NetFlow Alerts and Reports

ACE-SECURITY

Audit, Reporting and Alerts

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

ZTA should allow developers and administrators sufficient flexibility to satisfy their business requirements while using logs and audit actions to identify access behavior patterns. Policy Engine (PE) and Policy Admin (PA) components must be properly configured and monitored, and any configuration changes must be logged and subject to audit.

- Ability to replay topology

- Audit trail

- Alters based on performance, network behavior, etc.

- Out-of-the-box and custom reports

Network insights API

RBAC
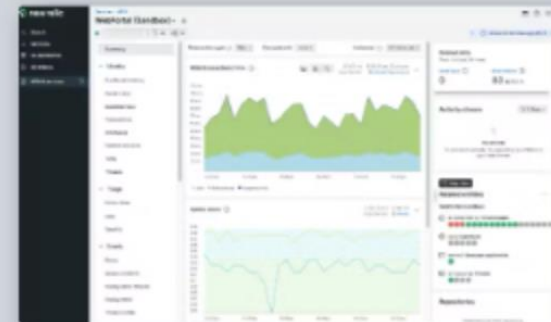
RBAC: Role-Based Access Control
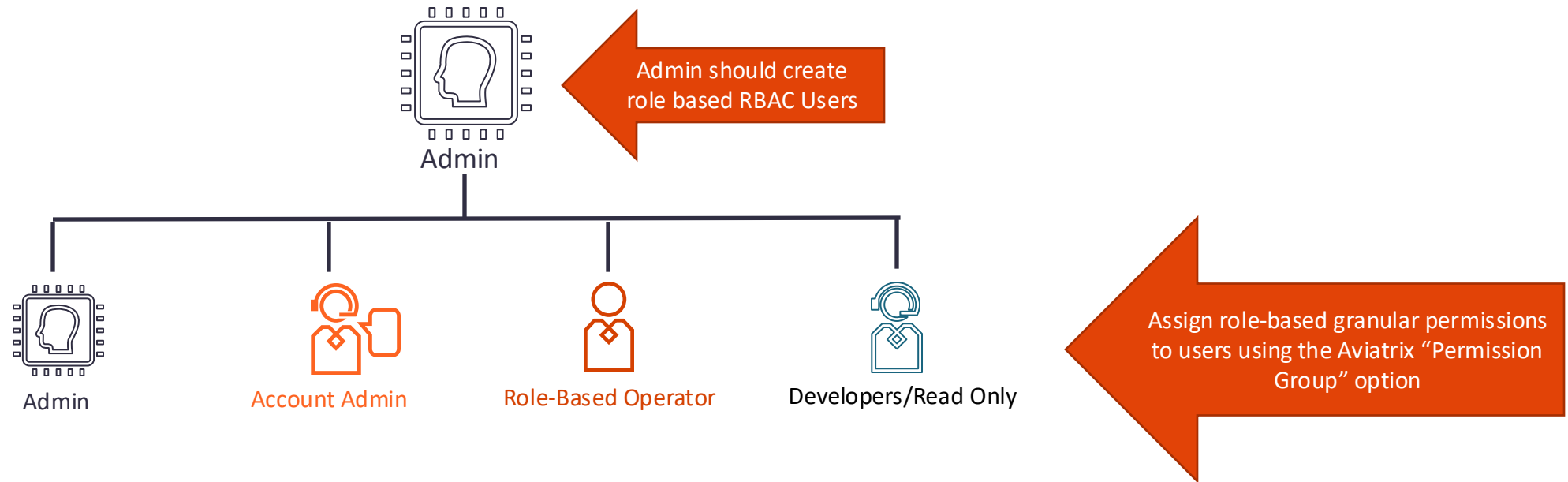
Aviatrix RBAC is based on the "Users" and "Permission Group" concept

Admin should create role based RBAC Users

Admin

Admin   Account Admin   Role-Based Operator   Developers/Read Only

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

CoPilot

Search

- Dashboard
- Cloud Fabric
- Networking
- Security
- Groups
- Cloud Resources
- Monitor
- Diagnostics
- Administration
  - User Access
  - Reports

User Access | **Users** | Permission Group | Access 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

Permission Group (part.1)

Permission Group (part.2)

Create Permission Group ?

Name

Network-team

Users

johndoe ✕   ✕ ⌄

Access Accounts

aws-account ✕   ✕ ⌄

[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

☑ **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 ✕ ⌄

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

onelogin

okta

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

okta

Sign In

Username

Password

☐ Remember me

Sign In

aviatrix

Username

Password

SIGN IN

Forgot password?

OR

aviatrix_saml_controller

SIGN IN WITH SAML

Admin/Super-Users
Admin

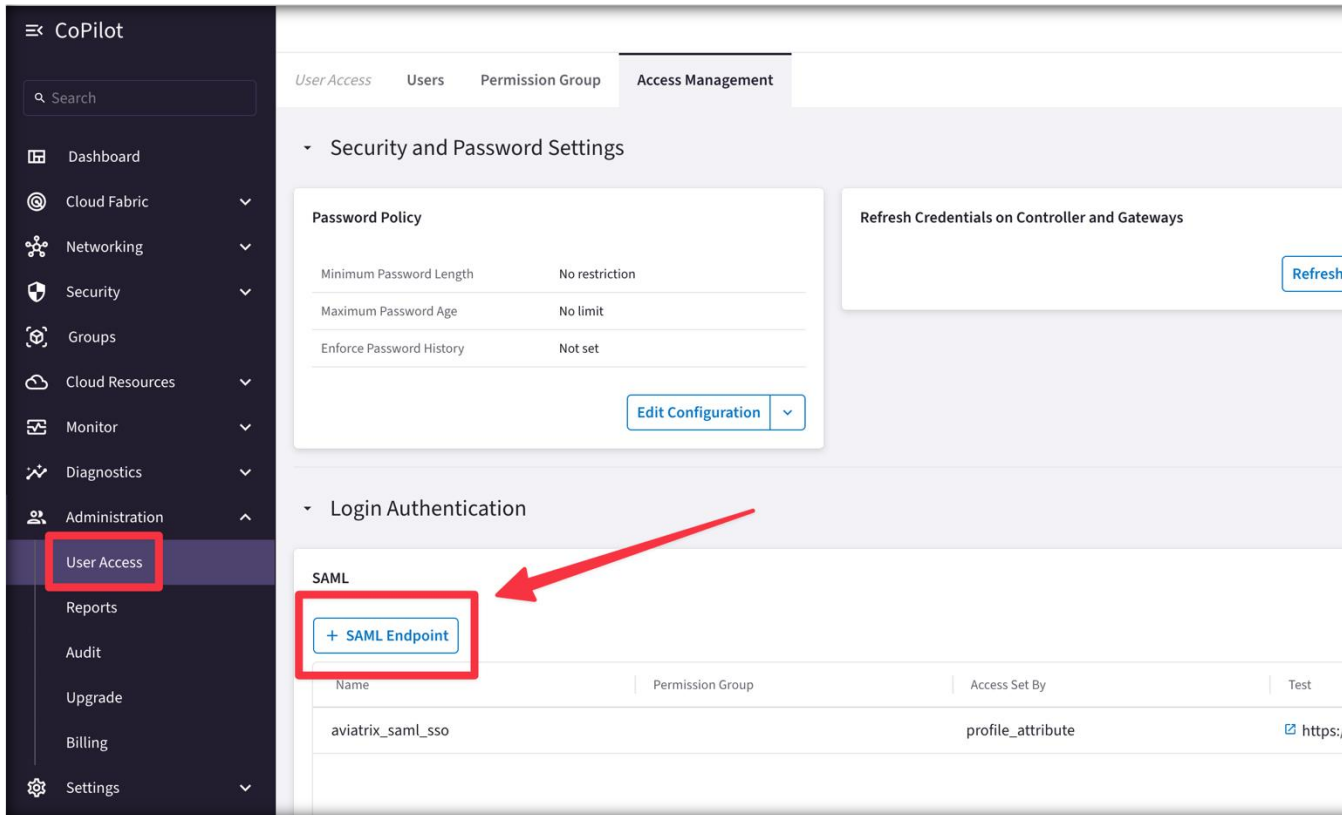Account Admins
Account-A&B

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**

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