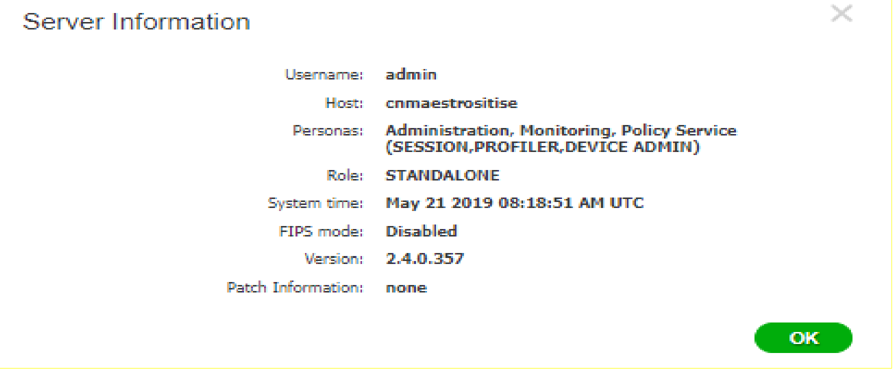
This Document is best viewed in Web Layout

Setting up Cisco-ISE for RADIUS Authentication to Support Cambium cnPilot Products.

Setting up Cisco ISE for RADIUS Services

Overview

This document presents basic configuration of Cisco ISE 2.4.0.357 as RADIUS server.



Server Information

Username:	admin
Host:	cnmaestrositise
Personas:	Administration, Monitoring, Policy Service (SESSION,PROFILER,DEVICE ADMIN)
Role:	STANDALONE
System time:	May 21 2019 08:18:51 AM UTC
FIPS mode:	Disabled
Version:	2.4.0.357
Patch Information:	none

Pre-requisites

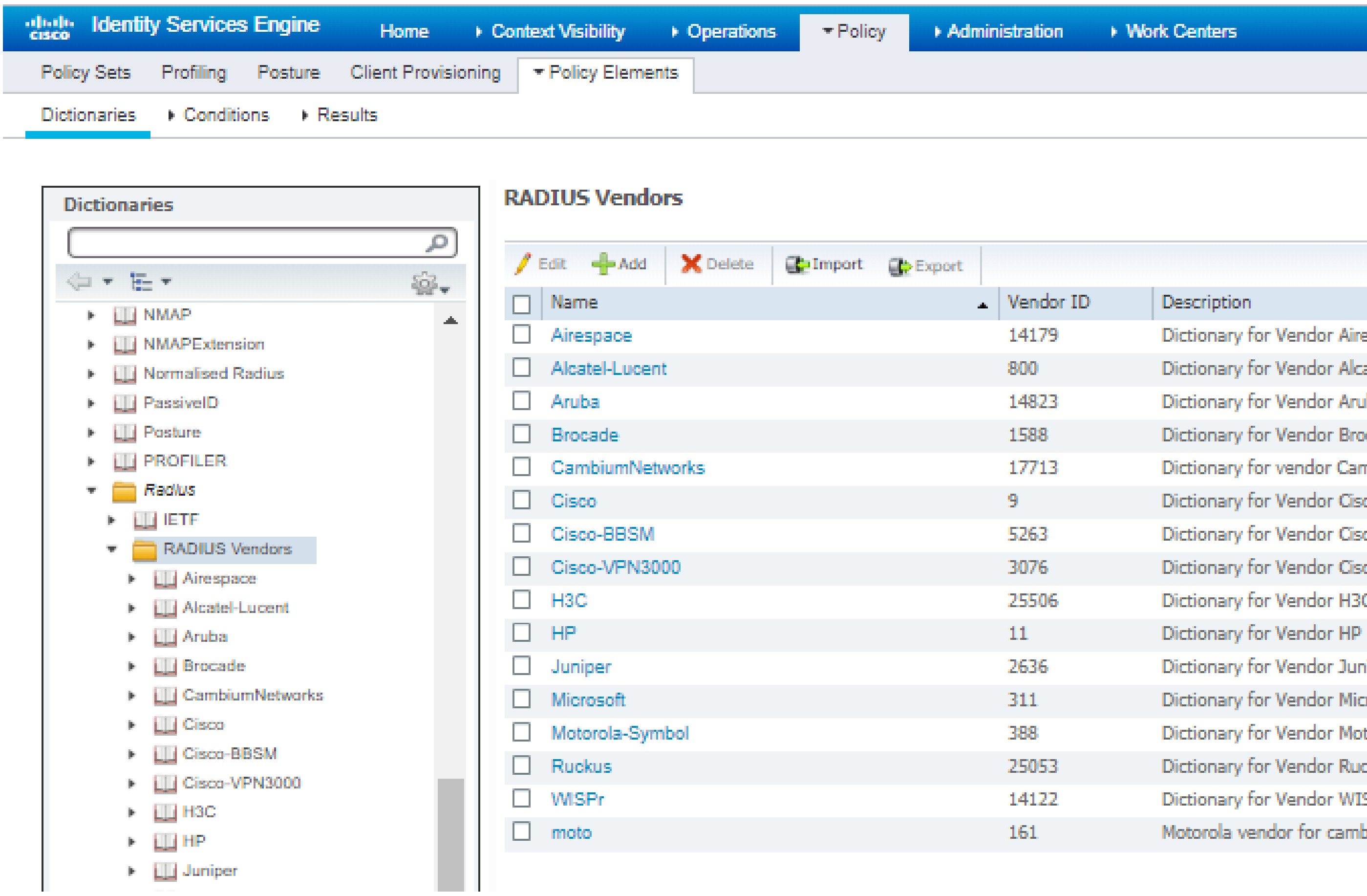
1. Cisco ISE Installed on VM
2. Latest Chrome/Firefox browser

Configuration:

The steps below configure the Cisco-ISE server for RADIUS authentication to be used by Cambium products.

Step1: Adding new RADIUS Vendor

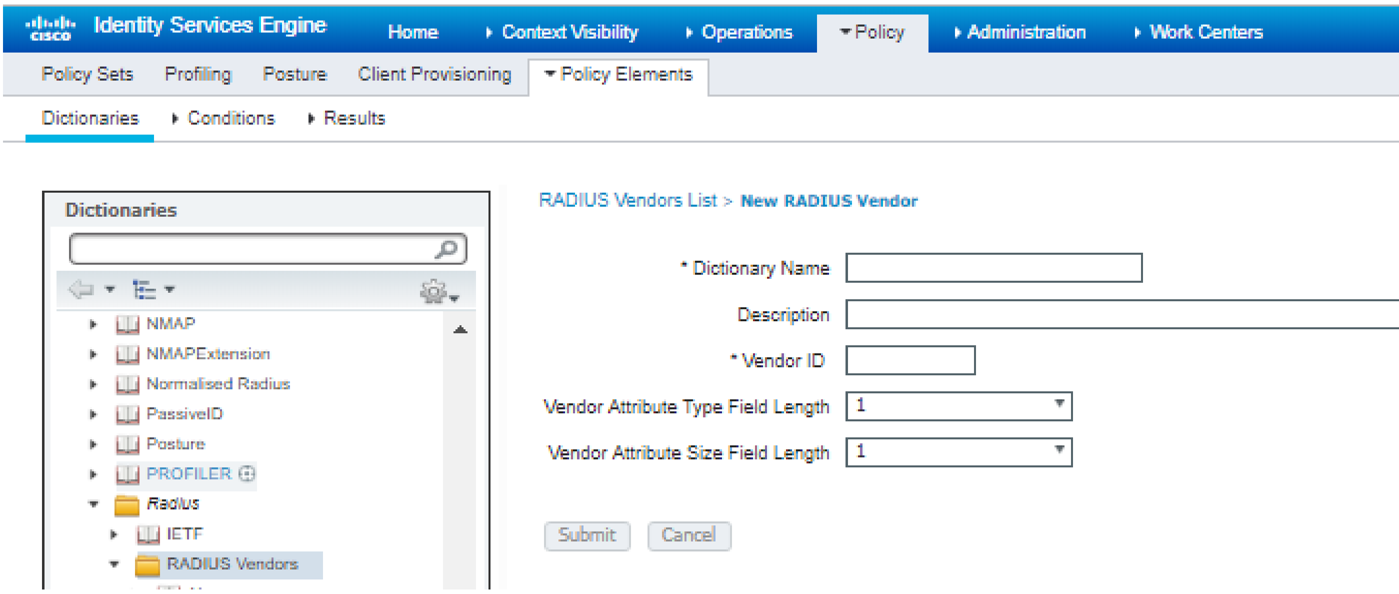
1. Navigate to Policy > Policy Elements > Dictionaries > System > Radius > RADIUS Vendors



RADIUS Vendors

□	Name	Vendor ID	Description
□	Airespace	14179	Dictionary for Vendor Aire
□	Alcatel-Lucent	800	Dictionary for Vendor Alca
□	Aruba	14823	Dictionary for Vendor Aru
□	Brocade	1588	Dictionary for Vendor Bro
□	CambiumNetworks	17713	Dictionary for vendor Cam
□	Cisco	9	Dictionary for Vendor Cisc
□	Cisco-BBSM	5263	Dictionary for Vendor Cisc
□	Cisco-VPN3000	3076	Dictionary for Vendor Cisc
□	H3C	25506	Dictionary for Vendor H3C
□	HP	11	Dictionary for Vendor HP
□	Juniper	2636	Dictionary for Vendor Jun
□	Microsoft	311	Dictionary for Vendor Mic
□	Motorola-Symbol	388	Dictionary for Vendor Mot
□	Ruckus	25053	Dictionary for Vendor Ruc
□	WISPr	14122	Dictionary for Vendor WIS
□	moto	161	Motorola vendor for camb

2. Click Add and provide proper details in the required fields, then click on submit.

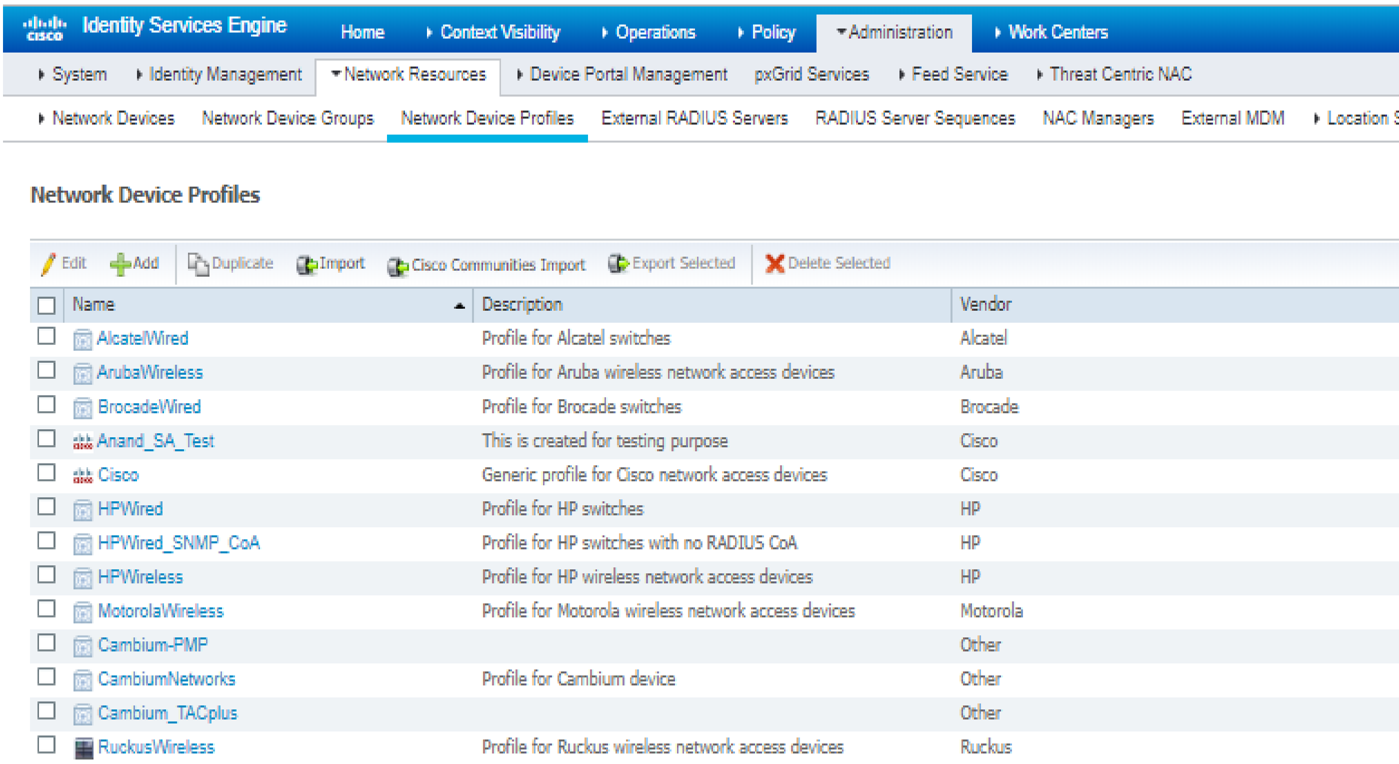


RADIUS Vendors List > **New RADIUS Vendor**

* Dictionary Name
Description
* Vendor ID
Vendor Attribute Type Field Length: 1
Vendor Attribute Size Field Length: 1

Step2: Adding Network Device Profiles

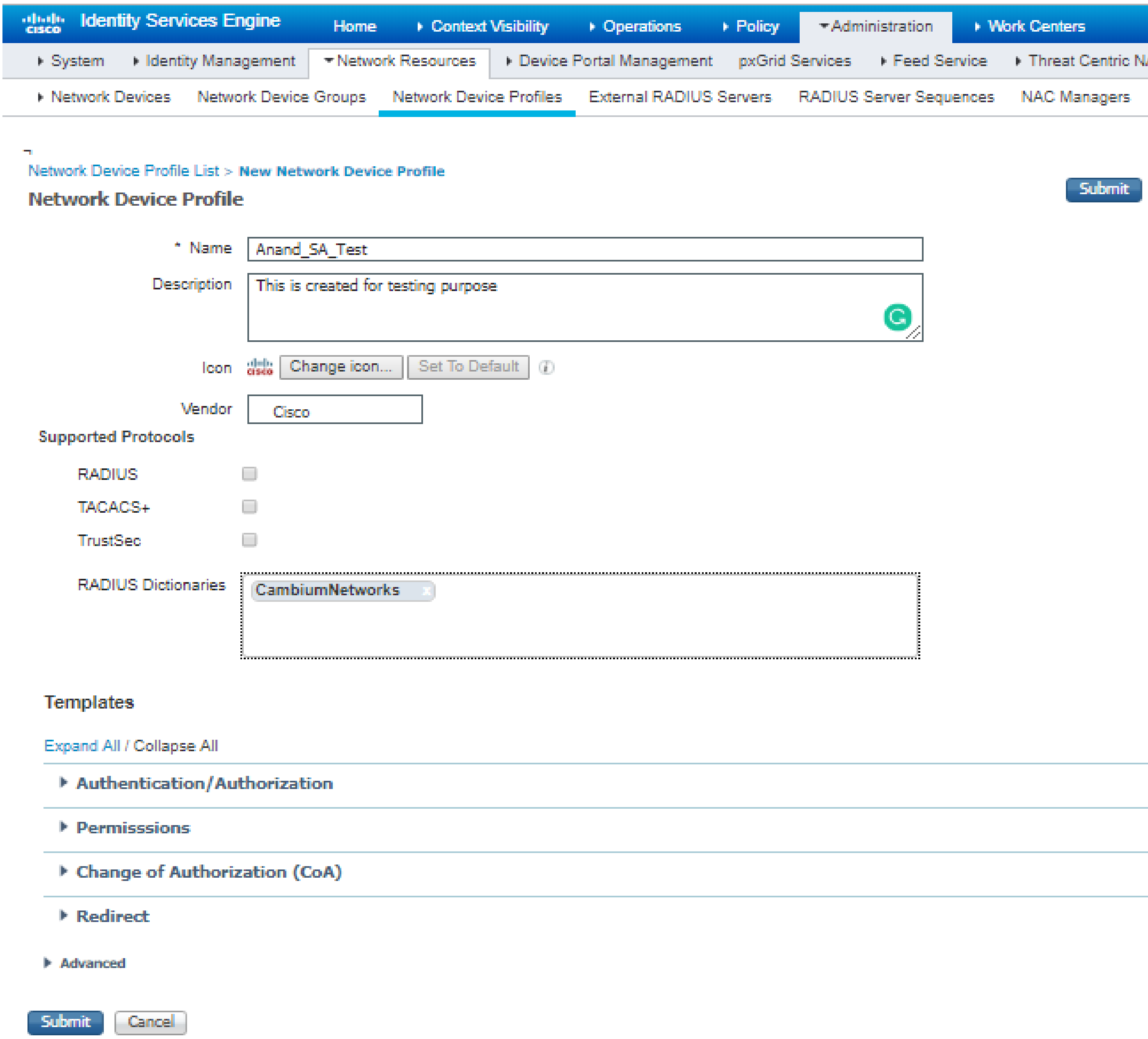
1. Navigate to Administration > Network Resources > Network Device Profiles > Click +Add



Network Device Profiles

□	Name	Description	Vendor
□	AlcatelWired	Profile for Alcatel switches	Alcatel
□	ArubaWireless	Profile for Aruba wireless network access devices	Aruba
□	BrocadeWired	Profile for Brocade switches	Brocade
□	Anand_SA_Test	This is created for testing purpose	Cisco
□	Cisco	Generic profile for Cisco network access devices	Cisco
□	HPWired	Profile for HP switches	HP
□	HPWired_SNMP_CoA	Profile for HP switches with no RADIUS CoA	HP
□	HPWireless	Profile for HP wireless network access devices	HP
□	MotorolaWireless	Profile for Motorola wireless network access devices	Motorola
□	Cambium-PMP		Other
□	CambiumNetworks	Profile for Cambium device	Other
□	Cambium_TACplus		Other
□	RuckusWireless	Profile for Ruckus wireless network access devices	Ruckus

2. Provide valid details and submit



Network Device Profile

* Name: Anand_SA_Test

Description: This is created for testing purpose

Vendor: Cisco

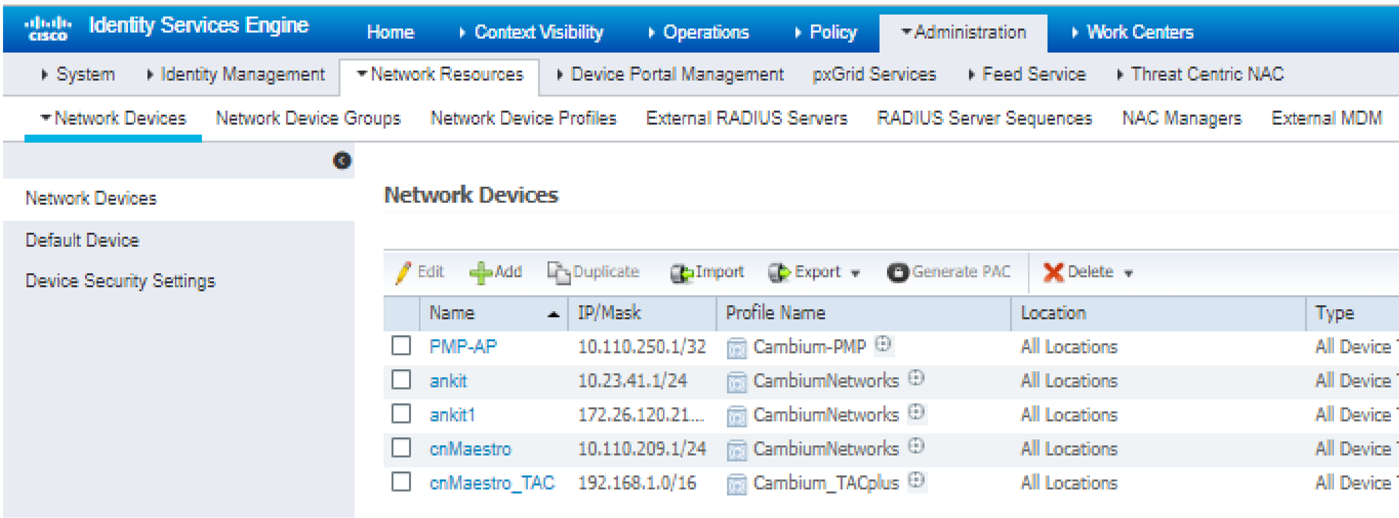
Supported Protocols

- RADIUS □
- TACACS+ □
- TrustSec □

RADIUS Dictionaries: CambiumNetworks

Step3: Adding Network Device

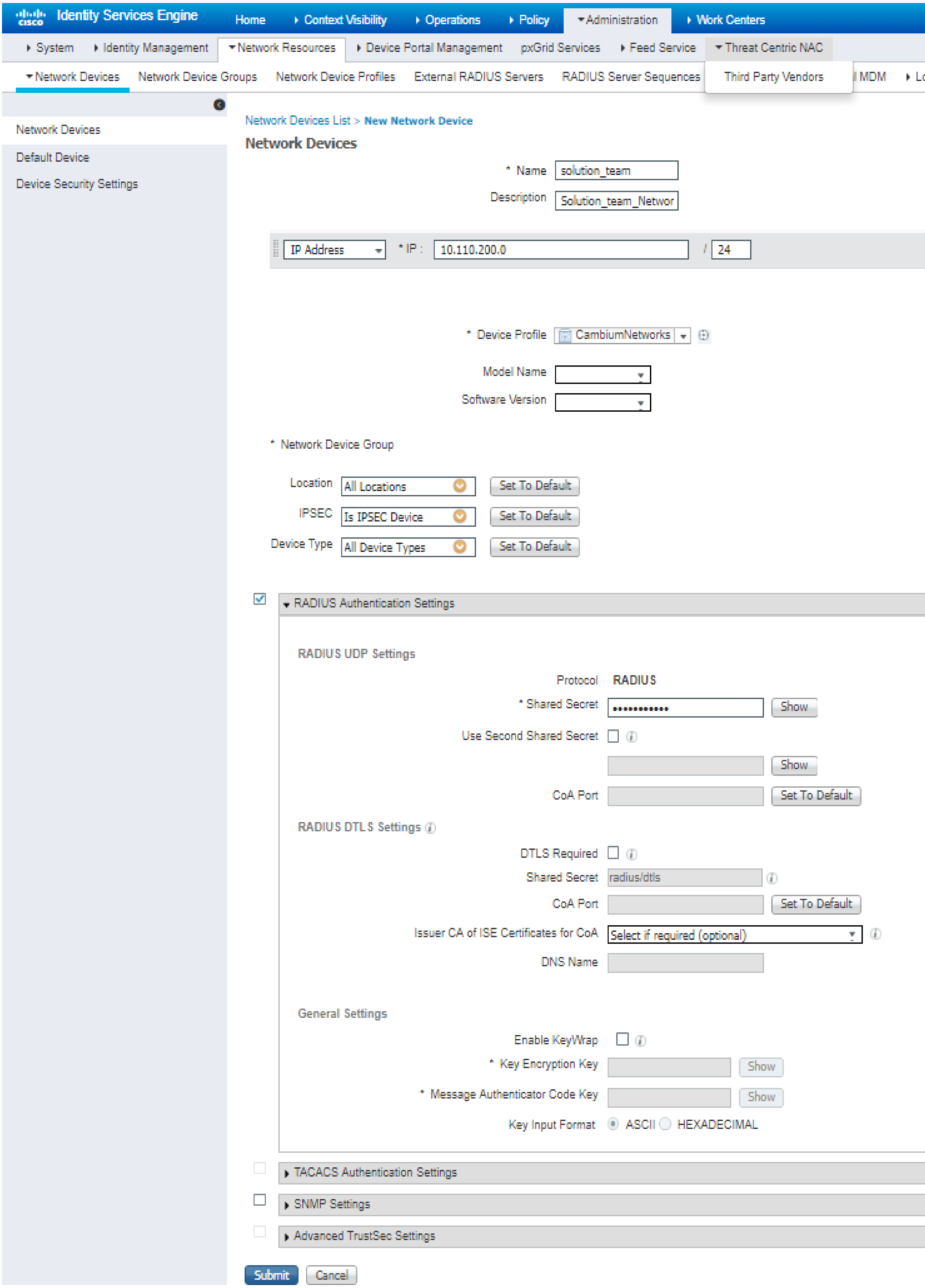
1. Navigate to Administration > Network Resources > Network Devices



Network Devices

	Name	IP/Mask	Profile Name	Location	Type
□	PMP-AP	10.110.250.1/32	Cambium-PMP	All Locations	All Device
□	ankit	10.23.41.1/24	CambiumNetworks	All Locations	All Device
□	ankit1	172.26.120.21...	CambiumNetworks	All Locations	All Device
□	cnMaestro	10.110.209.1/24	CambiumNetworks	All Locations	All Device
□	cnMaestro_TAC	192.168.1.0/16	Cambium_TACplus	All Locations	All Device

2. Click +Add ,
3. Provide Name, description, IP Address/Range,
4. Select the newly created device profile. (in the previous step)
5. Let Network device group values be default.
6. Enable Radius Authentication Settings and configure Shared secret.
7. Save



Network Devices

* Name: solution_team

Description: Solution_team_Networ

IP Address * IP : 10.110.200.0 / 24

* Device Profile: CambiumNetworks

Model Name:

Software Version:

* Network Device Group

Location: All Locations [Set To Default]

IPSEC: Is IPSEC Device [Set To Default]

Device Type: All Device Types [Set To Default]

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: •••••••••••• [Show]

Use Second Shared Secret: □

[Show]

CoA Port: [Set To Default]

RADIUS DTLS Settings

DTLS Required: □

Shared Secret: radius/dtls

CoA Port: [Set To Default]

Issuer CA of ISE Certificates for CoA: Select if required (optional)

DNS Name:

General Settings

Enable KeyWrap: □

* Key Encryption Key: [Show]

* Message Authenticator Code Key: [Show]

Key Input Format: ● ASCII ○ HEXADECIMAL

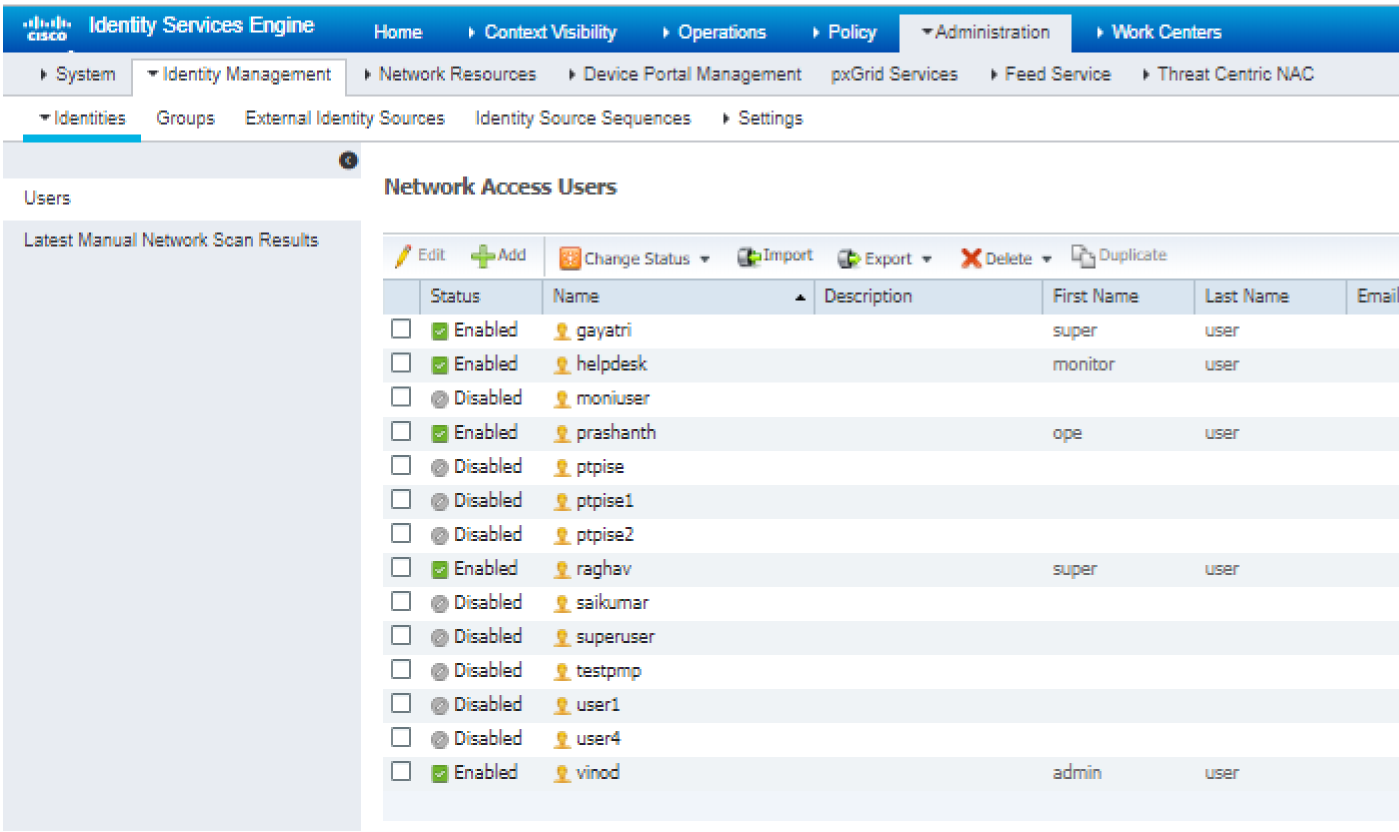
□ TACACS Authentication Settings

□ SNMP Settings

□ Advanced TrustSec Settings

Step 4: Creating User Identities

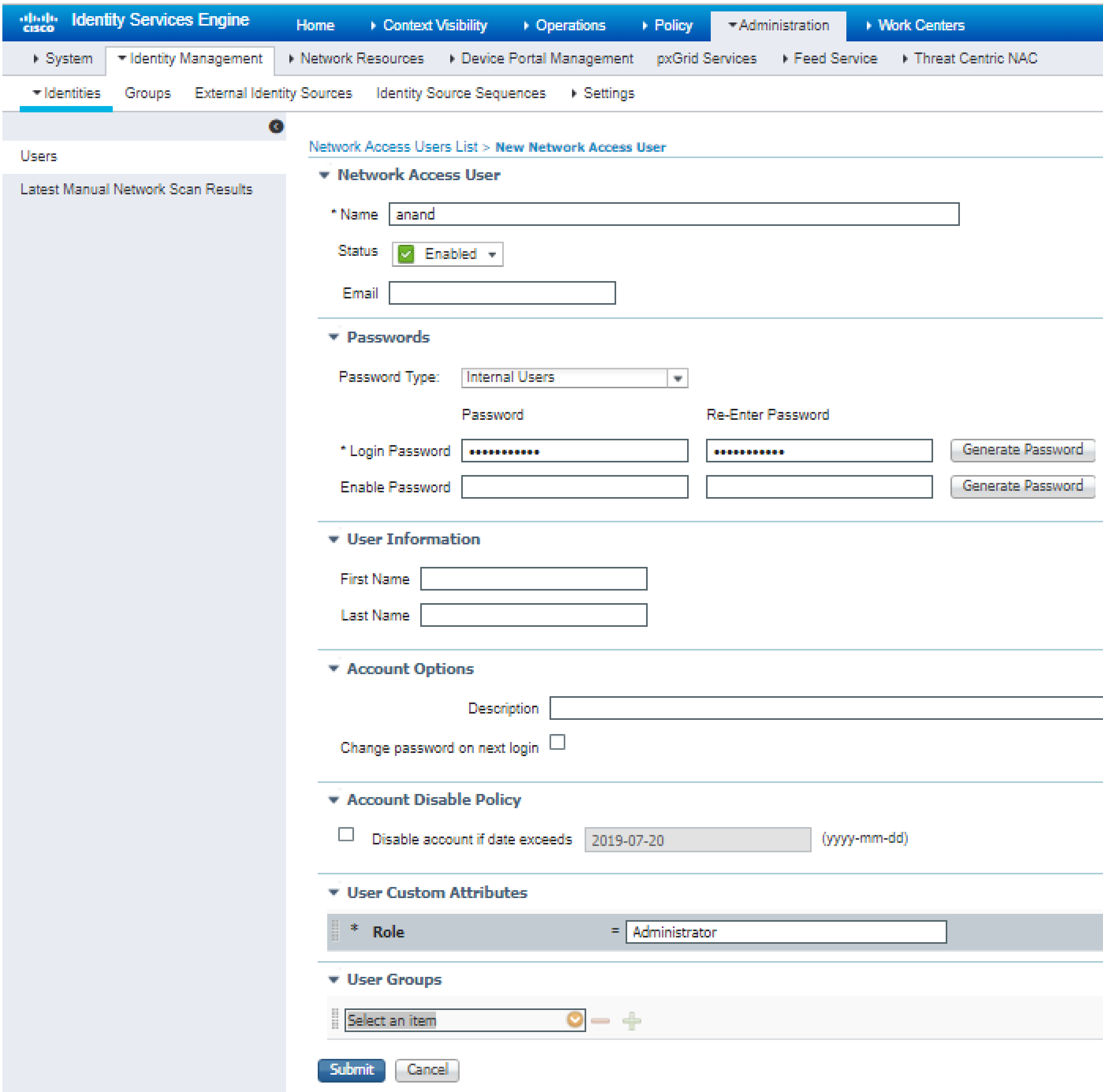
1. Navigate to Identity Management > Identities >



Network Access Users

	Status	Name	Description	First Name	Last Name	Email
□	Enabled	gayatri		super	user	
□	Enabled	helpdesk		monitor	user	
□	Disabled	moniuser				
□	Enabled	prashanth		ope	user	
□	Disabled	ptpise				
□	Disabled	ptpise1				
□	Disabled	ptpise2				
□	Enabled	raghav		super	user	
□	Disabled	saikumar				
□	Disabled	superuser				
□	Disabled	testpmp				
□	Disabled	user1				
□	Disabled	user4				
□	Enabled	vinod		admin	user	

2. Click + Add and fill the details as mentioned below
3. Name: Name of the user (need to be unique)
4. Status: Enabled by default
5. Email: Email address of the user (optional)
6. Login Password: Password as per password policy
7. User Custom Attributes : Assign a role for the user
8. Click submit



Network Access User

* Name: anand

Status: ☑ Enabled

Email:

Passwords

Password Type: Internal Users

	Password	Re-Enter Password
* Login Password	••••••••••••	••••••••••••
Enable Password		

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login □

Account Disable Policy

□ Disable account if date exceeds 2019-07-20 (yyyy-mm-dd)

User Custom Attributes

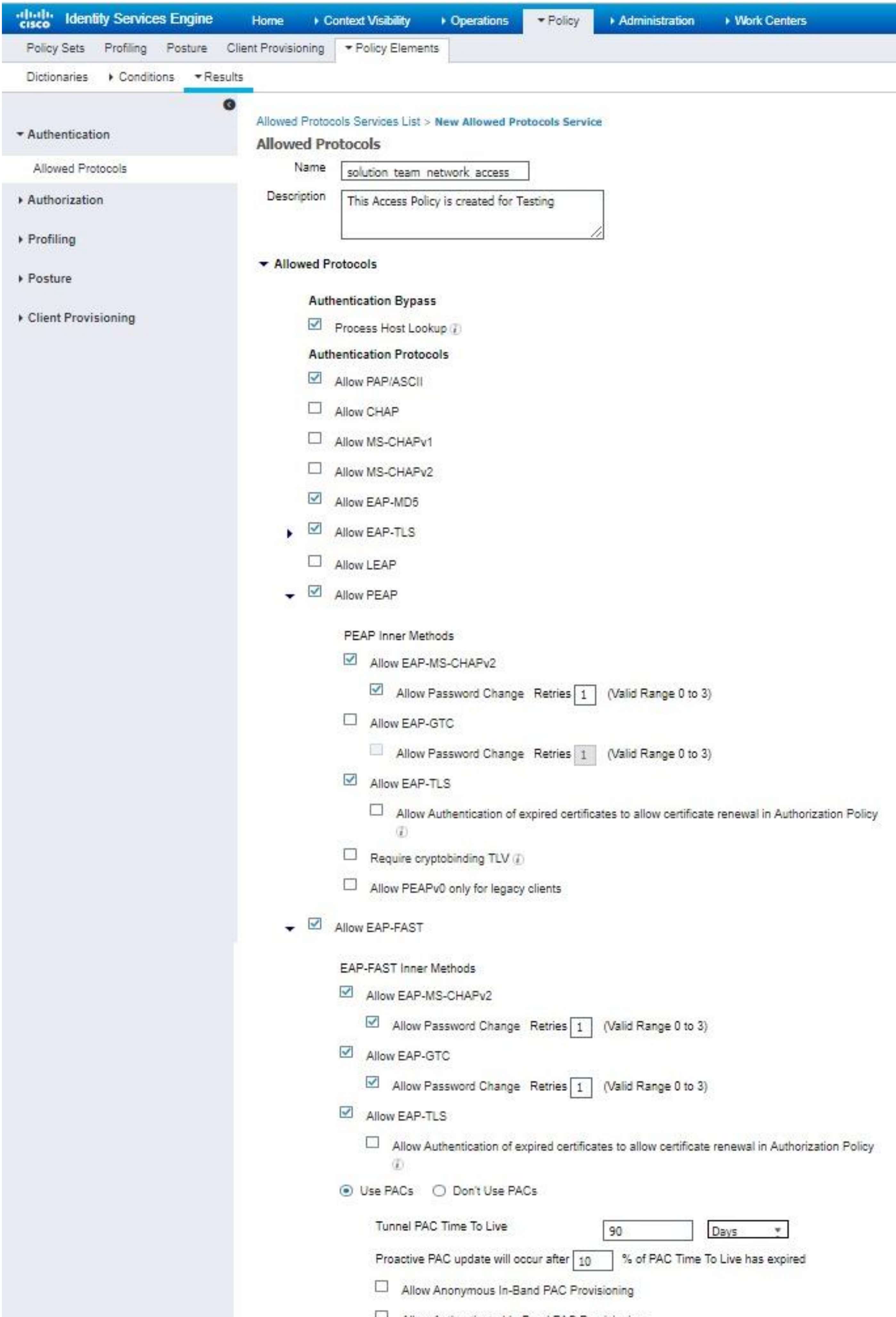
* Role = Administrator

User Groups

Select an item

Step 5: Selection of Authentication Protocols

1. Navigate to Policy > Policy Elements > Results
2. Navigate to Authentication > Allowed Protocols



Allowed Protocols Services List > **New Allowed Protocols Service**

Allowed Protocols

Name: solution_team_network_access

Description: This Access Policy is created for Testing

Allowed Protocols

Authentication Bypass

☑ Process Host Lookup

Authentication Protocols

☑ Allow PAP/ASCII

□ Allow CHAP

□ Allow MS-CHAPv1

□ Allow MS-CHAPv2

☑ Allow EAP-MD5

☑ Allow EAP-TLS

□ Allow LEAP

☑ Allow PEAP

PEAP Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

□ Allow EAP-GTC

□ Allow Password Change Retries 1 (Valid Range 0 to 3)

☑ Allow EAP-TLS

□ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

□ Require cryptobinding TLV

□ Allow PEAPv0 only for legacy clients

☑ Allow EAP-FAST

EAP-FAST Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

☑ Allow EAP-GTC

☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

☑ Allow EAP-TLS

□ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

● Use PACs ○ Don't Use PACs

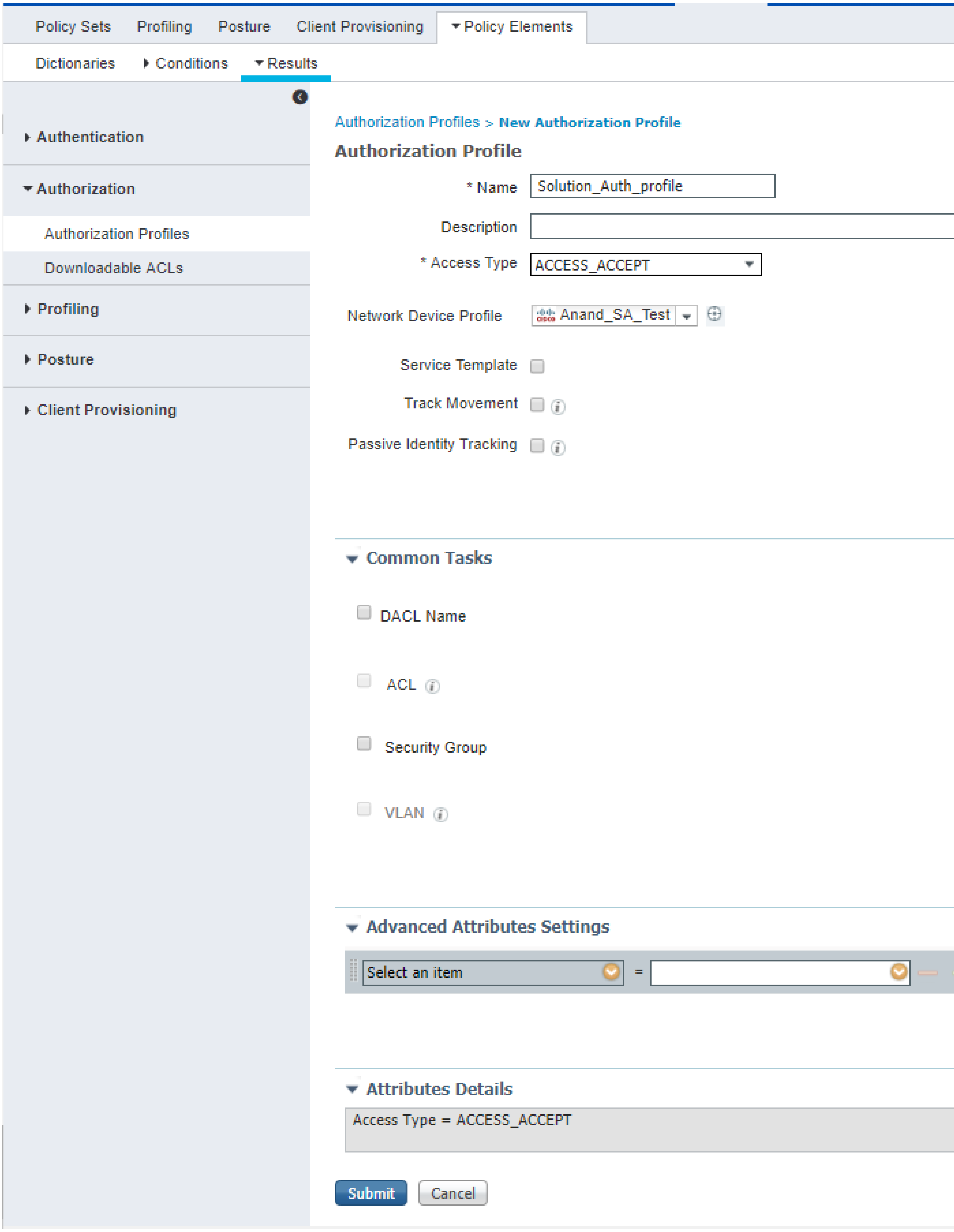
Tunnel PAC Time To Live 90 Days

Proactive PAC update will occur after 10 % of PAC Time To Live has expired

□ Allow Anonymous In-Band PAC Provisioning

Step 6: Creation of Authorization Profiles

1. Navigate to Policy > Policy Elements > Results
2. Navigate to Authorization > Authorization Profiles and click + Add
3. Name: Provide valid name
4. Access Type: ACCESS ACCEPT
5. Network Device Profile: Select the profile you created for Radius
6. Click on Submit



Authorization Profile

* Name: Solution_Auth_profile

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Anand_SA_Test

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

□ DACL Name

□ ACL

□ Security Group

□ VLAN

Advanced Attributes Settings

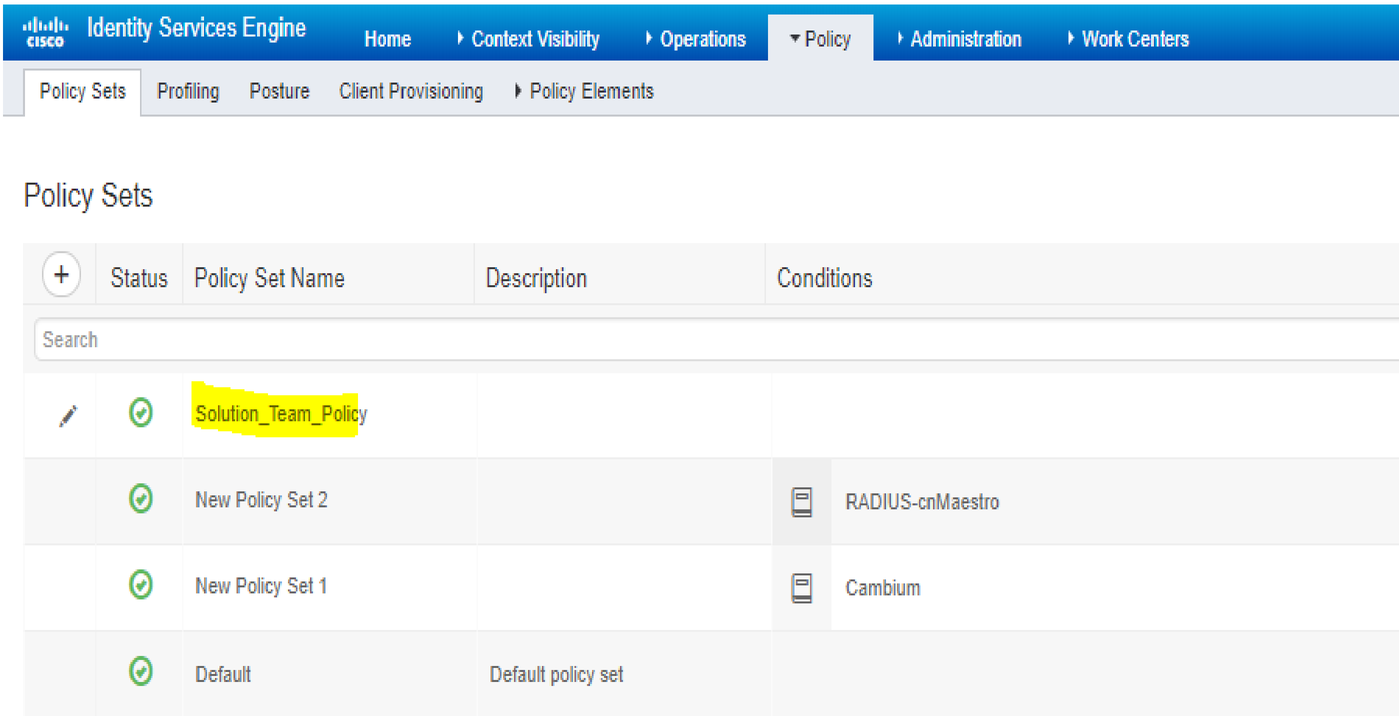
Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT

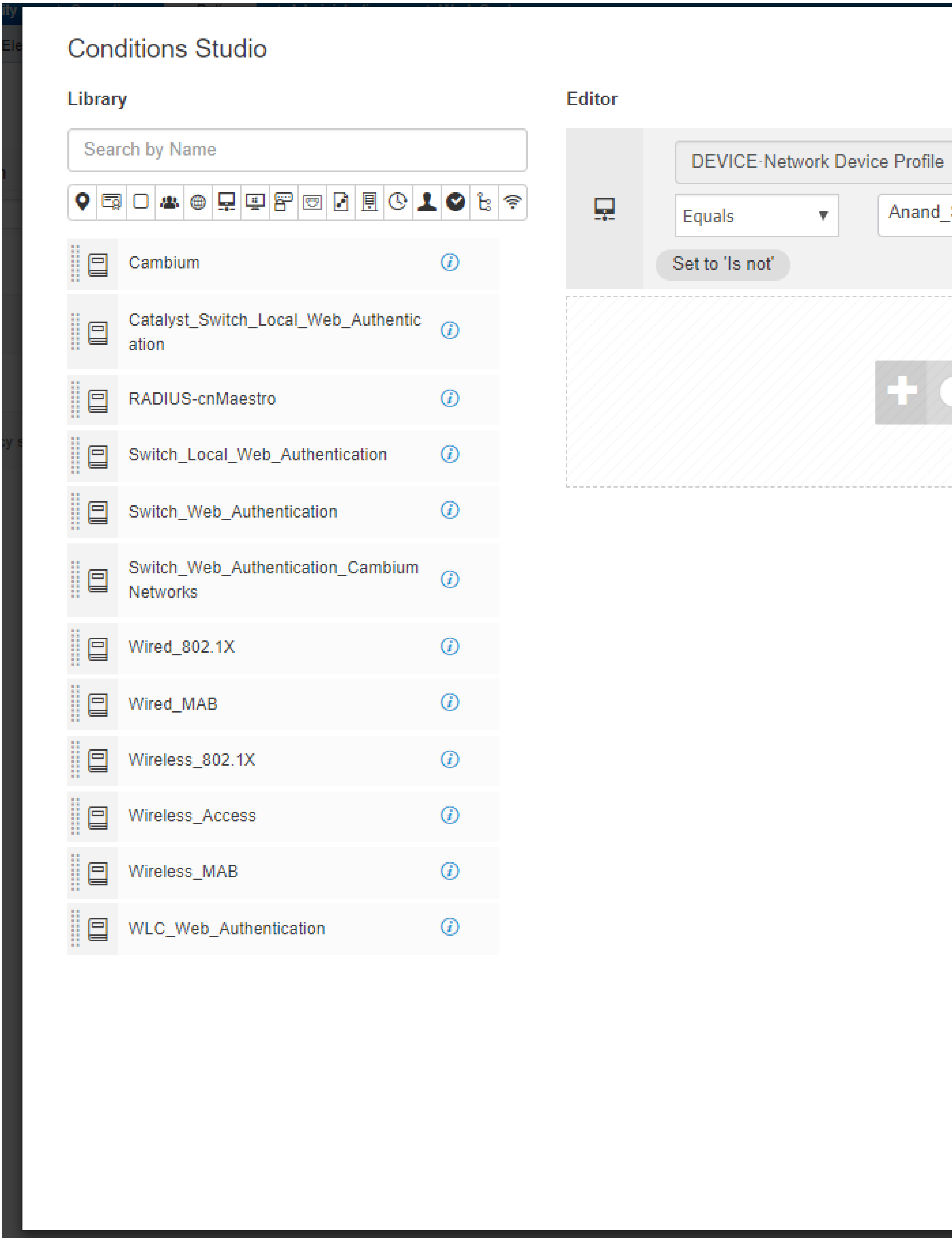
Step7: Creation of Policy Sets

1. Navigate to Policy > Policy Sets
2. Click on + symbol and Add the rules
3. Select Allowed protocols as “solution_team_network_access”



+	Status	Policy Set Name	Description	Conditions
✎	✓	Solution_Team_Policy		
	✓	New Policy Set 2		RADIUS-cnMaestro
	✓	New Policy Set 1		Cambium
	✓	Default	Default policy set	

4. Click on + symbol and select the conditions studio, User can select existing rules from conditions studio or can create a new one and save
5. Click Editor to add an attribute and add a rule which equals to Network device profile, so that requests coming from particular device IP ranges will be hitting to this policy.



Conditions Studio

Library

Search by Name

- Cambium
- Catalyst_Switch_Local_Web_Authentication
- RADIUS-cnMaestro
- Switch_Local_Web_Authentication
- Switch_Web_Authentication
- Switch_Web_Authentication_Cambium Networks
- Wired_802.1X
- Wired_MAB
- Wireless_802.1X
- Wireless_Access
- Wireless_MAB
- WLC_Web_Authentication

Editor

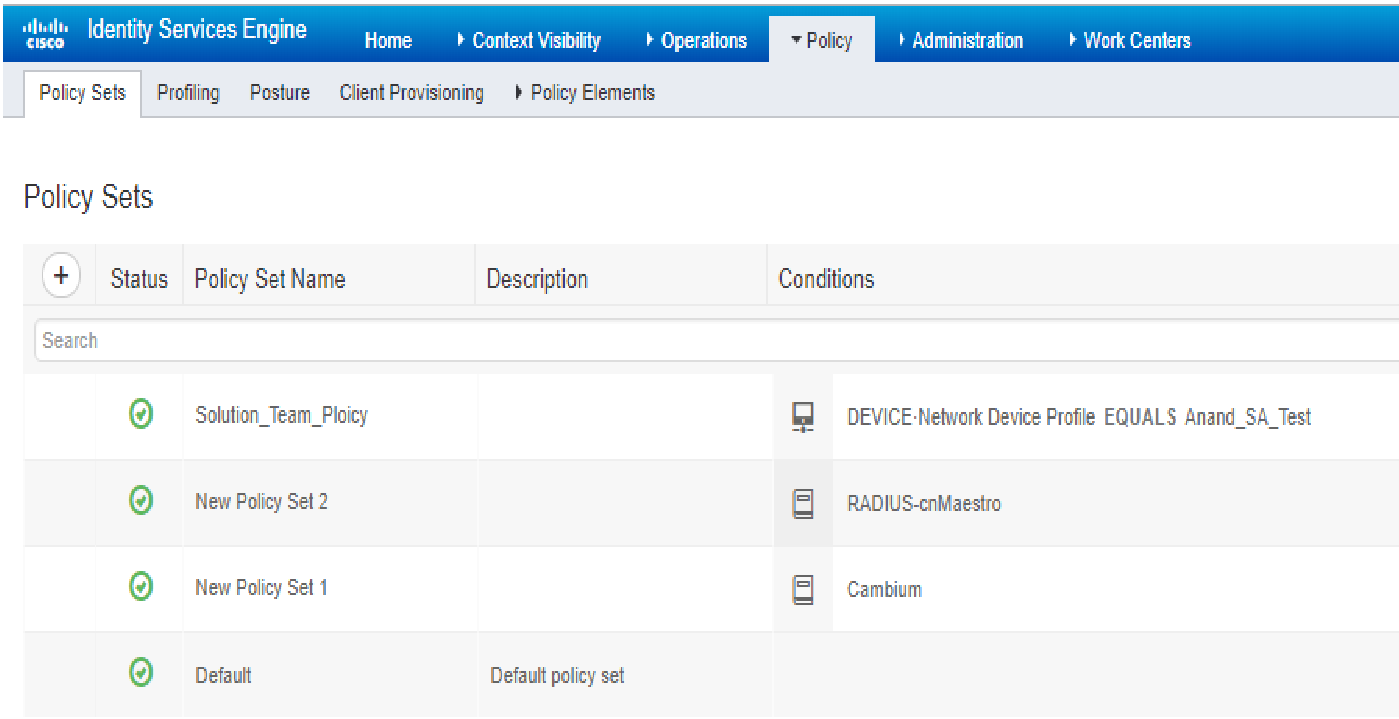
DEVICE·Network Device Profile

Equals ▼

Anand_

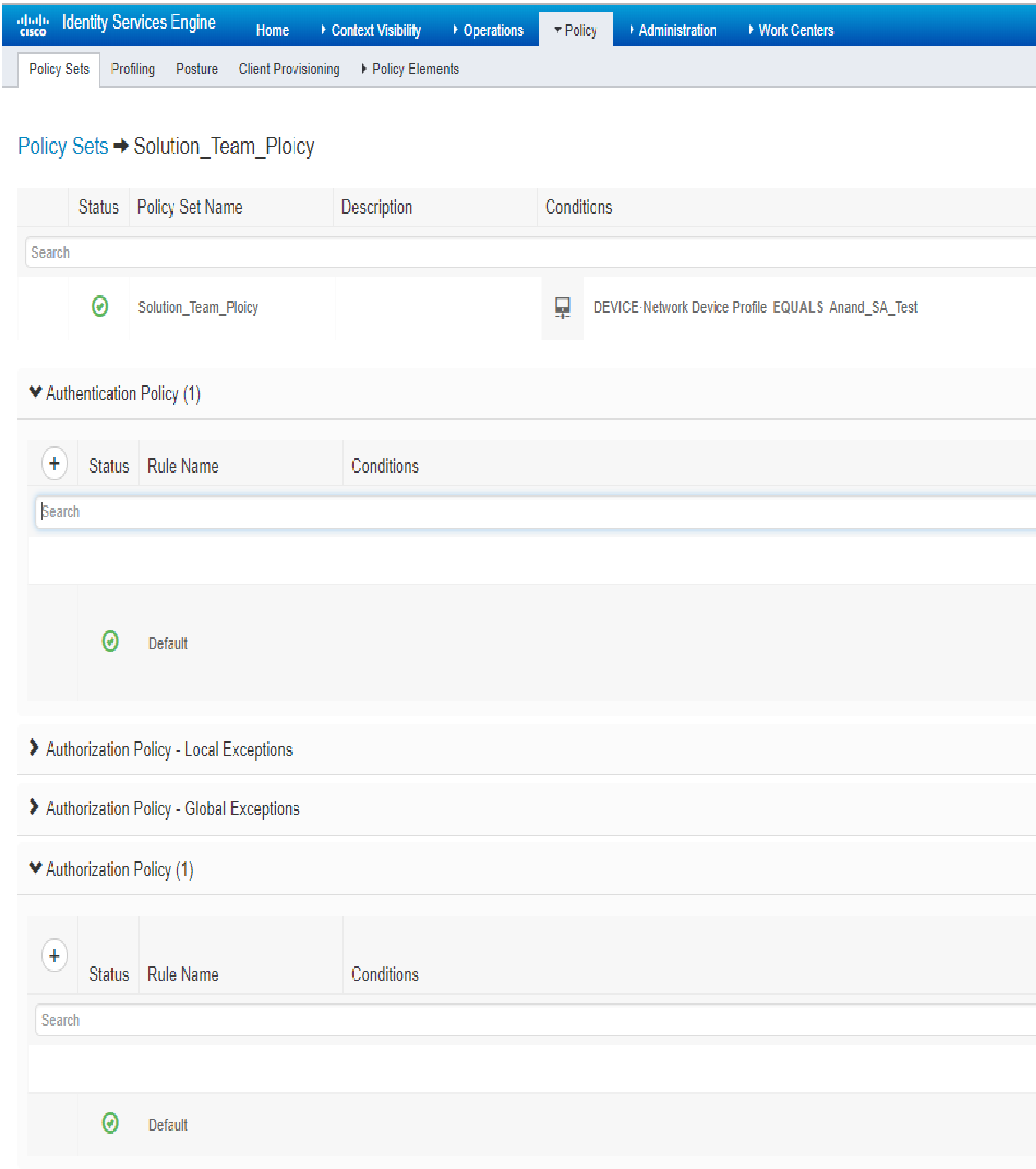
Set to 'Is not'

6. Select the new policy and click on Authentication policy and use internal users.
7. Select the appropriate Authorization policy
8. Save the policy.



Policy Sets

+	Status	Policy Set Name	Description	Conditions
	✓	Solution_Team_Ploicy		DEVICE·Network Device Profile EQUALS Anand_SA_Test
	✓	New Policy Set 2		RADIUS-cnMaestro
	✓	New Policy Set 1		Cambium
	✓	Default	Default policy set	



Policy Sets ➡ Solution_Team_Ploicy

Status	Policy Set Name	Description	Conditions
✓	Solution_Team_Ploicy		DEVICE·Network Device Profile EQUALS Anand_SA_Test

Authentication Policy (1)

Status	Rule Name	Conditions
✓	Default	

Authorization Policy - Local Exceptions

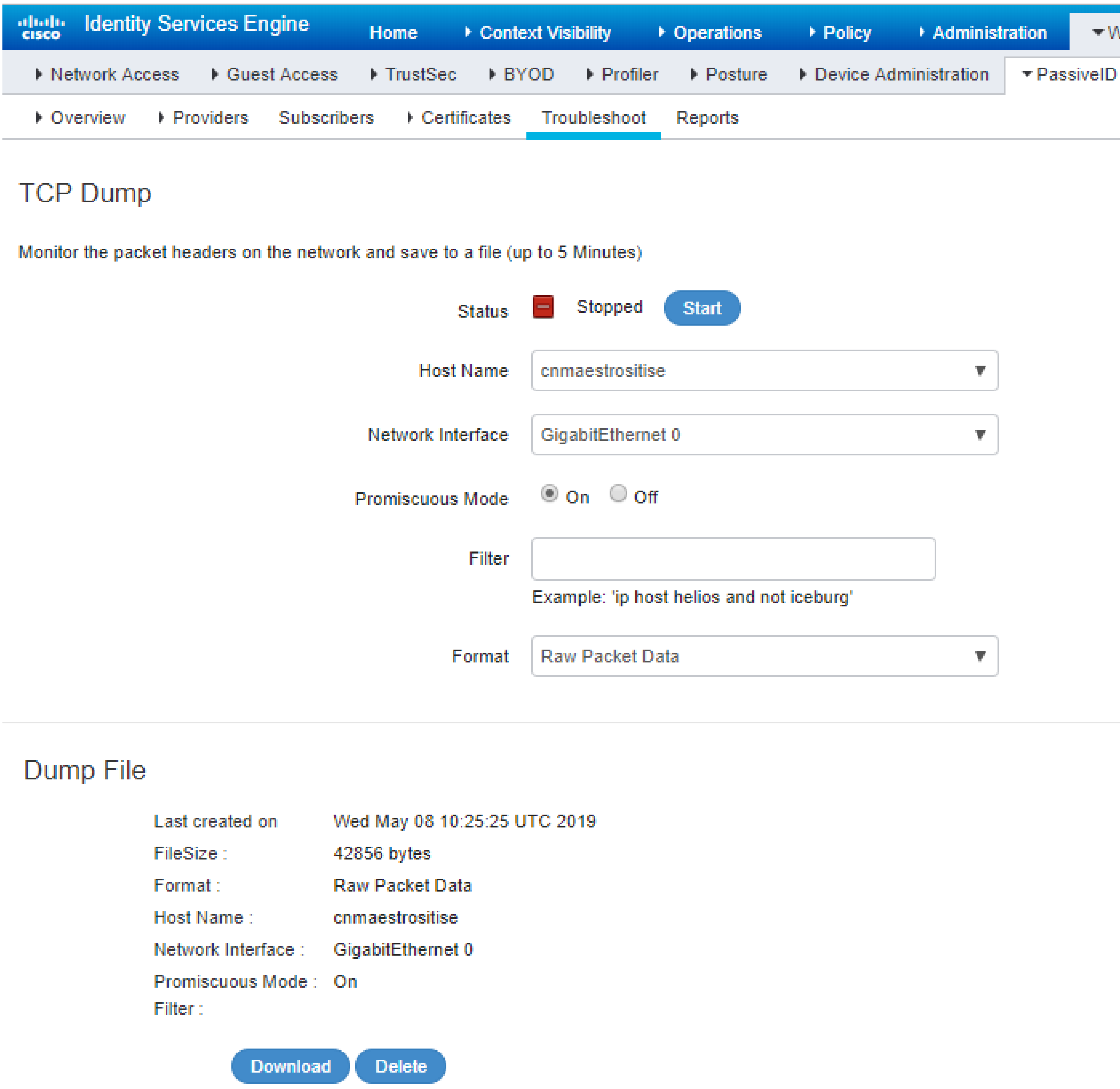
Authorization Policy - Global Exceptions

Authorization Policy (1)

Status	Rule Name	Conditions
✓	Default	

Step 8: Troubleshooting

1. Navigate to Work Centers > Passive ID > Troubleshoot
2. Start TCP dump before client connects to RADIUS server.
3. Stop TCP dump once client disconnects and download the file.
4. Wireshark or any other sniffers can be used to analyse the dump.



TCP Dump

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

Status 🟥 Stopped

Host Name: cnmaestrositise

Network Interface: GigabitEthernet 0

Promiscuous Mode: ● On ○ Off

Filter:

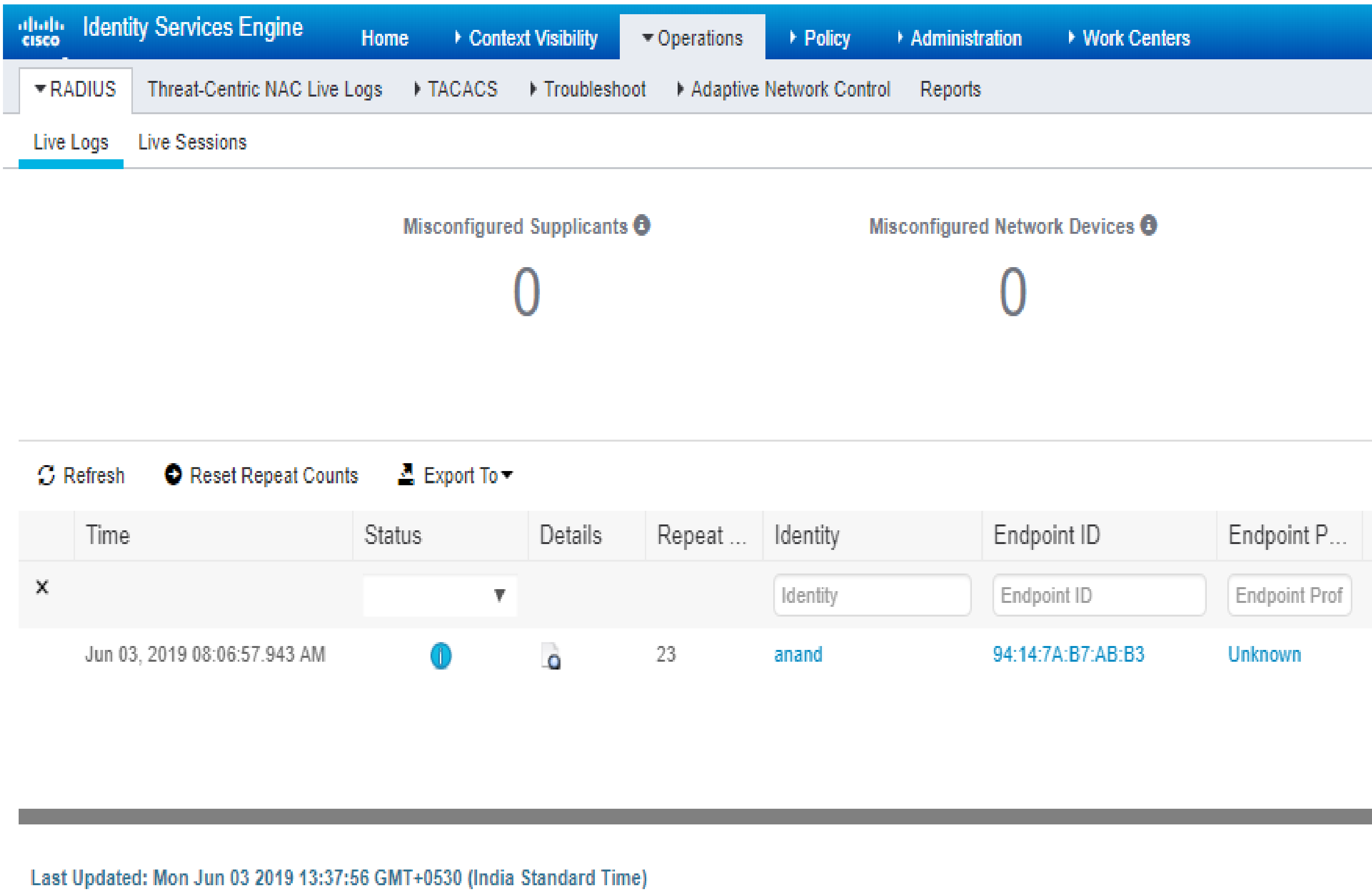
Example: 'ip host helios and not iceburg'

Format: Raw Packet Data

Dump File

Last created on	Wed May 08 10:25:25 UTC 2019
FileSize :	42856 bytes
Format :	Raw Packet Data
Host Name :	cnmaestrositise
Network Interface :	GigabitEthernet 0
Promiscuous Mode :	On
Filter :	

5. User can Navigate to Live Logs under Operations > RADIUS > Live Logs and can check the client entries which have tried to contact the ISE RADIUS service.



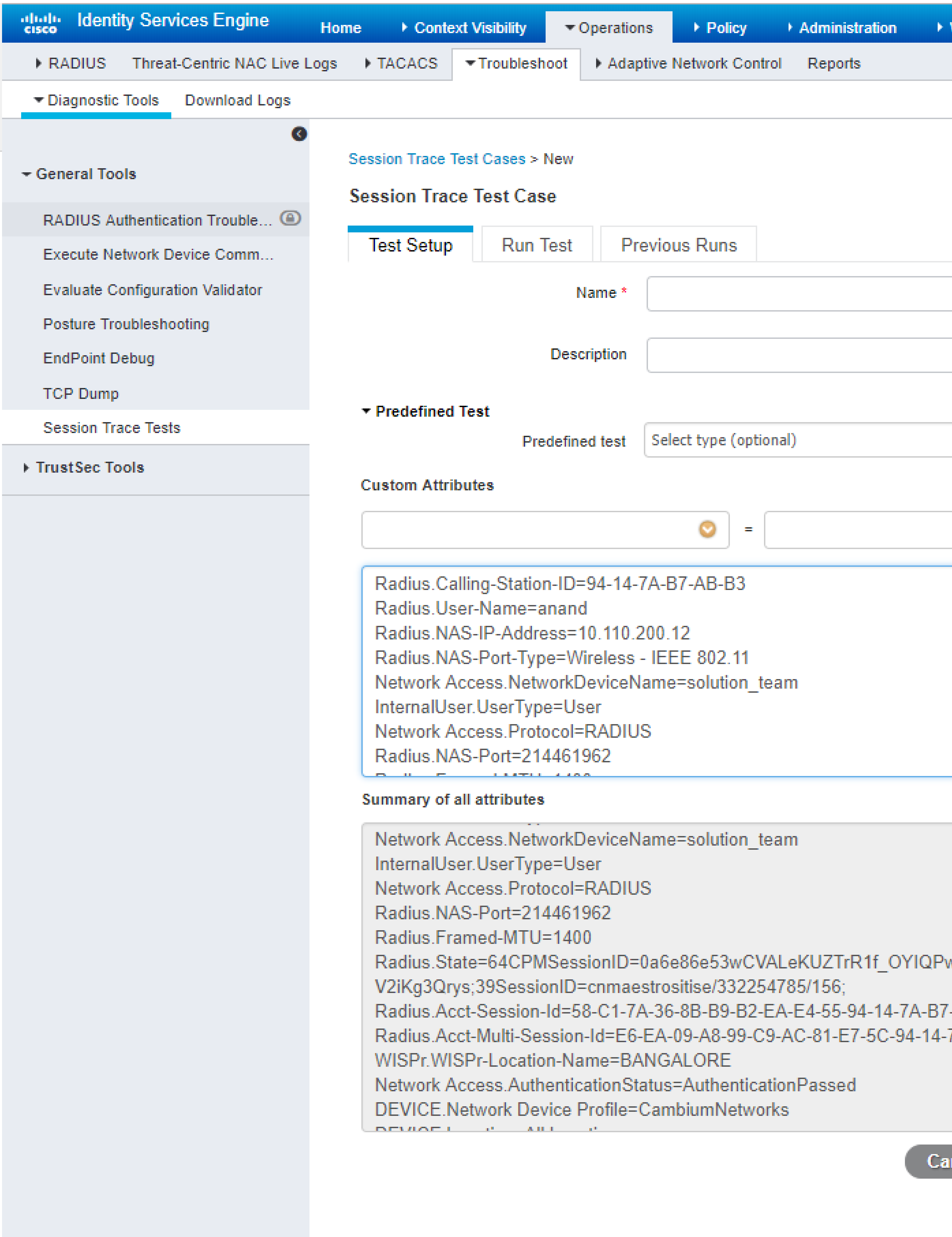
Misconfigured Supplicants 0

Misconfigured Network Devices 0

	Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...
×		▼			Identity	Endpoint ID	Endpoint Prof
	Jun 03, 2019 08:06:57.943 AM	●		23	anand	94:14:7A:B7:AB:B3	Unknown

Last Updated: Mon Jun 03 2019 13:37:56 GMT+0530 (India Standard Time)

6. For detailed steps, Click on icon under details in Radius live logs table and will open in the new tab as shown below
7. For Session trace details, please click on troubleshoot and select session trace Tests



Session Trace Test Case

Name *

Description

Predefined Test

Predefined test: Select type (optional)

Custom Attributes

=

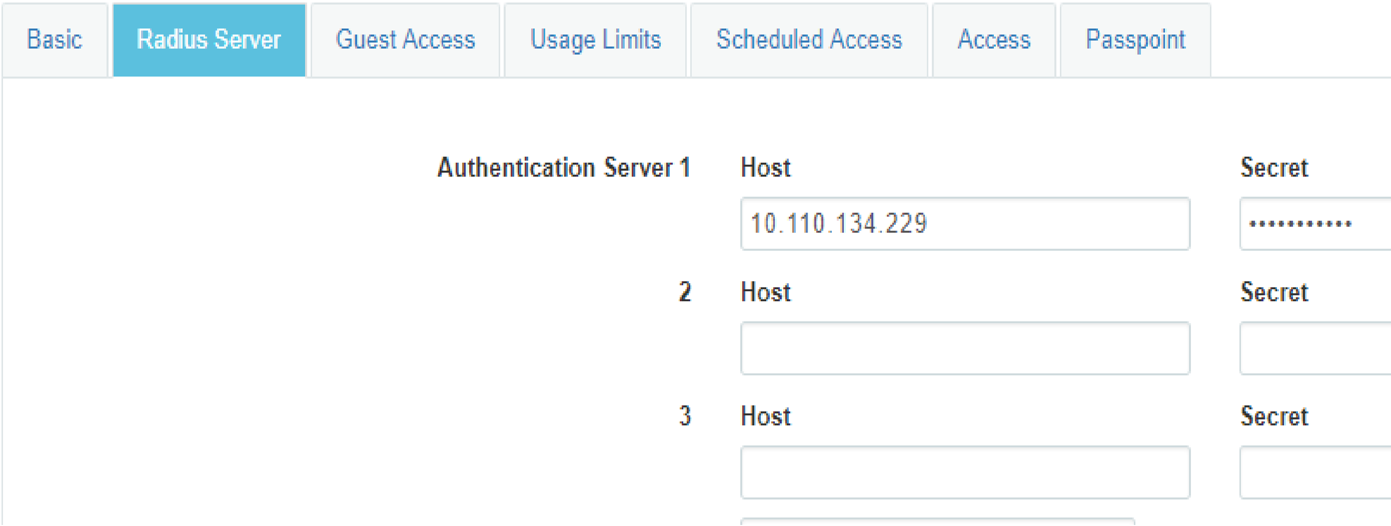
```
Radius.Calling-Station-ID=94-14-7A-B7-AB-B3
Radius.User-Name=anand
Radius.NAS-IP-Address=10.110.200.12
Radius.NAS-Port-Type=Wireless - IEEE 802.11
Network Access.NetworkDeviceName=solution_team
InternalUser.UserType=User
Network Access.Protocol=RADIUS
Radius.NAS-Port=214461962
```

Summary of all attributes

```
Network Access.NetworkDeviceName=solution_team
InternalUser.UserType=User
Network Access.Protocol=RADIUS
Radius.NAS-Port=214461962
Radius.Framed-MTU=1400
Radius.State=64CPMSessionID=0a6e86e53wCVALeKUZTrR1f_OYIQPw
V2iKg3Qrys;39SessionID=cnmaestrositise/332254785/156;
Radius.Acct-Session-Id=58-C1-7A-36-8B-B9-B2-EA-E4-55-94-14-7A-B7-
Radius.Acct-Multi-Session-Id=E6-EA-09-A8-99-C9-AC-81-E7-5C-94-14-7
WISPr.WISPr-Location-Name=BANGALORE
Network Access.AuthenticationStatus=AuthenticationPassed
DEVICE.Network Device Profile=CambiumNetworks
```

Step 9: cnPilot Configuration

1. Navigate to WLAN > Create/Select the WLAN where “WPA2 enterprise” is enabled,
2. Select Radius server tab of the respective WLAN



Authentication Server 1 Host 10.110.134.229 Secret ••••••••••••

2 Host Secret

3 Host Secret