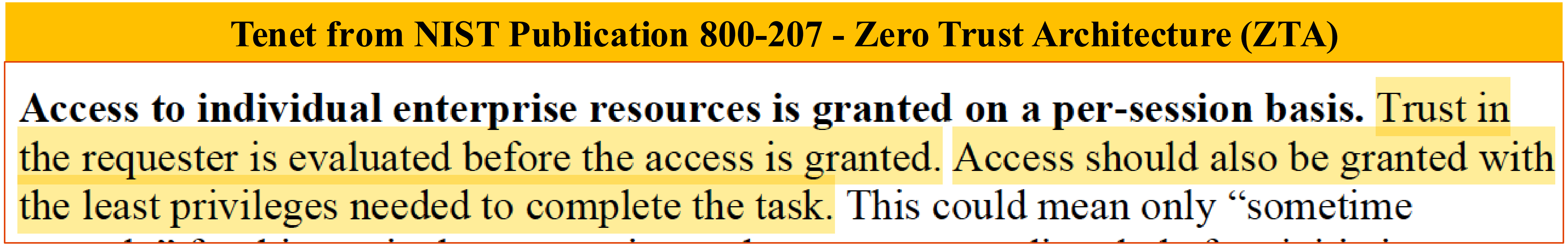
AVIATRIX
ACE
AVIATRIX CERTIFIED
ENGINEER

AVIATRIX
ACE
SECURITY
SPECIALTY

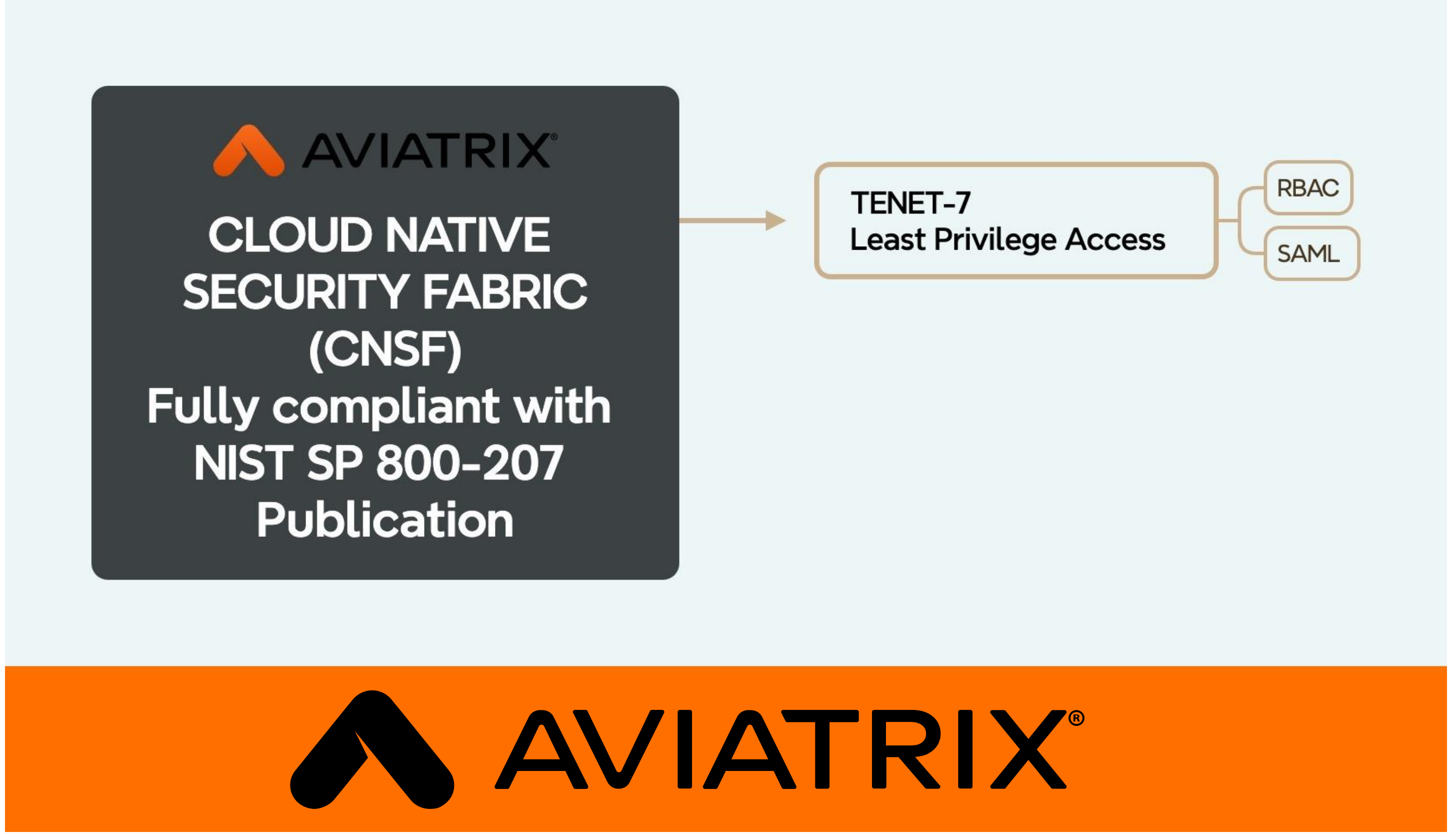
Tenet-7: Least Privilege Access

Audit, Reporting and Alerts



Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

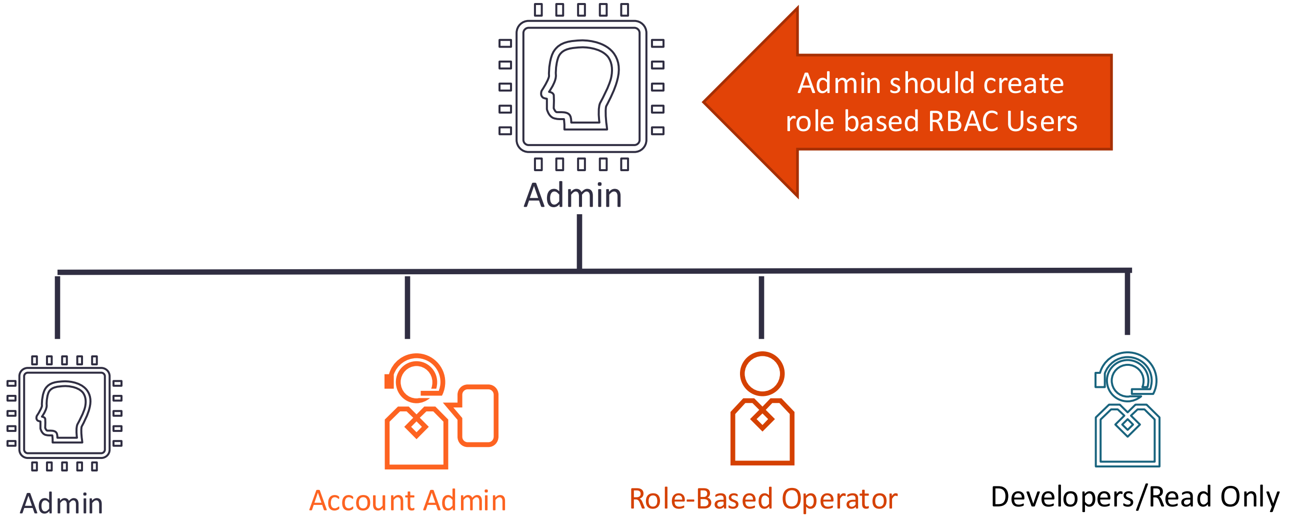
Access to individual enterprise resources is granted on a per-session basis. Trust in the requester is evaluated before the access is granted. Access should also be granted with the least privileges needed to complete the task. This could mean only "sometime



CLOUD NATIVE SECURITY FABRIC (CNSF)
Fully compliant with NIST SP 800-207 Publication

RBAC: Role-Based Access Control

Aviatrix RBAC is based on the “Users” and “Permission Group” concept



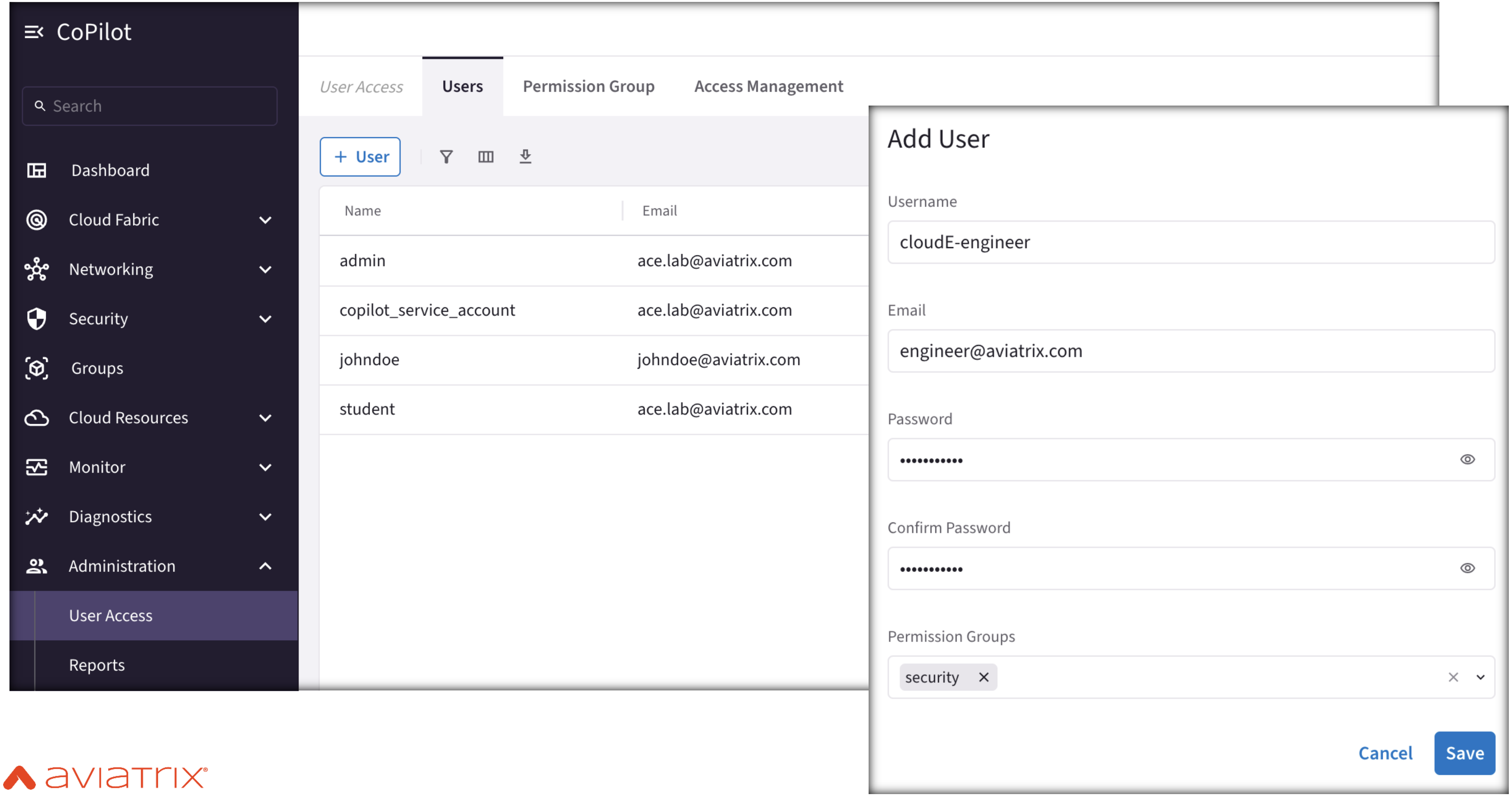
Admin should create role based RBAC Users

Assign role-based granular permissions to users using the Aviatrix “Permission Group” option

RBAC with SAML/OKTA

https://www.youtube.com/watch?v=l9zmZTaVUo8

User Access- CoPilot



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

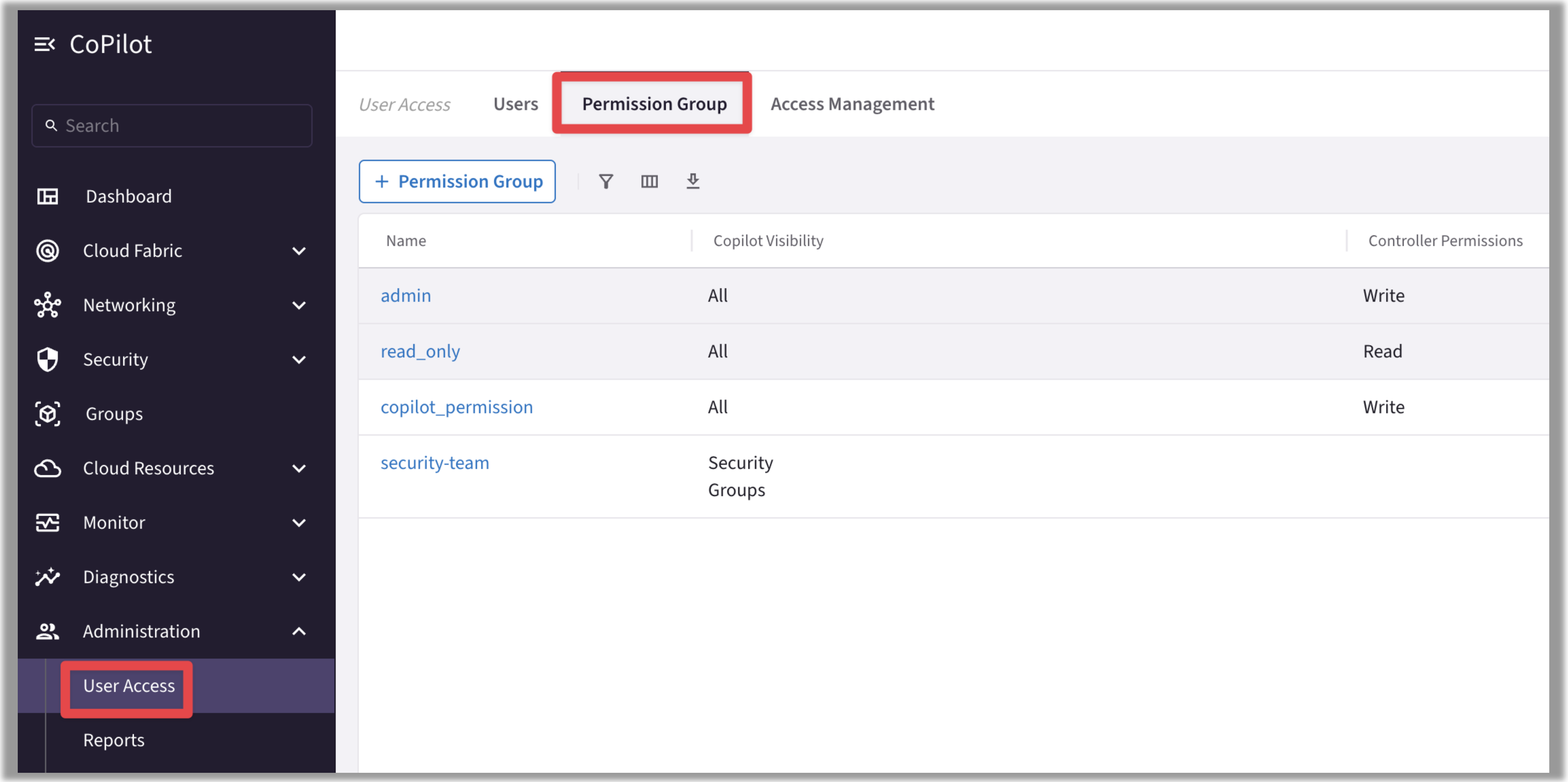
Email: engineer@aviatrix.com

Password: •••••••••••

Confirm Password: •••••••••••

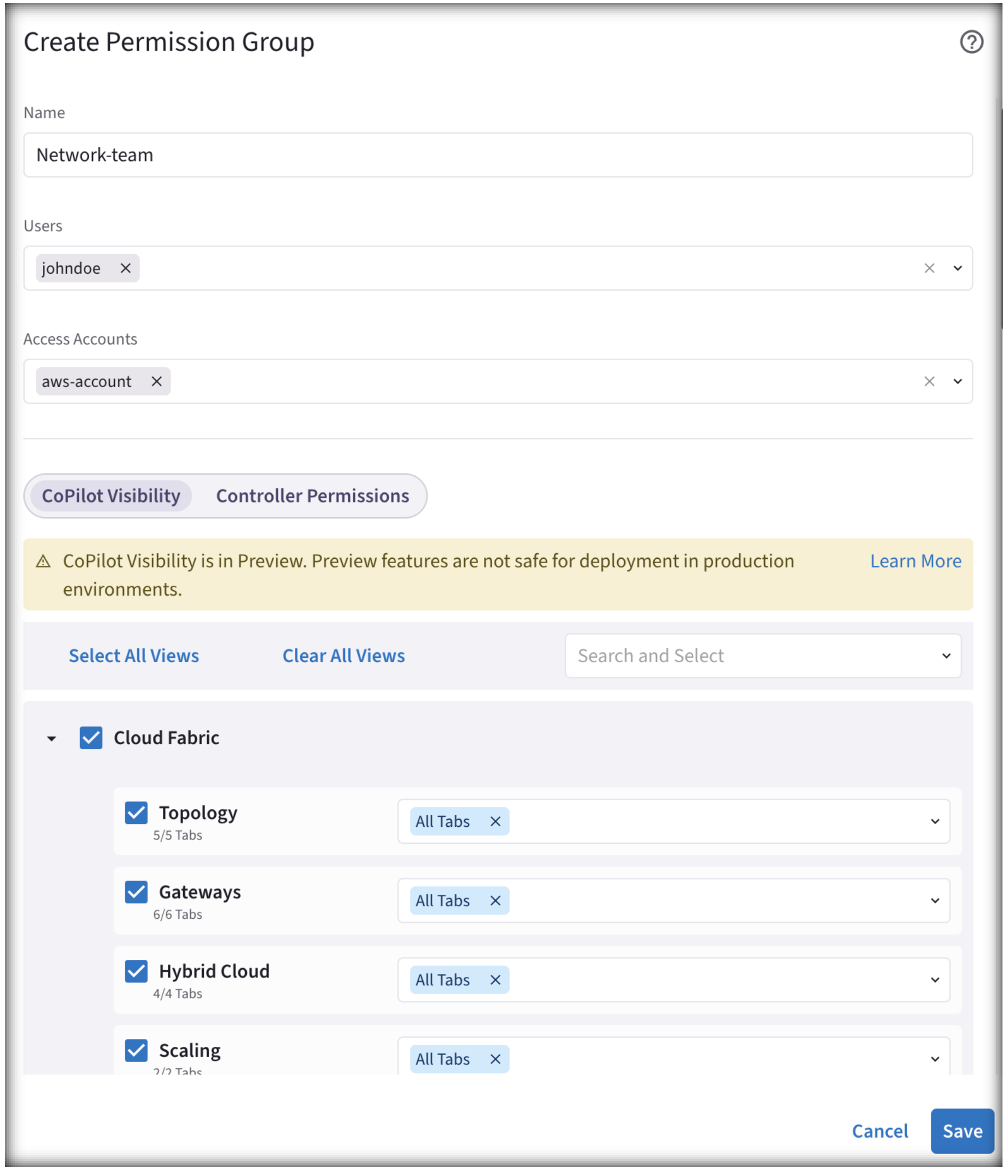
Permission Groups: security ✕

Permission Group (part.1)



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

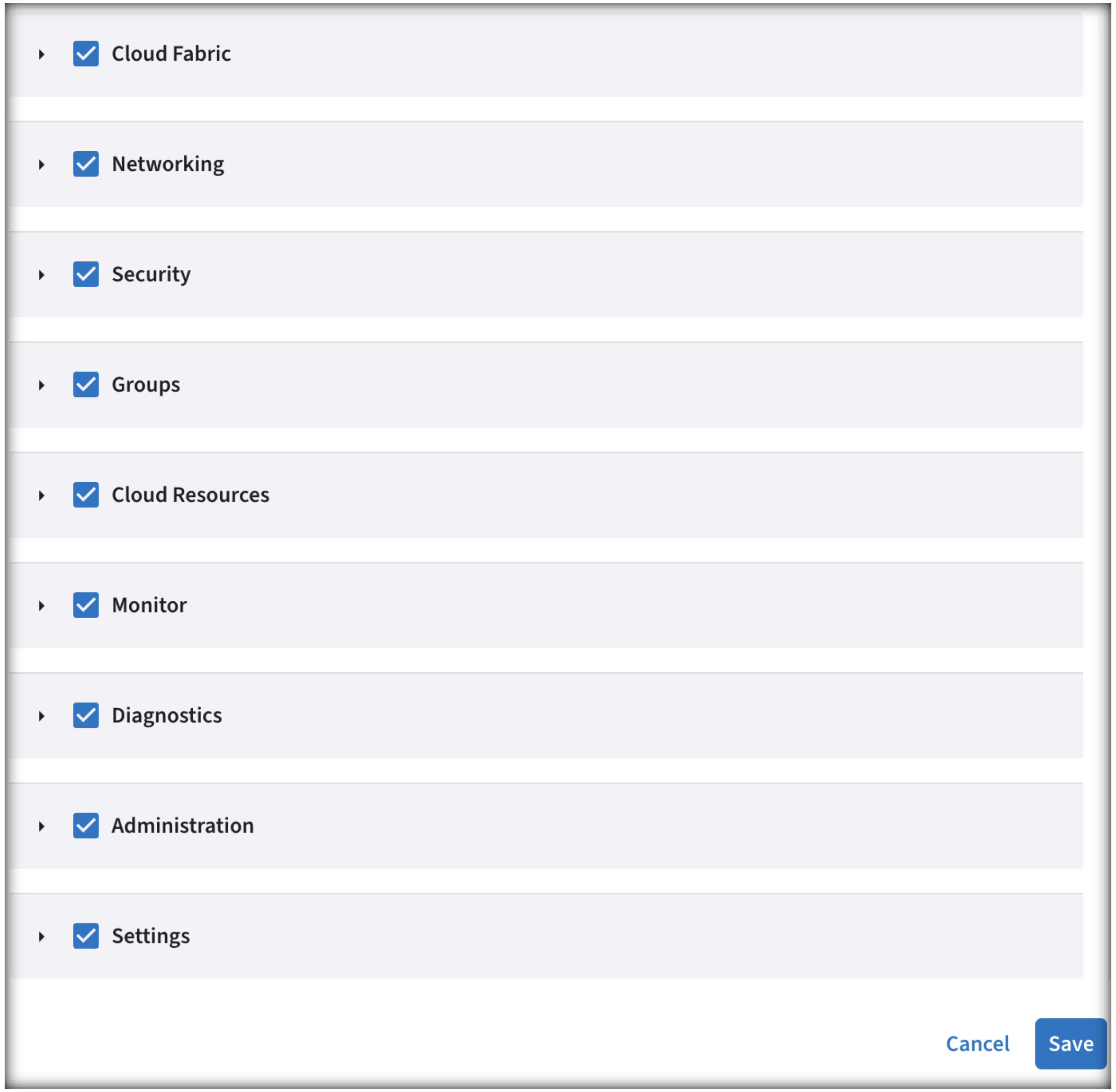
Users: johndoe ✕

Access Accounts: aws-account ✕

⚠ CoPilot Visibility is in Preview. Preview features are not safe for deployment in production environments. Learn More

☑ Cloud Fabric

☑ Topology 5/5 Tabs	All Tabs ✕
☑ Gateways 6/6 Tabs	All Tabs ✕
☑ Hybrid Cloud 4/4 Tabs	All Tabs ✕
☑ Scaling 2/2 Tabs	All Tabs ✕



- ☑ Cloud Fabric
- ☑ Networking
- ☑ Security
- ☑ Groups
- ☑ Cloud Resources
- ☑ Monitor
- ☑ Diagnostics
- ☑ 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

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

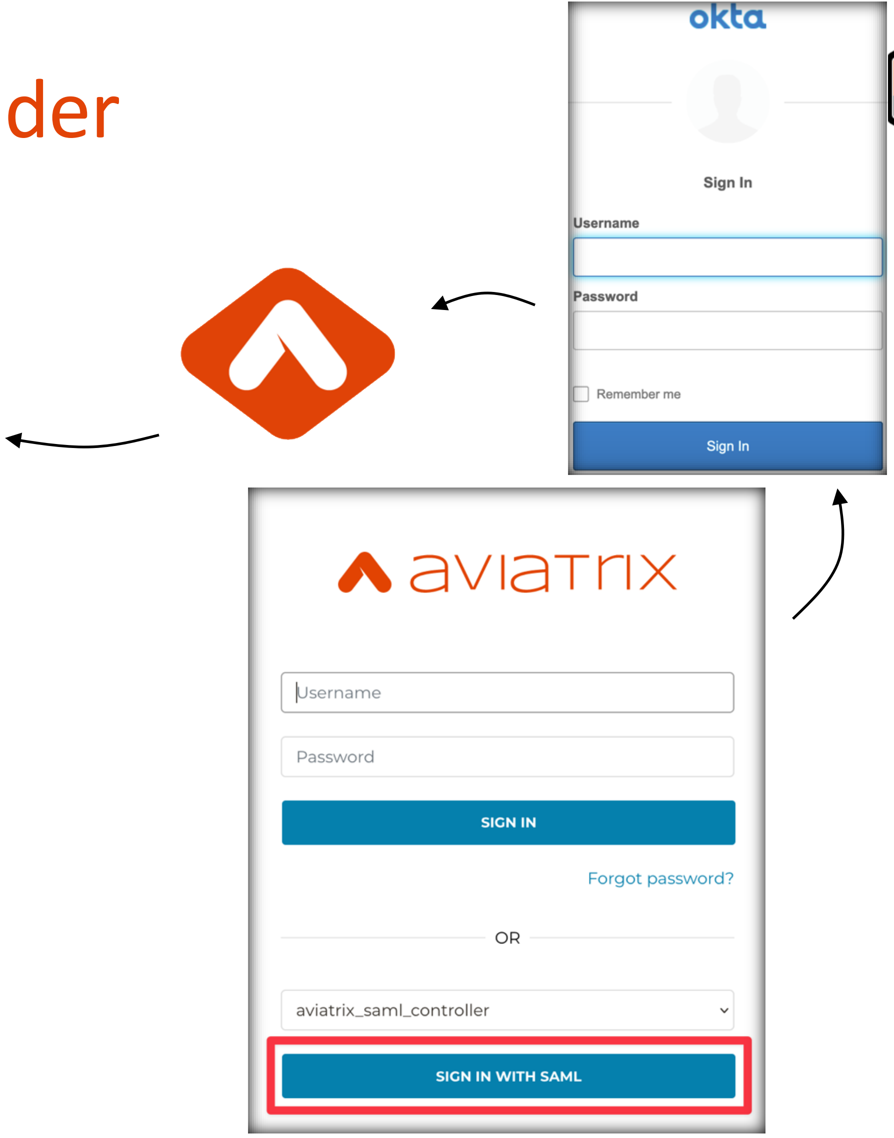
Super-Users

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

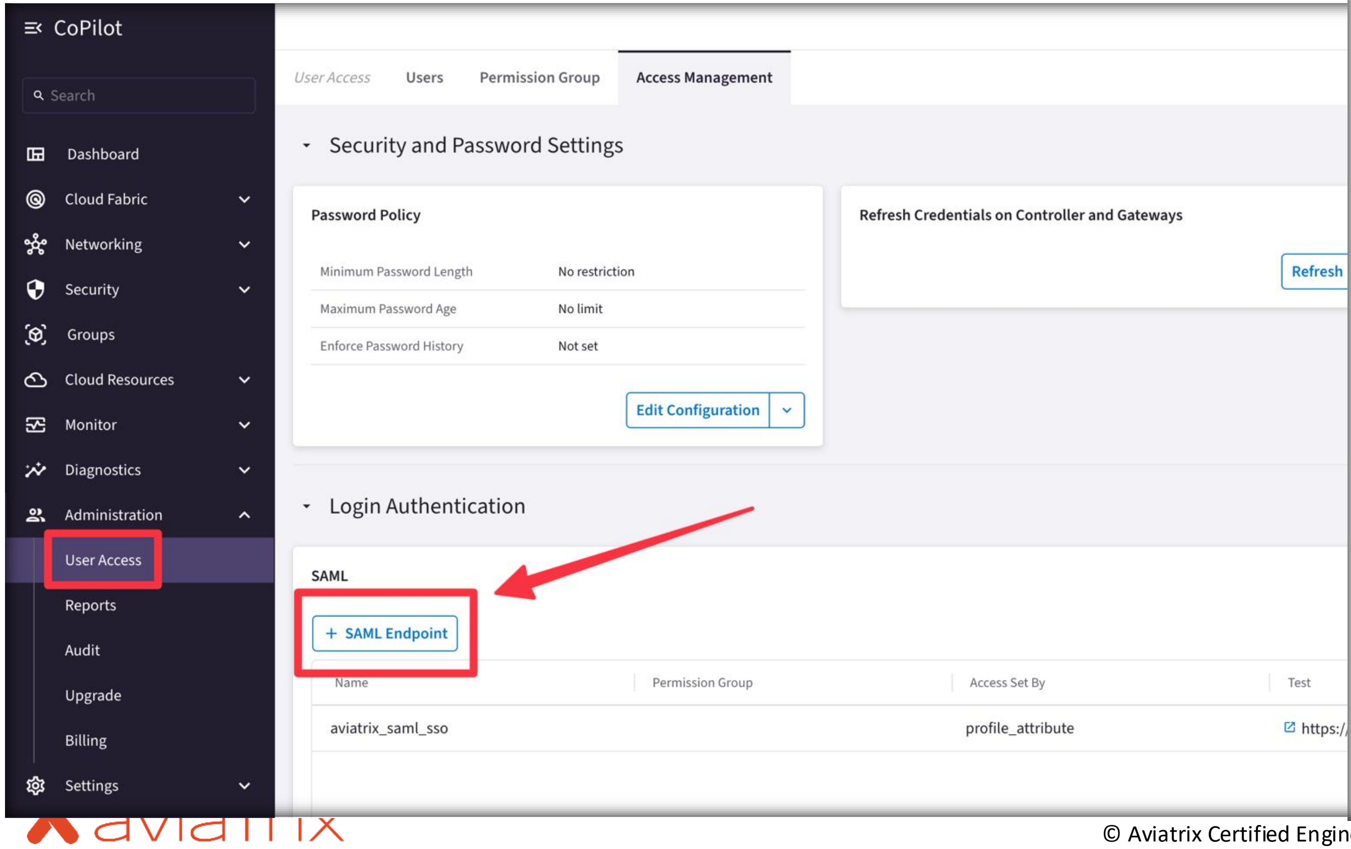
Security-User
SecOps

Developers/Read Only
Developer

Configuring SAML Authentication

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**



User Access | Users | Permission Group | Access Management

Security and Password Settings

Password Policy

Minimum Password Length	No restriction
Maximum Password Age	No limit
Enforce Password History	Not set

Edit Configuration

Refresh Credentials on Controller and Gateways

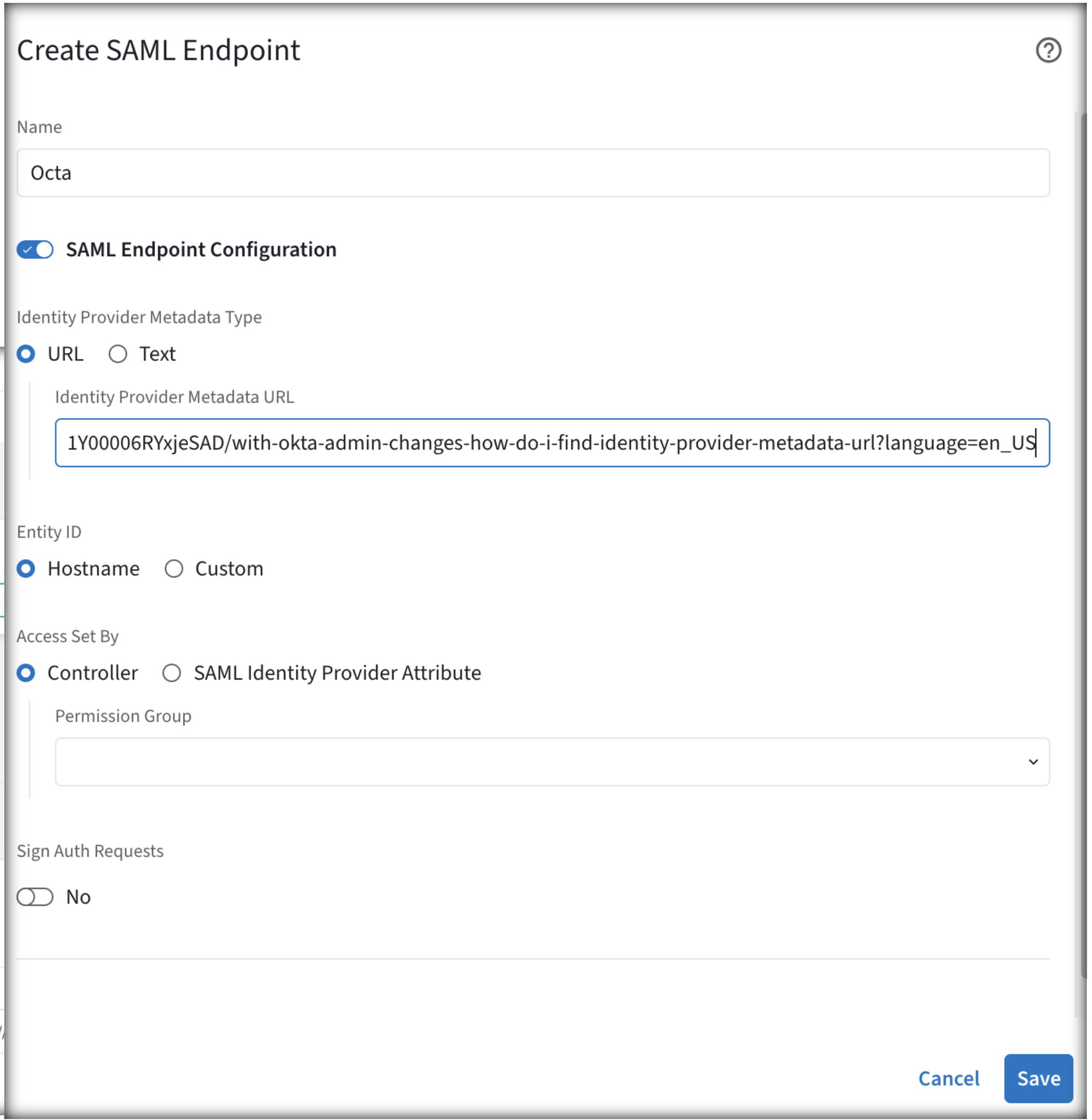
Refresh

Login Authentication

SAML

+ SAML Endpoint

Name	Permission Group	Access Set By	Test
aviatrix_saml_sso		profile_attribute	https:/



Create SAML Endpoint

Name
Octa

SAML Endpoint Configuration

Identity Provider Metadata Type
● URL ○ Text

Identity Provider Metadata URL
1Y00006RYxjeSAD/with-okta-admin-changes-how-do-i-find-identity-provider-metadata-url?language=en_US

Entity ID
● Hostname ○ Custom

Access Set By
● Controller ○ SAML Identity Provider Attribute

Permission Group

Sign Auth Requests
No

Cancel Save

THANK YOU

AVIATRIX

ACE

AVIATRIX CERTIFIED ENGINEER