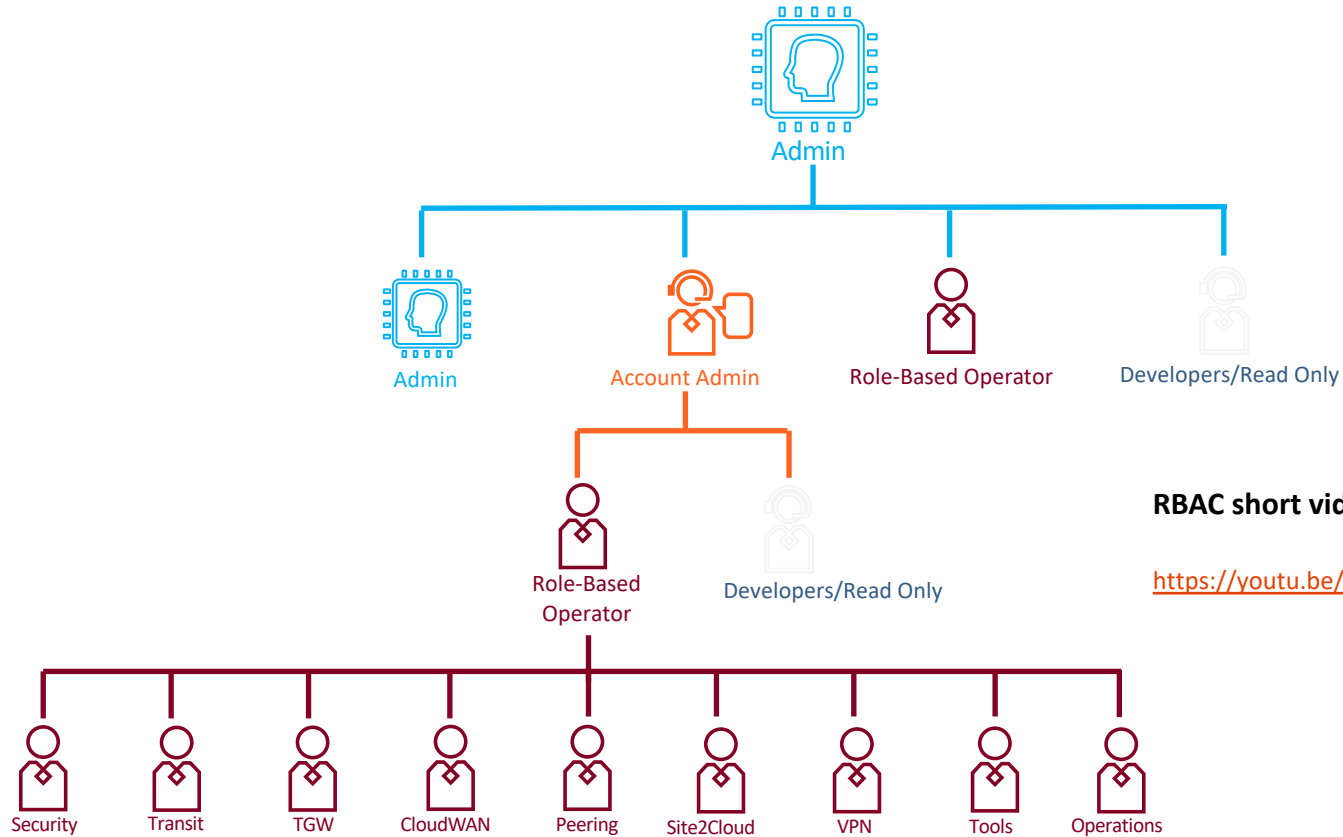




Role-Based Access Control (RBAC)

ACE Solutions Architecture Technical Team

RBAC: Role-Based Access Control



RBAC short video for better understanding

<https://youtu.be/ZRGIDY5xVqU>

User Access- CoPilot



CoPilot

Search

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 Filter Grid Download

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

Email

Password

Confirm Password

Permission Groups

You can leave it empty and assign a permission group later

Cancel Save

Aviatrix RBAC Control



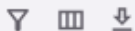
☰ CoPilot

🔍 Search

- 👤 SmartGroups
- ☁️ Cloud Resources
- 📊 Monitor
- 🔧 Diagnostics
- 💰 Billing & Cost
- 👤 Administration
- User Access**
- 📄 Reports
- 🔍 Audit

User Access Users **Permission Group** Access Management

+ Permission Group



Name	Copilot Visibility	Controller Permissions
admin	All	Write
read_only	All	Read
copilot_permission	All	Write
security	All	Security - Write
operations	All	Dashboard - Write
networking	All	Write
Aviatrix Demo Contro...	All	Write

Permission Sets



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

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



onelogin

okta



G Suite



AWS SSO



SAML Integration Example – Identity Provider

RBAC User: developer

RBAC User: Admin

RBAC User: Account_A-B

RBAC User: SecOps

read_only

Super-Users

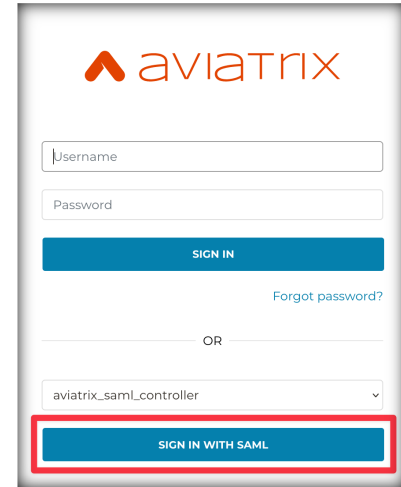
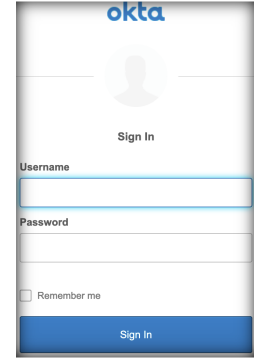
Account-Admin

Account Admins (A&B)

Account Admins (C&D)

Security-Users

RBAC-User	Permissions
developer	Read Only
Admin	Super User (Admin)
Account_A-B	CSP Account Admin for Accounts A&B Only
SecOps	Security User



Admin/Super-Users
Admin



Account Admins
Account-A&B



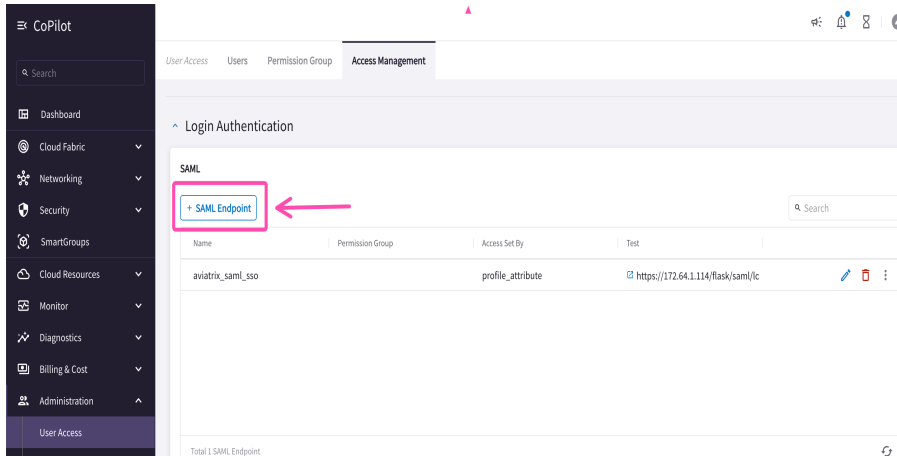
Security-User
SecOps



Developers/Read Only
Developer

Configuring SAML Authentication:

Go to Administration > User Access > Access Management.
Under Login Authentication, click +SAML Endpoint.



Create SAML Endpoint

Name

SAML Endpoint Configuration

Identity Provider Metadata Type
 URL Text

Identity Provider Metadata URL

Entity ID
 Hostname Custom

Access Set By
 Controller SAML Identity Provider Attribute

Permission Group

Sign Auth Requests
 No

Custom SAML Request Template



Authentication

Users can be authenticated **Locally** or using **SAML IDP**

The screenshot displays the Aviatix Access Management interface. On the left is a dark sidebar with a search bar and a list of navigation items: Networking, Security, SmartGroups, Cloud Resources, Monitor, Diagnostics, Billing & Cost, Administration, User Access (highlighted), and Reports. The main content area has tabs for User Access, Users, Permission Group, and Access Management (selected). Below the tabs is a 'history' section with a 'Manage Policy' button. The 'Login Authentication' section is expanded to show 'SAML' configuration. A '+ SAML Endpoint' button is visible. A search bar is present on the right. Below is a table with columns: Name, Permission Group, Access Set By, and Test.

Name	Permission Group	Access Set By	Test
aviatrix_saml_sso		profile_attribute	https://172.64.1.114/flask/saml/login/aviatrix_



Next: Design Exercise