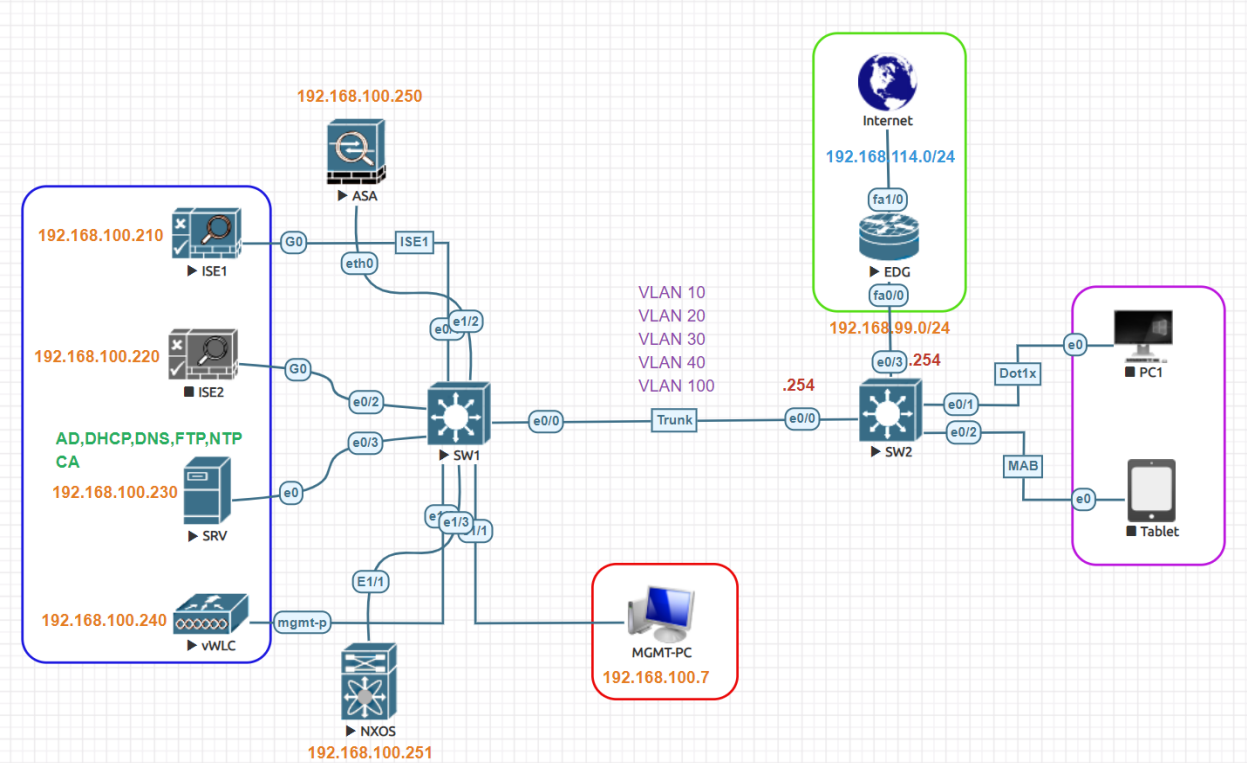
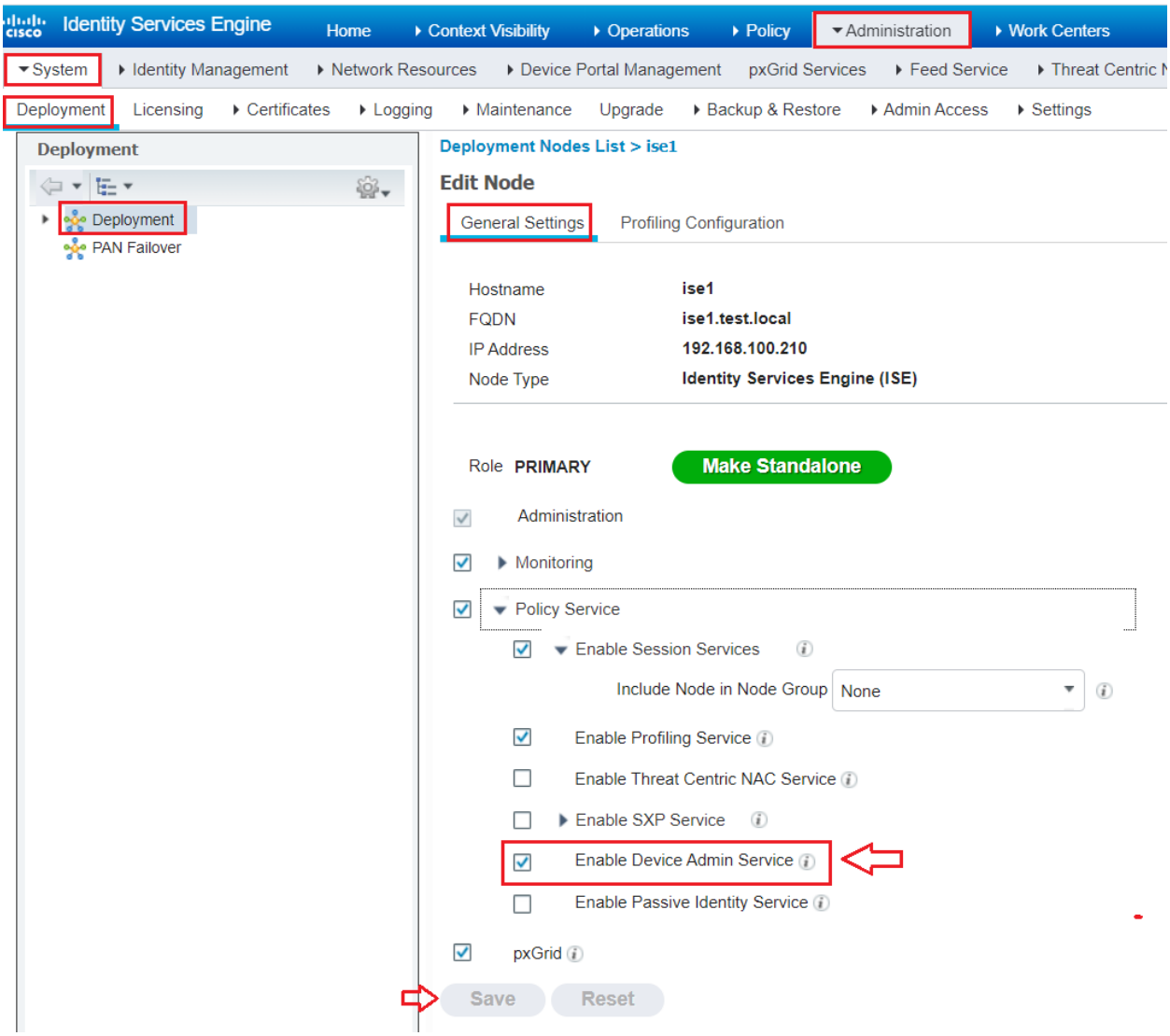
ASA Firewall Device Administration Lab:



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	Admin1/AdminGroup
Support Readonly Access User/Group	Sup1/SupportGroup
Test VLAN	VLAN 100
VLAN Subnet	192.168.100.0/24
VLAN 100 Gateway	192.168.100.254
Network Device	Cisco ASA Firewall
Authentication Switch MGMT IP	192.168.100.254
ASA TACACS Interface	Ethernet 0/2
Network Device IP Address	192.168.100.250

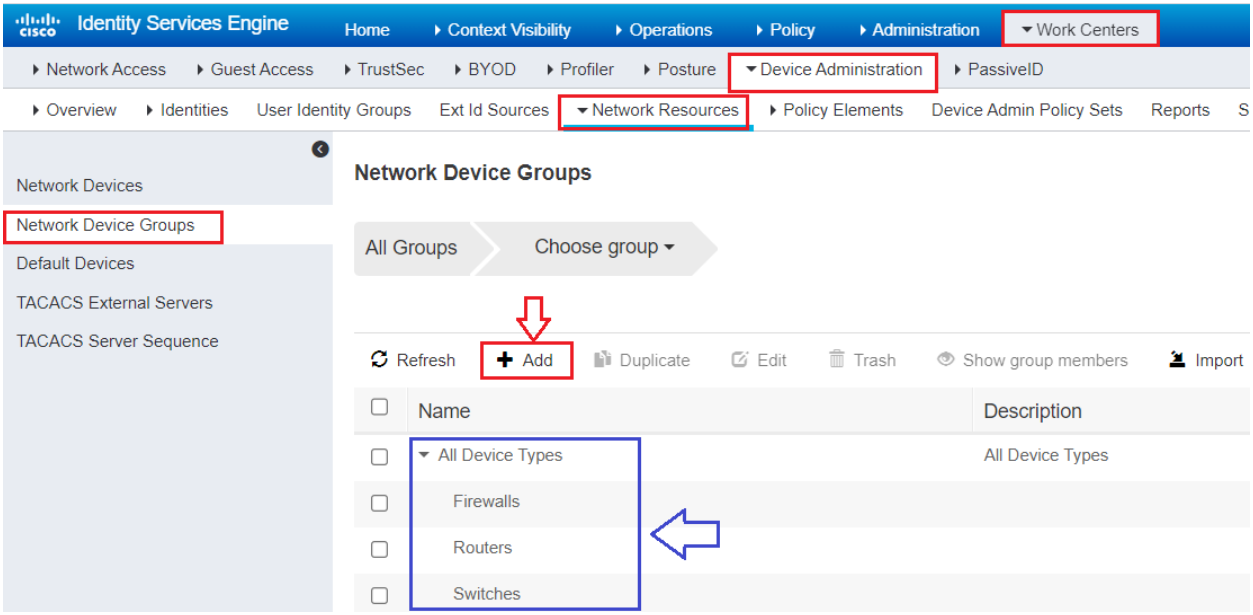
Enable TACACS+:

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



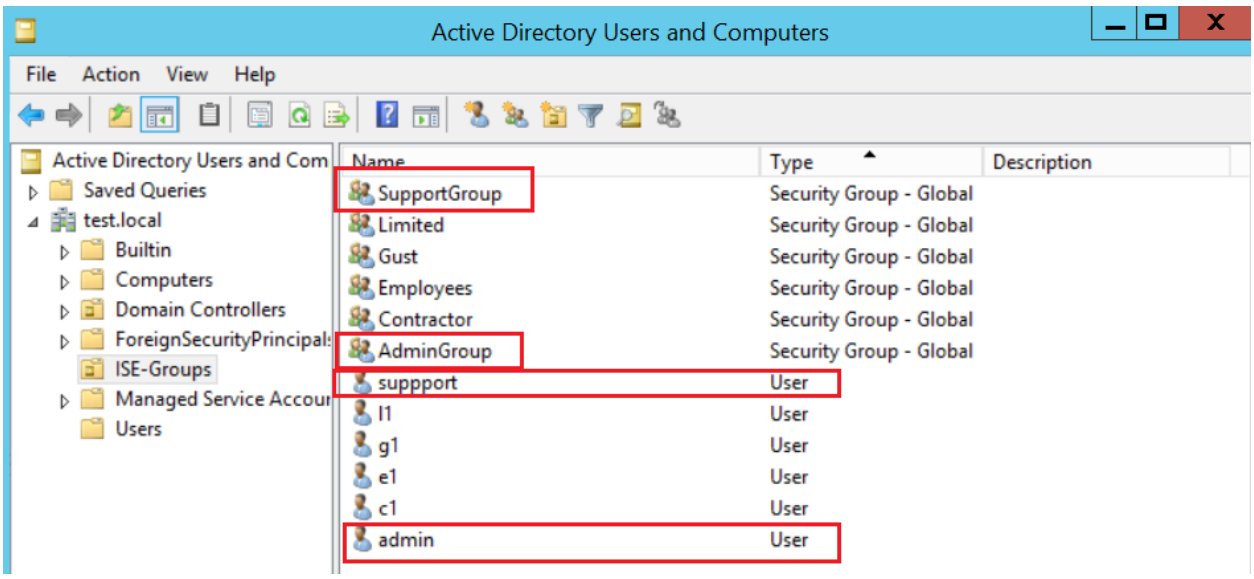
Create Device Groups:

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 admin1 and sup1

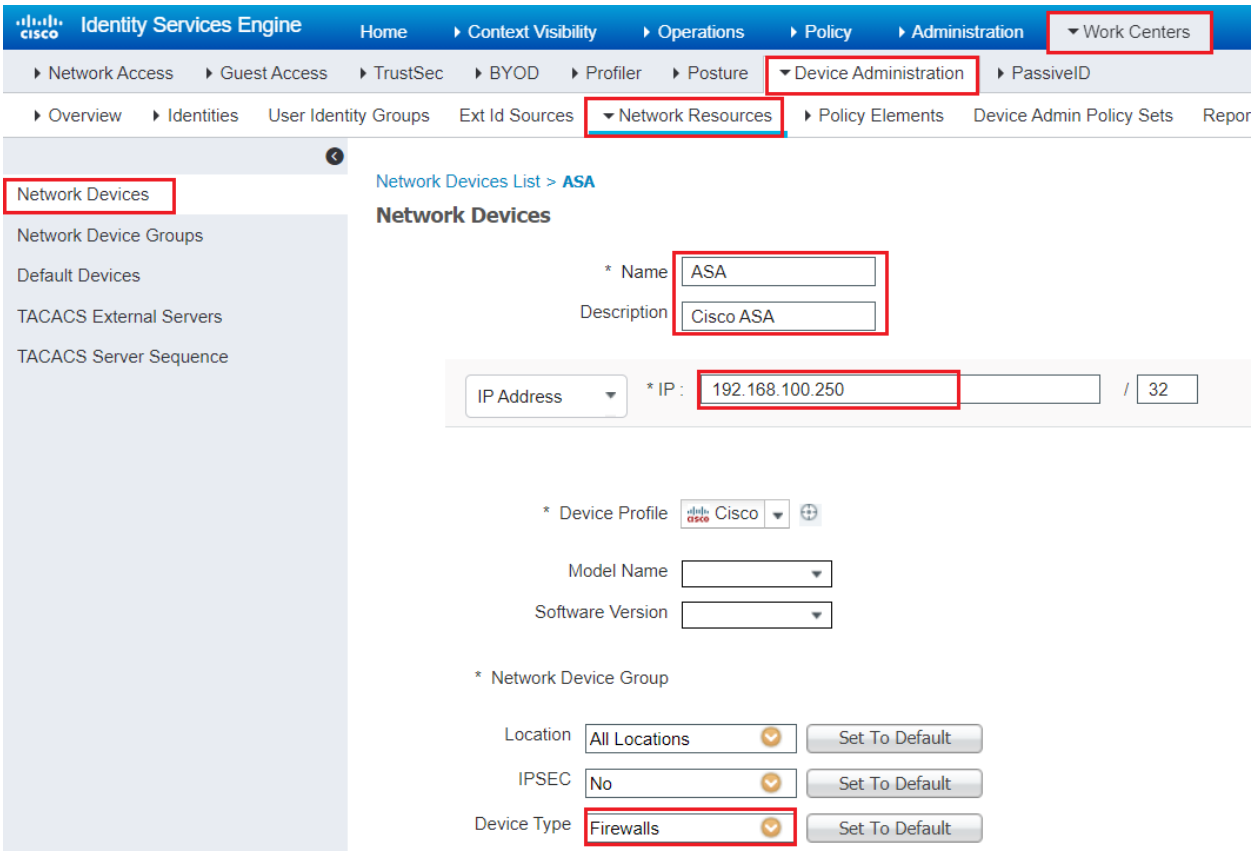


Choose Administration > Identity Management > External Identity Sources > Active Directory. Click the Groups Tab. Click on Add and then Select Groups from Directory.

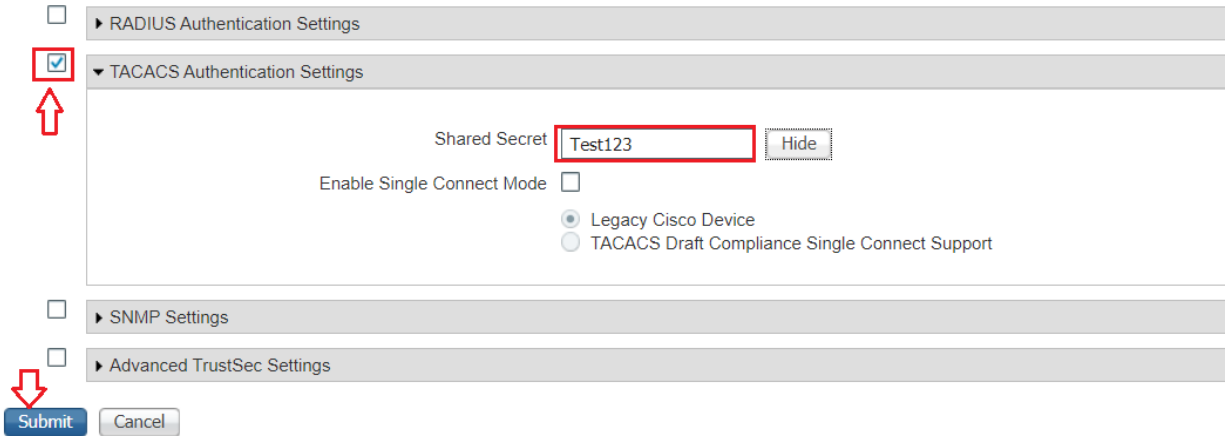
Adding Network Devices:

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

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

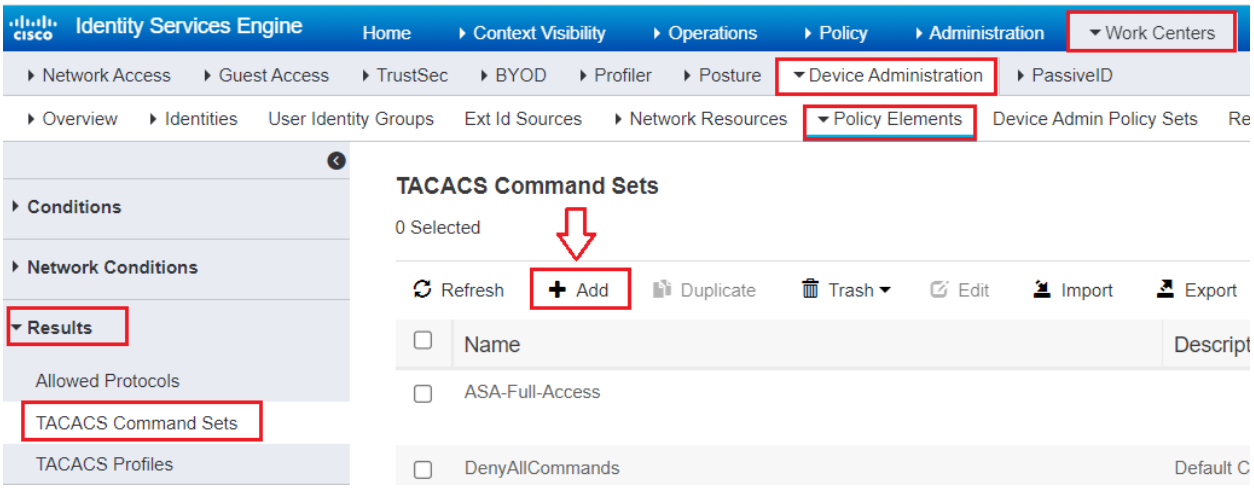


Configure TACACS authentication Settings put Shared Secret Key in this case Test123

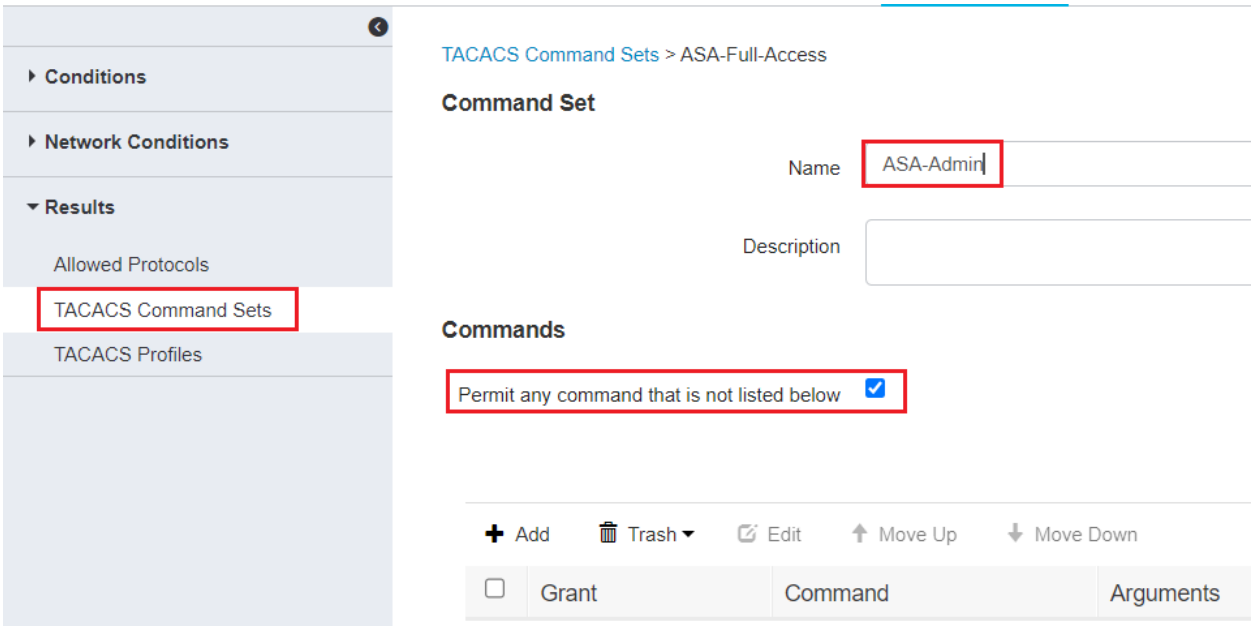


Create Command Sets:

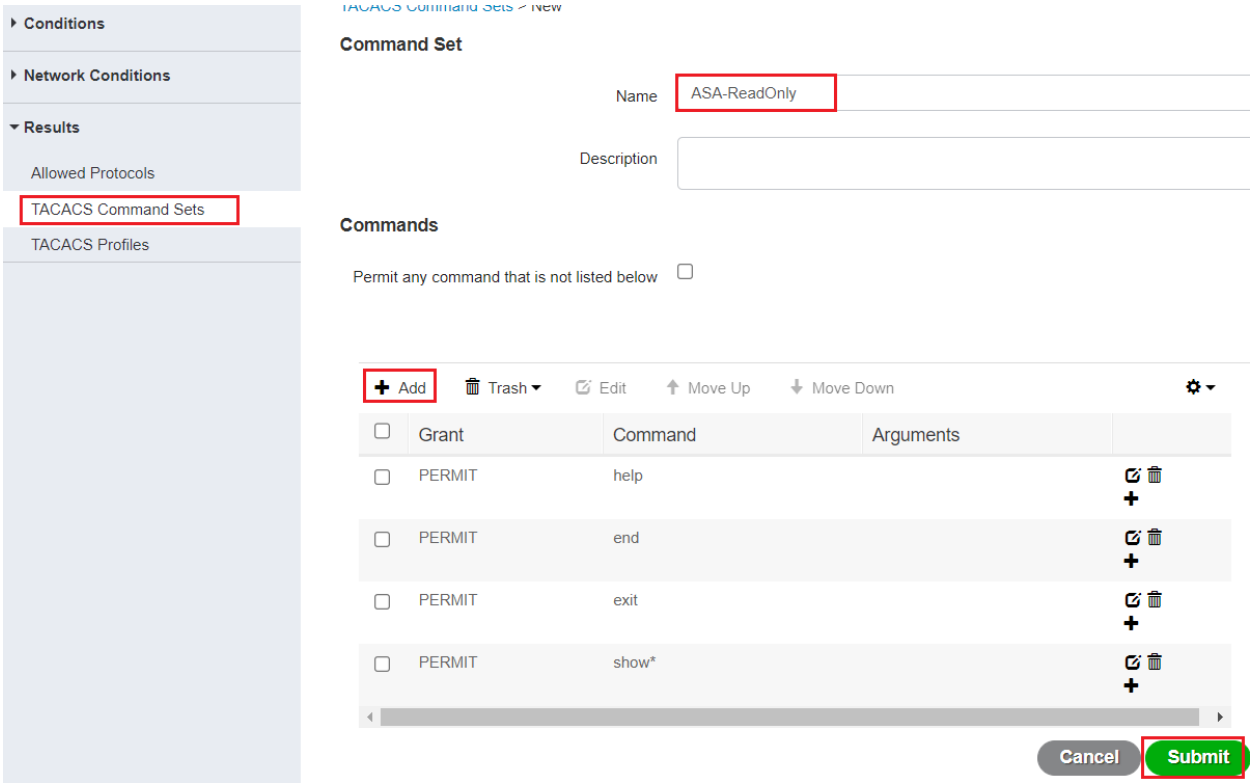
We will create two TACACS Command Sets for each profile. Navigate to Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets. Click Add



For example, we have created ASA-Admin which allows all commands. Check the box under Commands 'Permit any command that is not listed below' and don't add any command.

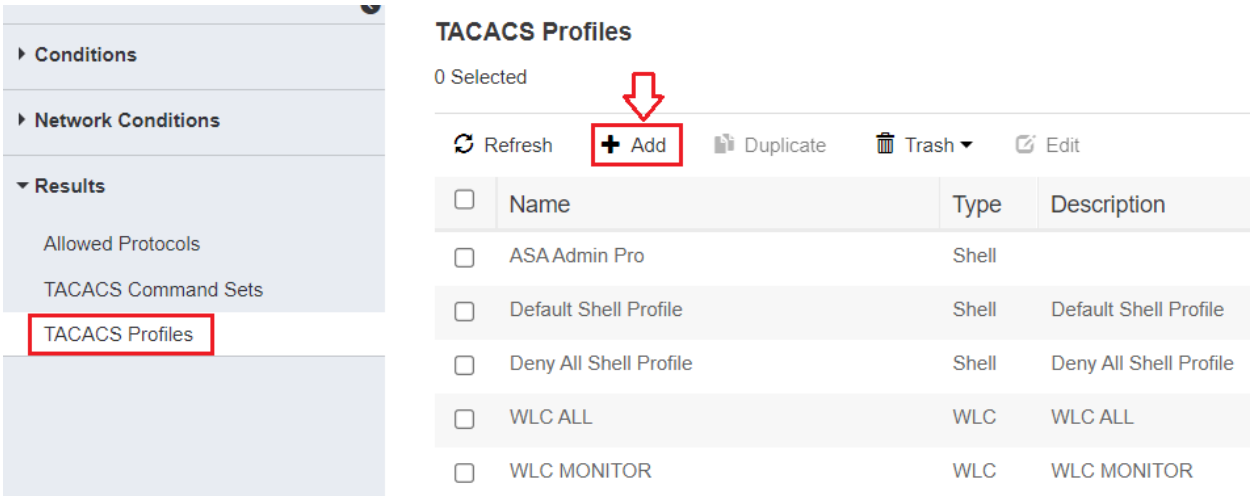


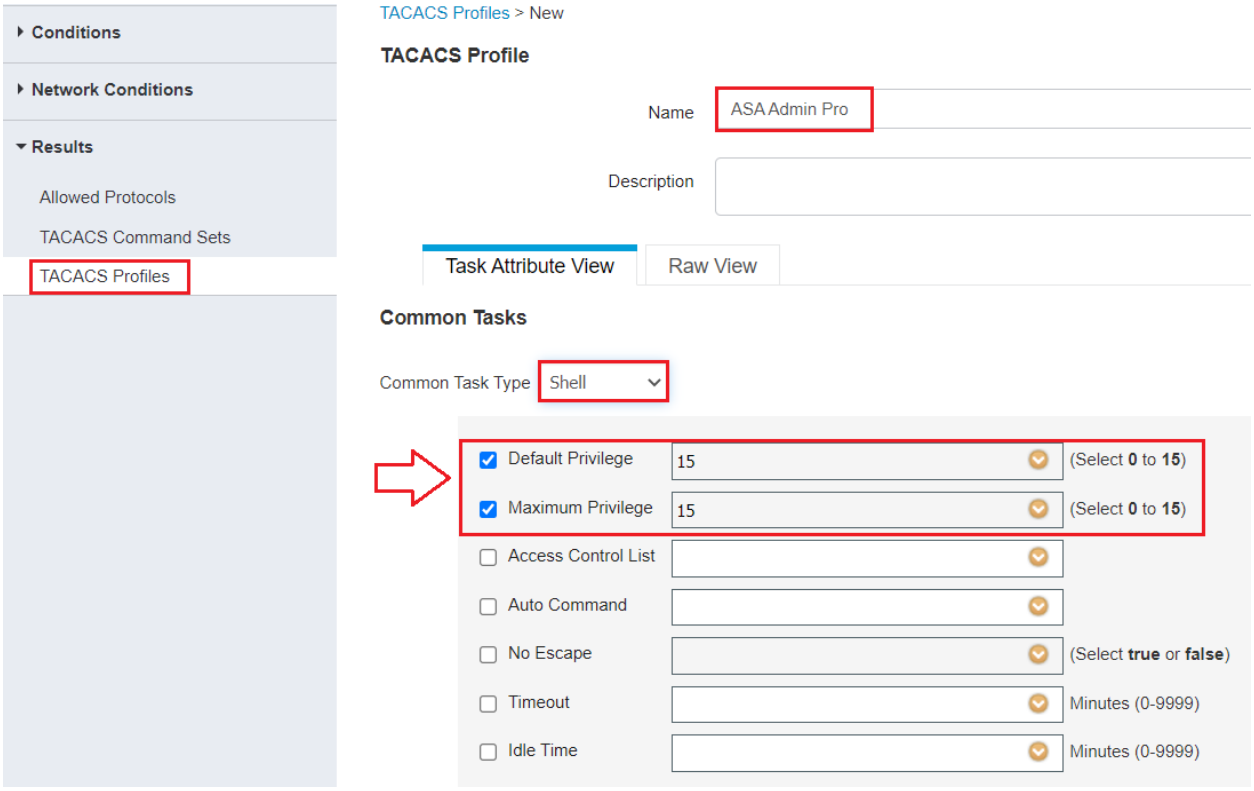
Another command set named ASA-ReadOnly is created that allows only show and few other commands. * is used for wild card.

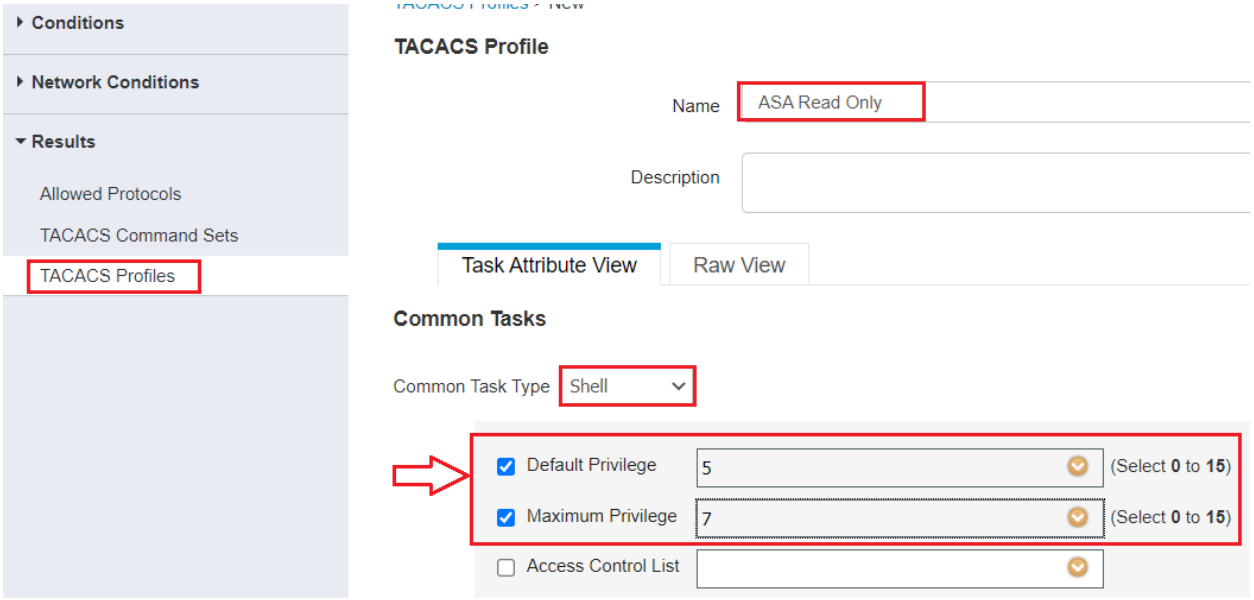


Create TACACS Profiles:

Let's create two TACACS Profiles for our Admins and Support Users. Navigate to Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles click Add.

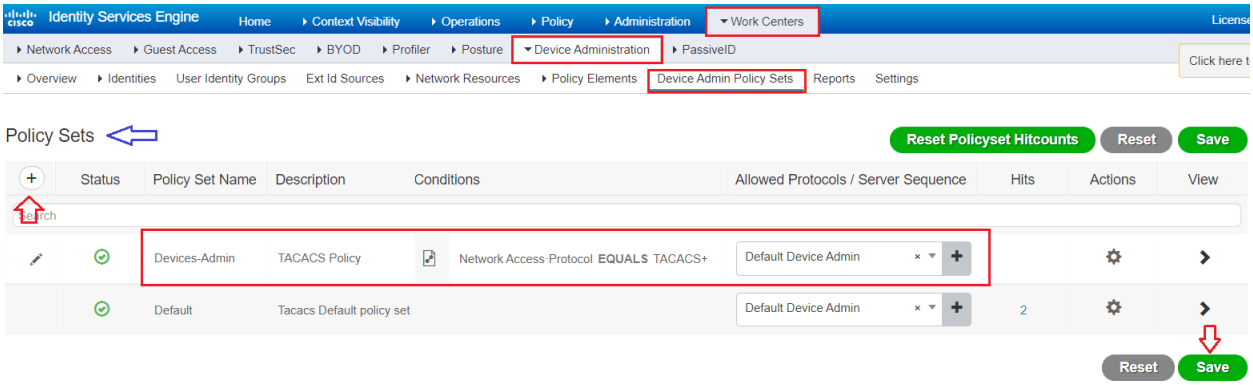



Conditions
Network Conditions
Results
Allowed Protocols
TACACS Command Sets
TACACS Profiles
TACACS Profiles > New
TACACS Profile
Name
ASA Admin Pro
Description
Task Attribute View
Raw View
Common Tasks
Common Task Type
Shell
Default Privilege
15
(Select 0 to 15)
Maximum Privilege
15
(Select 0 to 15)
Access Control List
Auto Command
No Escape
(Select true or false)
Timeout
Minutes (0-9999)
Idle Time
Minutes (0-9999)


Conditions
Network Conditions
Results
Allowed Protocols
TACACS Command Sets
TACACS Profiles
TACACS Profile
Name
ASA Read Only
Description
Task Attribute View
Raw View
Common Tasks
Common Task Type
Shell
Default Privilege
5
(Select 0 to 15)
Maximum Privilege
7
(Select 0 to 15)
Access Control List

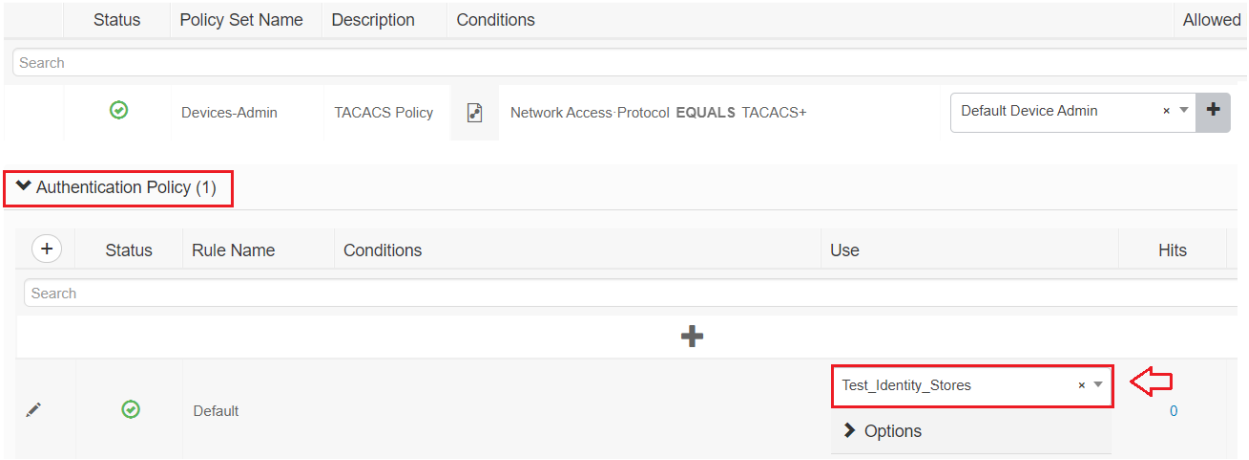
Device Administration Policy:

Here we will call all the items configured earlier. Navigate to Work Centers > Device Administration > Device Admin Policy Sets and add new policy or use default. Click small arrow button on right side of policy to expand.

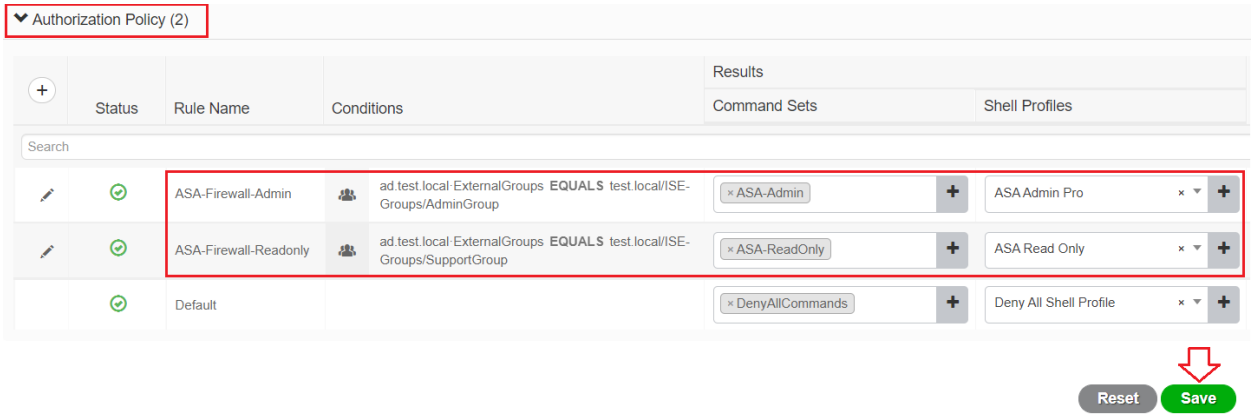


Create Authentication Policy and use internal or external users in our case both.

Policy Sets ➔ Devices-Admin



Then, configure authorization Policies under 'Authorization Policy'.

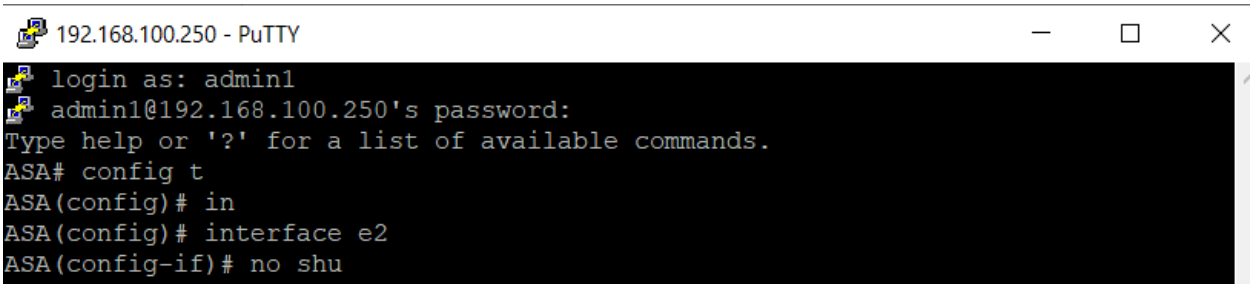


Cisco ASA Firewall Configuration:

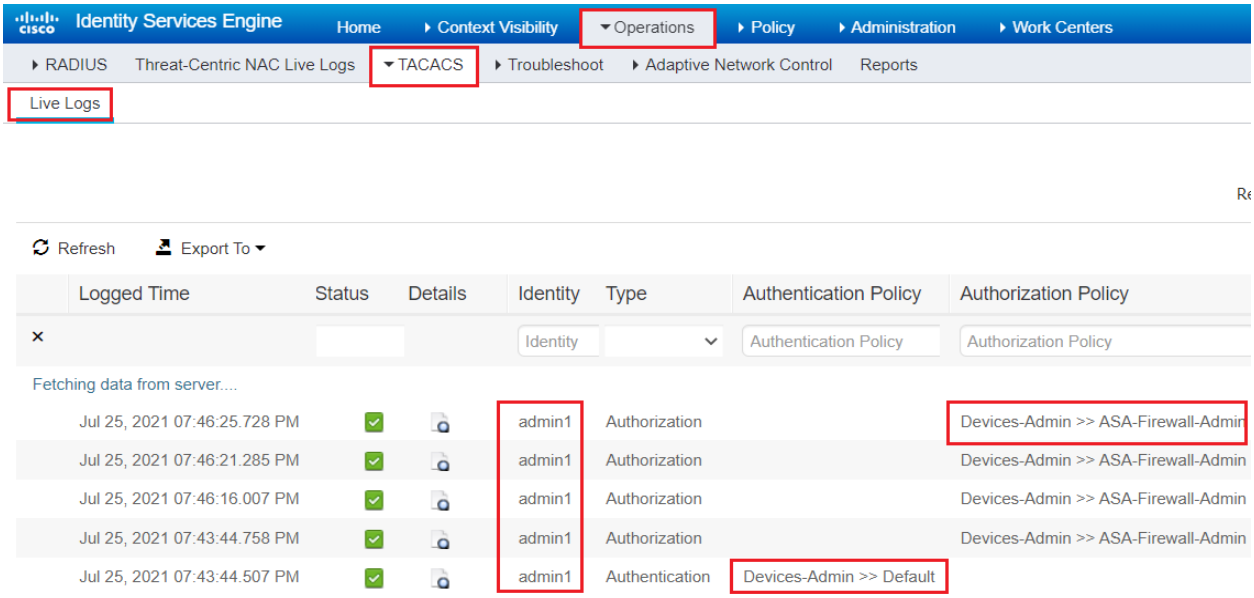
ciscoasa(config)# hostname ASA
ASA(config)# interface e0 ASA(config-if)# nameif inside ASA(config-if)# security-level 100 ASA(config-if)# ip address 192.168.100.250 ASA(config-if)# no shutdown ASA(config-if)# exit
ASA(config)# crypto key generate rsa modulus 2048
ASA(config)# enable password 123
ASA(config)# username admin password 123 privilege 15
ASA(config)# ssh 0 0 inside
ASA(config)# telnet 0 0 inside
ASA(config)# aaa-server MY_AAA protocol tacacs+
ASA(config-aaa-server-group)# aaa-server MY_AAA (inside) host 192.168.100.210 ASA(config-aaa-server-host)# key Test123 ASA(config-aaa-server-host)# exit
ASA(config)# aaa authentication serial console MY_AAA LOCAL
ASA(config)# aaa authentication telnet console MY_AAA LOCAL
ASA(config)# aaa authentication ssh console MY_AAA LOCAL
ASA(config)# aaa authentication enable console MY_AAA LOCAL
ASA(config)# aaa accounting serial console MY_AAA
ASA(config)# aaa accounting telnet console MY_AAA
ASA(config)# aaa accounting ssh console MY_AAA
ASA(config)# aaa accounting enable console MY_AAA
ASA(config)# aaa accounting command MY_AAA
ASA(config)# aaa authorization exec authentication-server auto-enable
ASA(config)# aaa authorization command MY_AAA LOCAL

Testing and Verification:

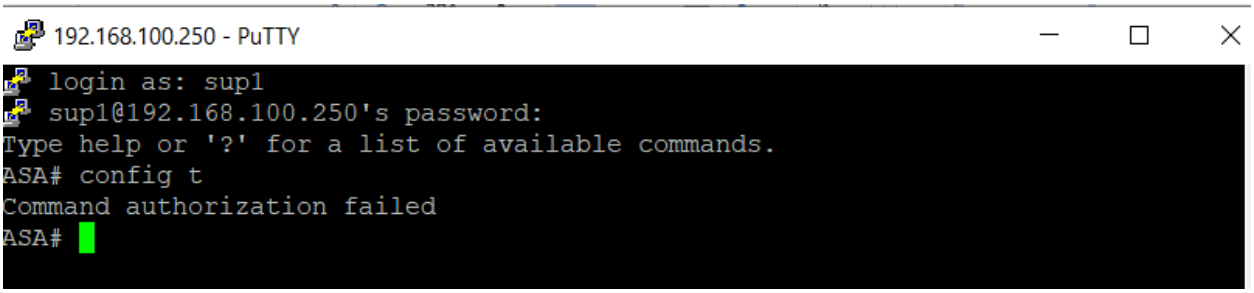
We can test our configuration by login into the Cisco ASA Firewall by SSH. Let's try using the admin1 user credential.



We can monitor the authentication/authorization logs on ISE Operations > TACACS > Live Logs. The admin1 user was successfully authenticated and authorized to run privileged commands.



Now let's try again using support account users sup1. The user sup1 was successfully authenticated but wasn't authorized to run privileged commands.



We can monitor the authentication/authorization logs on ISE Operations > TACACS > Live Logs.