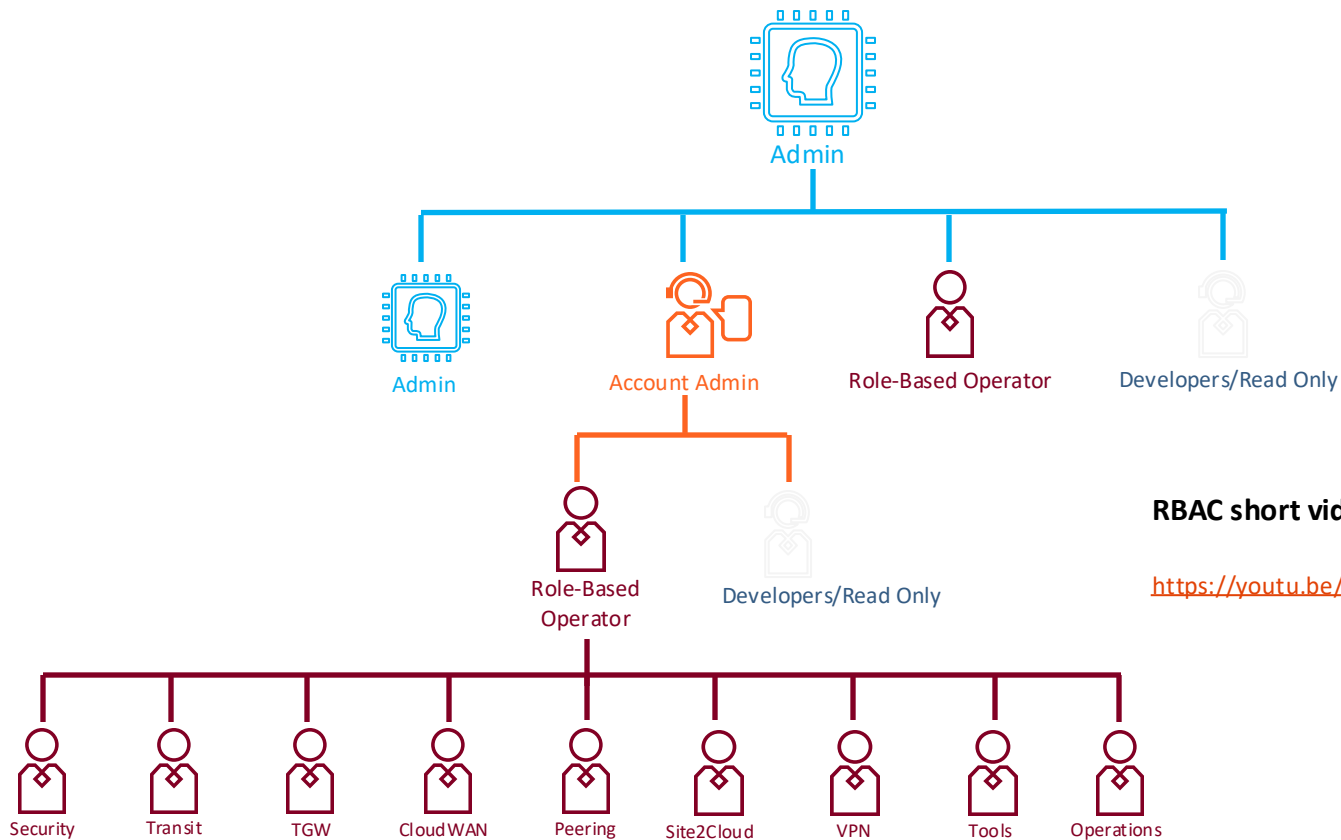




Role-Based Access Control (RBAC)

ACE Team

RBAC: Role-Based Access Control



RBAC short video for better understanding

<https://youtu.be/ZRGIDY5xVqU>

User Access- CoPilot



☰ CoPilot

Dashboard

Cloud Fabric

Networking

Security

Groups

Cloud Resources

Monitor

Diagnostics

Administration

User Access

Reports

User AccessUsersPermission GroupAccess Management

+ User

Name	Email
admin	ace.lab@aviatrix.com
copilot_service_account	ace.lab@aviatrix.com
johndoe	johndoe@aviatrix.com
student	ace.lab@aviatrix.com

Add User

Username

cloudE-engineer

Email

engineer@aviatrix.com

Password

.....

👁

Confirm Password

.....

👁

Permission Groups

security ×

× ▾

Cancel

Save

The Aviatrix logo, consisting of an orange triangle followed by the word 'aviatrix' in lowercase.

Permission Group (part.1)



☰ CoPilot

🔍 Search

Dashboard

Cloud Fabric

Networking

Security

Groups

Cloud Resources

Monitor

Diagnostics

Administration

User Access

Reports

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-team	Security Groups	

Permission Group (part.2)



Create Permission Group?

Name

Network-team

Users

johndoe x v

Access Accounts

aws-account x v

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 v

Cloud Fabric

Topology

5/5 Tabs

All Tabs x v

Gateways

6/6 Tabs

All Tabs x v

Hybrid Cloud

4/4 Tabs

All Tabs x v

Scaling

7/7 Tabs

All Tabs x v

Cancel

Save

Cloud Fabric

Networking

Security

Groups

Cloud Resources

Monitor

Diagnostics

Administration

Settings

Cancel

Save

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: developer

read_only

RBAC User: Admin

Super-Users

RBAC User: Account_A-B

Account-Admin

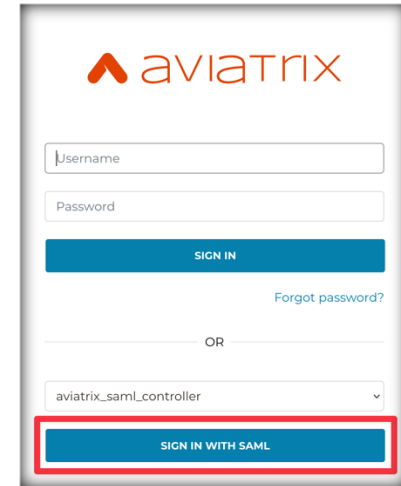
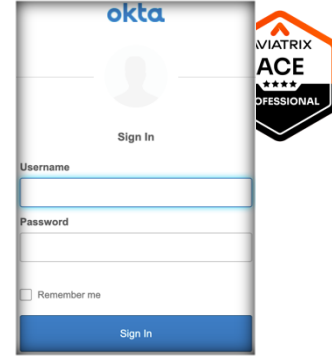
Account Admins (A&B)

Account Admins (C&D)

RBAC User: SecOps

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



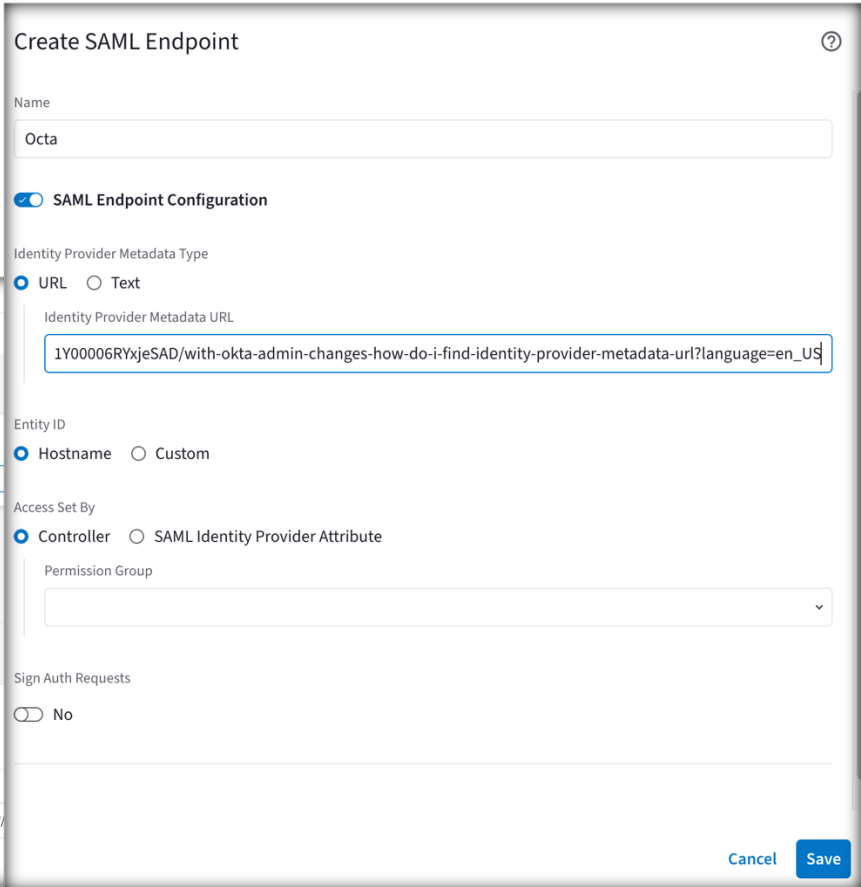
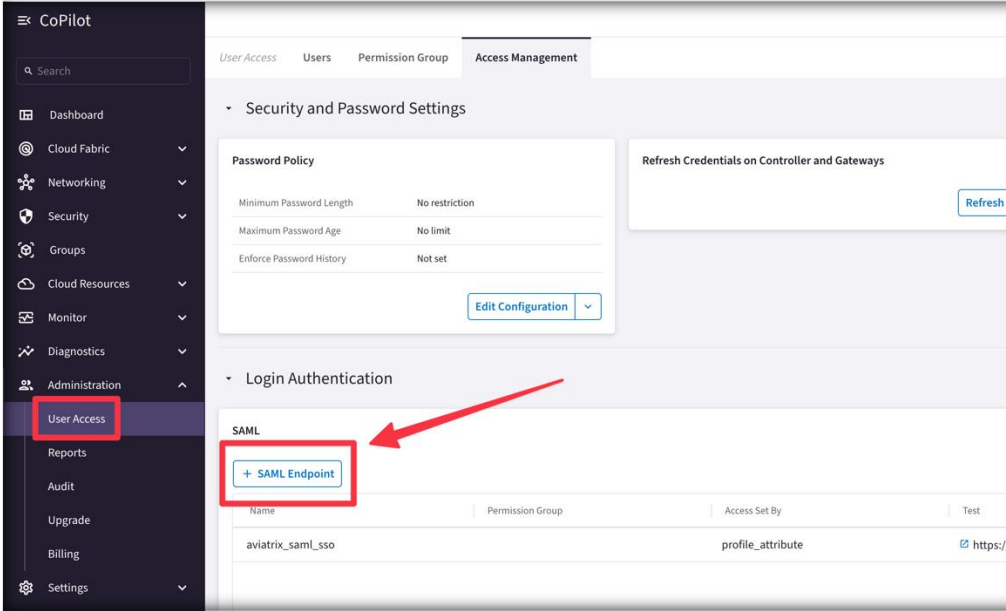
Developers/Read Only
Developer

Configuring SAML Authentication:

User can be authenticated using the local database or using the SAML Integration.

Go to *CoPilot > Administration > User Access > Access Management*

Under Login Authentication, click **+SAML Endpoint**





Next: Design Exercise