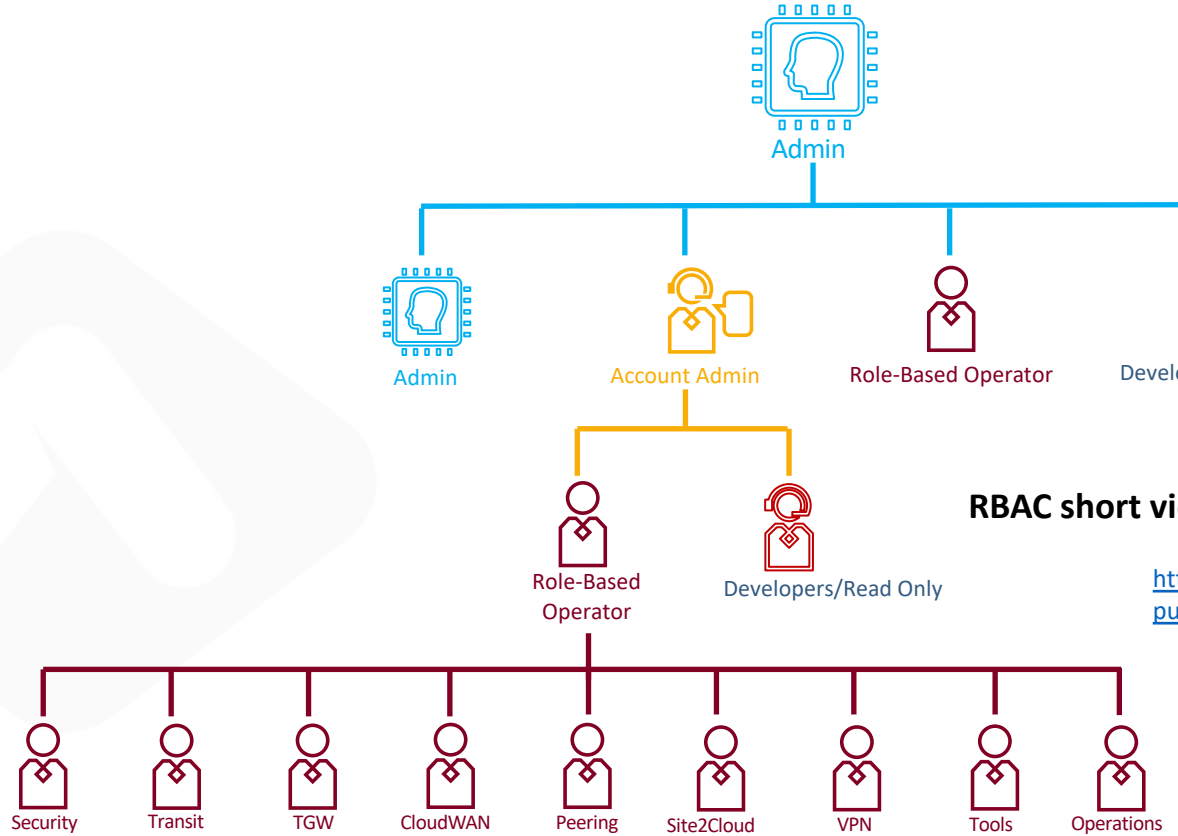
Role-Based Access Control (RBAC)

Solutions Engineering

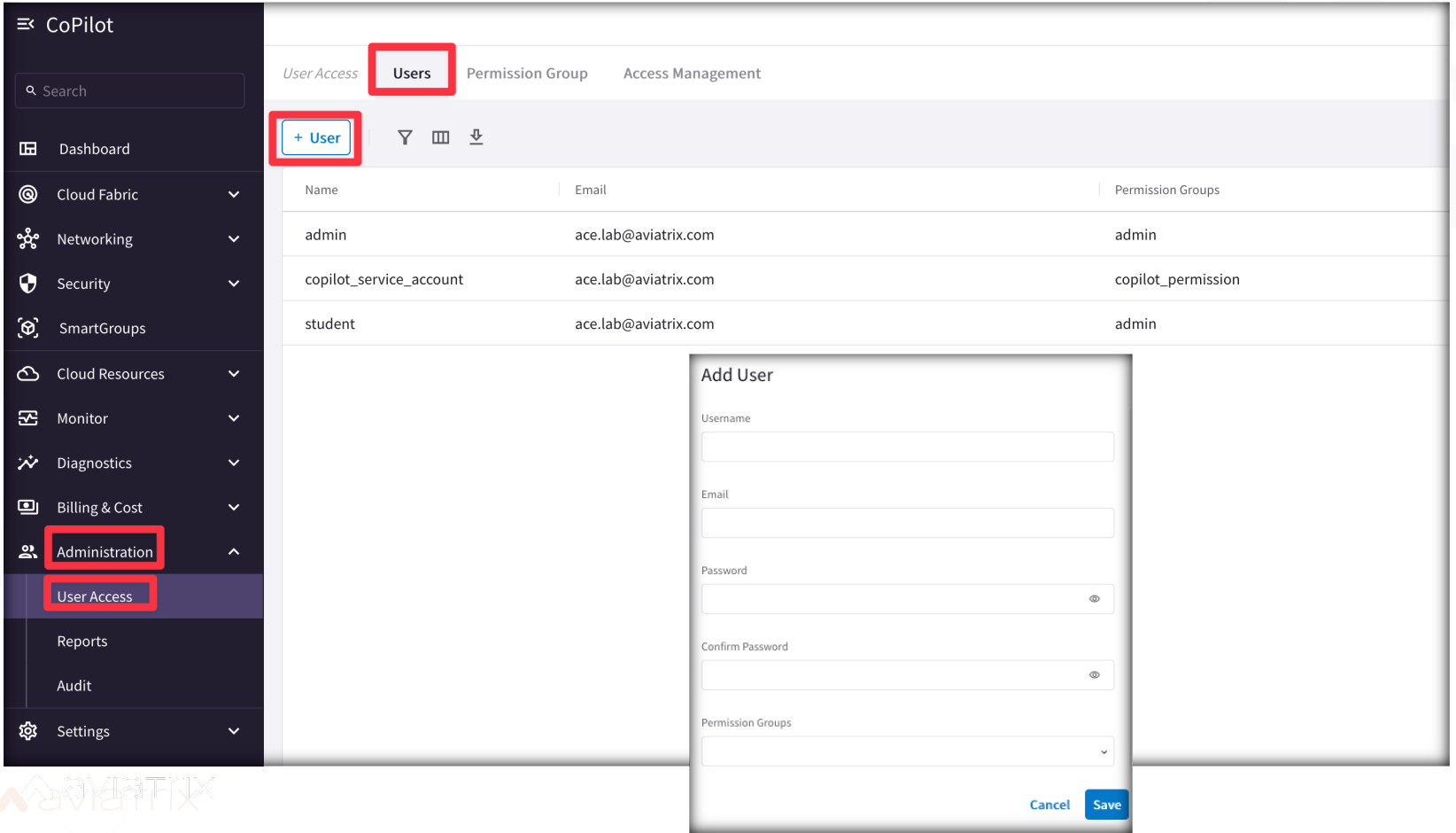
RBAC: Role-Based Access Control



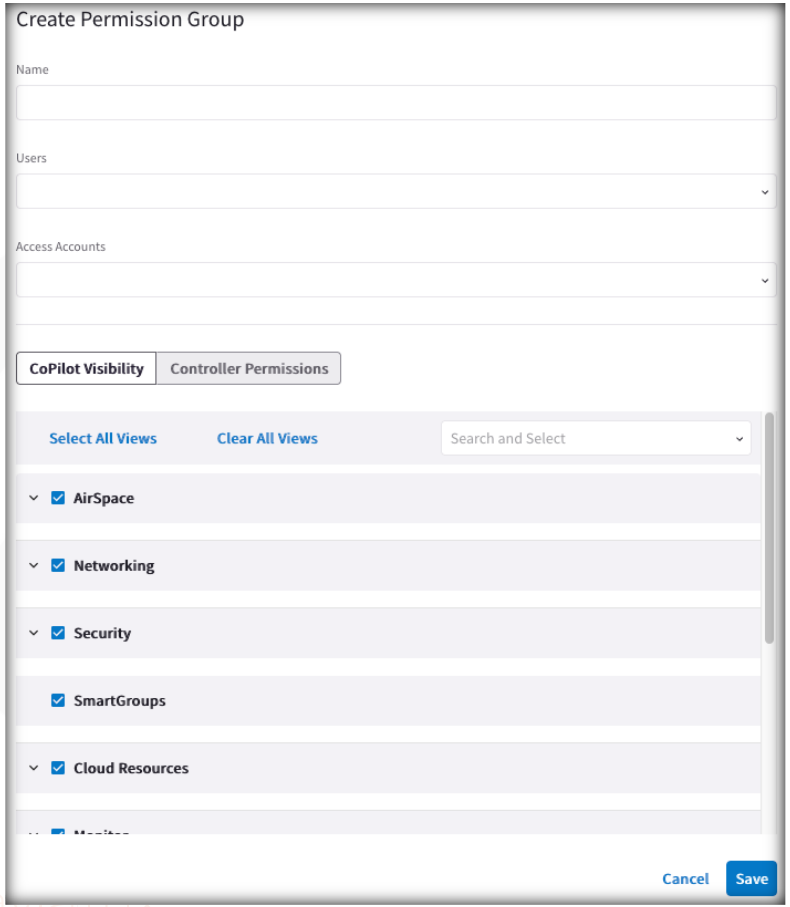
RBAC short video for better understanding

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

User Access- CoPilot



Permission Sets – CoPilot/Controller



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

DUO Azure Active Directory

Ping Identity. G Suite

AWS SSO

thycotic and Centrify are now Delinea.
Delinea
Defining the boundaries of access

RBAC Example – Okta

RBAC User : saad-developer@aviatrix.com → read_only

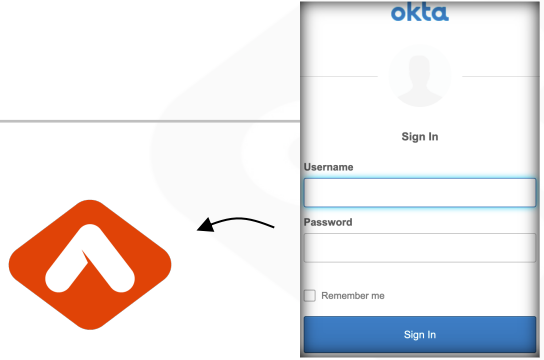
RBAC User : saad@aviatrix.com → Super-Users

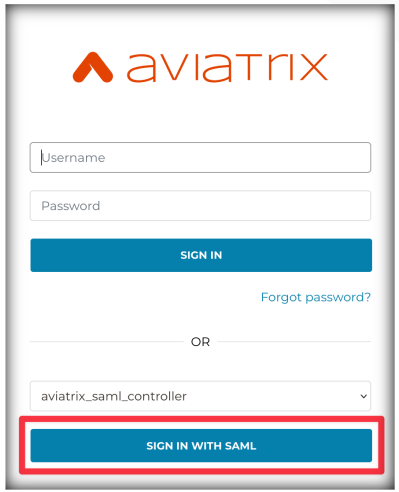
Account-Admin

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

Admin/Super-Users
Saad

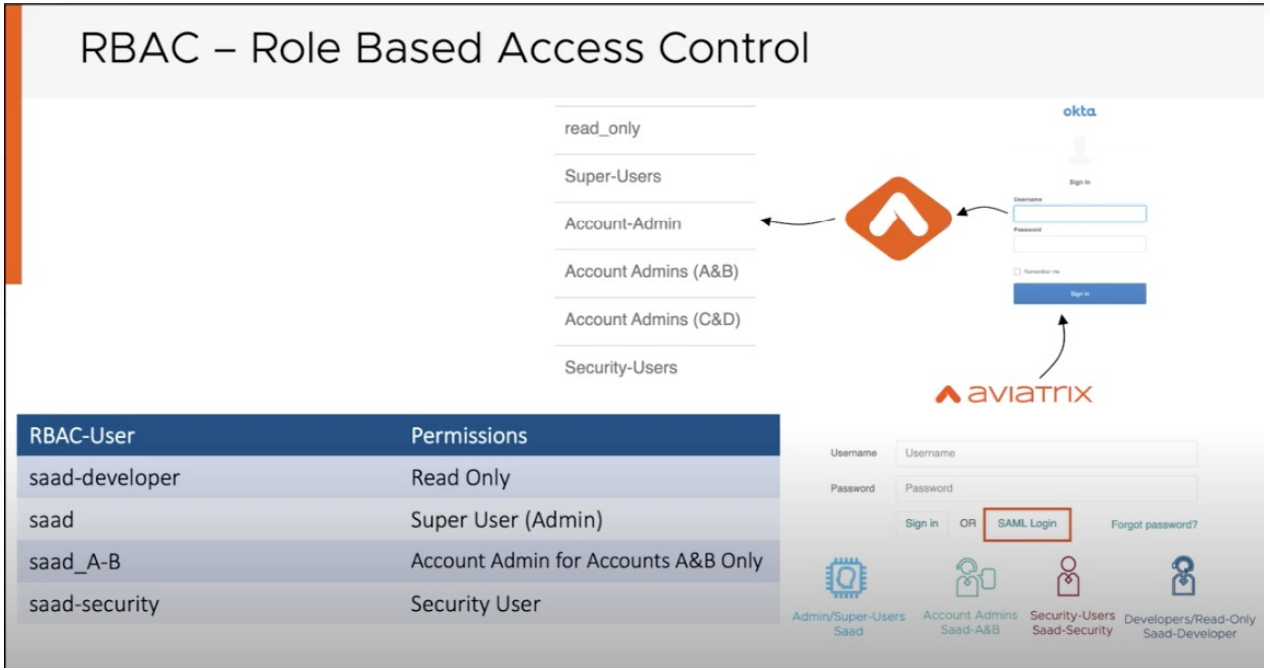
Account Admins
Saad-A&B

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



Next: Lab 5 - RBAC