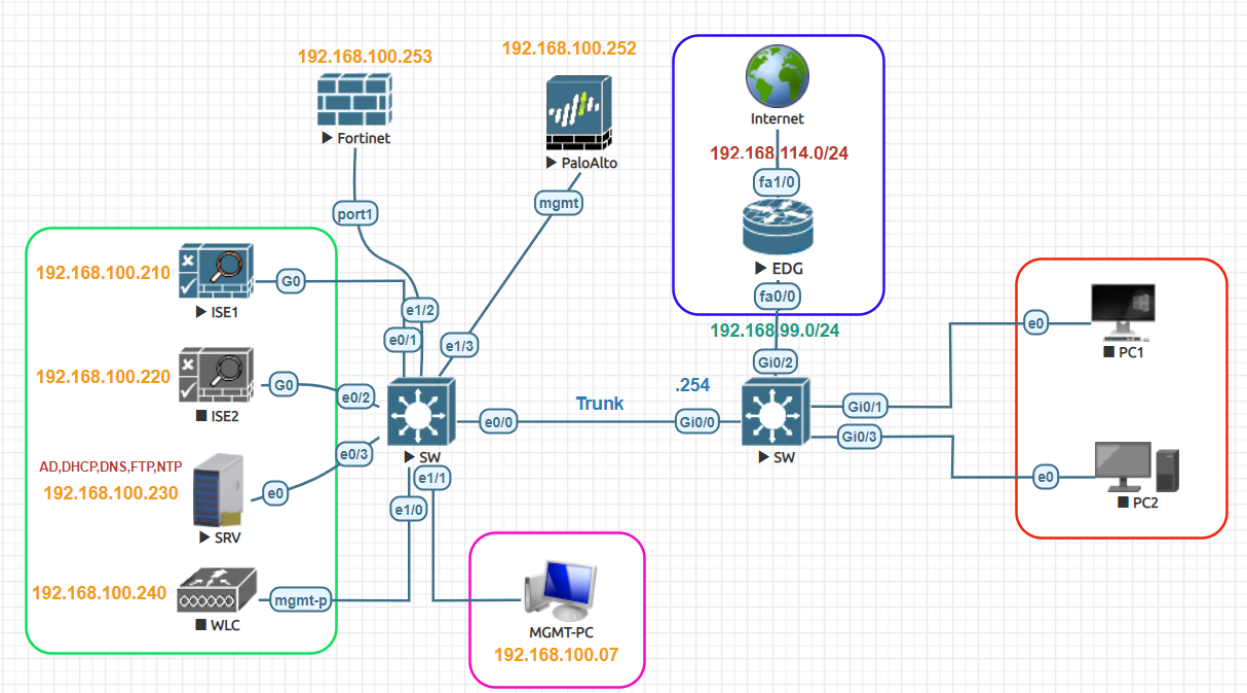
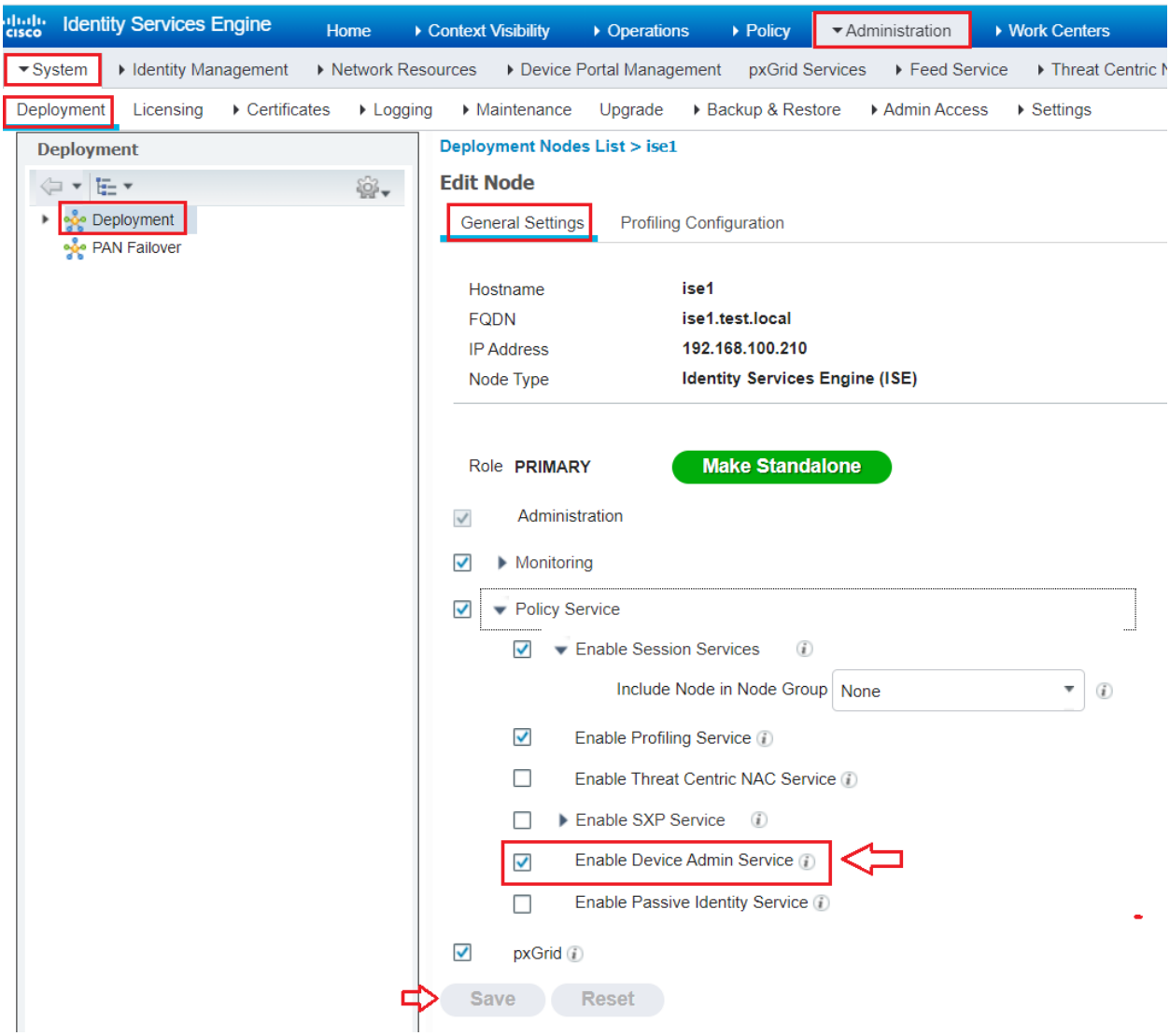
Palo Alto FW Device Administration Lab:



Cisco ISE Primary IP Address	192.168.100.210
Cisco ISE Secondary IP Address	192.168.100.220
AD, DNS and CA Server IP Address	192.168.100.230
Domain Name:	test.local
Admin Full Access User/Group	Ad1/AdminGroup
Support Readonly Access User/Group	Sp1/SupportGroup
Test VLAN	VLAN 100
VLAN Subnet	192.168.100.0/24
VLAN 100 Gateway	192.168.100.254
Network Device	Palo Alto Firewall
Authentication Switch MGMT IP	192.168.100.254
Palo Alto Firewall Interface	MGMT
Network Device IP Address	192.168.100.252

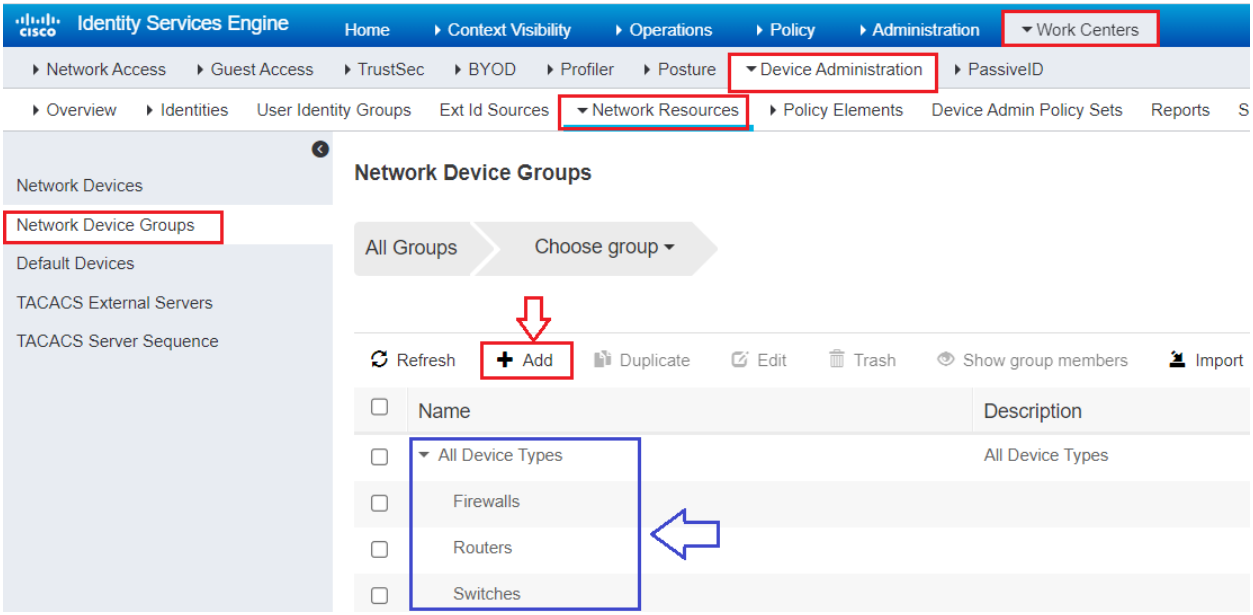
Enable TACACS+:

Navigate to Administration > System > Deployment > Under General Setting, check the box Enable Device Admin Service. Click Save.



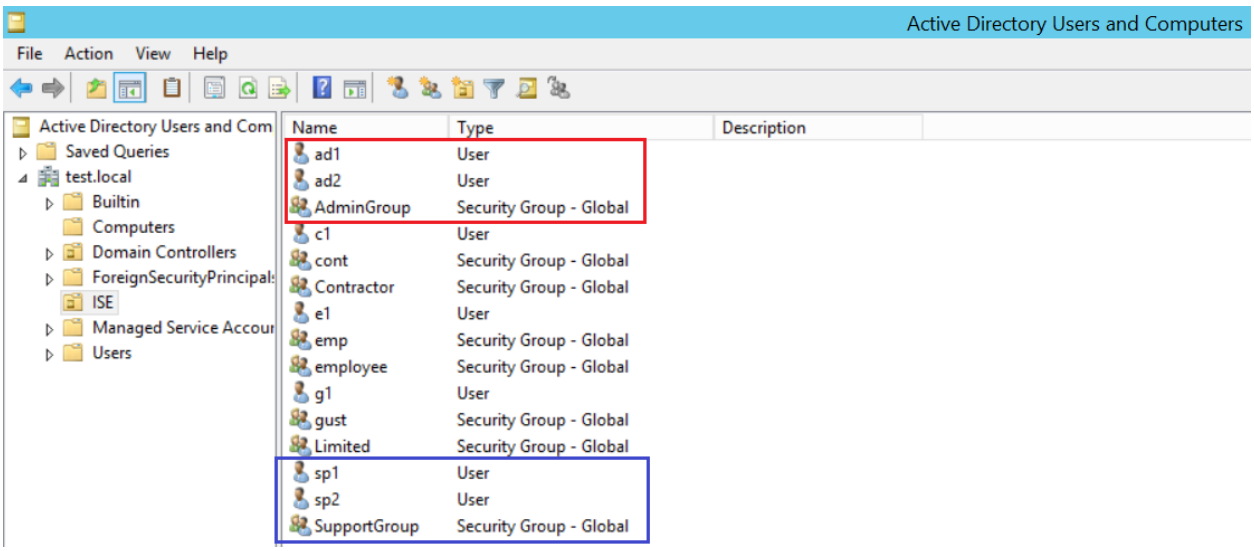
Create Device Groups:

Create device groups. We can group devices based on type or location. Work Centers> Device Administration > Network Resources > Network Device Groups



Create Groups and Users:

Create two groups in Active Directory and for test purpose create two users and add them to groups. Two Groups SupportGroup and AdminGroup and two users ad1 and sp1

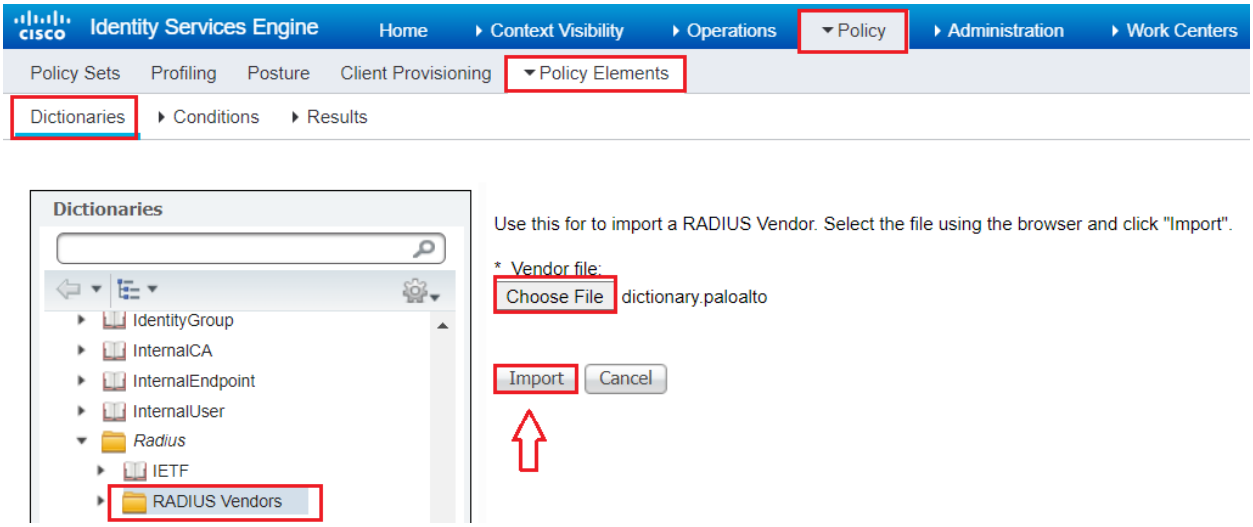


Choose Administration > Identity Management > External Identity Sources > Active Directory. Click the Groups Tab. Click on Add and then Select Groups from Directory.

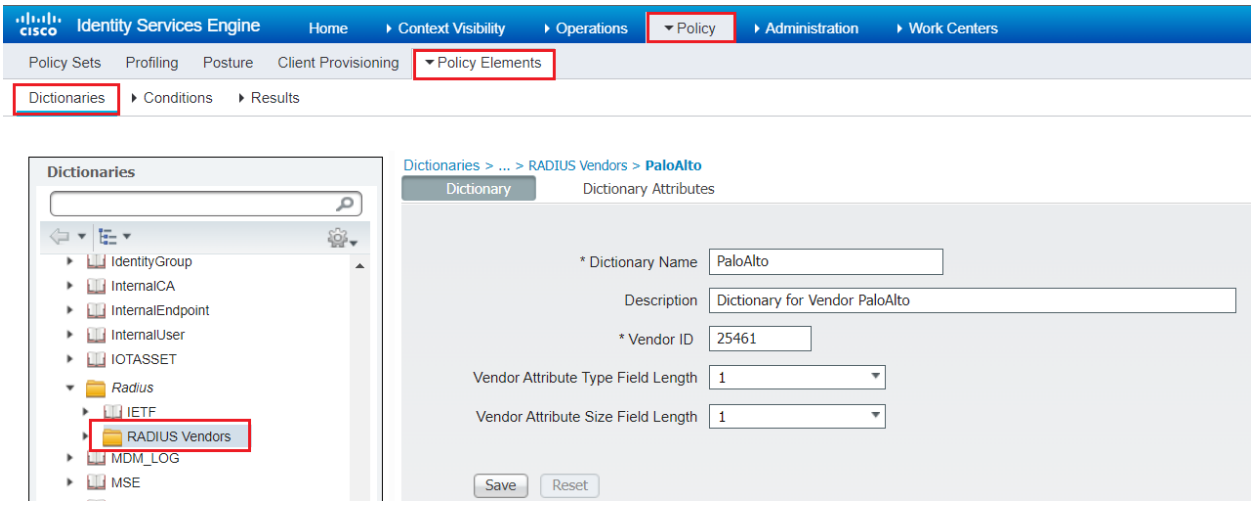
Palo Alto RADIUS Dictionary:

Palo Alto Radius dictionary defines the authentication attributes needed for communication between a PA and Cisco ISE server. You can download the dictionary from here: https://docs.paloaltonetworks.com/resources/radius-dictionary.html

Navigate to Policy>Policy Elements>Dictionaries>System -> RADIUS -> RADIUS Vendors. Click import and Choose File then click on Import.



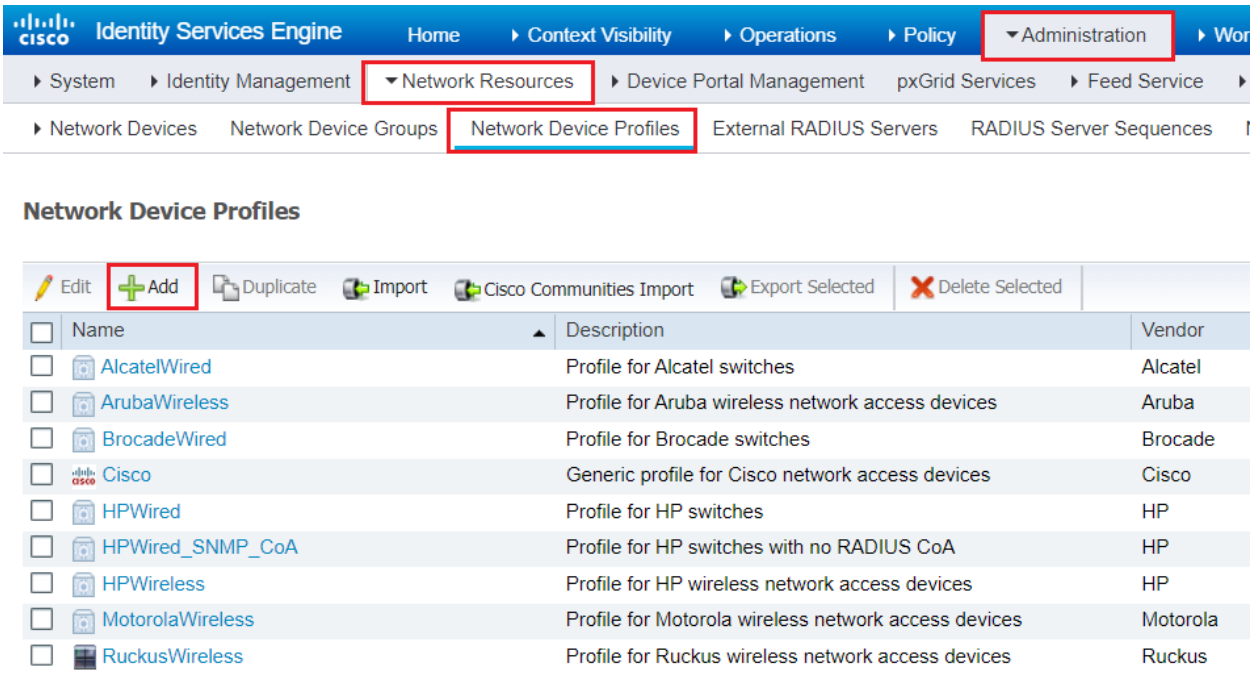
To verify Dictionary, go to Policy >Policy Elements > Dictionary System -> RADIUS -> RADIUS Vendors click on Dictionary to check and verify it.



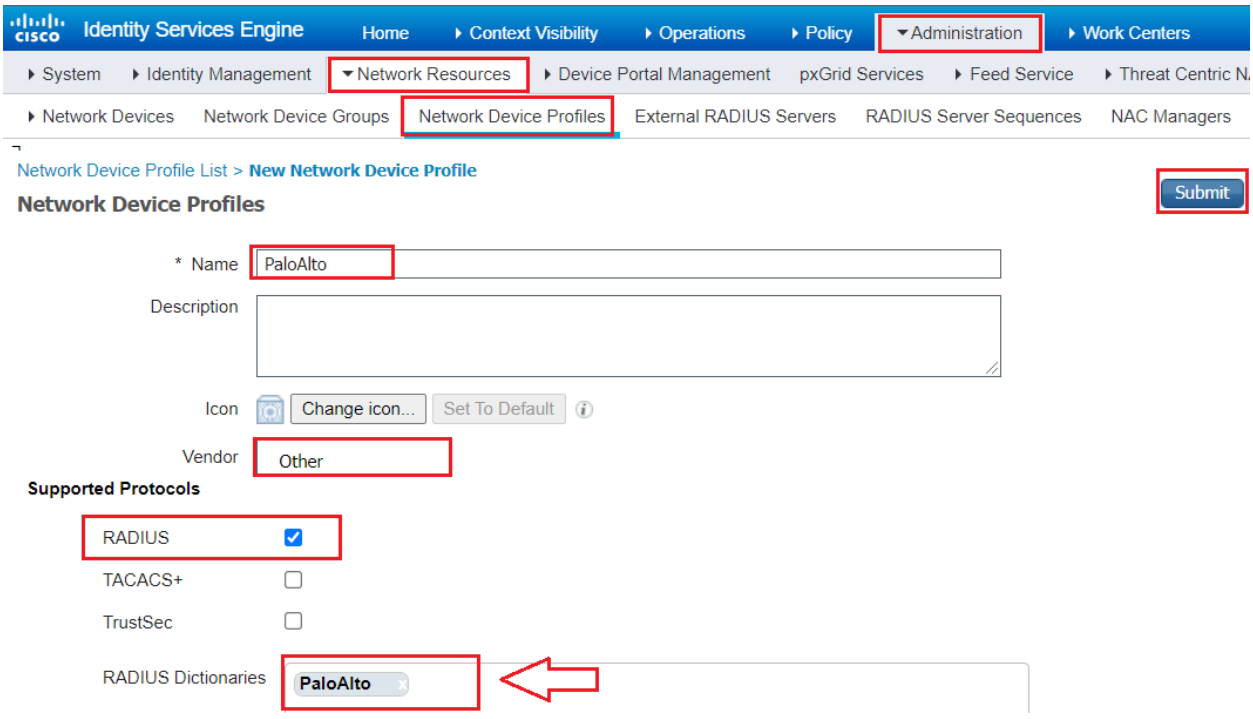
To verify Dictionary Attribute, go to Policy >Policy Elements > Dictionary System -> RADIUS -> RADIUS Vendors click on Dictionary then click Dictionary Attributes to check and verify it.

Network Device Profiles:

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



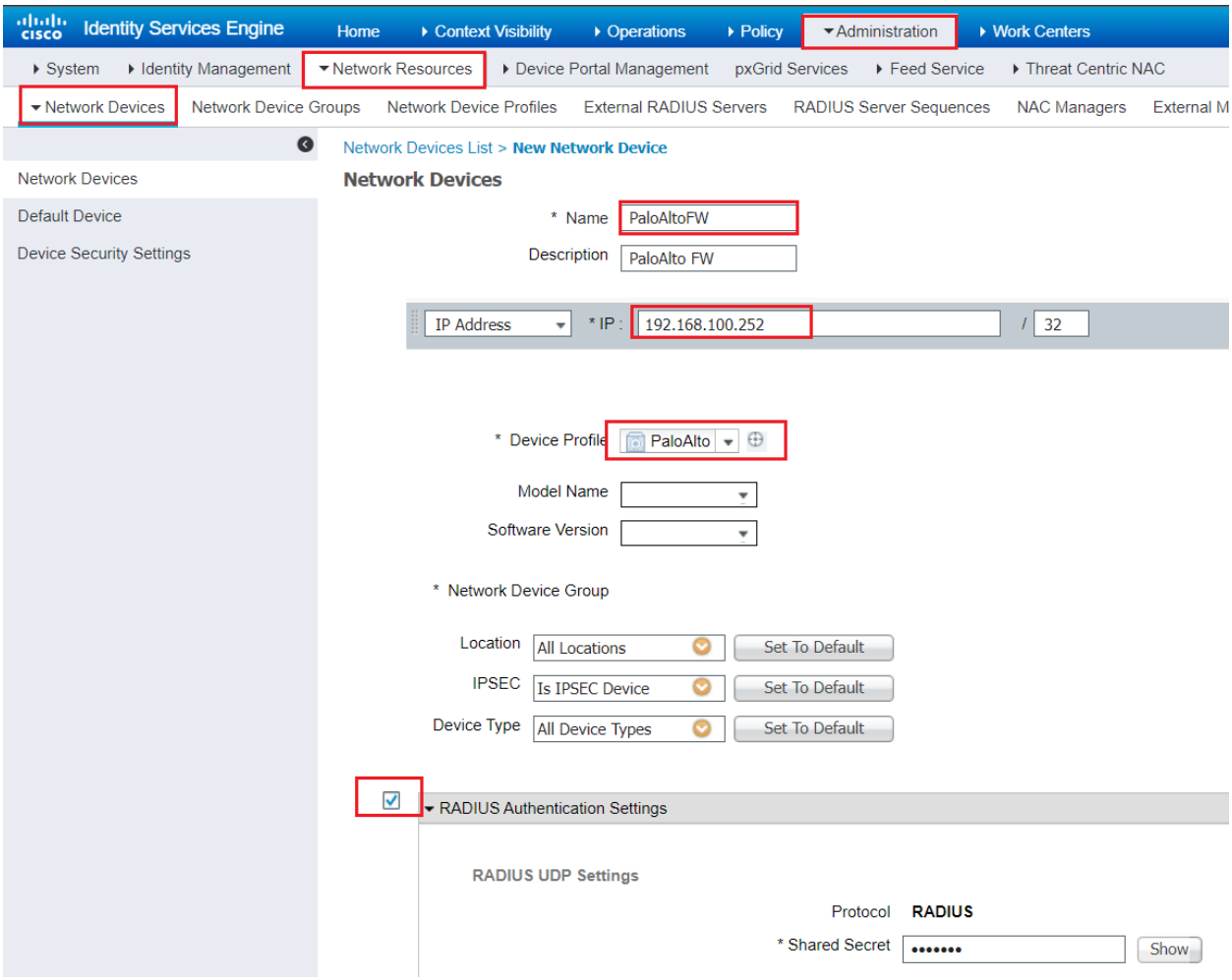
Provide valid details Name in this case PaloAlto, Vender, Support Protocols and choose RADIUS Dictionary and submit.



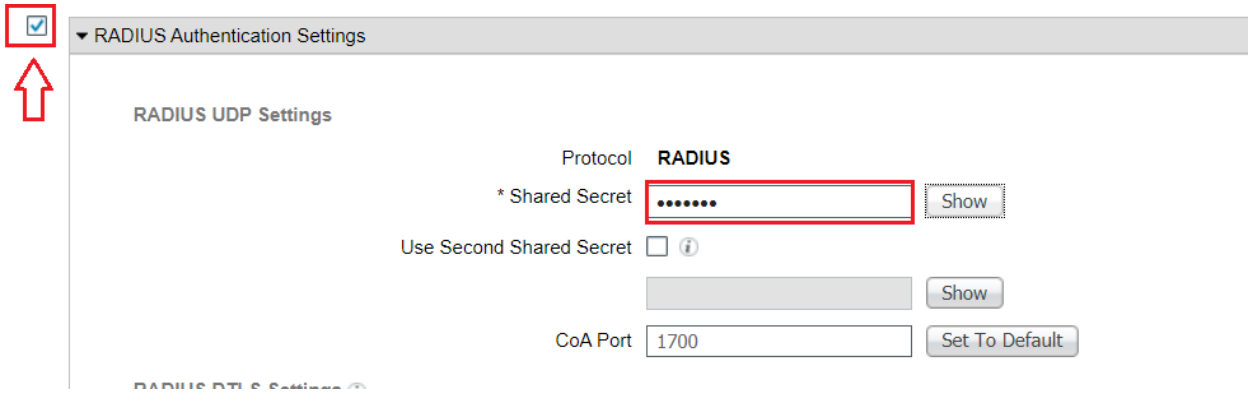
Adding Network Devices:

Work Centers> Device Administration > Network Resources > Network Devices. Click Add

Provide Name & IP address of Network device to be added. Select device group.



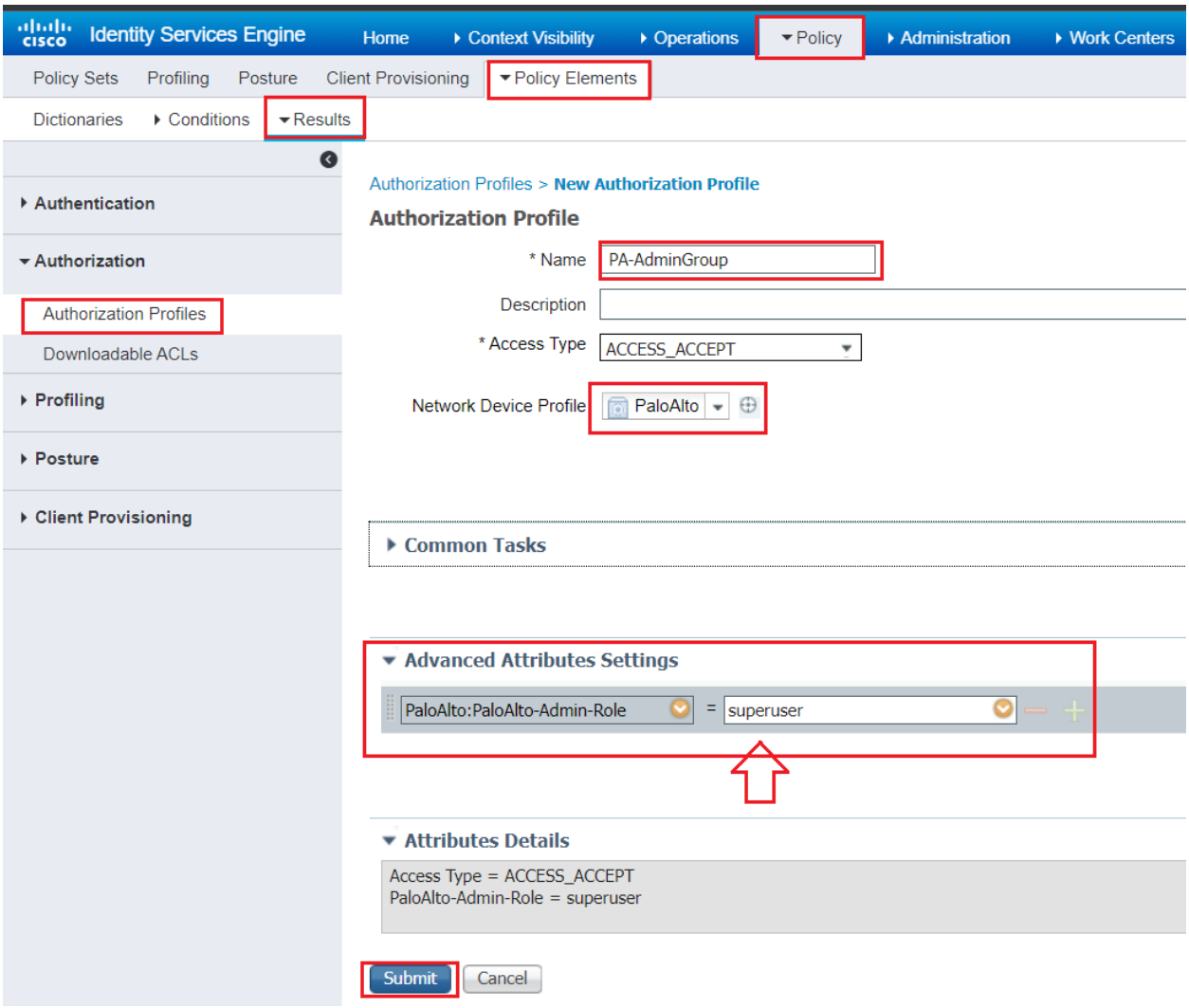
Configure RADIUS authentication Settings put Shared Secret Key in this case Test123



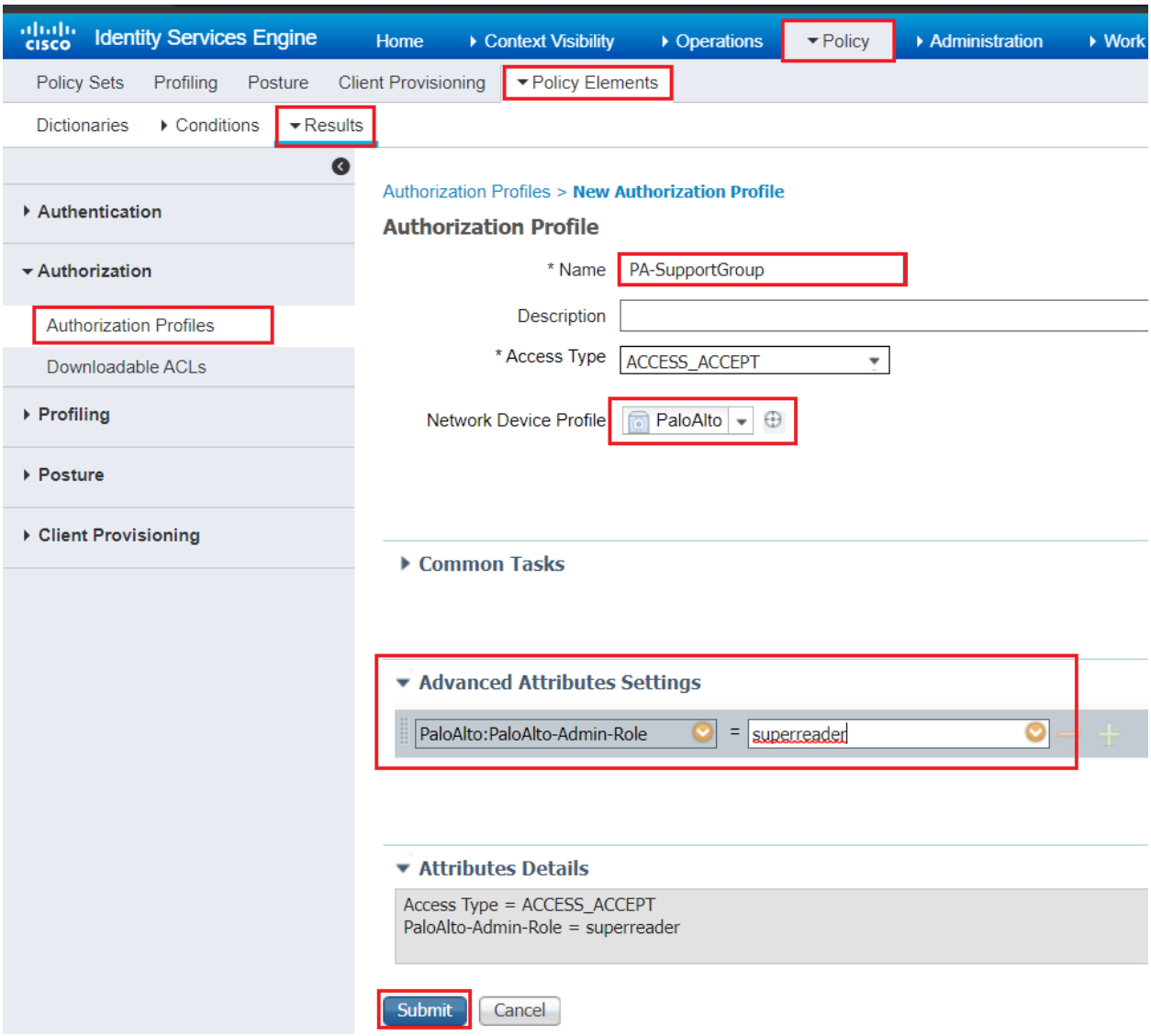
Authorization Profile:

Let's created two authorization profiles which we will used later in the policy. Use two of the predefined roles. (superuser, superreader). Please make sure that you select the 'Palo' Network Device Profile. If you want to use custom Admin Roles, the names must match on the PA and Cisco ISE.

Navigate to Policy > Policy Elements > Results. Navigate to Authorization > Authorization Profiles and click + Add. Name: Provide valid name. Access Type: ACCESS ACCEPT. Network Device Profile: Select the profile you created for Radius in this case PaloAlto. In advanced Attributes Settings choose PaloAlto: PaloAlto-Admin-Role and type superuser. Click on Submit

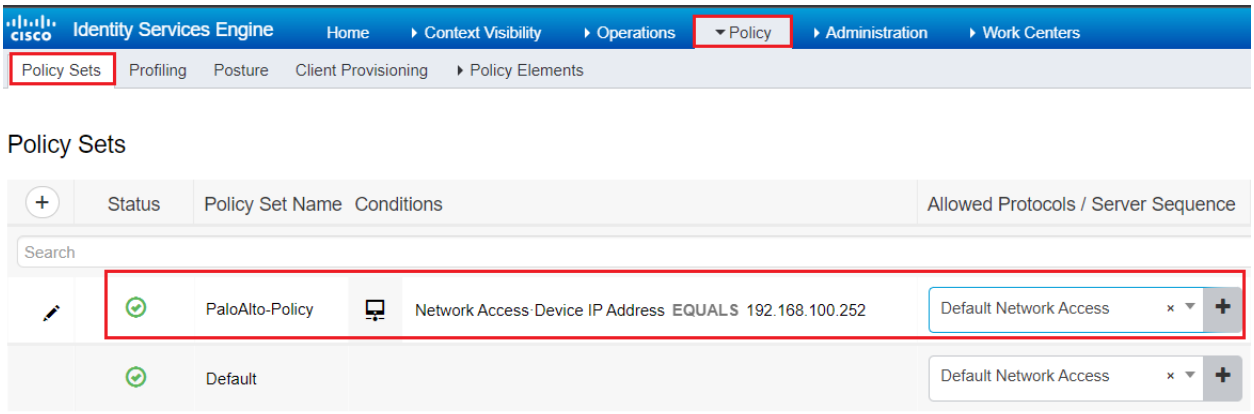


Navigate to Policy > Policy Elements > Results. Navigate to Authorization > Authorization Profiles and click + Add. Name: Provide valid name. Access Type: ACCESS ACCEPT. Network Device Profile: Select the profile you created for Radius in this case PaloAlto. In advanced Attributes Settings choose PaloAlto: PaloAlto-Admin-Role and type superreader. Click on Submit.

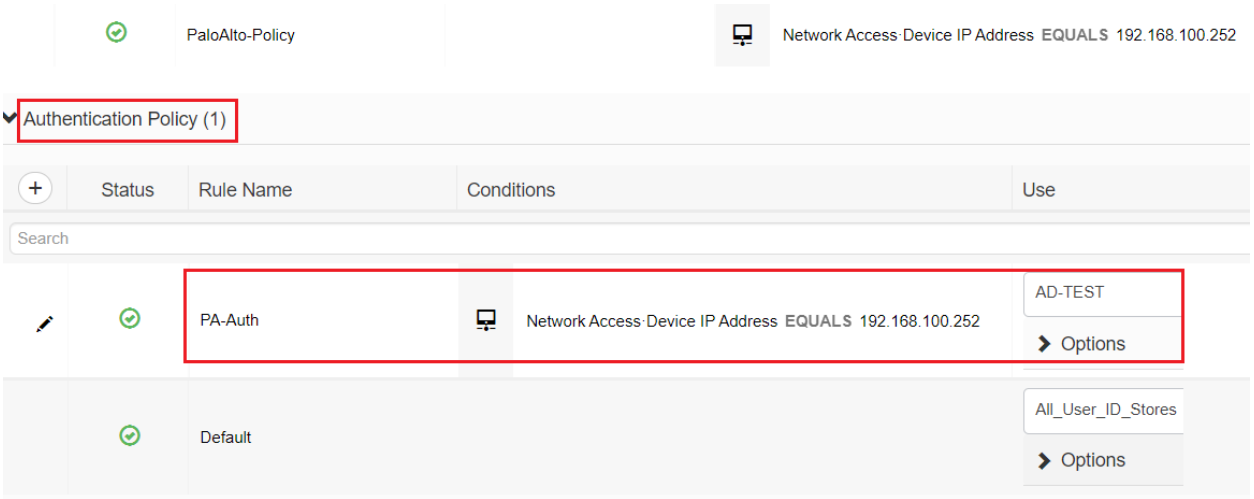


Device Administration Policy:

Navigate to Policy > Policy Sets and add new policy or use default. Click small arrow button on right side of policy to expand.



Create Authentication Policy and use Active Directory users in our case both.



Then, configure authorization Policies under 'Authorization Policy'.