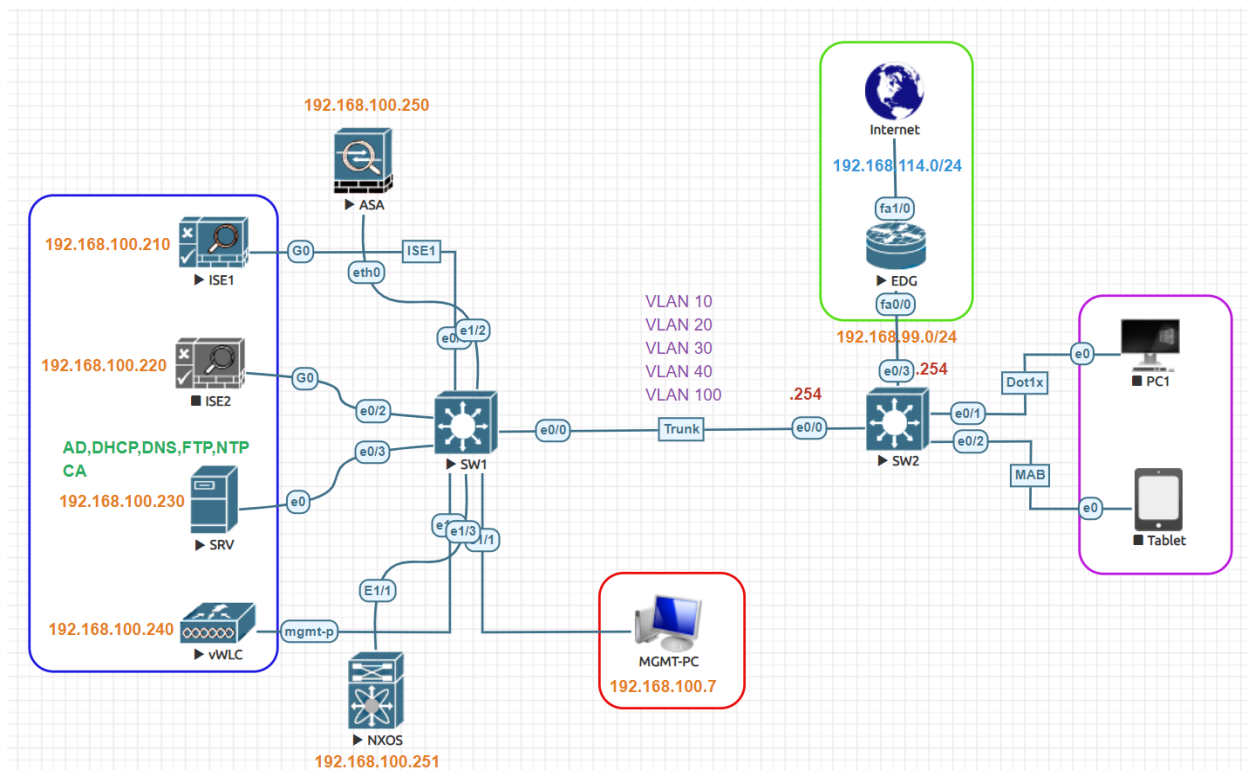


## ASA Firewall Device Administration Lab:



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

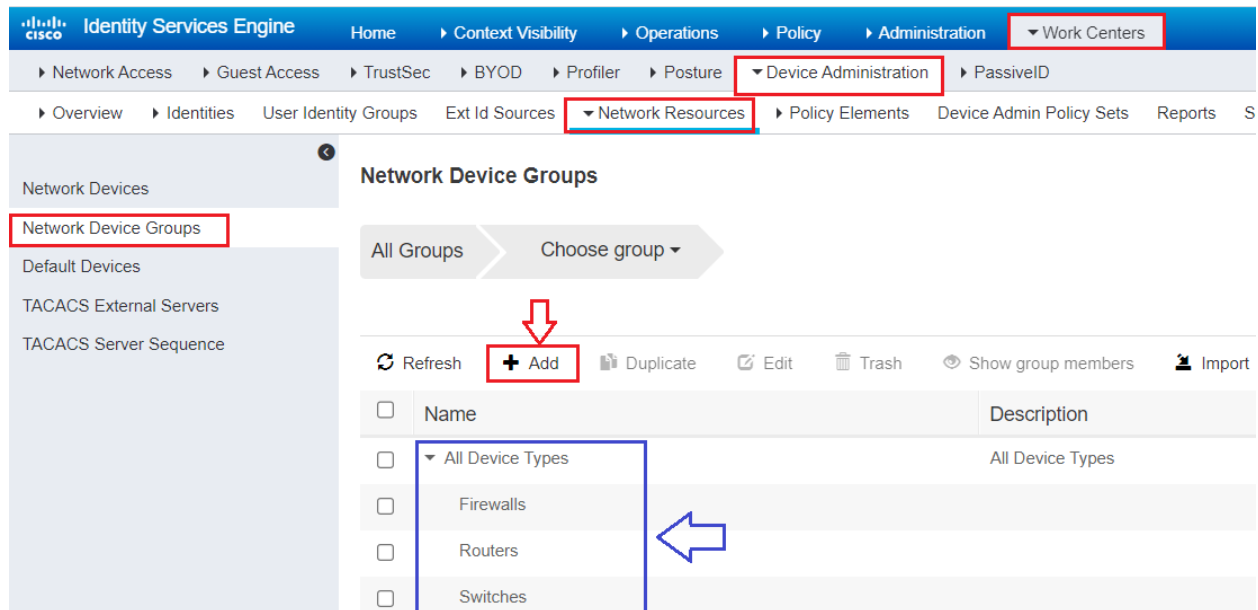
## Enable TACACS+:

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

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration' (highlighted with a red box), and 'Work Centers'. The left sidebar shows 'System' (highlighted with a red box) and 'Deployment' (highlighted with a red box). The main content area is titled 'Deployment Nodes List > ise1' and 'Edit Node'. The 'General Settings' tab is selected, showing fields for Hostname (ise1), FQDN (ise1.test.local), IP Address (192.168.100.210), and Node Type (Identity Services Engine (ISE)). Below these fields, the 'Role' is set to 'PRIMARY', and a 'Make Standalone' button is visible. A list of services is shown with checkboxes: Administration, Monitoring, Policy Service, Enable Session Services, Include Node in Node Group (set to None), Enable Profiling Service, Enable Threat Centric NAC Service, Enable SXP Service, **Enable Device Admin Service** (checked and highlighted with a red box and an arrow), and Enable Passive Identity Service. The 'pxGrid' checkbox is also checked. At the bottom, the 'Save' button is highlighted with a red box and an arrow, and the 'Reset' button is visible.

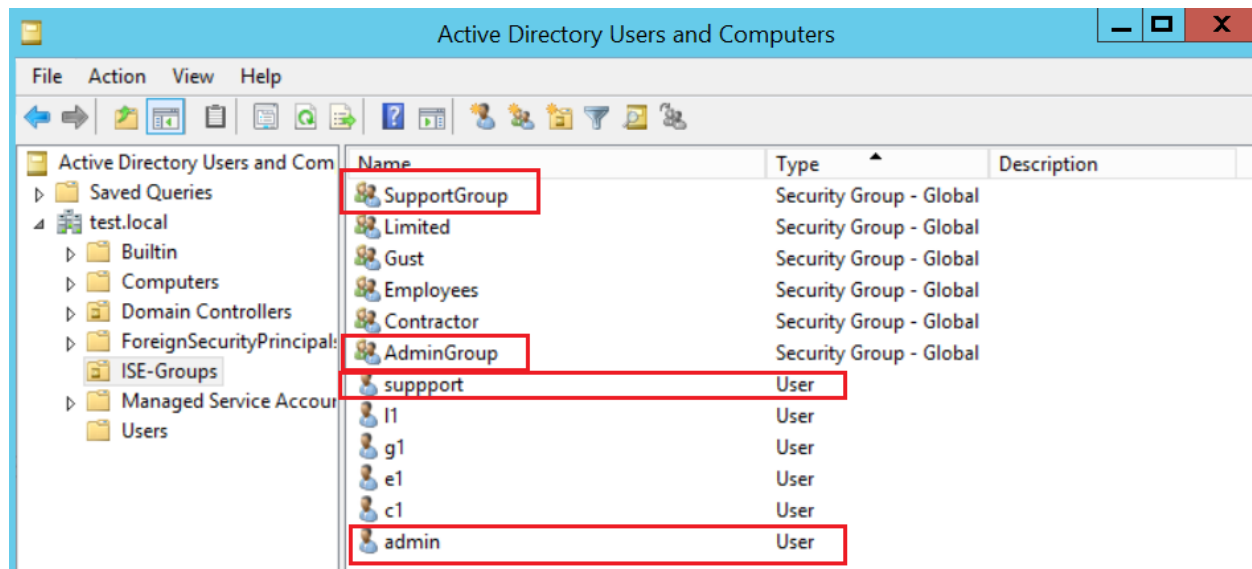
## Create Device Groups:

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.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

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

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

Network Devices List > ASA

**Network Devices**

\* Name ASA

Description Cisco ASA

IP Address \* IP : 192.168.100.250 / 32

\* Device Profile Cisco

Model Name

Software Version

\* Network Device Group

Location All Locations Set To Default

IPSEC No Set To Default

Device Type Firewalls Set To Default

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

☐ RADIUS Authentication Settings

☒ TACACS Authentication Settings

Shared Secret Test123 Hide

Enable Single Connect Mode ☐

☒ Legacy Cisco Device

☐ TACACS Draft Compliance Single Connect Support

☐ SNMP Settings

☐ Advanced TrustSec Settings

Submit Cancel

## 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**

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Work Centers' dropdown is expanded, showing 'Device Administration' and 'PassiveID'. Under 'Device Administration', 'Policy Elements' is selected. The left sidebar shows 'Conditions', 'Network Conditions', 'Results', and 'TACACS Profiles'. The 'Results' section is expanded, showing 'Allowed Protocols', 'TACACS Command Sets', and 'TACACS Profiles'. The main content area is titled 'TACACS Command Sets' and shows a list of command sets. A red arrow points to the '+ Add' button. The list includes 'ASA-Full-Access' and 'DenyAllCommands'.

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.

The screenshot shows the configuration page for the 'ASA-Admin' TACACS Command Set. The breadcrumb trail is 'TACACS Command Sets > ASA-Full-Access'. The 'Command Set' section has a 'Name' field with 'ASA-Admin' and a 'Description' field. The 'Commands' section has a checkbox labeled 'Permit any command that is not listed below' which is checked. The bottom of the page shows a table with columns 'Grant', 'Command', and 'Arguments'.

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

**Command Set**

Name: ASA-ReadOnly

Description:

**Commands**

Permit any command that is not listed below ☐

	Grant	Command	Arguments	
<input type="checkbox"/>	PERMIT	help		
<input type="checkbox"/>	PERMIT	end		
<input type="checkbox"/>	PERMIT	exit		
<input type="checkbox"/>	PERMIT	show*		

Cancel Submit

### 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

Refresh Add Duplicate Trash Edit

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	ASAAdmin Pro	Shell	
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR

► Conditions

► Network Conditions

▼ Results

Allowed Protocols

TACACS Command Sets

**TACACS Profiles**

TACACS Profiles > New

### TACACS Profile

Name **ASAAdmin Pro**

Description

Task Attribute View

Raw View

#### Common Tasks

Common Task Type **Shell**



<input checked="" type="checkbox"/> Default Privilege	15	(Select 0 to 15)
<input checked="" type="checkbox"/> Maximum Privilege	15	(Select 0 to 15)
<input type="checkbox"/> Access Control List		
<input type="checkbox"/> Auto Command		
<input type="checkbox"/> No Escape		(Select true or false)
<input type="checkbox"/> Timeout		Minutes (0-9999)
<input type="checkbox"/> Idle Time		Minutes (0-9999)

► Conditions

► Network Conditions

▼ Results

Allowed Protocols

TACACS Command Sets

**TACACS Profiles**

TACACS Profiles > New

### TACACS Profile

Name **ASA Read Only**

Description

Task Attribute View

Raw View

#### Common Tasks

Common Task Type **Shell**



<input checked="" type="checkbox"/> Default Privilege	5	(Select 0 to 15)
<input checked="" type="checkbox"/> Maximum Privilege	7	(Select 0 to 15)
<input type="checkbox"/> 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.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
On	Devices-Admin	TACACS Policy	Network Access Protocol EQUALS TACACS+	Default Device Admin			
On	Default	Tacacs Default policy set		Default Device Admin	2		

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

Policy Sets → Devices-Admin

Status	Rule Name	Conditions	Use	Hits
On	Default	Test_Identity_Stores	Options	0

Then, configure authorization Policies under '**Authorization Policy**'.

Status	Rule Name	Conditions	Results	Command Sets	Shell Profiles
On	ASA-Firewall-Admin	ad.test.local ExternalGroups EQUALS test.local/ISE-Groups/AdminGroup	ASA-Admin	ASA Admin Pro	
On	ASA-Firewall-Readonly	ad.test.local ExternalGroups EQUALS test.local/ISE-Groups/SupportGroup	ASA-Readonly	ASA Read Only	
On	Default		DenyAllCommands	Deny All Shell Profile	



## Cisco ASA Firewall Configuration:

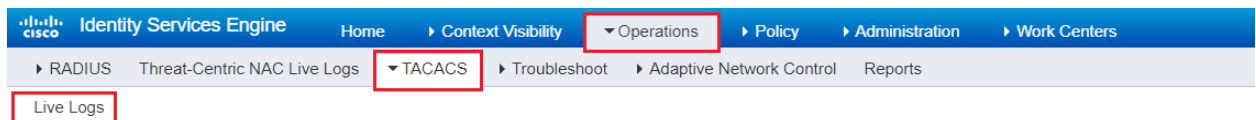
ciscoasa(config)# hostname ASA
ASA(config)# interface e0
ASA(config-if)# nameif inside
ASA(config-if)# security-level 100
ASA(config-if)# ip address 192.168.100.250
ASA(config-if)# no shutdown
ASA(config-if)# exit
ASA(config)# crypto key generate rsa modulus 2048
ASA(config)# enable password 123
ASA(config)# 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.

```
192.168.100.250 - PuTTY
login as: admin1
admin1@192.168.100.250's password:
Type help or '?' for a list of available commands.
ASA# config t
ASA(config)# in
ASA(config)# interface e2
ASA(config-if)# no shu
```

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.



Refresh	Export To	Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy
Fetching data from server....								
		Jul 25, 2021 07:46:25.728 PM	✓		admin1	Authorization	Devices-Admin >> ASA-Firewall-Admin	
		Jul 25, 2021 07:46:21.285 PM	✓		admin1	Authorization	Devices-Admin >> ASA-Firewall-Admin	
		Jul 25, 2021 07:46:16.007 PM	✓		admin1	Authorization	Devices-Admin >> ASA-Firewall-Admin	
		Jul 25, 2021 07:43:44.758 PM	✓		admin1	Authorization	Devices-Admin >> ASA-Firewall-Admin	
		Jul 25, 2021 07:43:44.507 PM	✓		admin1	Authentication	Devices-Admin >> Default	

## Authorization Details

Generated Time	2021-07-25 19:46:25.728 +0:00
Logged Time	2021-07-25 19:46:25.728
Epoch Time (sec)	1627242385
ISE Node	ise1
Message Text	Device-Administration: Command Authorization succeeded
Username	admin1
Network Device Name	ASA
Network Device IP	192.168.100.250

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

```
192.168.100.250 - PuTTY
login as: sup1
sup1@192.168.100.250's password:
Type help or '?' for a list of available commands.
ASA# config t
Command authorization failed
ASA#
```

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

Refresh Export To

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy
Jul 25, 2021 07:50:53.613 PM	✗		sup1	Authorization		Devices-Admin >> ASA-Firewall-Rea..
Jul 25, 2021 07:50:47.666 PM	✓		sup1	Authorization		Devices-Admin >> ASA-Firewall-Rea..
Jul 25, 2021 07:50:47.318 PM	✓		sup1	Authentication	Devices-Admin >> Default	

## Authorization Details

Generated Time	2021-07-25 19:50:53.613 +0:00
Logged Time	2021-07-25 19:50:53.613
Epoch Time (sec)	1627242653
ISE Node	ise1
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule
Resolution	Check the SelectedCommandSet attributes to verify that the expected Command Sets were selected by the Authorization policy
Root Cause	The requested command failed to match a Permit rule in any of the Command Sets
Username	sup1
Network Device Name	ASA
Network Device IP	192.168.100.250