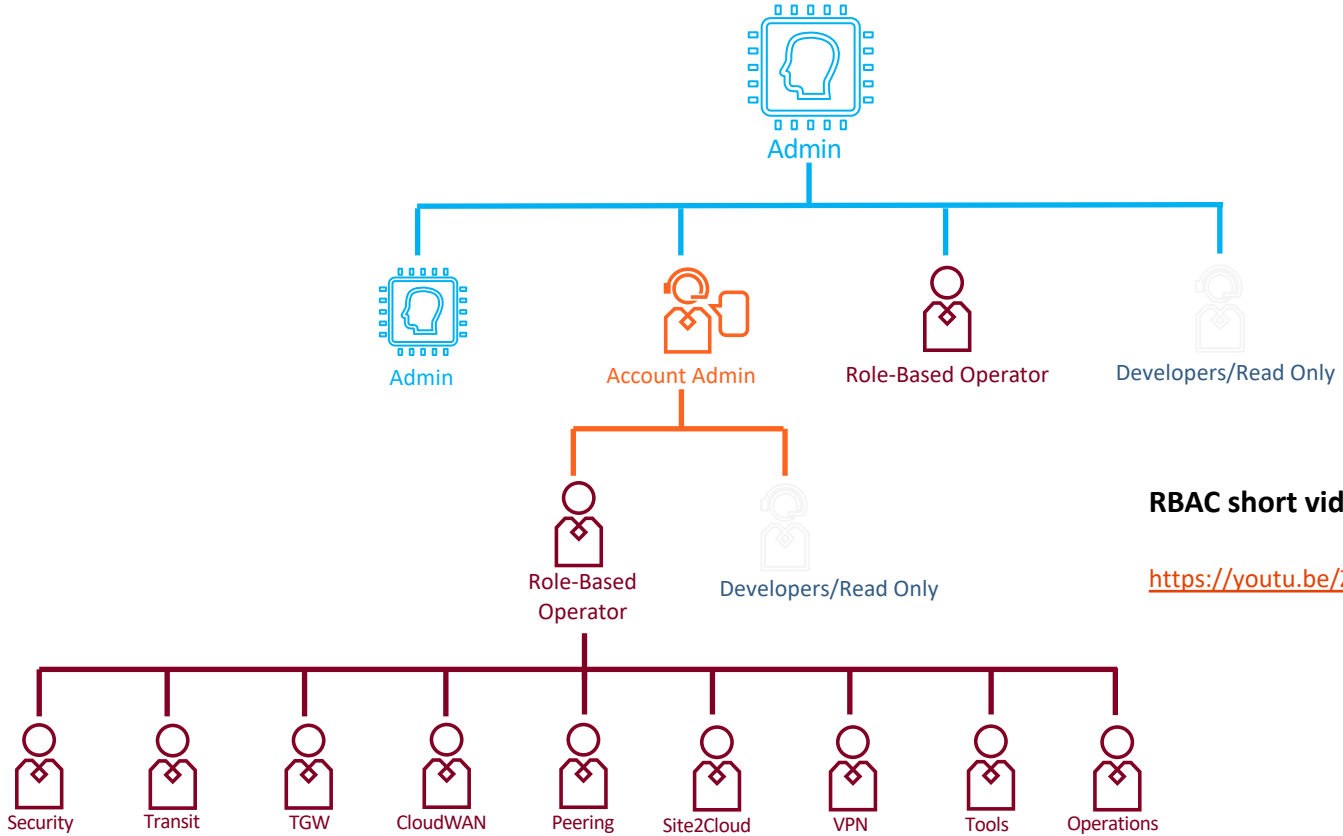
Role-Based Access Control (RBAC)

ACE Solutions Architecture Technical Team

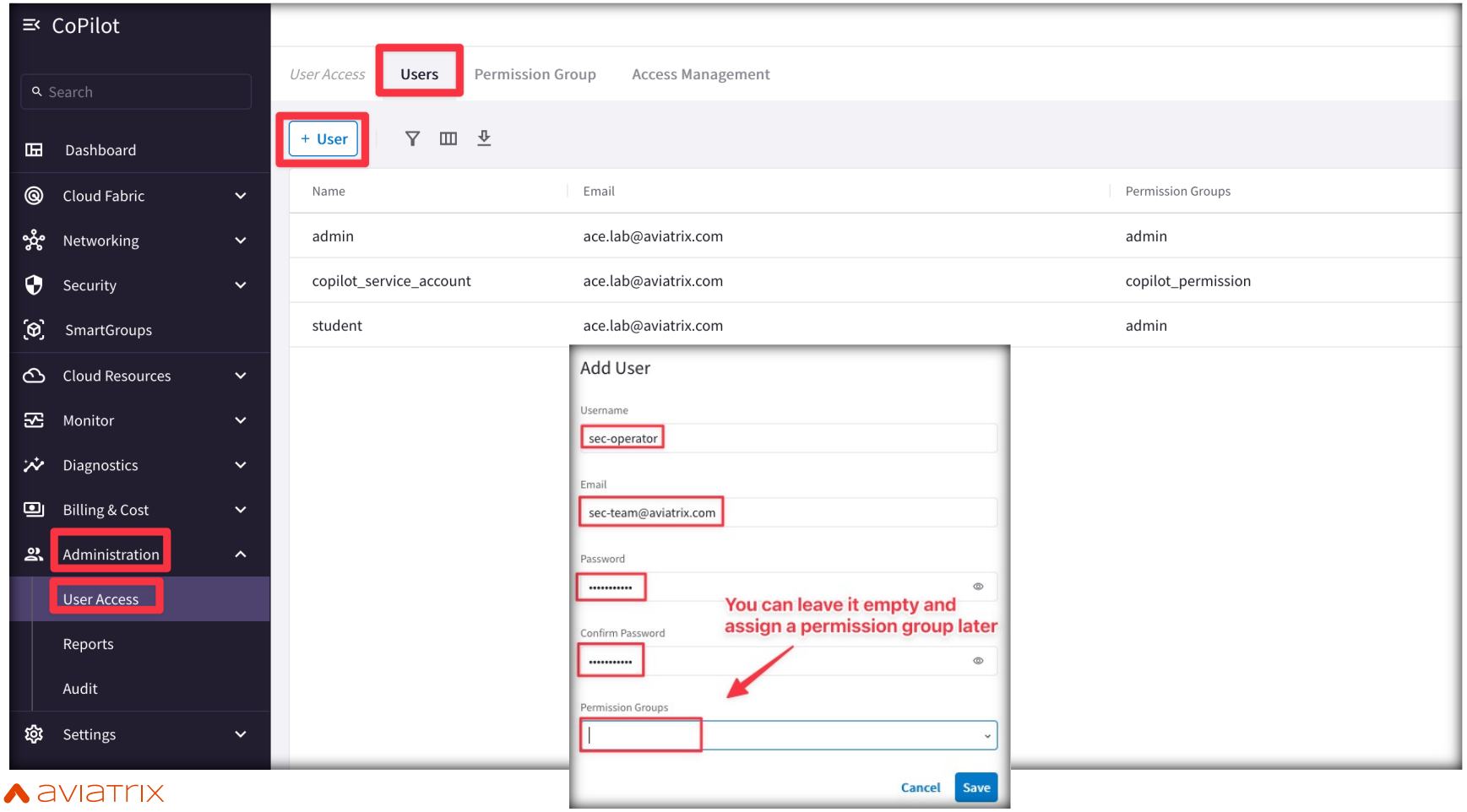
RBAC: Role-Based Access Control



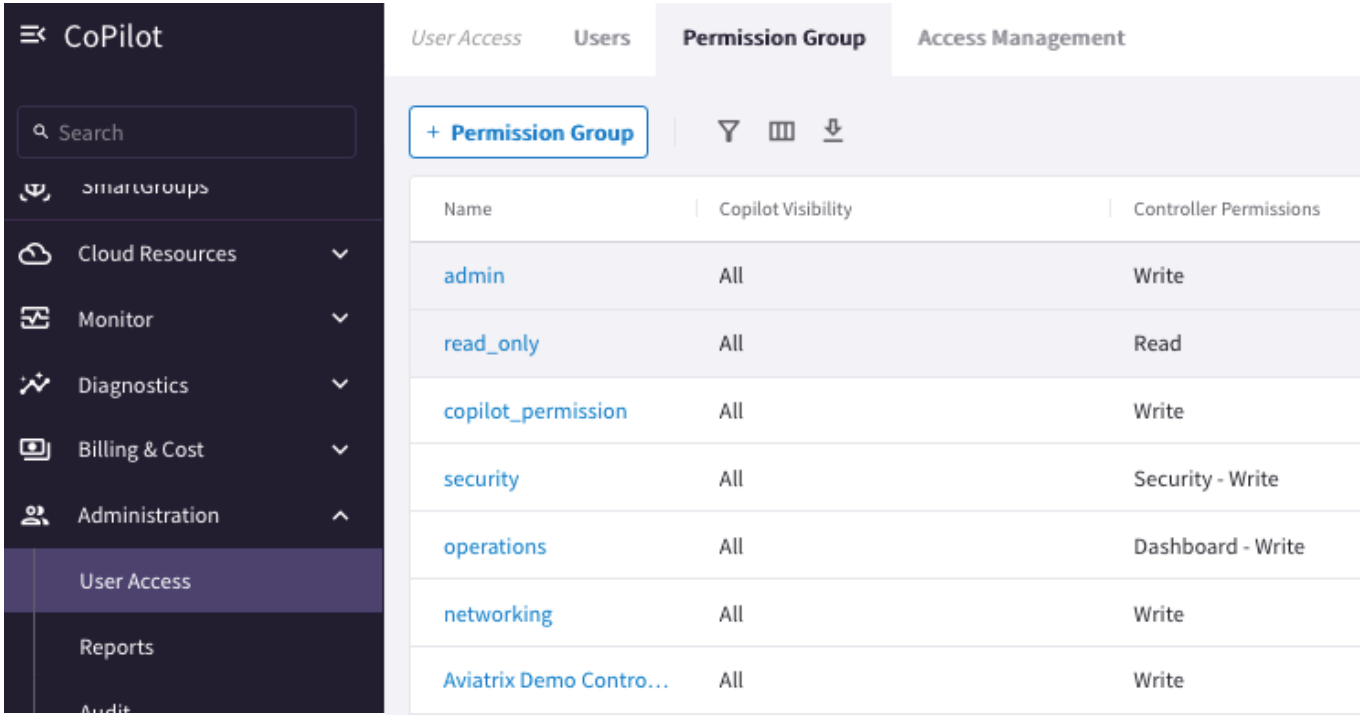
RBAC short video for better understanding

https://youtu.be/ZRGIDY5xVqU

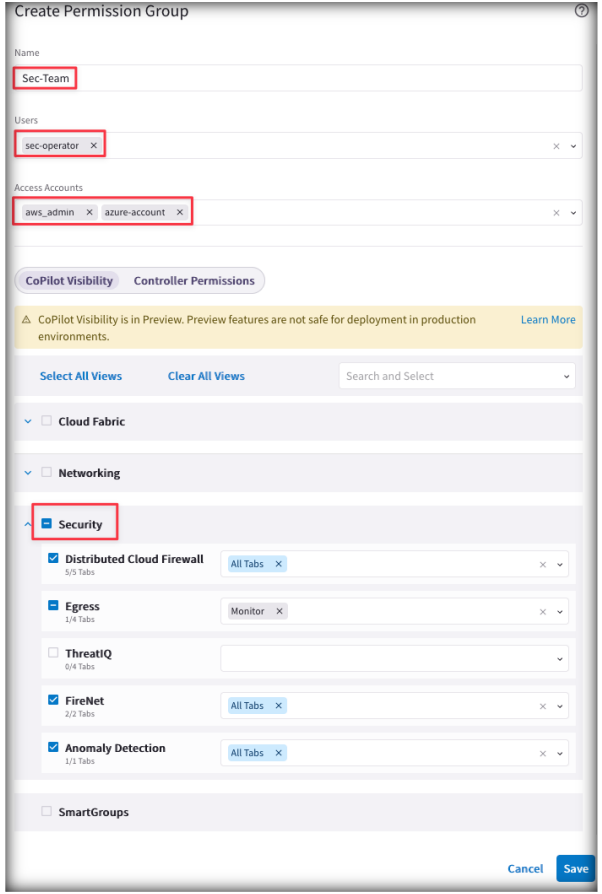
User Access- CoPilot

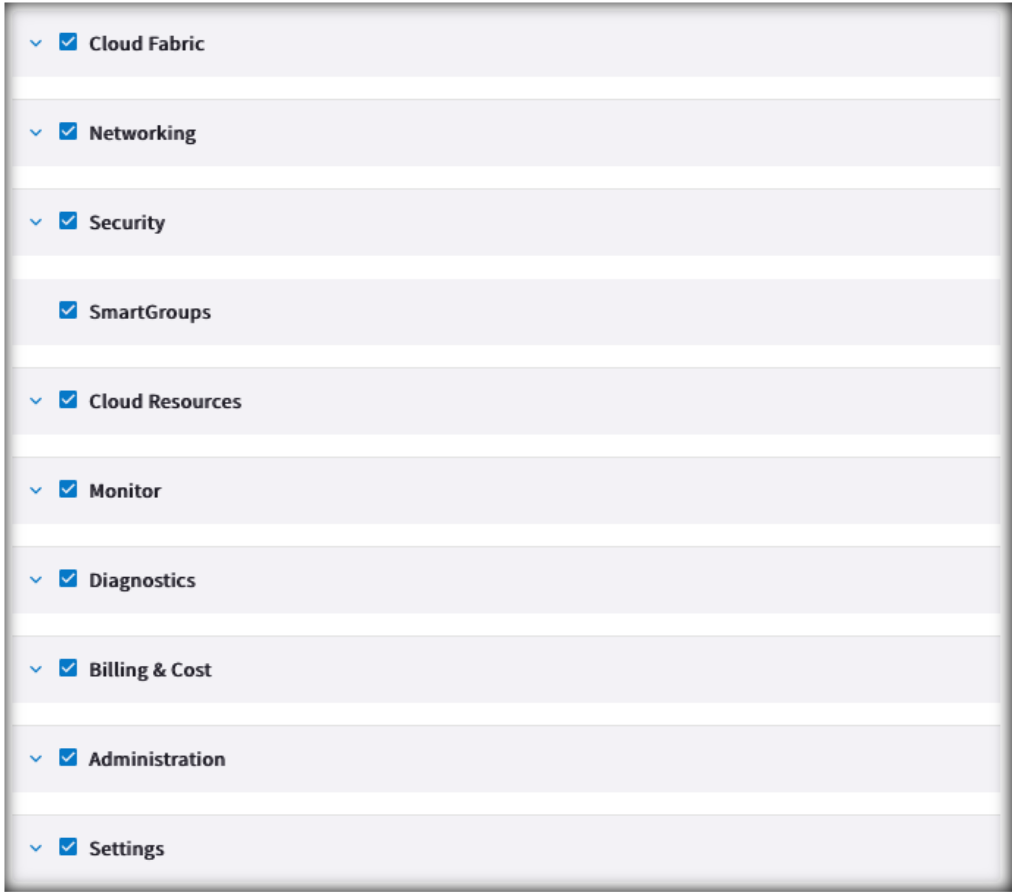


Aviatrix RBAC Control



Permission Sets





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

SAML Integration Example – Identity Provider

RBAC User: developer

RBAC User: Admin

RBAC User: Account_A-B

RBAC User: SecOps

read_only

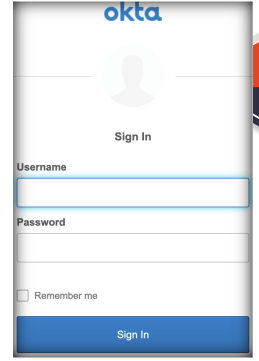
Super-Users

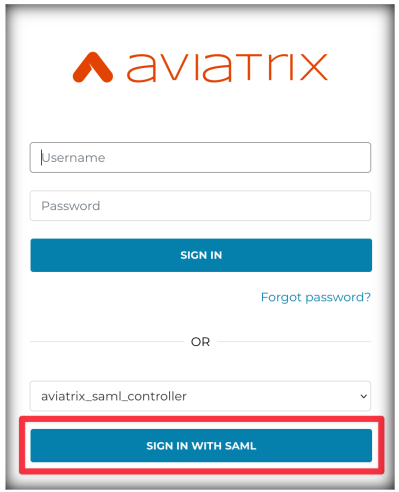
Account-Admin

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

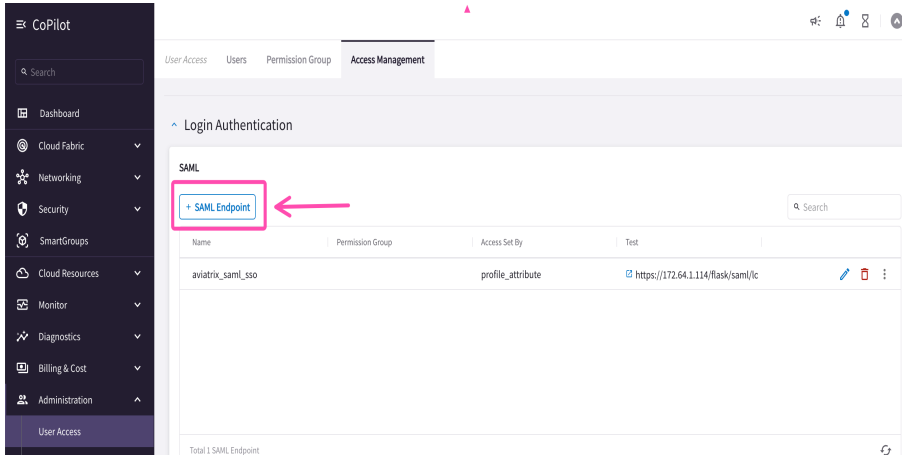
Account Admins
Account-A&B

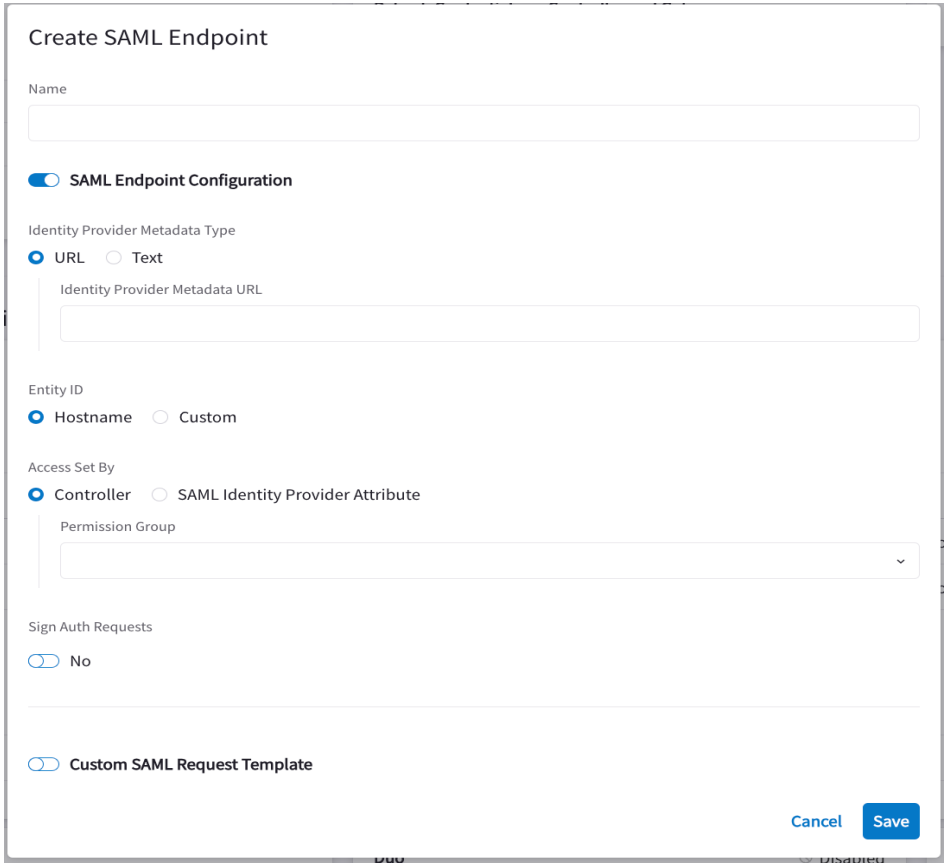
Security-User
SecOps

Developers/Read Only
Developer

Configuring SAML Authentication:

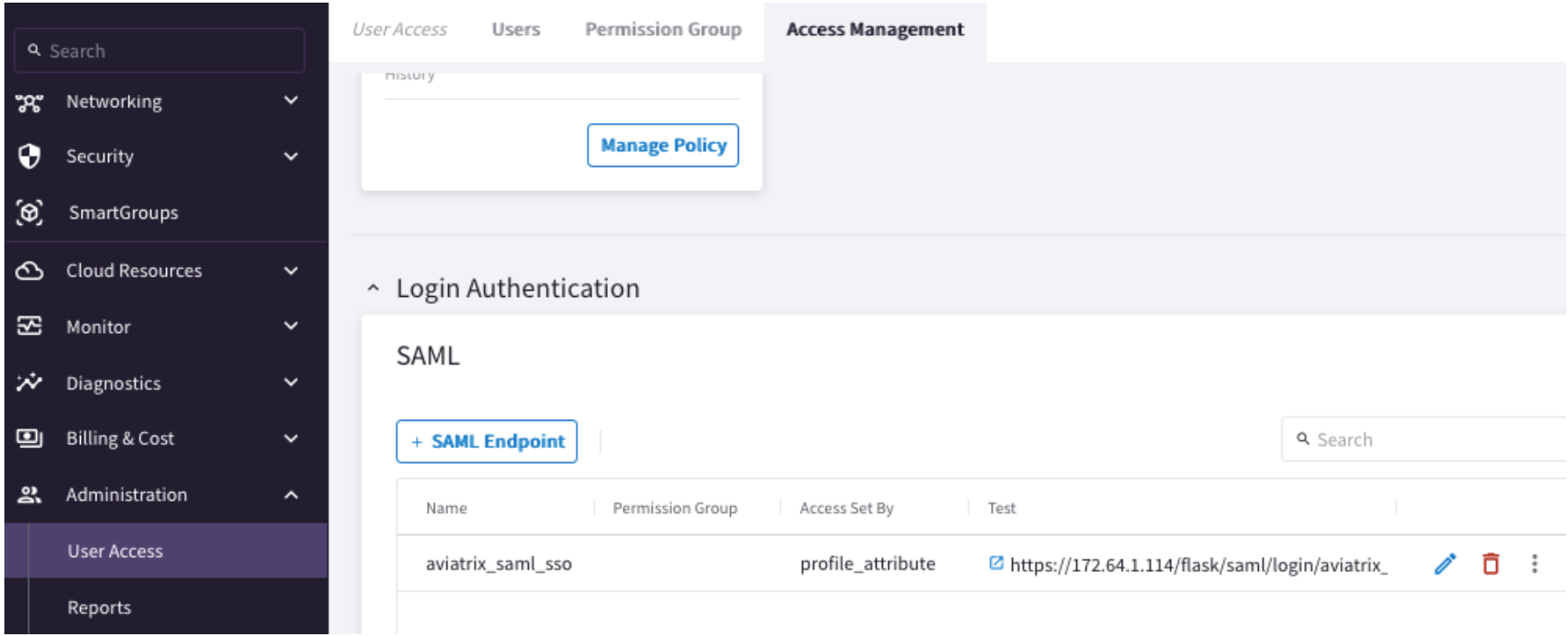
Go to Administration > User Access > Access Management.
Under Login Authentication, click +SAML Endpoint.





Authentication

Users can be authenticated **Locally or u**sing **SAML IDP**



Next: Design Exercise