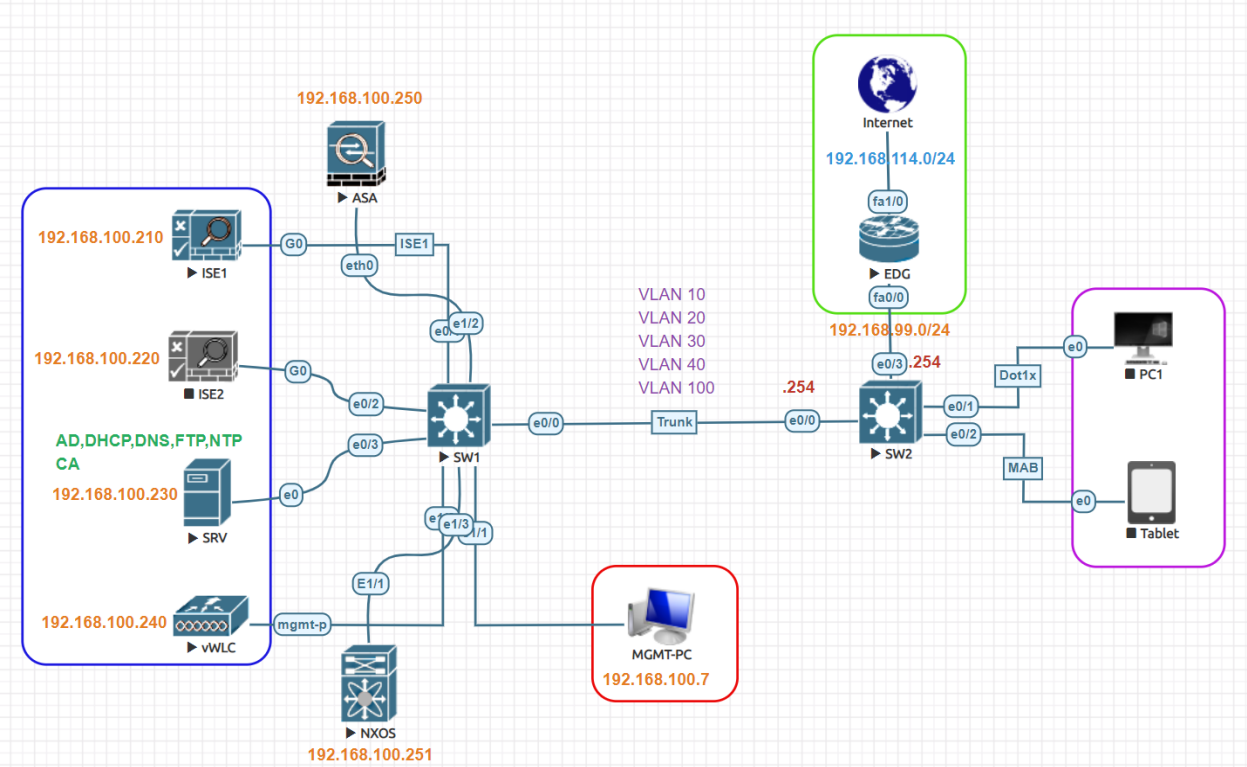
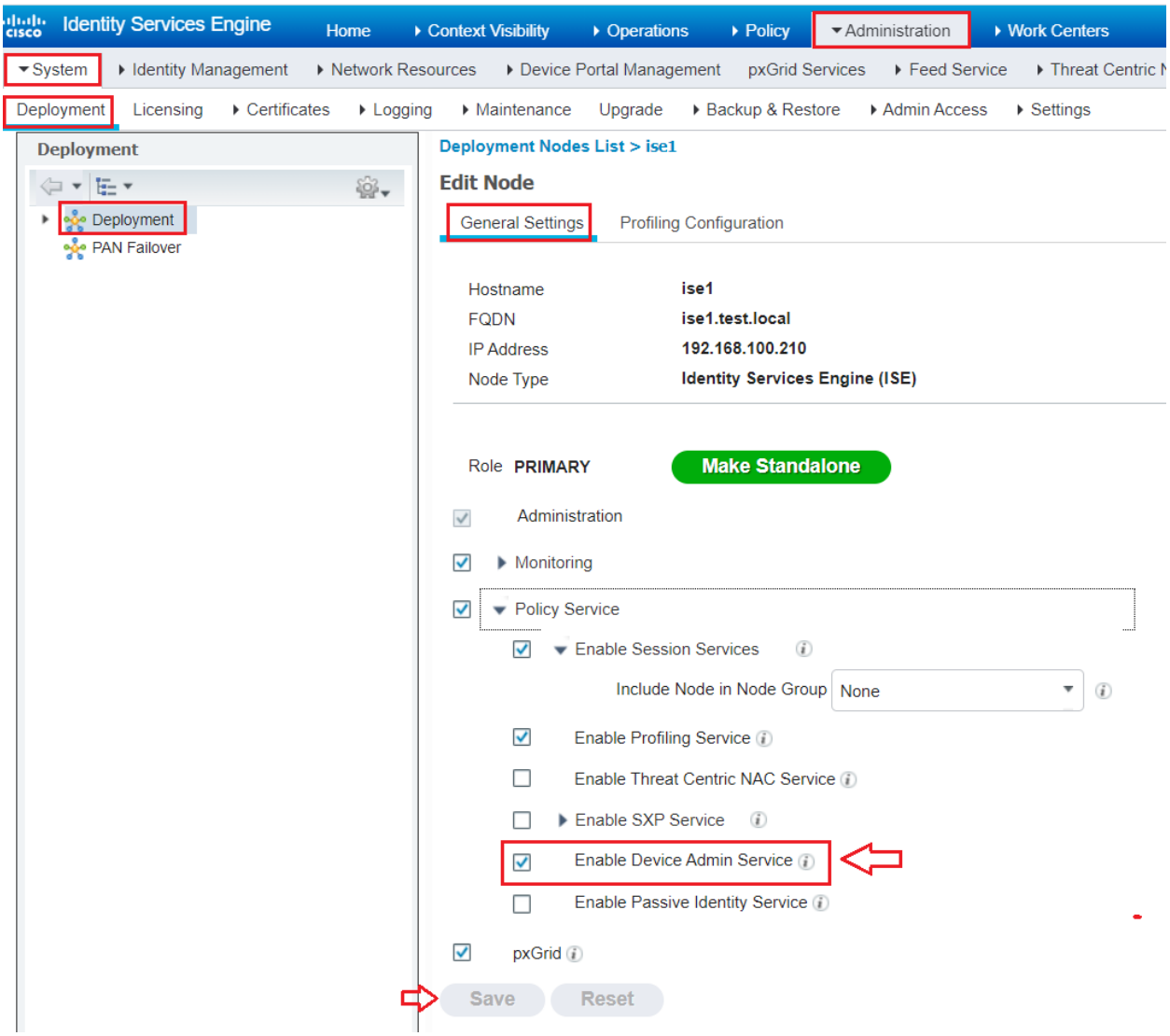
IOS Switch Device Administration Lab:



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 IOS Switch
Authentication Switch MGMT IP	192.168.100.254
NXOS TACACS Interface	Ethernet 1/3
Network Device IP Address	192.168.100.254

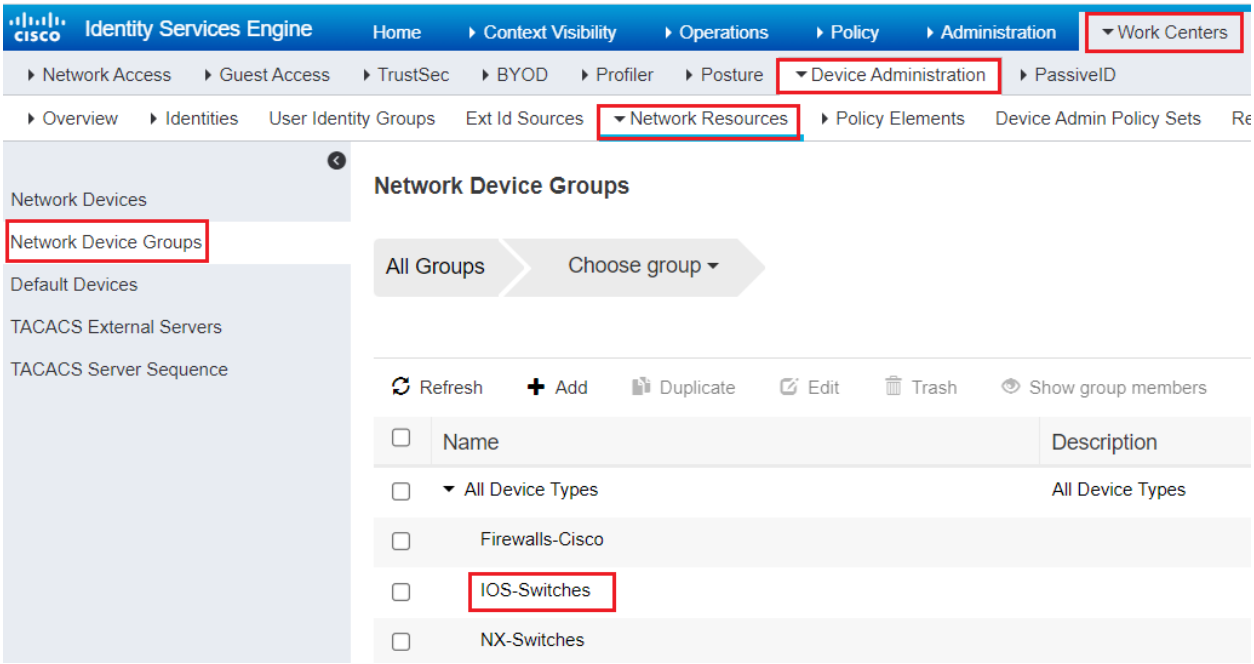
Enable TACACS+:

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



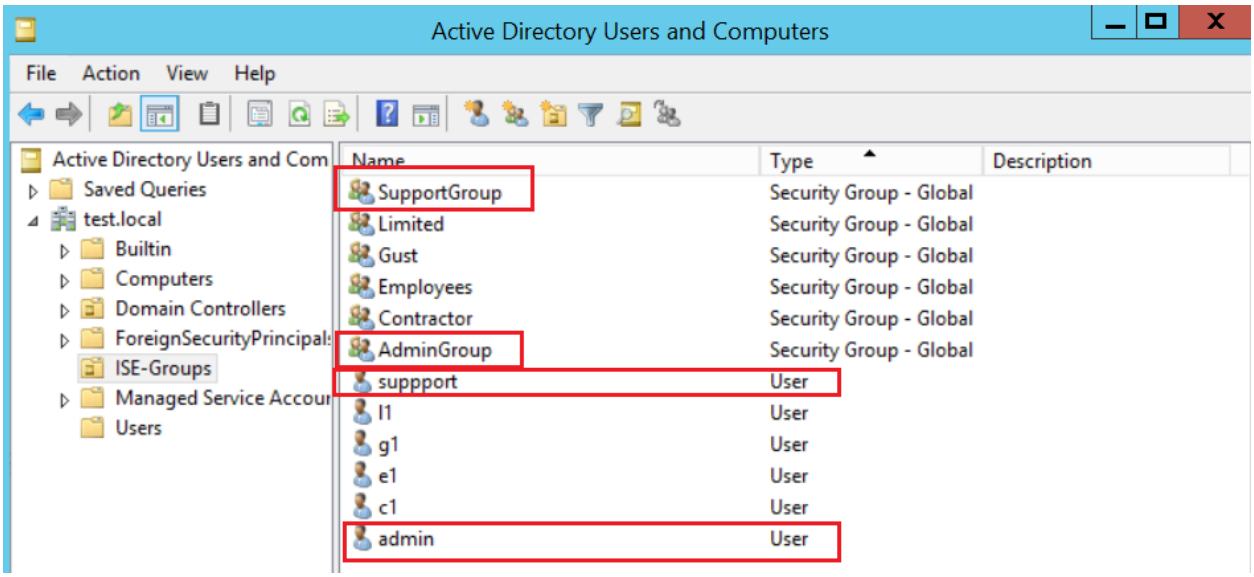
Create Device Groups:

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

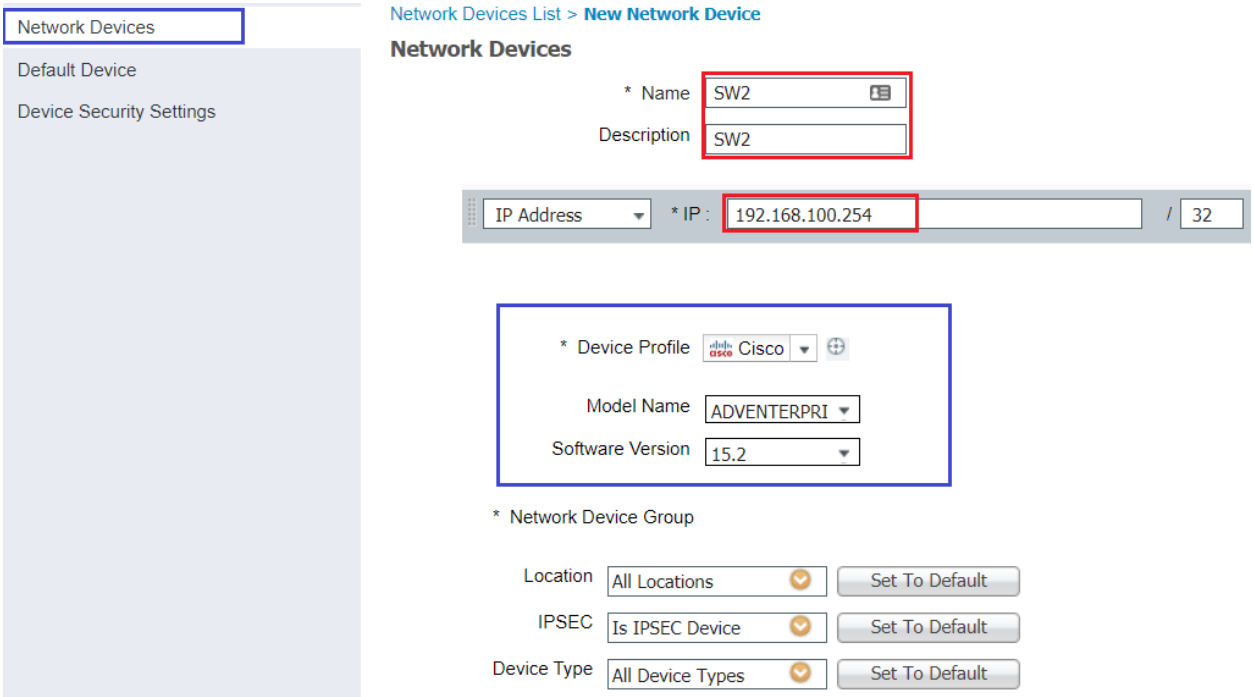


Choose Administration > Identity Management > External Identity Sources > Active Directory. Click the Groups Tab. Click on Add and then Select Groups from Directory.

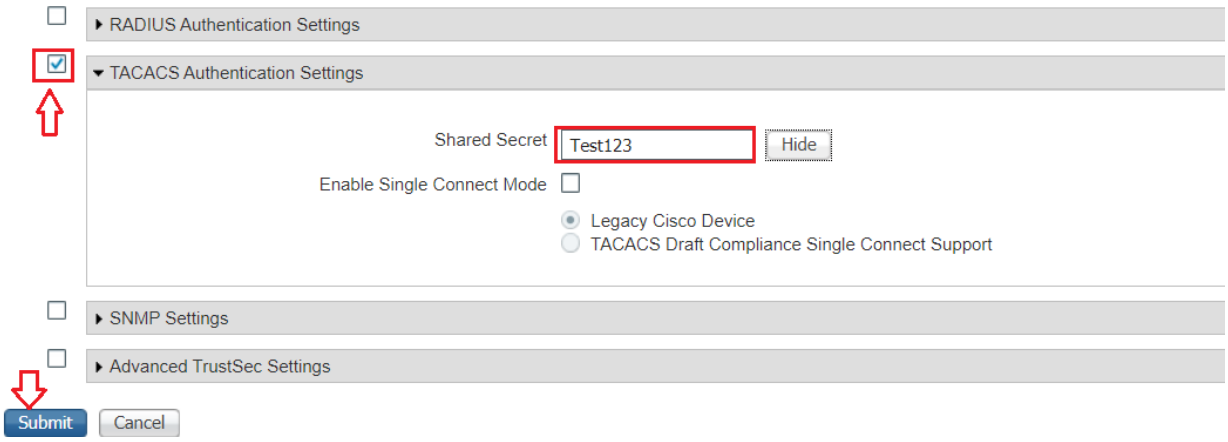
Adding Network Devices:

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

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

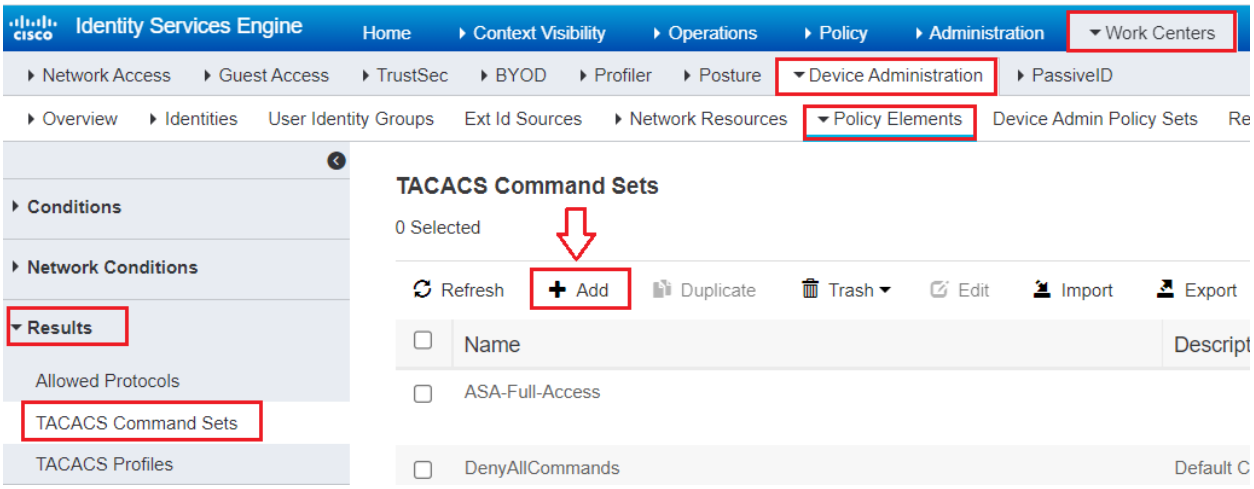


Configure TACACS authentication Settings put Shared Secret Key in this case Test123

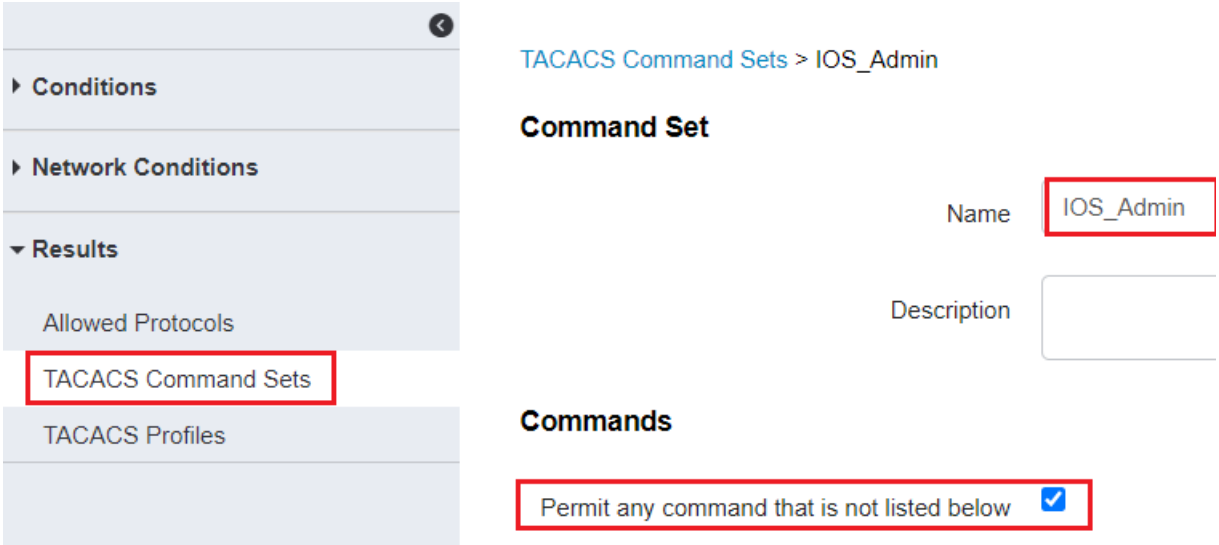


Create Command Sets:

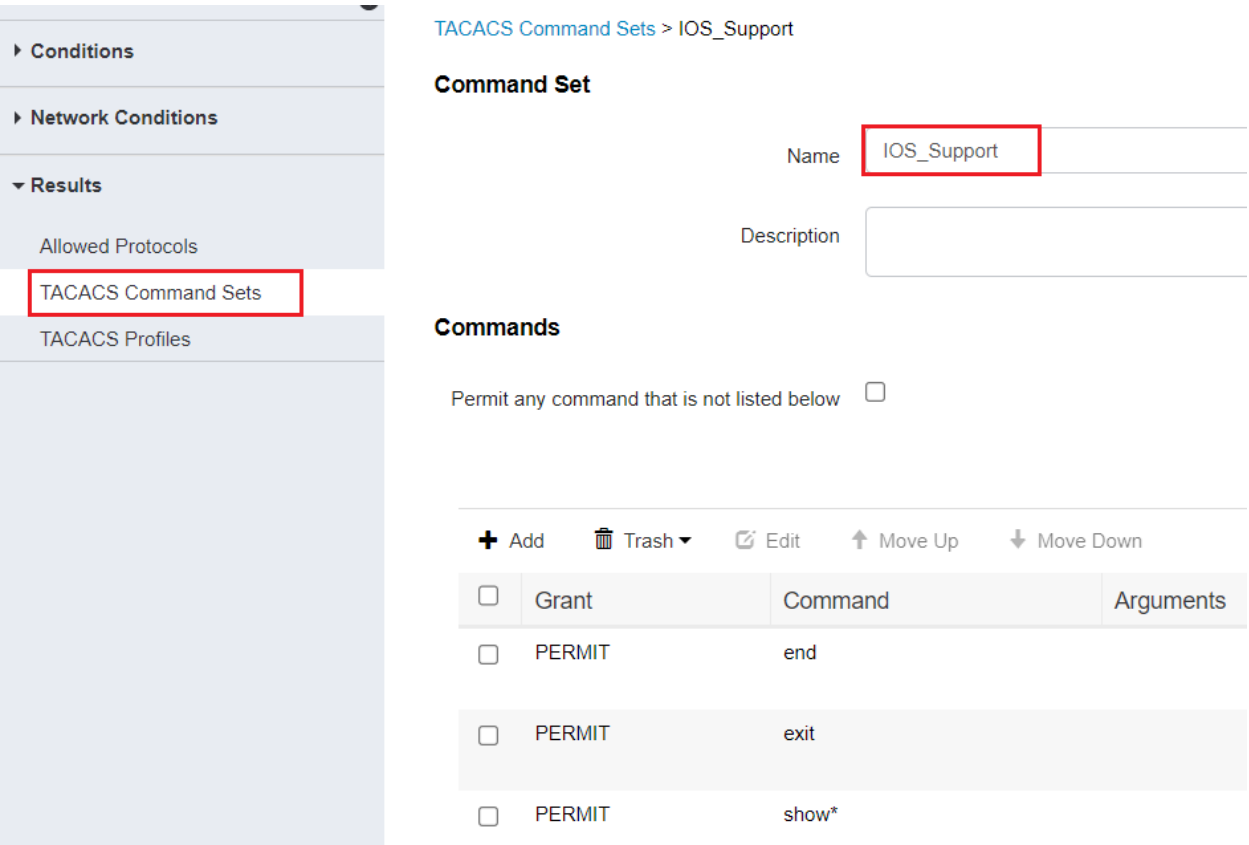
We will create two TACACS Command Sets for each profile. Navigate to Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets. Click Add



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

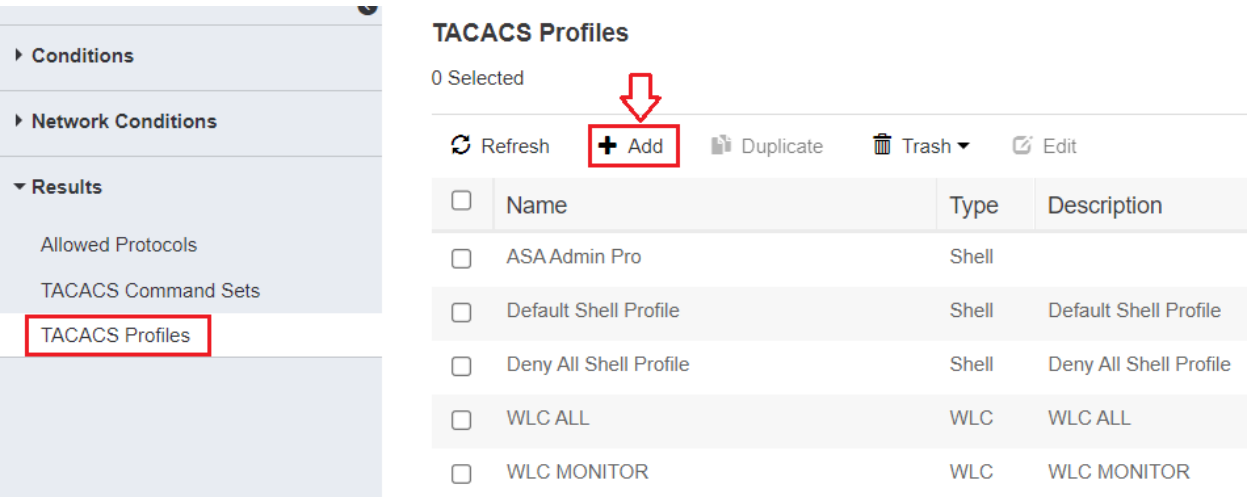


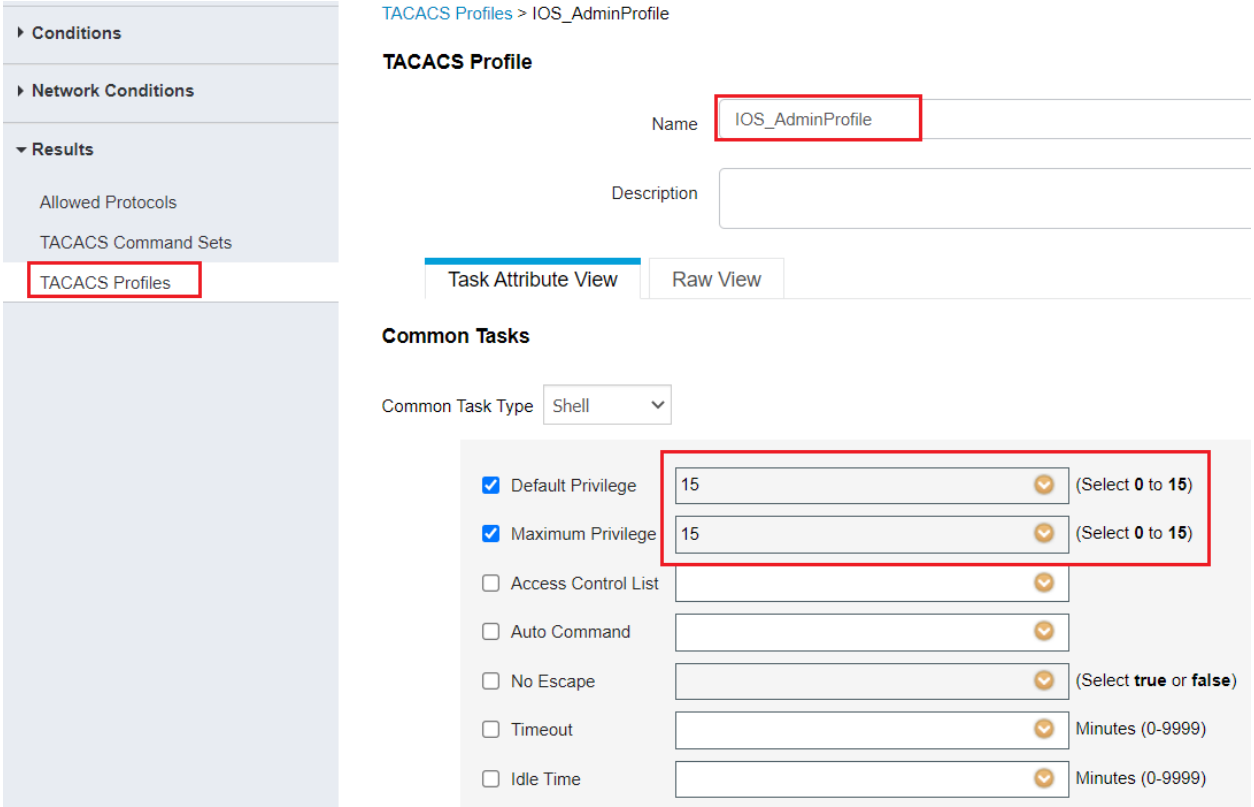
Another command set named IOS_Support is created that allows only show and few other commands. * is used for wild card.

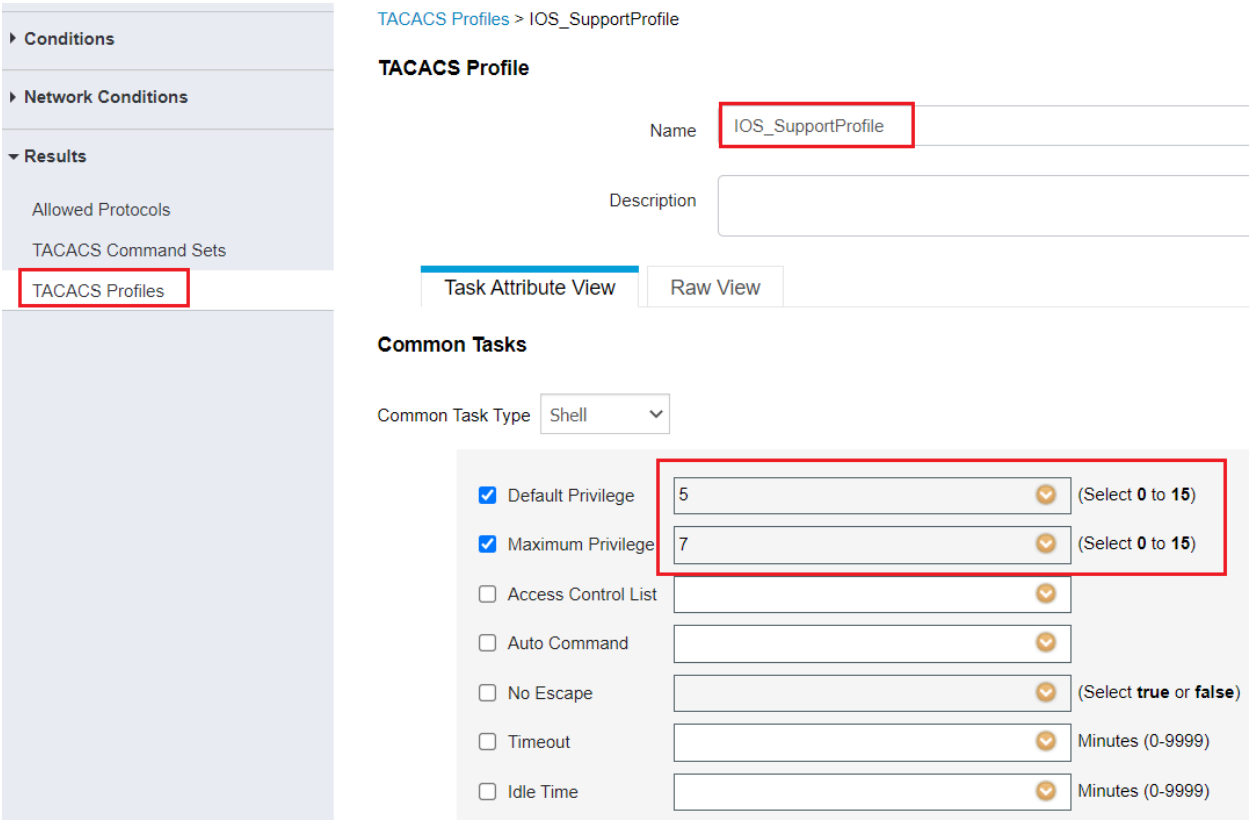


Create TACACS Profiles:

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.

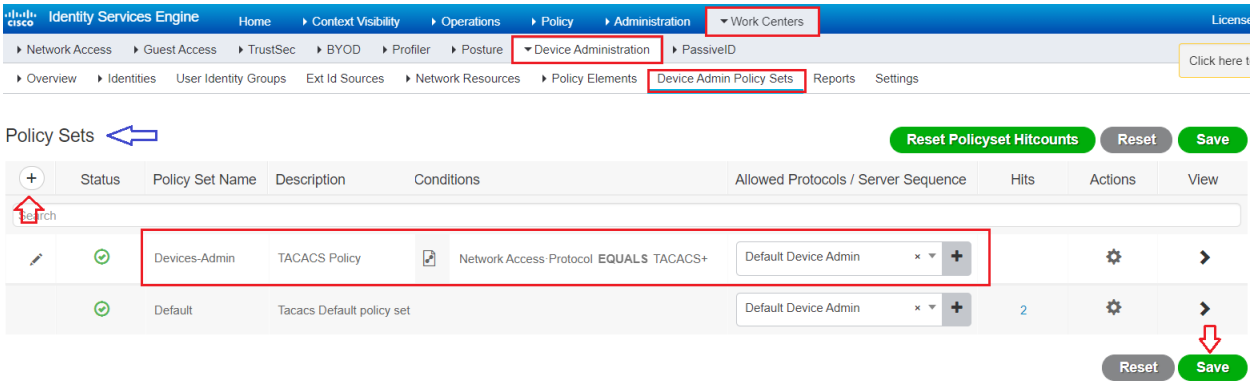



Conditions
Network Conditions
Results
Allowed Protocols
TACACS Command Sets
TACACS Profiles
TACACS Profiles > IOS_AdminProfile
TACACS Profile
Name
IOS_AdminProfile
Description
Task Attribute View
Raw View
Common Tasks
Common Task Type
Shell
Default Privilege
15
(Select 0 to 15)
Maximum Privilege
15
(Select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

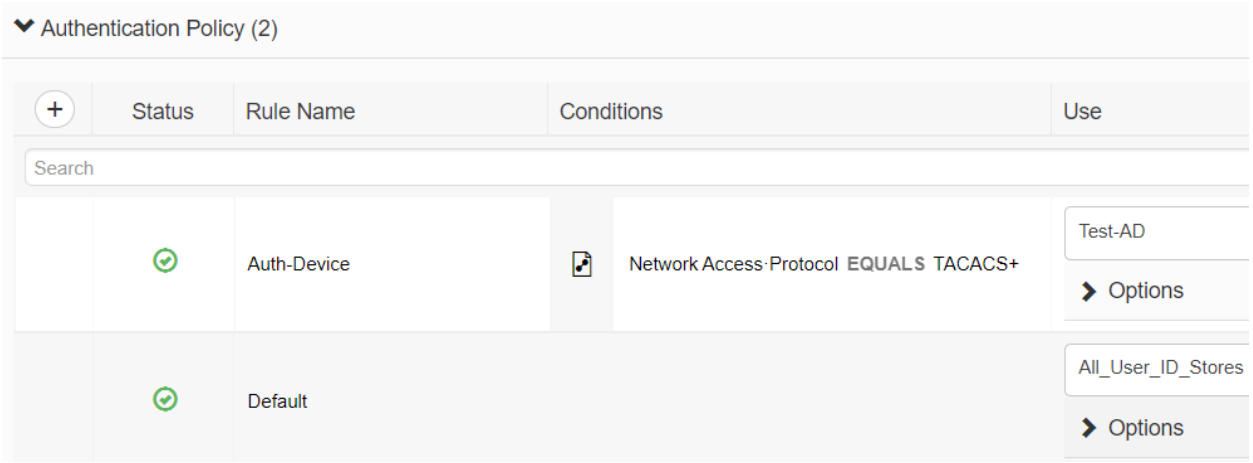

Conditions
Network Conditions
Results
Allowed Protocols
TACACS Command Sets
TACACS Profiles
TACACS Profiles > IOS_SupportProfile
TACACS Profile
Name
IOS_SupportProfile
Description
Task Attribute View
Raw View
Common Tasks
Common Task Type
Shell
Default Privilege
5
(Select 0 to 15)
Maximum Privilege
7
(Select 0 to 15)
Access Control List
Auto Command
No Escape
(Select true or false)
Timeout
Minutes (0-9999)
Idle Time
Minutes (0-9999)

Device Administration Policy:

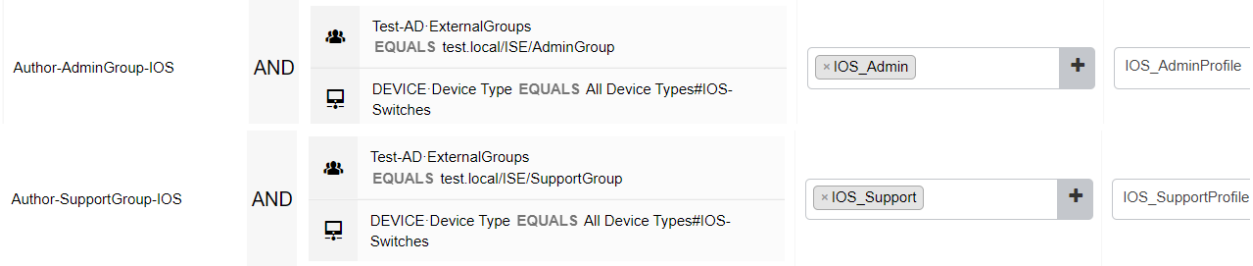
Here we will call all the items configured earlier. Navigate to Work Centers > Device Administration > Device Admin Policy Sets and add new policy or use default. Click small arrow button on right side of policy to expand.



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



Then, configure authorization Policies under 'Authorization Policy'.



Cisco IOS Switch Configuration:

```
SW2(config)#aaa new-model
SW2(config)#tacacs server ISE
SW2(config-server-tacacs)#address ipv4 192.168.100.210
SW2(config-server-tacacs)#key Test123
SW2(config)#aaa authentication login default group tacacs+ local
SW2(config)#aaa authentication enable default group tacacs+ enable
SW2(config)#aaa authorization exec default group tacacs+ local
SW2(config)#aaa authorization commands 0 default group tacacs+ local
SW2(config)#aaa authorization commands 1 default group tacacs+ local
SW2(config)#aaa authorization commands 15 default group tacacs+ local
SW2(config)#aaa authorization config-commands
SW2(config)#aaa accounting exec default start-stop group tacacs+
SW2(config)#aaa accounting commands 0 default start-stop group tacacs+
SW2(config)#aaa accounting commands 1 default start-stop group tacacs+
SW2(config)#aaa accounting commands 15 default start-stop group tacacs+
SW2(config)#aaa accounting connection default start-stop group tacacs+
```

```
SW2(config)#line vty 0 4
SW2(config-line)#authorization commands 0 default
SW2(config-line)#authorization commands 1 default
SW2(config-line)#authorization commands 15 default
SW2(config-line)#authorization exec default
SW2(config-line)#login authentication default
SW2(config-line)#accounting exec default
SW2(config-line)#accounting commands 0 default
SW2(config-line)#accounting commands 1 default
SW2(config-line)#accounting commands 15 default
SW2(config-line)#accounting connection default
```

Testing and Verification:

We can test our configuration by login into the Cisco IOS Switch by SSH. Let's try using the ad1 user credential.

192.168.100.254 - PuTTY

```
login as: ad1
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

SW2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#
```

We can monitor the authentication/authorization logs on ISE Operations > TACACS > Live Logs. The ad1 user was successfully authenticated and authorized to run privileged commands.

Overview

Request Type	Authorization
Status	Pass
Session Key	ise1/428077735/91
Message Text	Device-Administration: Command Authorization succeeded
Username	ad1
Authorization Policy	Device-Policy >> Author-AdminGroup-IOS
Shell Profile	
Matched Command Set	IOS_Admin
Command From Device	configure terminal

Now let's try again using support account users sp1. The user sp1 was successfully authenticated but wasn't authorized to run privileged commands.

192.168.100.254 - PuTTY

```
login as: sp1
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

SW2#config t
       ^
% Invalid input detected at '^' marker.

SW2#
```

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

Overview

Request Type	Authorization
Status	Pass
Session Key	ise1/428077735/94
Message Text	Device-Administration: Session Authorization succeeded
Username	sp1
Authorization Policy	Device-Policy >> Author-SupportGroup-IOS
Shell Profile	IOS_SupportProfile
Matched Command Set	
Command From Device	