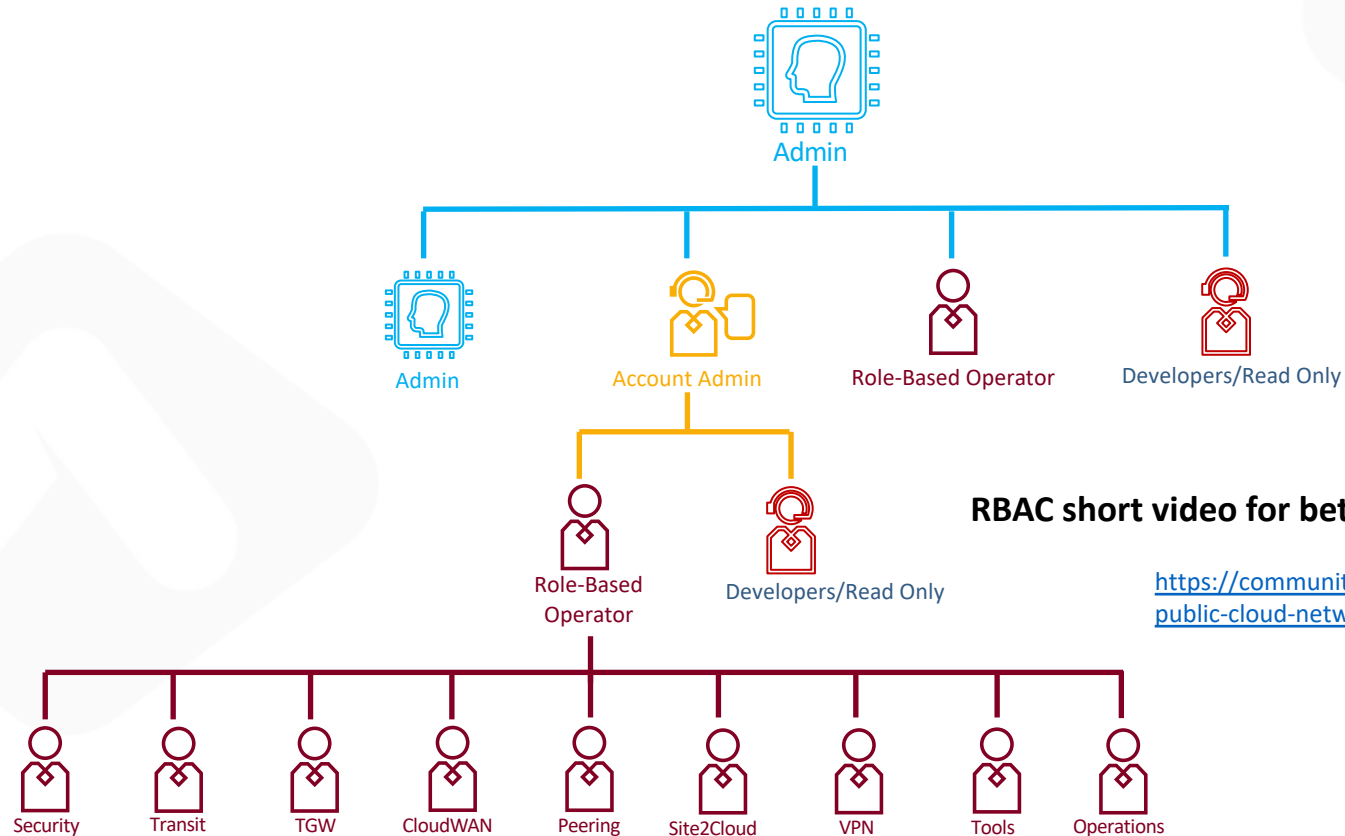




# Role-Based Access Control (RBAC)

Solutions Engineering

# 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

The screenshot displays the CoPilot User Access interface. On the left is a dark sidebar with navigation options: Dashboard, Cloud Fabric, Networking, Security, SmartGroups, Cloud Resources, Monitor, Diagnostics, Billing & Cost, Administration (highlighted with a red box), User Access (highlighted with a red box), Reports, Audit, and Settings. The main content area has tabs for User Access, Users (highlighted with a red box), Permission Group, and Access Management. Below the Users tab is a '+ User' button (highlighted with a red box) and icons for filter, table view, and download. A table lists existing users with columns for Name, Email, and Permission Groups.

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

An 'Add User' modal is open in the foreground, containing the following fields:

- Username:
- Email:
- Password:  (with an eye icon for visibility toggle)
- Confirm Password:  (with an eye icon for visibility toggle)
- Permission Groups:

At the bottom of the modal are 'Cancel' and 'Save' buttons.

# Permission Sets – CoPilot/Controller

### Create Permission Group

Name

Users

Access Accounts

**CoPilot Visibility** Controller Permissions

Select All Views Clear All Views Search and Select

- ✓ AirSpace
- ✓ Networking
- ✓ Security
- ✓ SmartGroups
- ✓ Cloud Resources
- ✓ Monitor

Cancel Save

- ✓ AirSpace
- ✓ Networking
- ✓ Security
- ✓ SmartGroups
- ✓ Cloud Resources
- ✓ Monitor
- ✓ Troubleshoot
- ✓ Billing & Cost
- ✓ Administration
- ✓ Settings

# 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

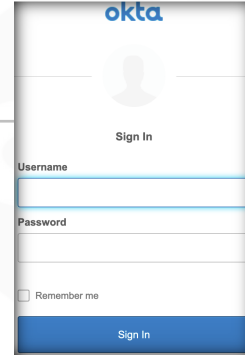
Super User (Admin)

saad\_A-B

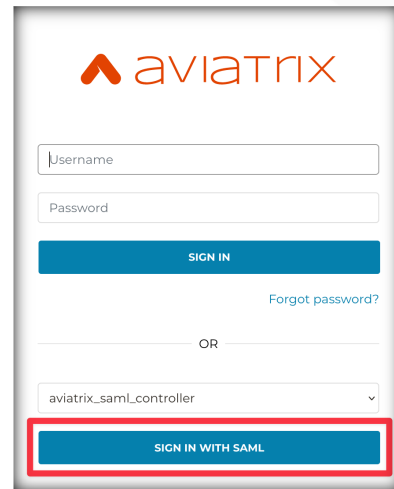
Account Admin for Accounts A&B Only

saad-security

Security User

Okta login form with fields for Username, Password, and a Sign In button. A 'Remember me' checkbox is also present.



Aviatrix login form with fields for Username, Password, and a SIGN IN button. A 'Forgot password?' link is below the password field. Below the SIGN IN button is an 'OR' separator, followed by a dropdown menu showing 'aviatrix\_saml\_controller' and a 'SIGN IN WITH SAML' button highlighted with a red box.



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

okta

Sign In

Username

Password

Remember Me

Sign In

aviatrix

Username

Password

Sign in OR SAML Login Forgot password?

Admin/Super-Users Saad

Account Admins Saad-A&B

Security-Users Saad-Security

Developers/Read-Only Saad-Developer



Next: Lab 4 - RBAC