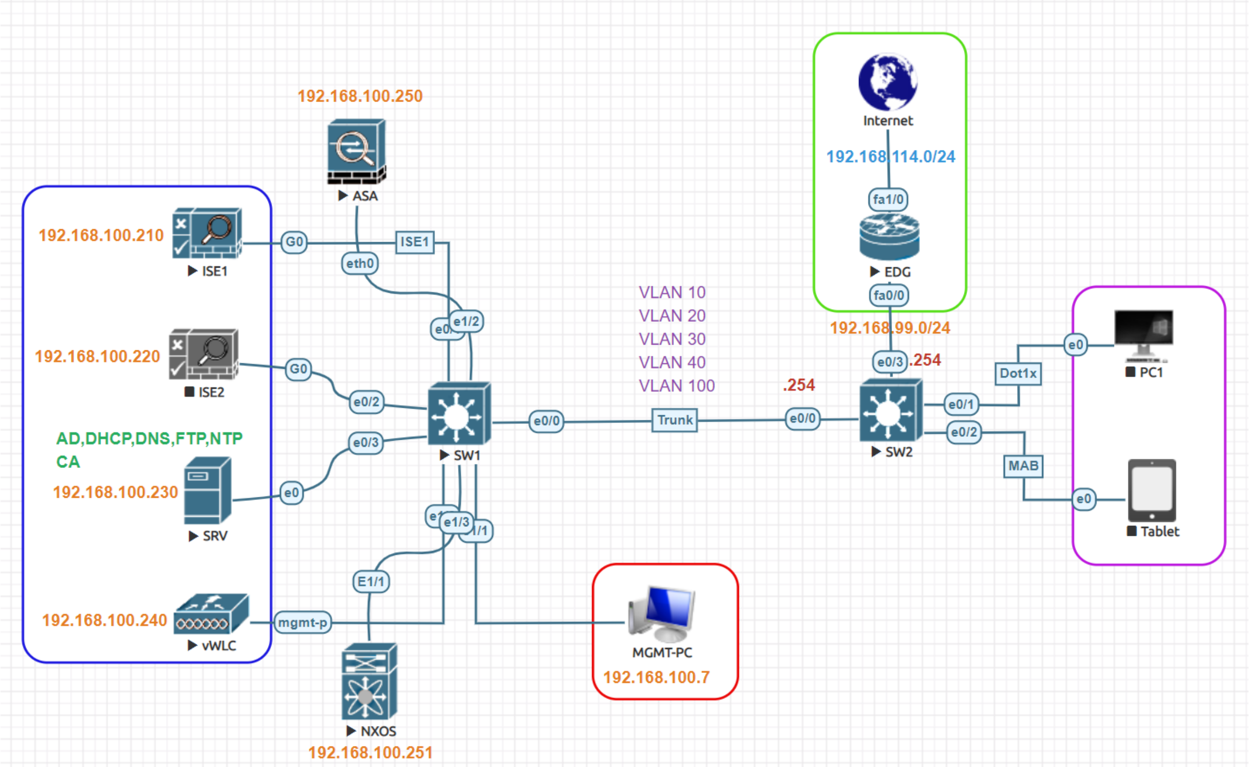
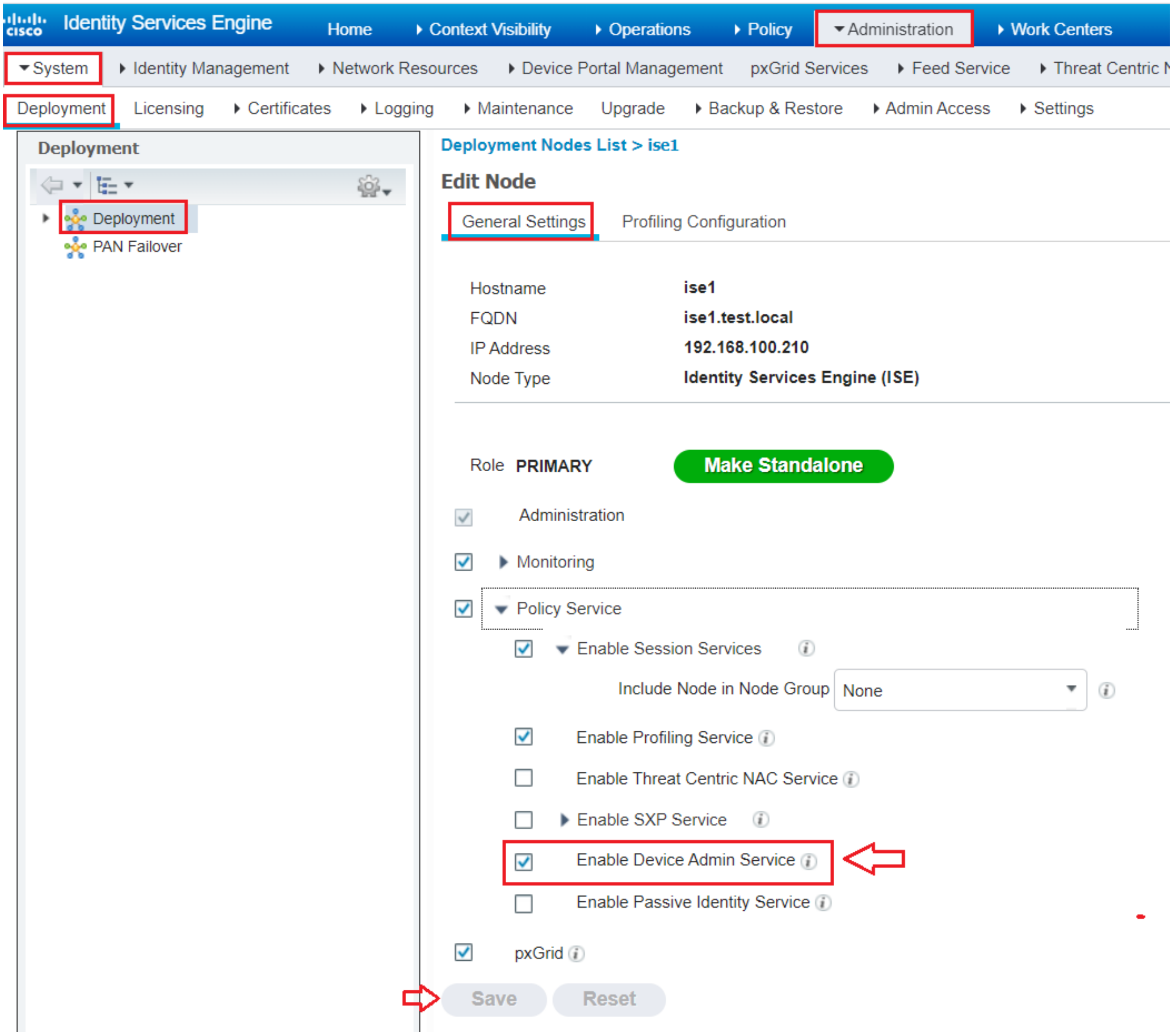
# NX-OS Device Administration Lab:



| | |
|---|---|
| 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 Nexus Switch |
| Authentication Switch MGMT IP | 192.168.100.254 |
| NXOS TACACS Interface | Ethernet 1/3 |
| Network Device IP Address | 192.168.100.251 |

## Enable TACACS+:

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



| | |
|---|---|
| Hostname | ise1 |
| FQDN | ise1.test.local |
| IP Address | 192.168.100.210 |
| Node Type | Identity Services Engine (ISE) |

Role PRIMARY

☑ Administration

☑ Monitoring

☑ Policy Service

☑ Enable Session Services

Include Node in Node Group None

☑ Enable Profiling Service

□ Enable Threat Centric NAC Service

□ Enable SXP Service

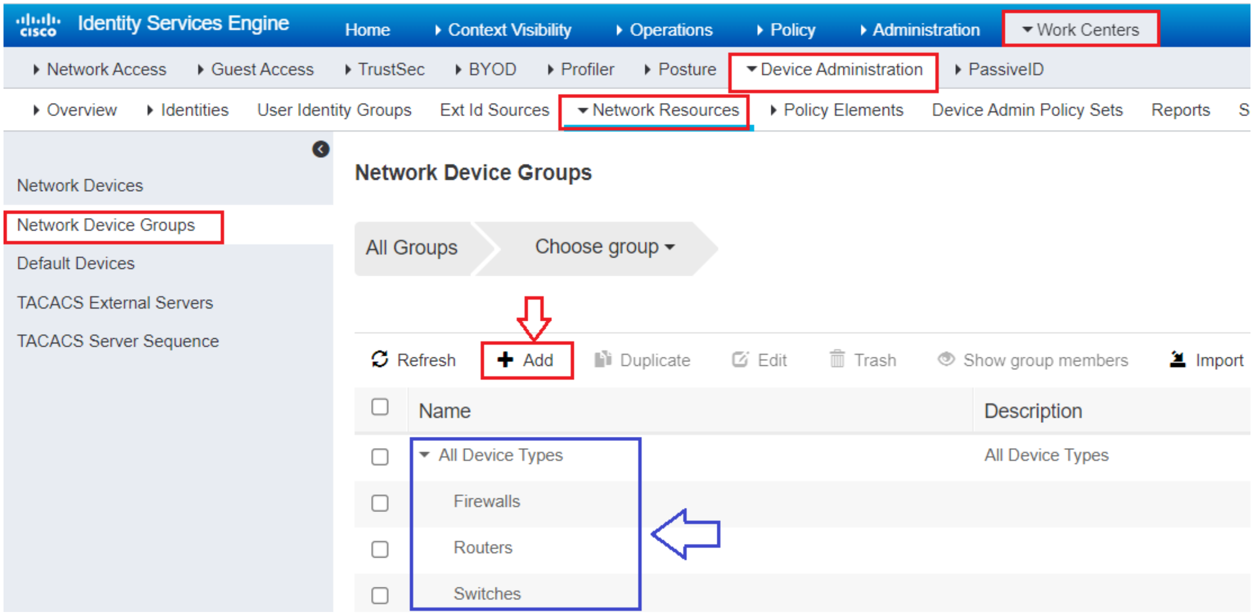
☑ Enable Device Admin Service

□ Enable Passive Identity Service

☑ pxGrid

## Create Device Groups:

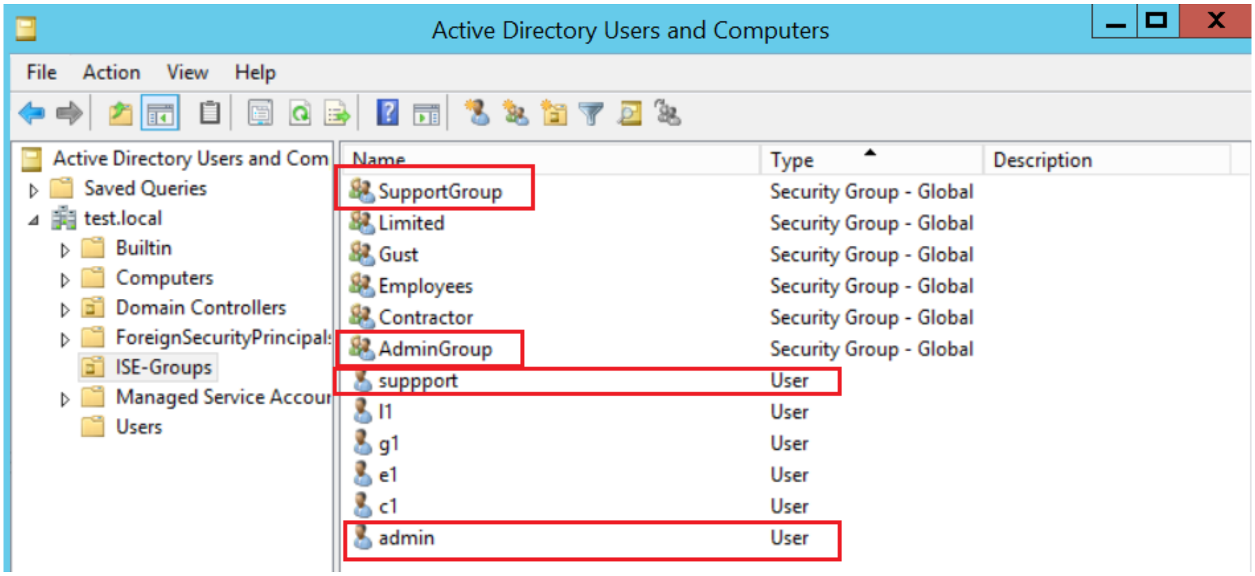
Create device groups. We can group devices based on type or location. Work Centers> Device Administration > Network Resources > Network Device Groups



| | Name | Description |
|---|---|---|
| □ | All Device Types | All Device Types |
| □ | Firewalls | |
| □ | Routers | |
| □ | Switches | |

## 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



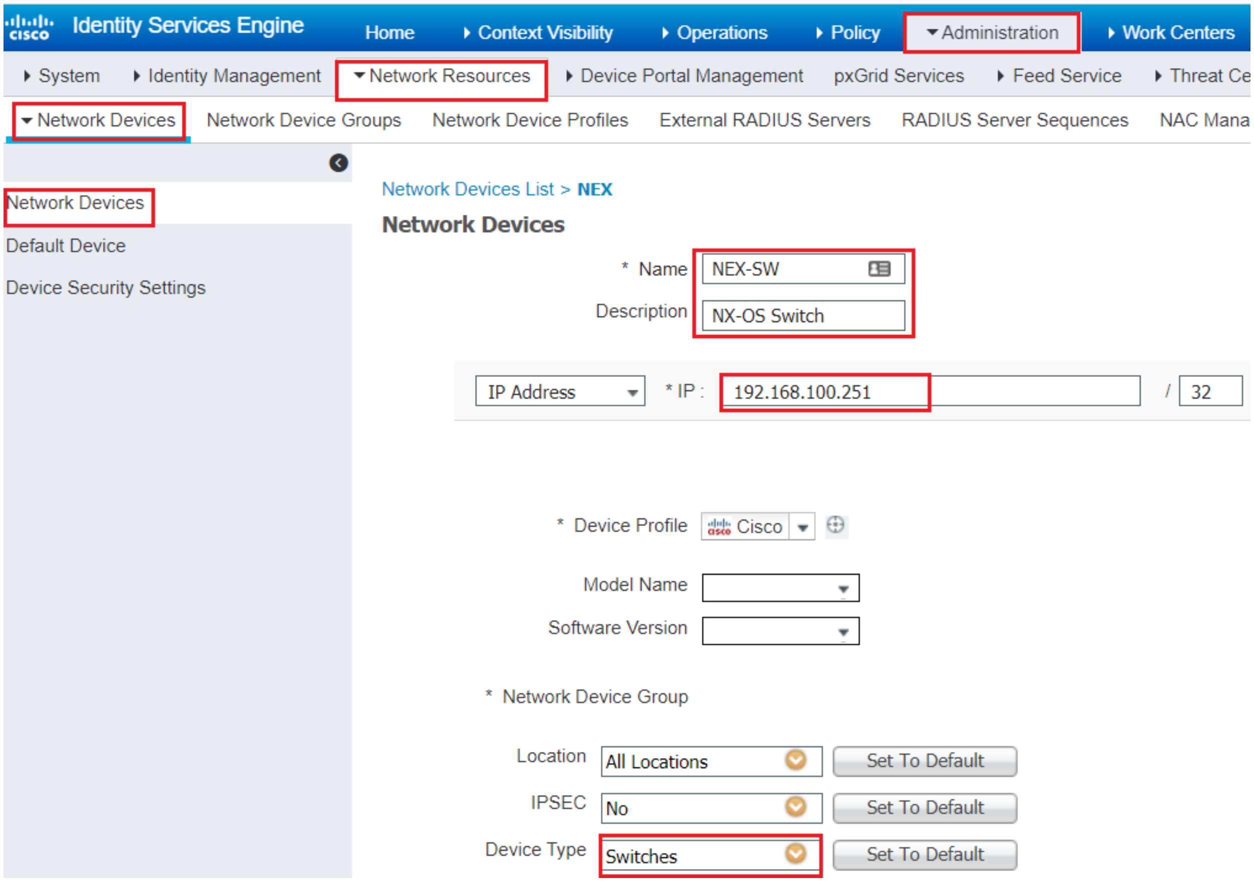
| Name | Type | Description |
|---|---|---|
| SupportGroup | Security Group - Global | |
| Limited | Security Group - Global | |
| Gust | Security Group - Global | |
| Employees | Security Group - Global | |
| Contractor | Security Group - Global | |
| AdminGroup | Security Group - Global | |
| suppport | User | |
| l1 | User | |
| g1 | User | |
| e1 | User | |
| c1 | User | |
| admin | User | |

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.



Network Devices

* Name: NEX-SW

Description: NX-OS Switch

IP Address * IP : 192.168.100.251 / 32

* Device Profile: Cisco

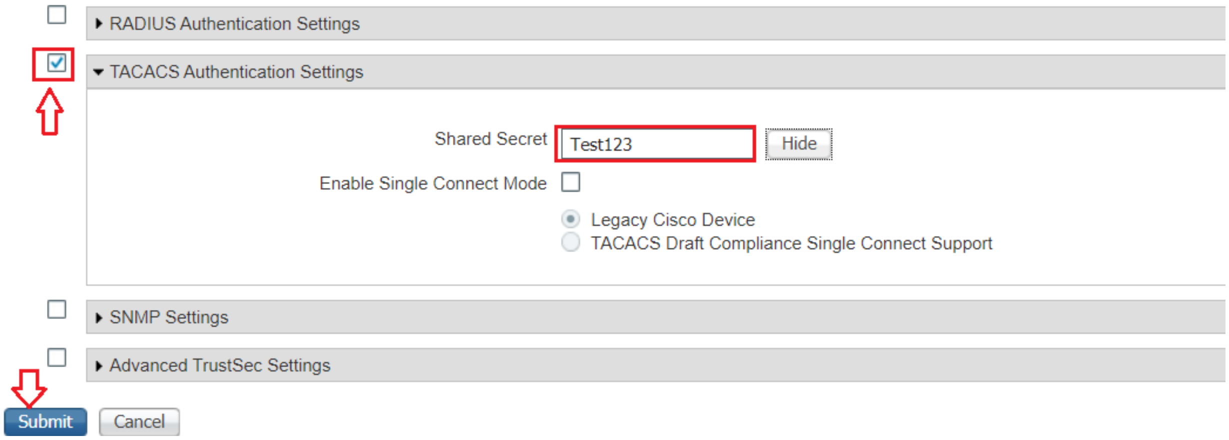
Model Name:

Software Version:

* Network Device Group

| | | |
|---|---|---|
| Location | All Locations | Set To Default |
| IPSEC | No | Set To Default |
| Device Type | Switches | Set To Default |

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



□ RADIUS Authentication Settings

☑ TACACS Authentication Settings

Shared Secret: Test123

Enable Single Connect Mode □

● Legacy Cisco Device

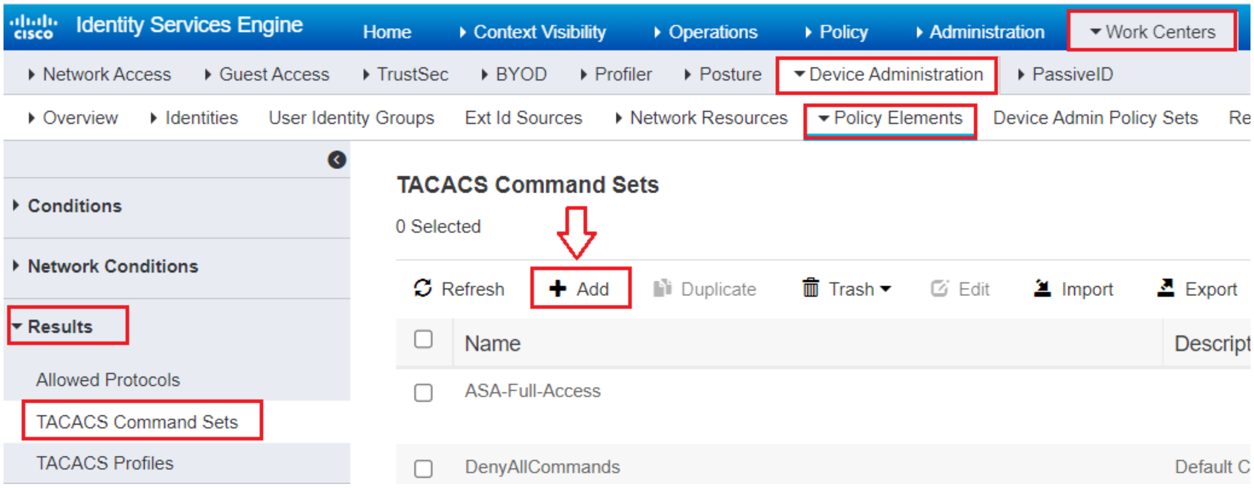
○ TACACS Draft Compliance Single Connect Support

□ SNMP Settings

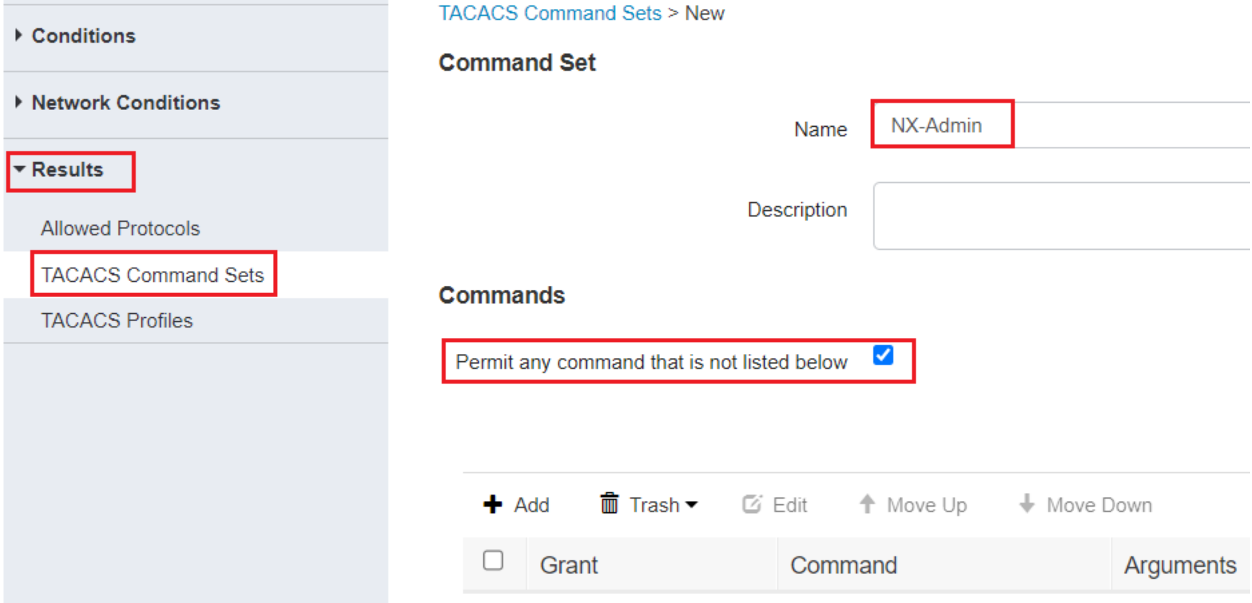
□ Advanced TrustSec Settings

## 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 NX-Admin which allows all commands. Check the box under Commands 'Permit any command that is not listed below' and don't add any command.

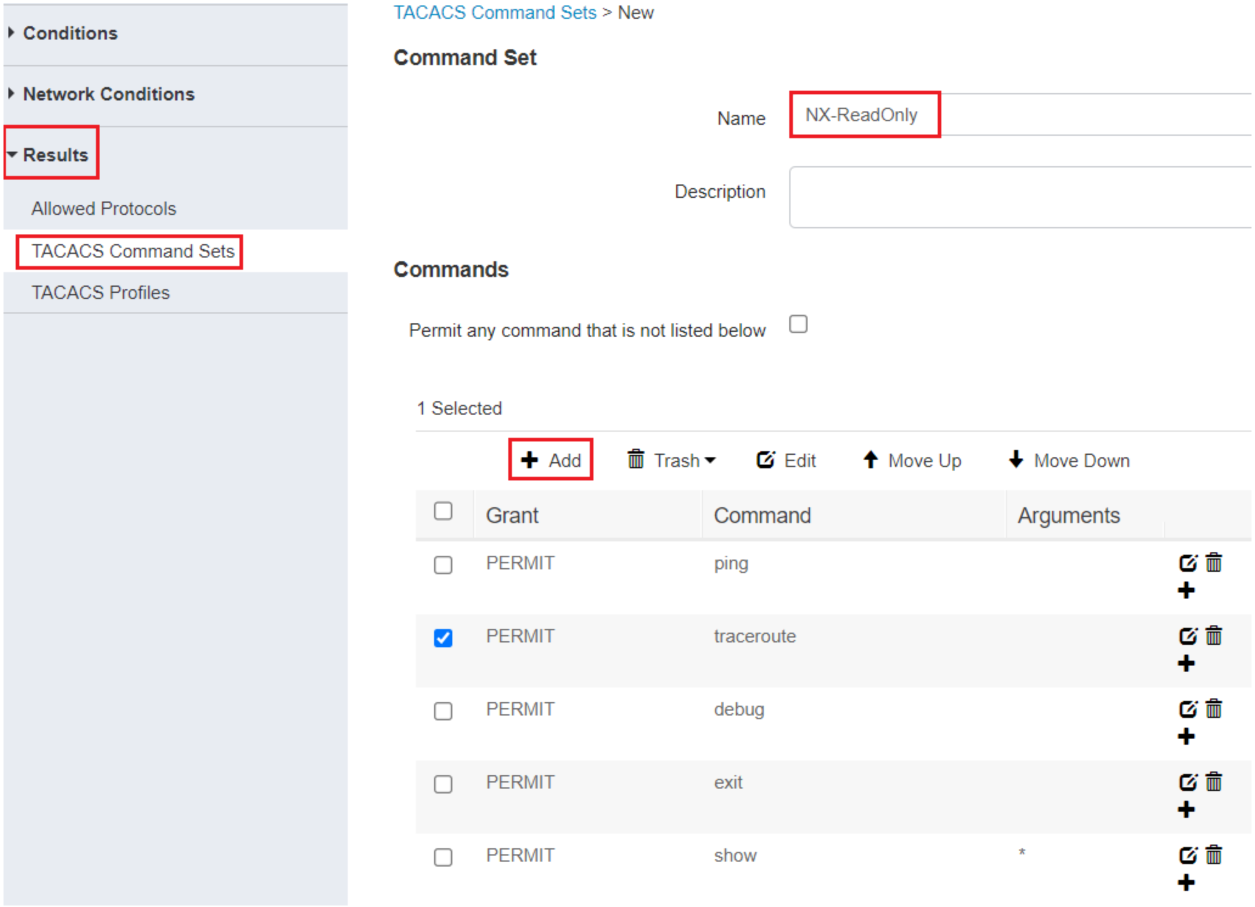


Name: NX-Admin

Description:

Permit any command that is not listed below ☑

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



**Command Set**

Name: NX-ReadOnly

Description:

**Commands**

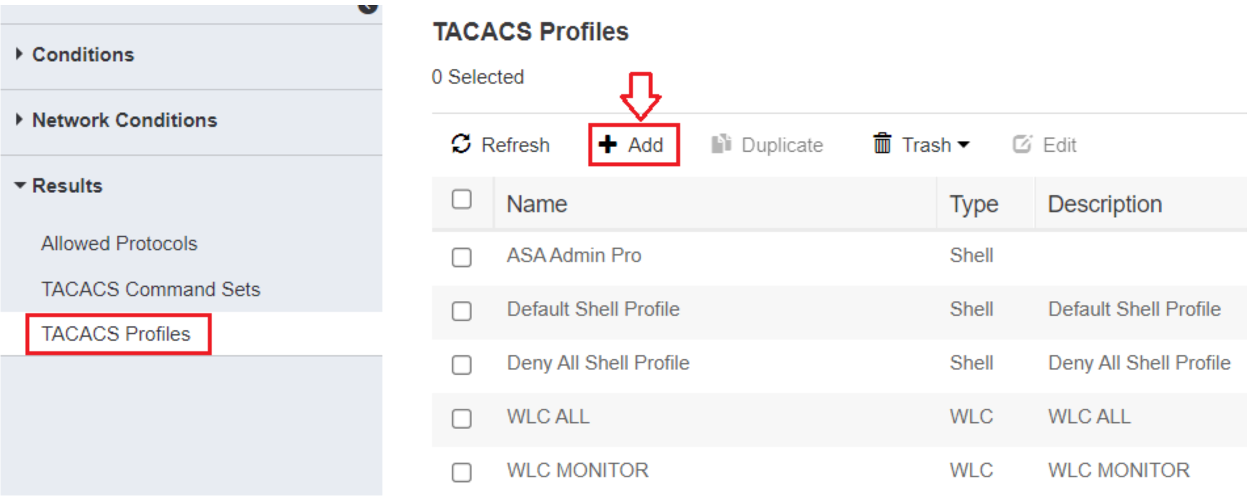
Permit any command that is not listed below □

1 Selected

| □ | Grant | Command | Arguments |
|---|---|---|---|
| □ | PERMIT | ping | |
| ☑ | PERMIT | traceroute | |
| □ | PERMIT | debug | |
| □ | PERMIT | exit | |
| □ | PERMIT | show | * |

## Create TACACS Profiles:

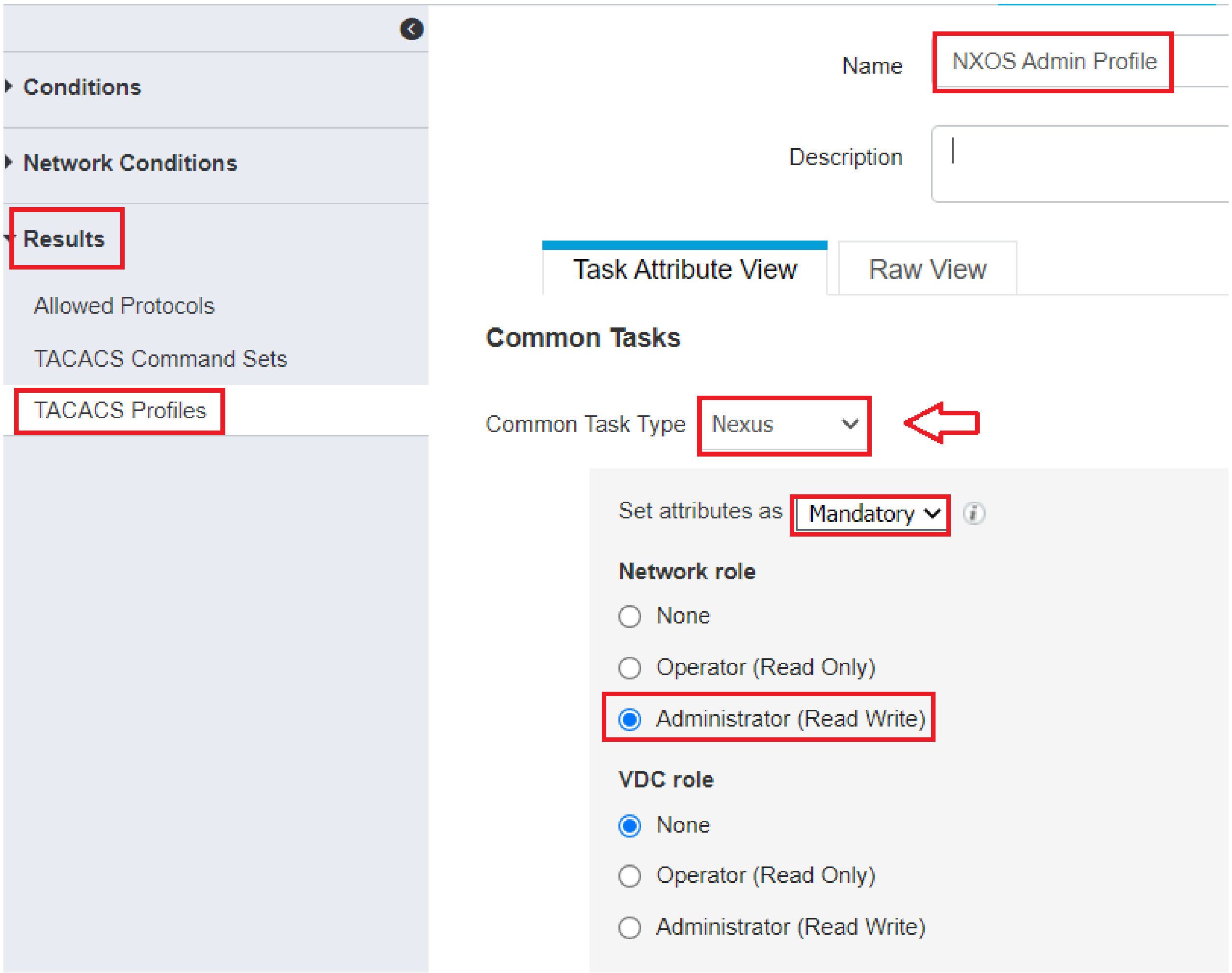
Let’s create two TACACS Profiles for our Admins and Support Users. Navigate to Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles click Add.



**TACACS Profiles**

0 Selected

| □ | Name | Type | Description |
|---|---|---|---|
| □ | ASA Admin Pro | Shell | |
| □ | Default Shell Profile | Shell | Default Shell Profile |
| □ | Deny All Shell Profile | Shell | Deny All Shell Profile |
| □ | WLC ALL | WLC | WLC ALL |
| □ | WLC MONITOR | WLC | WLC MONITOR |



Name: NXOS Admin Profile

Description:

Common Tasks

Common Task Type: Nexus

Set attributes as: Mandatory

Network role

○ None

○ Operator (Read Only)

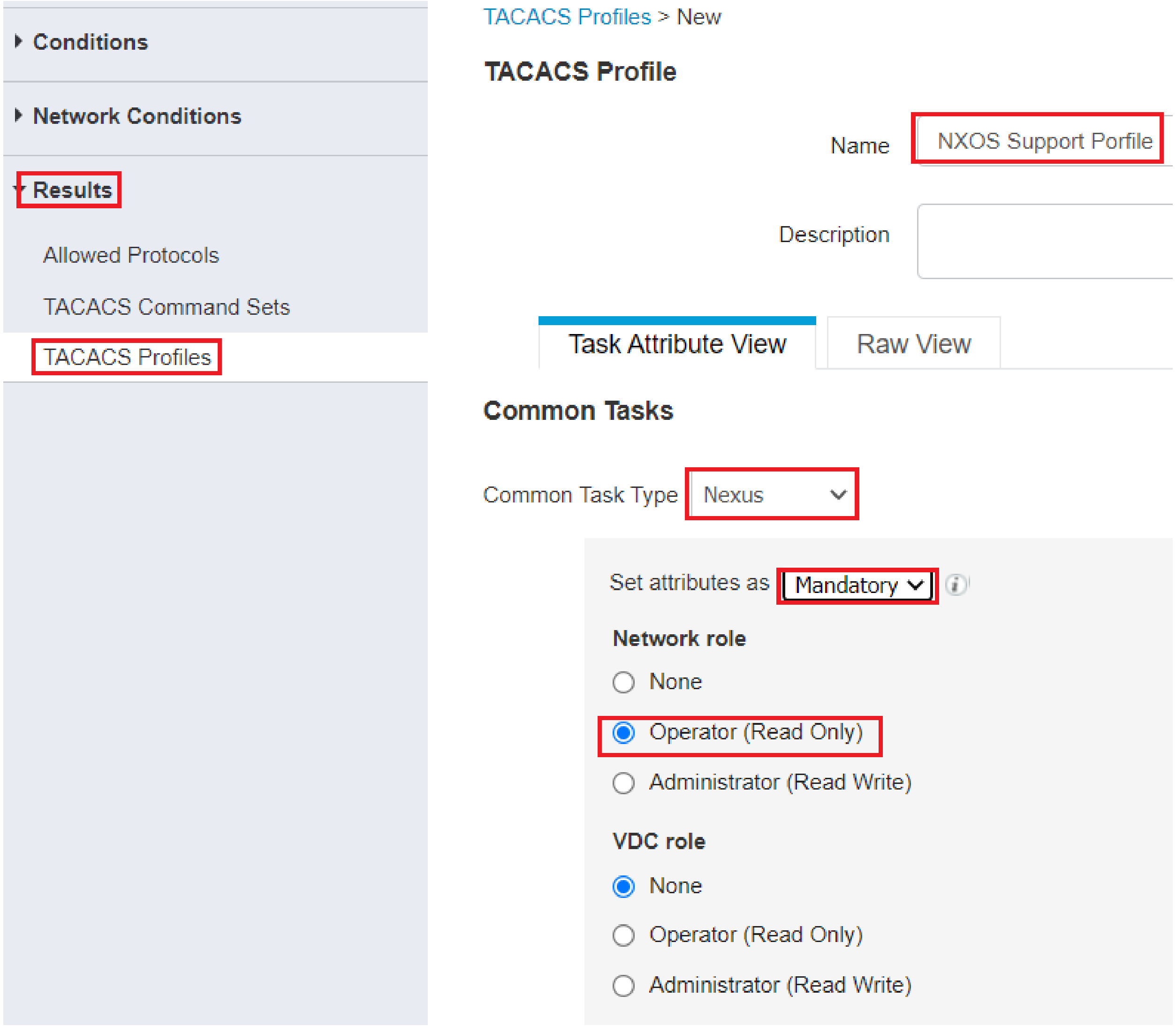
● Administrator (Read Write)

VDC role

● None

○ Operator (Read Only)

○ Administrator (Read Write)



TACACS Profiles > New

TACACS Profile

Name: NXOS Support Porfile

Description:

Common Tasks

Common Task Type: Nexus

Set attributes as: Mandatory

Network role

○ None

● Operator (Read Only)

○ Administrator (Read Write)

VDC role

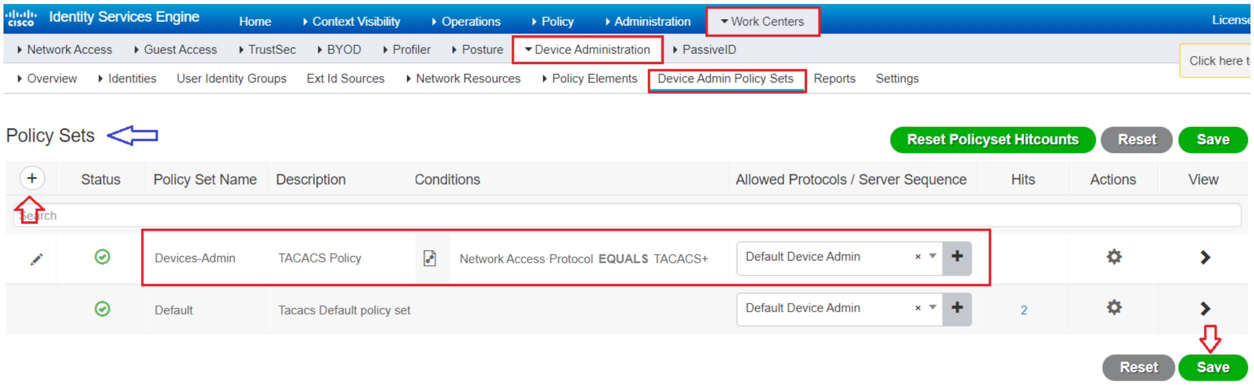
● None

○ Operator (Read Only)

○ Administrator (Read Write)

## 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.



Identity Services Engine | Home | ▸ Context Visibility | ▸ Operations | ▸ Policy | ▸ Administration | ▾ Work Centers | License

▸ Network Access | ▸ Guest Access | ▸ TrustSec | ▸ BYOD | ▸ Profiler | ▸ Posture | ▾ Device Administration | ▸ PassiveID | Click here t

▸ Overview | ▸ Identities | User Identity Groups | Ext Id Sources | ▸ Network Resources | ▸ Policy Elements | Device Admin Policy Sets | Reports | Settings

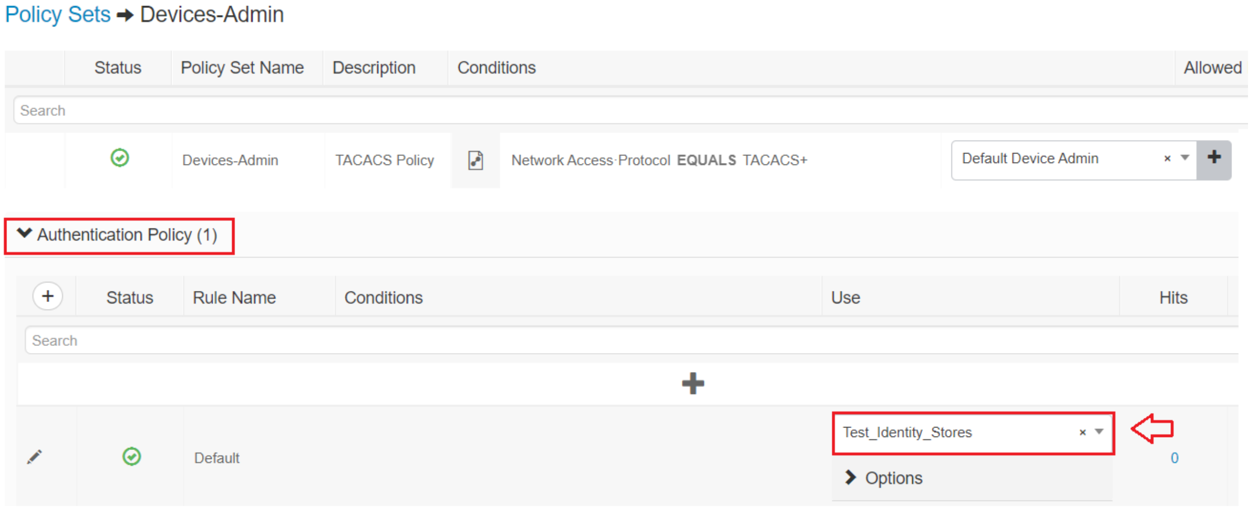
Policy Sets

Reset Policyset Hitcounts | Reset | Save

| + | Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits | Actions | View |
|---|---|---|---|---|---|---|---|---|
| Search | | | | | | | | |
| | ✓ | Devices-Admin | TACACS Policy | Network Access·Protocol **EQUALS** TACACS+ | Default Device Admin | | ⚙ | > |
| | ✓ | Default | Tacacs Default policy set | | Default Device Admin | 2 | ⚙ | > |

Reset | Save

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



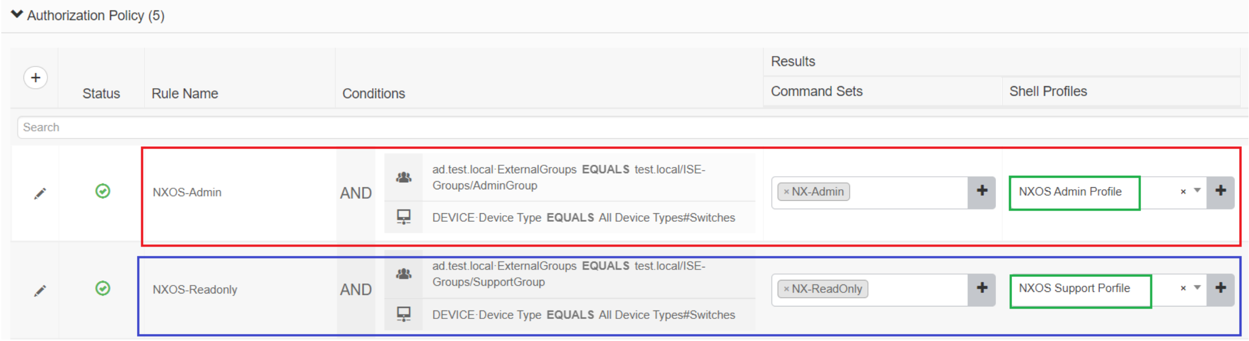
Policy Sets ➡ Devices-Admin

| Status | Policy Set Name | Description | Conditions | Allowed |
|---|---|---|---|---|
| Search | | | | |
| ✓ | Devices-Admin | TACACS Policy | Network Access·Protocol **EQUALS** TACACS+ | Default Device Admin |

▾ Authentication Policy (1)

| + | Status | Rule Name | Conditions | Use | Hits |
|---|---|---|---|---|---|
| Search | | | | | |
| | ✓ | Default | | Test_Identity_Stores<br>> Options | 0 |

Then, configure authorization Policies under 'Authorization Policy'.

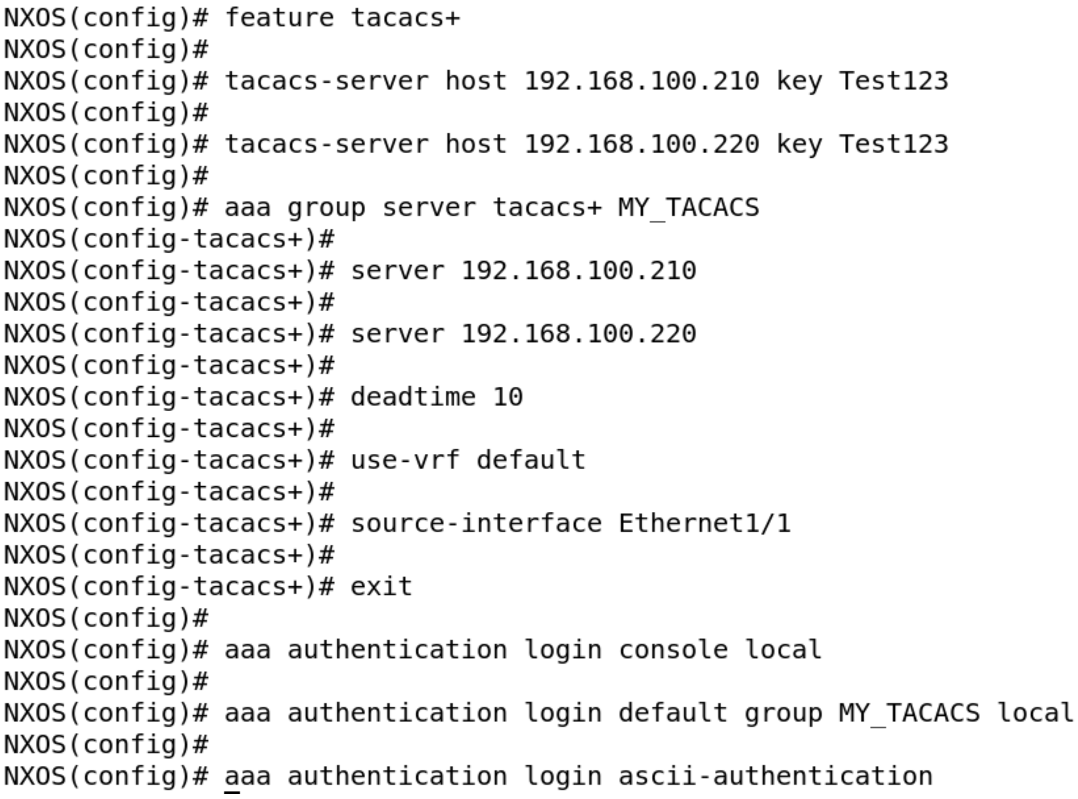


▾ Authorization Policy (5)

| + | Status | Rule Name | Conditions | Results: Command Sets | Results: Shell Profiles |
|---|---|---|---|---|---|
| Search | | | | | |
| | ✓ | NXOS-Admin | AND<br>ad.test.local·ExternalGroups **EQUALS** test.local/ISE-Groups/AdminGroup<br>DEVICE·Device Type **EQUALS** All Device Types#Switches | × NX-Admin | NXOS Admin Profile |
| | ✓ | NXOS-Readonly | AND<br>ad.test.local·ExternalGroups **EQUALS** test.local/ISE-Groups/SupportGroup<br>DEVICE·Device Type **EQUALS** All Device Types#Switches | × NX-ReadOnly | NXOS Support Porfile |

## Cisco NX-OS Configuration:

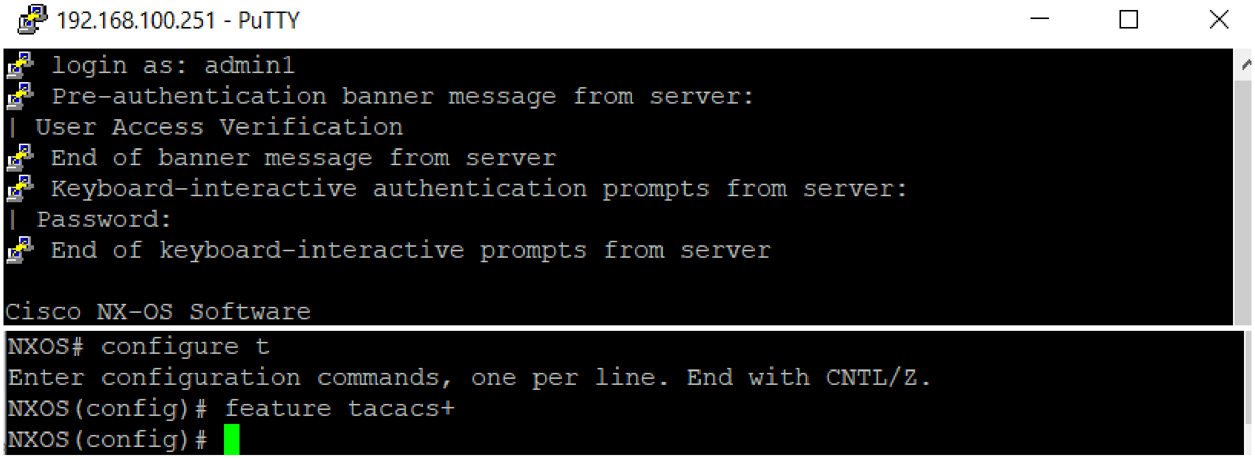
```
NXOS(config)# interface ethernet 1/1
NXOS(config-if)# no switchport
NXOS(config-if)# ip address 192.168.100.251 255.255.255.0
NXOS(config-if)# no shutdown
NXOS(config)# feature tacacs+
NXOS(config)# tacacs-server host 192.168.100.210 key Test123
NXOS(config)# tacacs-server host 192.168.100.220 key Test123
NXOS(config)# aaa group server tacacs+ MY_TACACS
NXOS(config-tacacs+)# server 192.168.100.210
NXOS(config-tacacs+)# server 192.168.100.220
NXOS(config-tacacs+)# deadtime 10
NXOS(config-tacacs+)# use-vrf default
NXOS(config-tacacs+)# source-interface Ethernet1/1
NXOS(config-tacacs+)# exit
NXOS(config)# aaa authentication login console local
NXOS(config)# aaa authentication login default group MY_TACACS local
NXOS(config)# aaa authentication login ascii-authentication
```



```
NXOS(config)# feature tacacs+
NXOS(config)#
NXOS(config)# tacacs-server host 192.168.100.210 key Test123
NXOS(config)#
NXOS(config)# tacacs-server host 192.168.100.220 key Test123
NXOS(config)#
NXOS(config)# aaa group server tacacs+ MY_TACACS
NXOS(config-tacacs+)#
NXOS(config-tacacs+)# server 192.168.100.210
NXOS(config-tacacs+)#
NXOS(config-tacacs+)# server 192.168.100.220
NXOS(config-tacacs+)#
NXOS(config-tacacs+)# deadtime 10
NXOS(config-tacacs+)#
NXOS(config-tacacs+)# use-vrf default
NXOS(config-tacacs+)#
NXOS(config-tacacs+)# source-interface Ethernet1/1
NXOS(config-tacacs+)#
NXOS(config-tacacs+)# exit
NXOS(config)#
NXOS(config)# aaa authentication login console local
NXOS(config)#
NXOS(config)# aaa authentication login default group MY_TACACS local
NXOS(config)#
NXOS(config)# aaa authentication login ascii-authentication
```

## Testing and Verification:

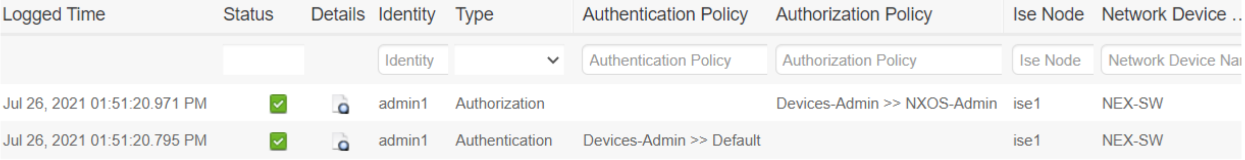
We can test our configuration by login into the Cisco ASA Firewall by SSH. Let's try using the admin1 user credential.



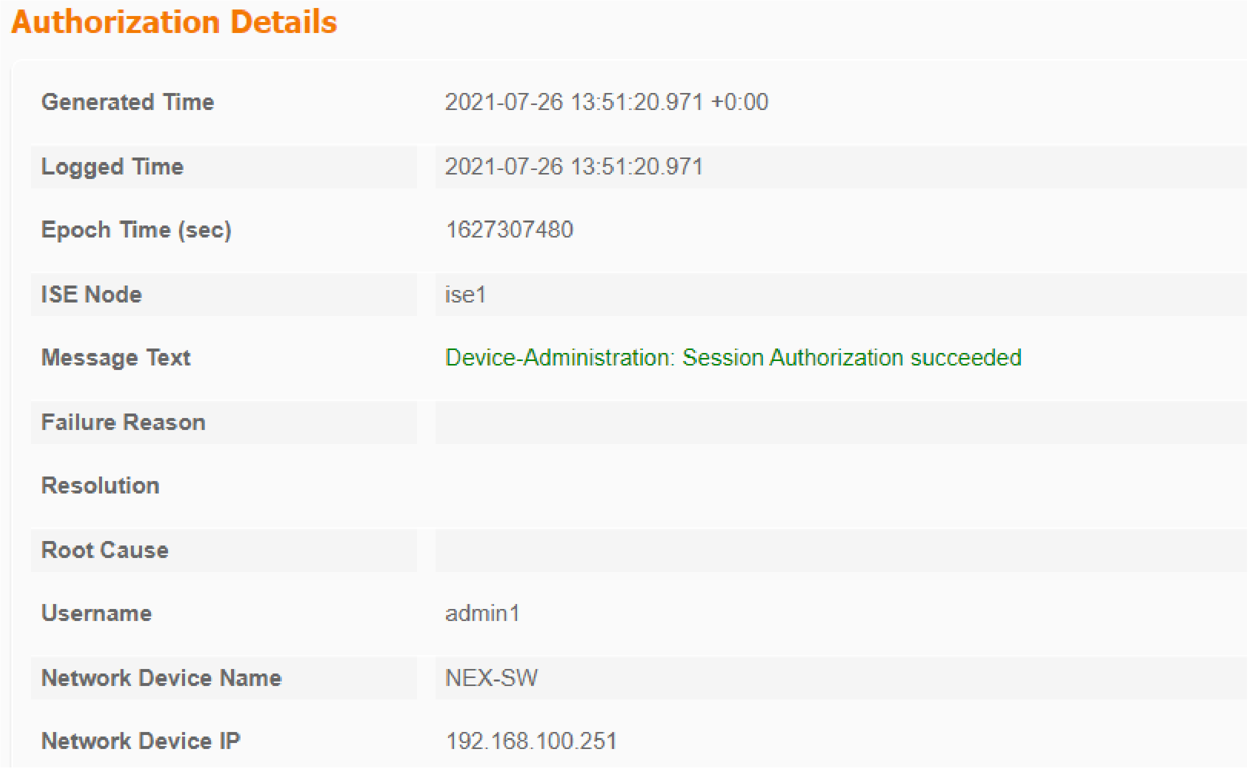
```
login as: admin1
Pre-authentication banner message from server:
| User Access Verification
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

Cisco NX-OS Software
NXOS# configure t
Enter configuration commands, one per line. End with CNTL/Z.
NXOS(config)# feature tacacs+
NXOS(config)#
```

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.



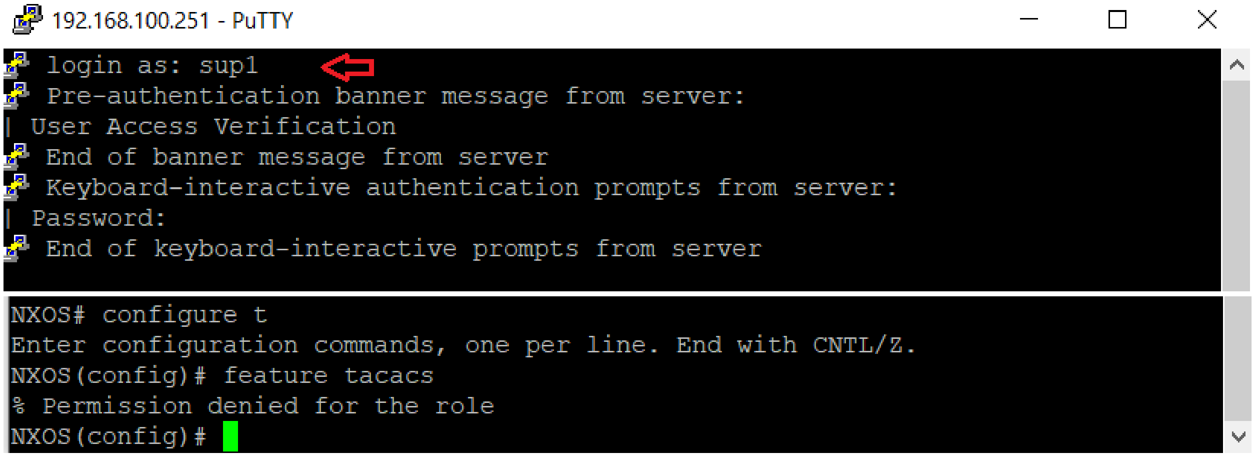
| Logged Time | Status | Details | Identity | Type | Authentication Policy | Authorization Policy | Ise Node | Network Device .. |
|---|---|---|---|---|---|---|---|---|
| | | | Identity | | Authentication Policy | Authorization Policy | Ise Node | Network Device Nai |
| Jul 26, 2021 01:51:20.971 PM | ✓ | | admin1 | Authorization | | Devices-Admin >> NXOS-Admin | ise1 | NEX-SW |
| Jul 26, 2021 01:51:20.795 PM | ✓ | | admin1 | Authentication | Devices-Admin >> Default | | ise1 | NEX-SW |



### Authorization Details

| | |
|---|---|
| Generated Time | 2021-07-26 13:51:20.971 +0:00 |
| Logged Time | 2021-07-26 13:51:20.971 |
| Epoch Time (sec) | 1627307480 |
| ISE Node | ise1 |
| Message Text | Device-Administration: Session Authorization succeeded |
| Failure Reason | |
| Resolution | |
| Root Cause | |
| Username | admin1 |
| Network Device Name | NEX-SW |
| Network Device IP | 192.168.100.251 |

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

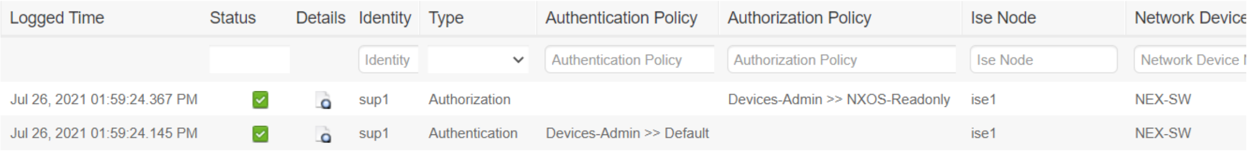


192.168.100.251 - PuTTY

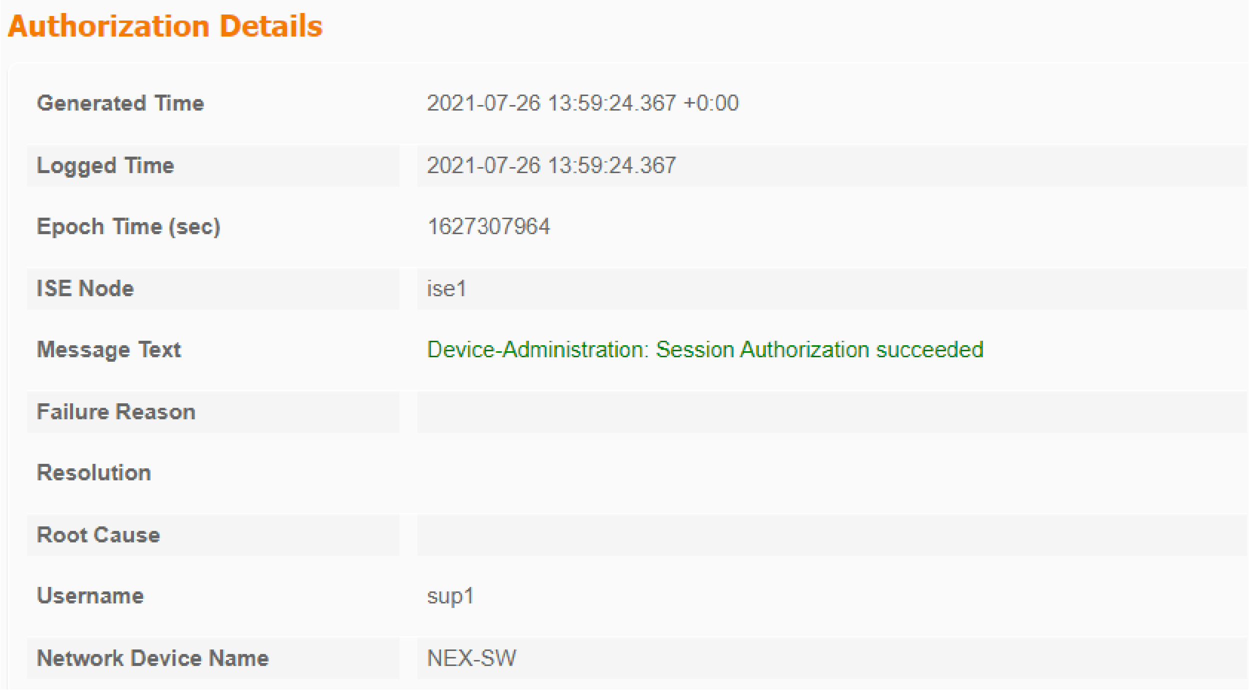
```
login as: sup1
Pre-authentication banner message from server:
| User Access Verification
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

NXOS# configure t
Enter configuration commands, one per line. End with CNTL/Z.
NXOS(config)# feature tacacs
% Permission denied for the role
NXOS(config)#
```

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



| Logged Time | Status | Details | Identity | Type | Authentication Policy | Authorization Policy | Ise Node | Network Device |
|---|---|---|---|---|---|---|---|---|
| | | | Identity | | Authentication Policy | Authorization Policy | Ise Node | Network Device I |
| Jul 26, 2021 01:59:24.367 PM | ✓ | | sup1 | Authorization | | Devices-Admin >> NXOS-Readonly | ise1 | NEX-SW |
| Jul 26, 2021 01:59:24.145 PM | ✓ | | sup1 | Authentication | Devices-Admin >> Default | | ise1 | NEX-SW |



## Authorization Details

| | |
|---|---|
| Generated Time | 2021-07-26 13:59:24.367 +0:00 |
| Logged Time | 2021-07-26 13:59:24.367 |
| Epoch Time (sec) | 1627307964 |
| ISE Node | ise1 |
| Message Text | Device-Administration: Session Authorization succeeded |
| Failure Reason | |
| Resolution | |
| Root Cause | |
| Username | sup1 |
| Network Device Name | NEX-SW |