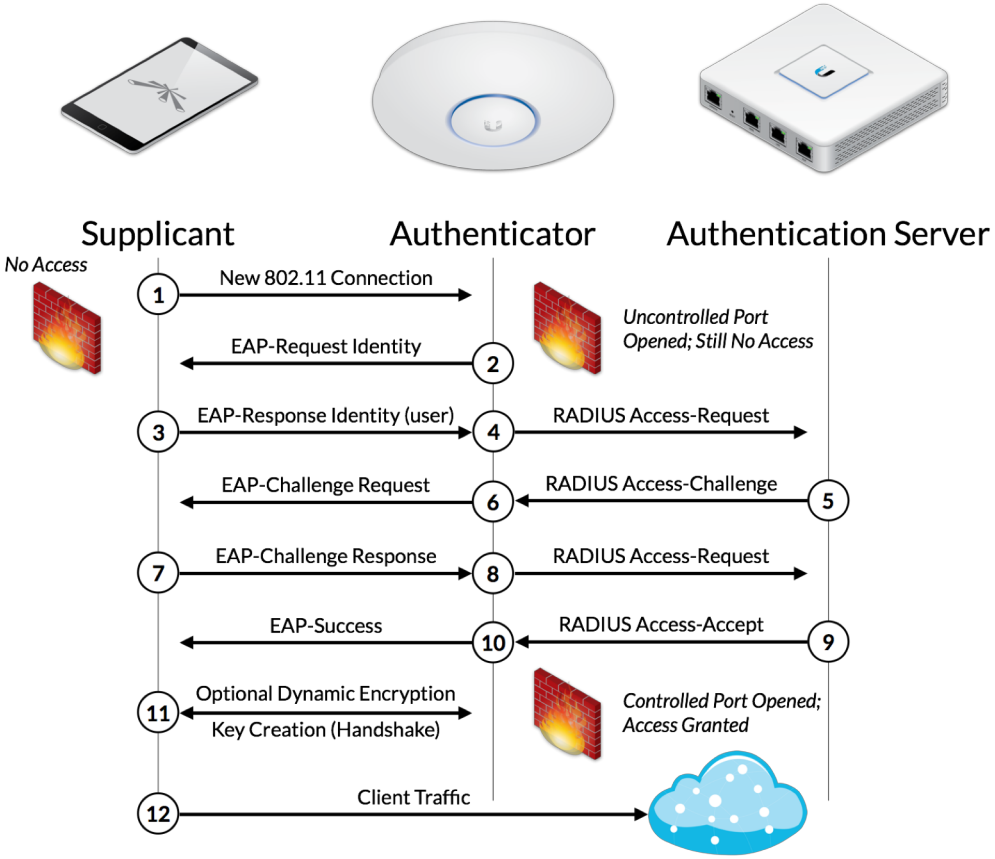
Aruba CPPM
(Clearpass Policy Manager)

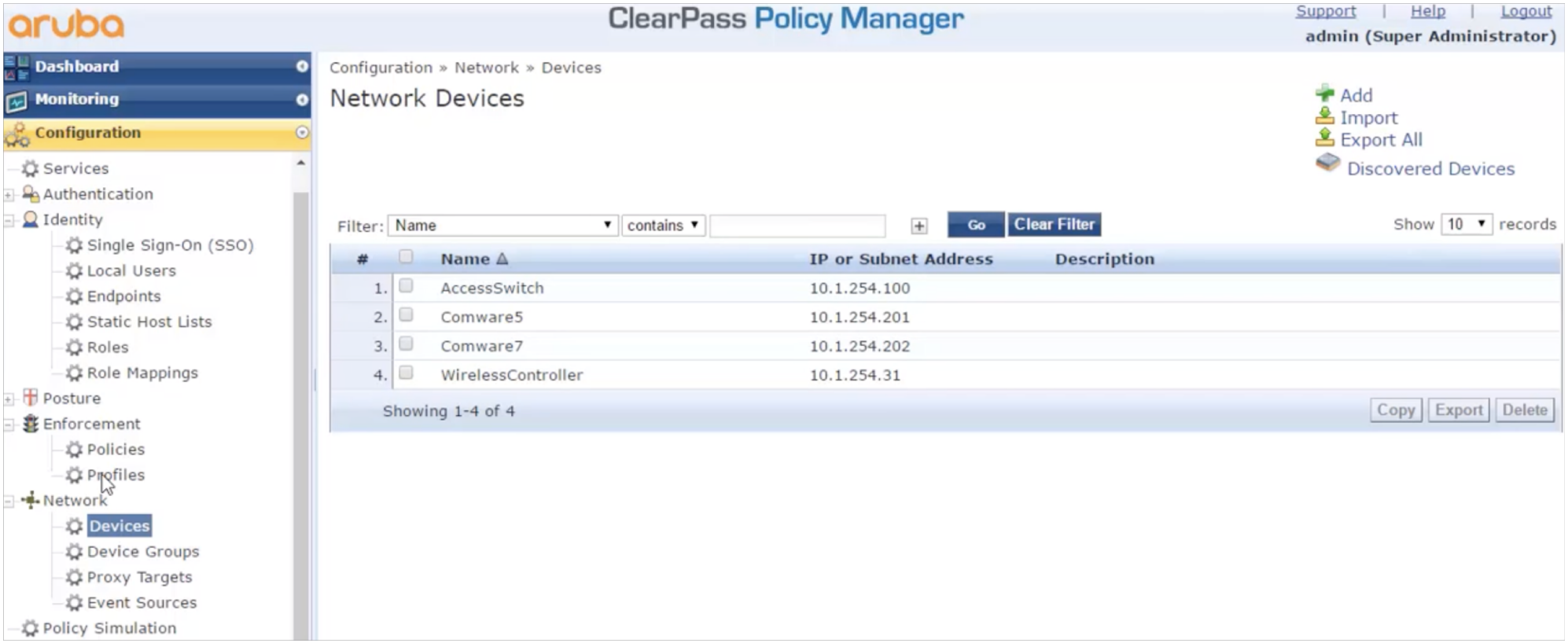
802.1X Authentication (EAP & RADIUS)



Configuring ClearPass for Mist as Radius Client

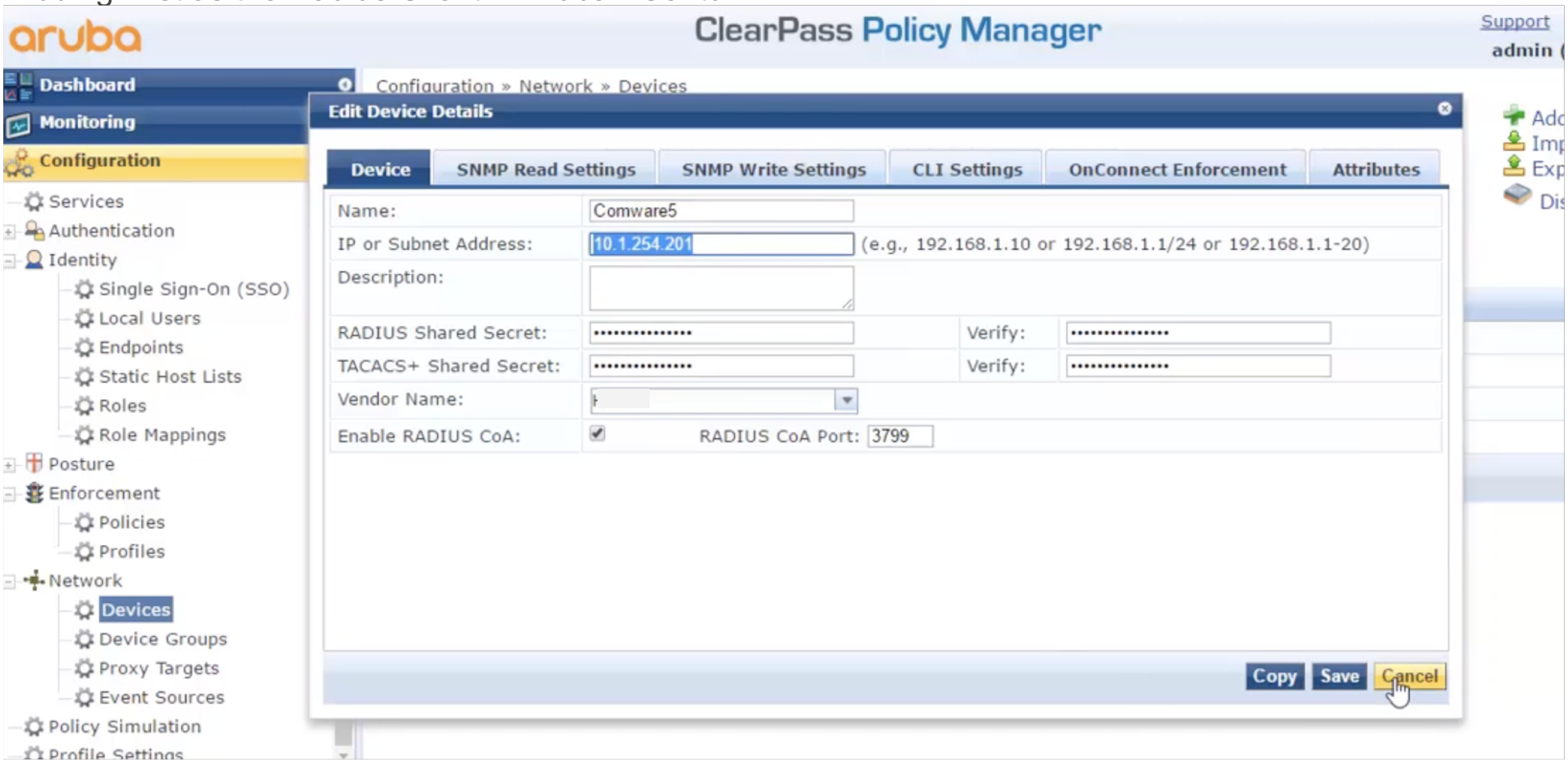
1) Adding Mist as the Radius Client in Aruba

Configuration >> Network >> Devices



Configuring ClearPass for Mist as Radius Client

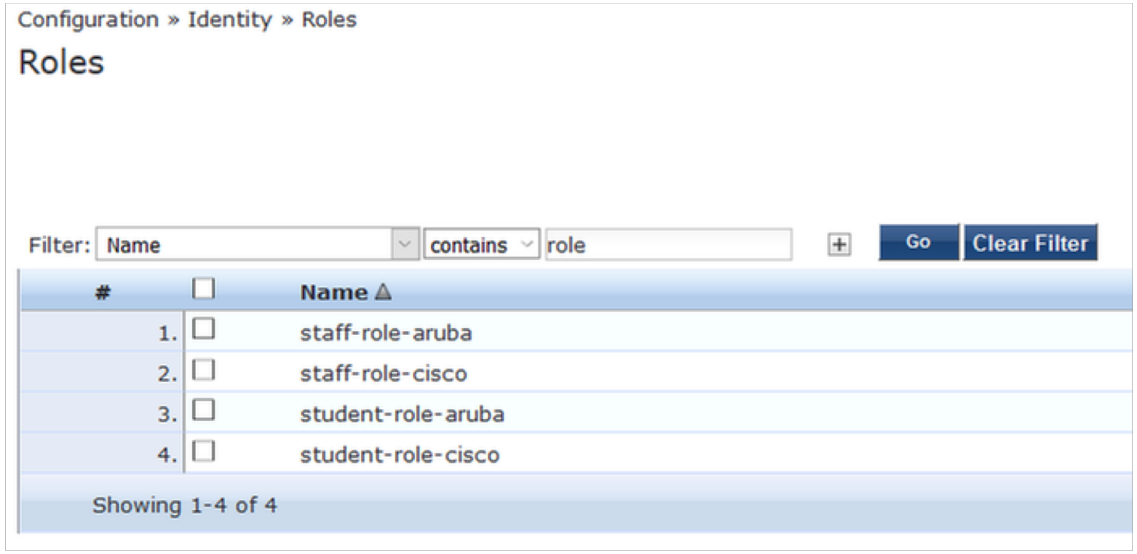
Adding Mist as the Radius Client in Aruba - Contd



Creating Roles in ClearPass

2) Adding a Role In Aruba

Configuration -> Identity -> Roles



Tie Role to the Group (AD)

3) Mapping AD Group to a Role In Aruba

Configuration -> Identity -> Roles Mappings -> Add

AVP tied to a Enforcement Profile

4) Add relevant attributes to the Enforcement Profile
(In this case, Airespace-ACL-Name and Airespace-Interface-Name)

Configuration -> Enforcement -> Profiles -> Edit Enforcement Profile

Summary | Profile | Attributes

Profile:

Name:	secure-staff-cisco
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

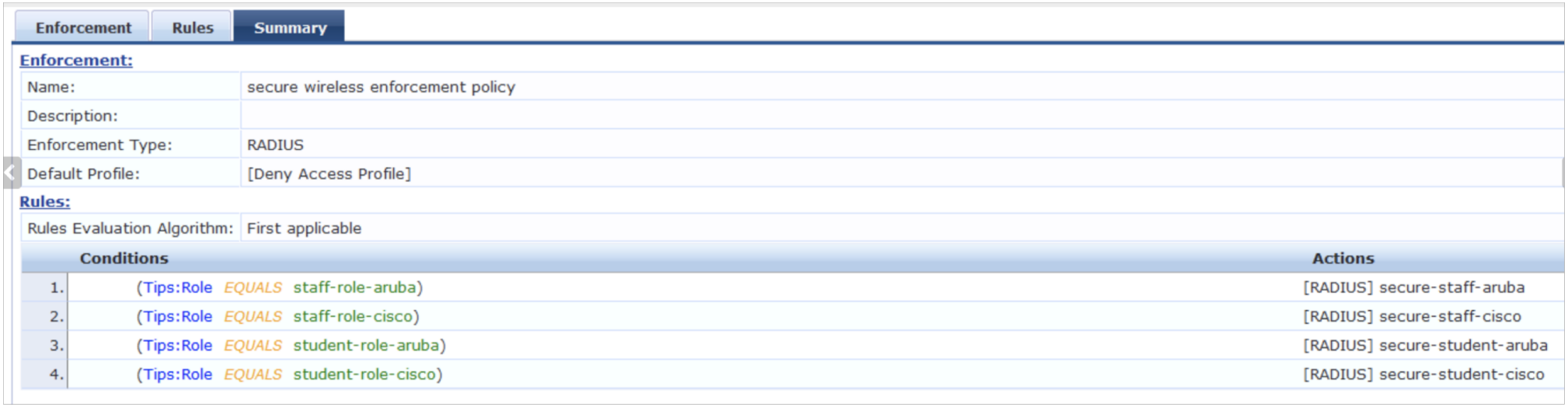
Attributes:

	Type	Name		Value
1.	Radius:Airespace	Airespace-ACL-Name	=	secure_user
2.	Radius:Airespace	Airespace-Interface-Name	=	staff_wifi

Policy Enforcement

5) Add Policy

Configuration -> Enforcement -> Policies -> Add



Enforcement | Rules | Summary

Enforcement:

Name:	secure wireless enforcement policy
Description:	
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

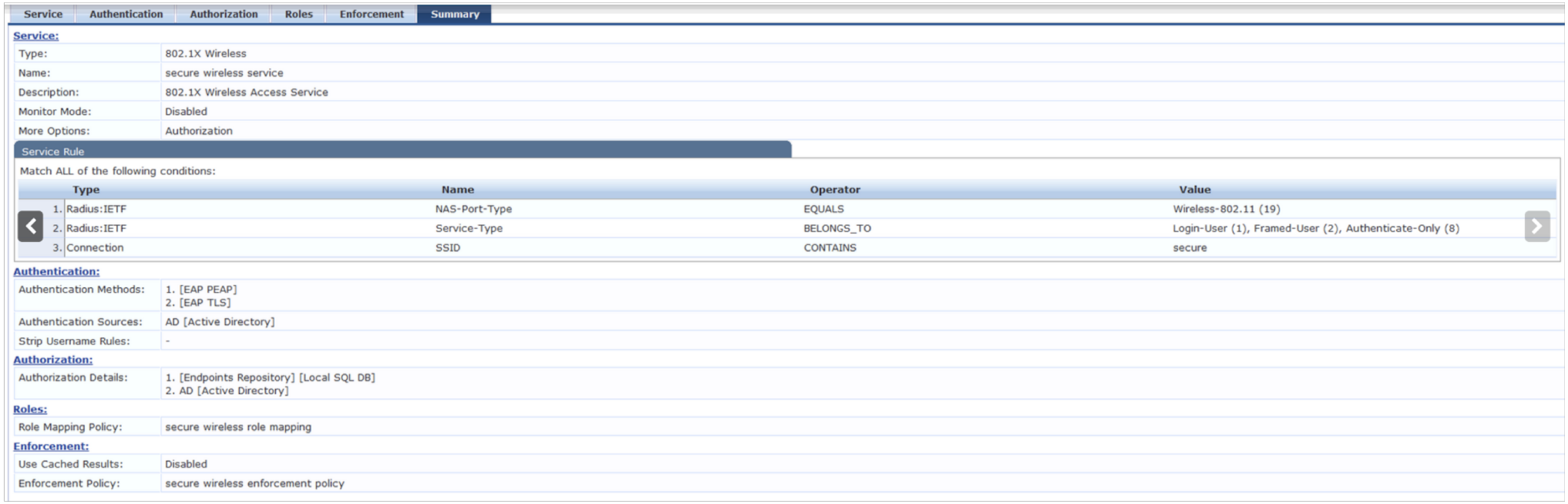
Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Tips:Role *EQUALS* staff-role-aruba)	[RADIUS] secure-staff-aruba
2.	(Tips:Role *EQUALS* staff-role-cisco)	[RADIUS] secure-staff-cisco
3.	(Tips:Role *EQUALS* student-role-aruba)	[RADIUS] secure-student-aruba
4.	(Tips:Role *EQUALS* student-role-cisco)	[RADIUS] secure-student-cisco

Bring it all together as a service

6) Configure Service to reflect the profile and policy
Configuration -> Services-> Add



Service | Authentication | Authorization | Roles | Enforcement | Summary

Service:

Type:	802.1X Wireless
Name:	secure wireless service
Description:	802.1X Wireless Access Service
Monitor Mode:	Disabled
More Options:	Authorization

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Connection	SSID	CONTAINS	secure

Authentication:

Authentication Methods:	1. [EAP PEAP] 2. [EAP TLS]
Authentication Sources:	AD [Active Directory]
Strip Username Rules:	-

Authorization:

Authorization Details:	1. [Endpoints Repository] [Local SQL DB] 2. AD [Active Directory]

Roles:

Role Mapping Policy:	secure wireless role mapping

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	secure wireless enforcement policy