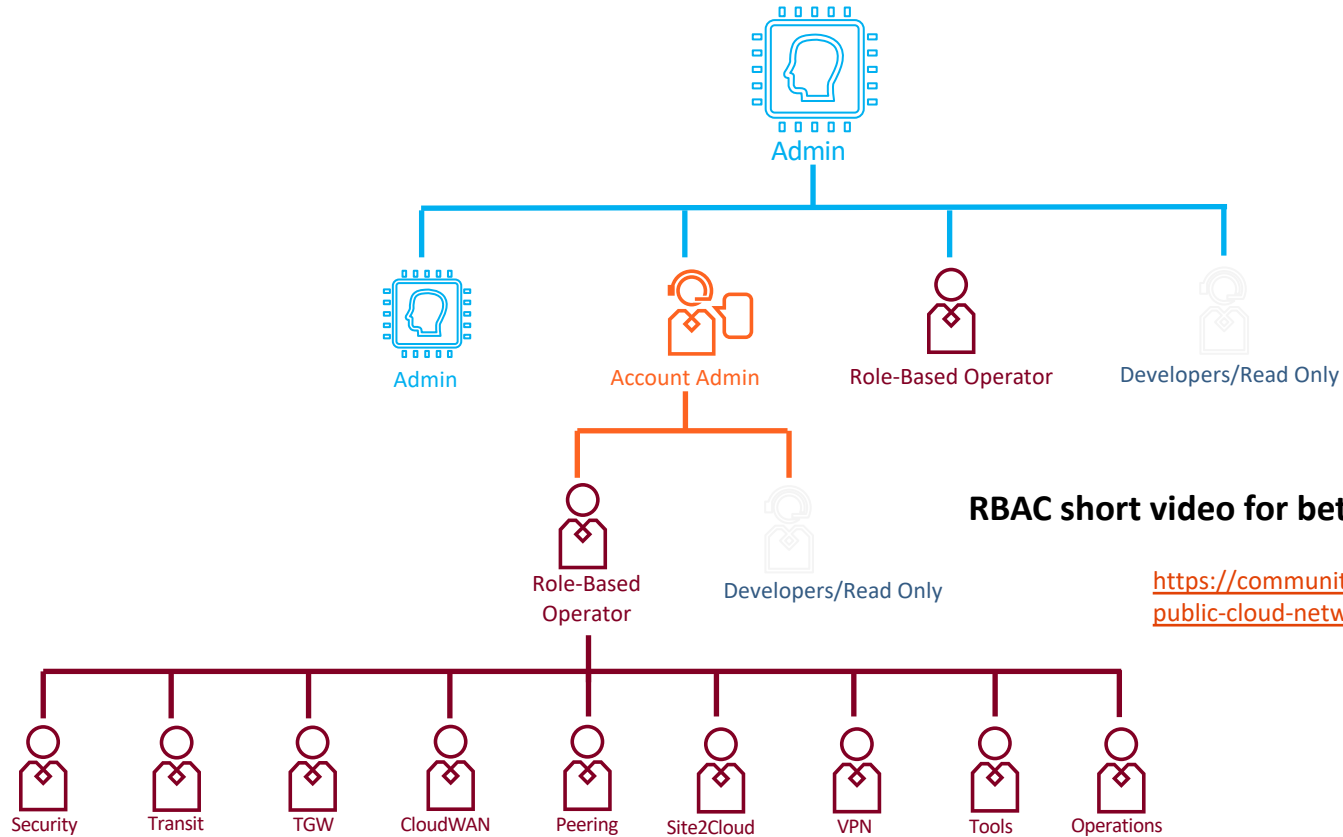




Role-Based Access Control (RBAC)

ACE Solutions Architecture Technical Team

RBAC: Role-Based Access Control



RBAC short video for better understanding

<https://community.aviatrix.com/t/x2hykxj/rbac-for-public-cloud-networking-and-security-aws-azure-gcp-oci>

User Access- CoPilot

☰ CoPilot

Dashboard

Cloud Fabric

Networking

Security

SmartGroups

Cloud Resources

Monitor

Diagnostics

Billing & Cost

Administration

User Access

Reports

Audit

Settings

User Access

Users

Permission Group

Access Management

+ User

Name	Email	Permission Groups
admin	ace.lab@aviatrix.com	admin
copilot_service_account	ace.lab@aviatrix.com	copilot_permission
student	ace.lab@aviatrix.com	admin

Add User

Username

sec-operator

Email

sec-team@aviatrix.com

Password

Confirm Password

Permission Groups

You can leave it empty and assign a permission group later

Cancel

Save

Permission Sets – CoPilot/Controller

Create Permission Group

Name

Users

Access Accounts

CoPilot Visibility Controller Permissions

CoPilot Visibility is in Preview. Preview features are not safe for deployment in production environments. [Learn More](#)

Select All Views Clear All Views Search and Select

- ☐ Cloud Fabric
- ☐ Networking
- ☒ **Security**
 - ☒ Distributed Cloud Firewall
 - ☒ Egress
 - ☐ ThreatIQ
 - ☒ FireNet
 - ☒ Anomaly Detection
- ☐ SmartGroups

Cancel Save

- ☒ **Cloud Fabric**
- ☒ **Networking**
- ☒ **Security**
- ☒ SmartGroups
- ☒ Cloud Resources
- ☒ Monitor
- ☒ Diagnostics
- ☒ Billing & Cost
- ☒ Administration
- ☒ Settings

**Network and Security
Services available on the
CoPilot**

Authentication Phase



- Users can be authenticated:
 - **Locally** on the Aviatrix Controller
 - Onboard Users (Admin, Operators, Developers, Read-Only)
 - Allowed to reset their password
 - Using **SAML IDP**
 - Onboard Users (Admin, Operators, Developers, Read-Only)
 - Other functionality depends on IDP



AWS SSO



SAML Integration Example – Identity Provider

 **RBAC User : saad-developer@aviatrix.com**

read_only

 **RBAC User : saad@aviatrix.com**

Super-Users

Account-Admin

 **RBAC User : saad_A-B@aviatrix.com**

Account Admins (A&B)

Account Admins (C&D)

 **RBAC User : saad-security@aviatrix.com**

Security-Users

RBAC-User

Permissions

saad-developer

Read Only

saad

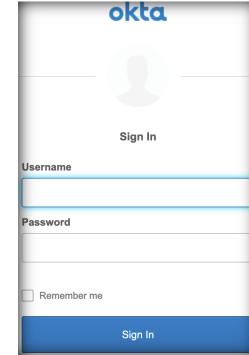
Super User (Admin)

saad_A-B

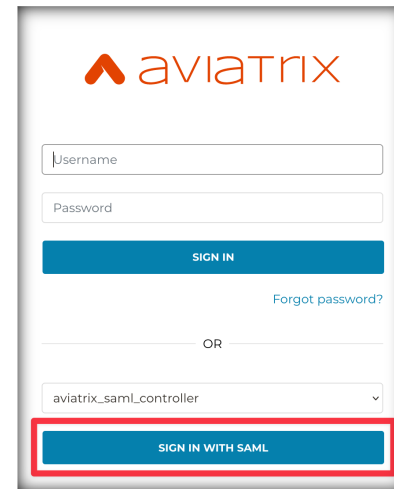
Account Admin for Accounts A&B Only

saad-security

Security User

Okta login form showing fields for Username, Password, and a Sign In button. A badge in the top right corner reads 'aviatrix ACE Aviatix Certified Engineer'.



Aviatrix login form showing fields for Username, Password, and a SIGN IN button. Below the SIGN IN button is a link for 'Forgot password?'. Below that is an 'OR' separator, followed by a dropdown menu showing 'aviatrix_saml_controller' and a 'SIGN IN WITH SAML' button highlighted with a red border.



Admin/Super-Users
Saad



Account Admins
Saad-A&B



Security-Users
Saad-Security



Developers/Read Only
Saad-Developer

Integration with OKTA – Step-by-Step Guide

<https://community.aviatrix.com/t/h7hyrmm/rbac-for-aws-azure-gcp-oci-step-by-step-integration-with-okta>

RBAC – Role Based Access Control

read_only

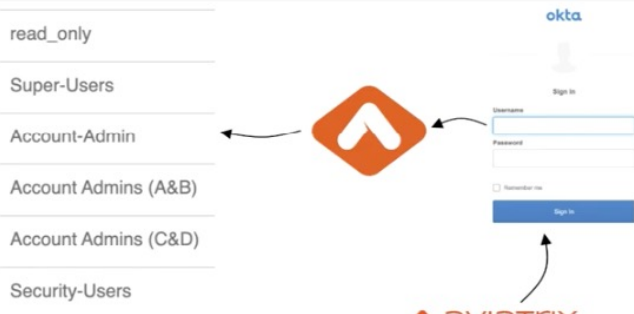
Super-Users

Account-Admin

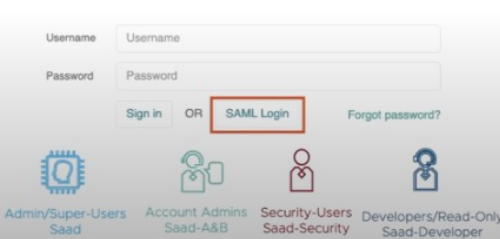
Account Admins (A&B)

Account Admins (C&D)

Security-Users



RBAC-User	Permissions
saad-developer	Read Only
saad	Super User (Admin)
saad_A-B	Account Admin for Accounts A&B Only
saad-security	Security User





Next: Lab 4 - RBAC