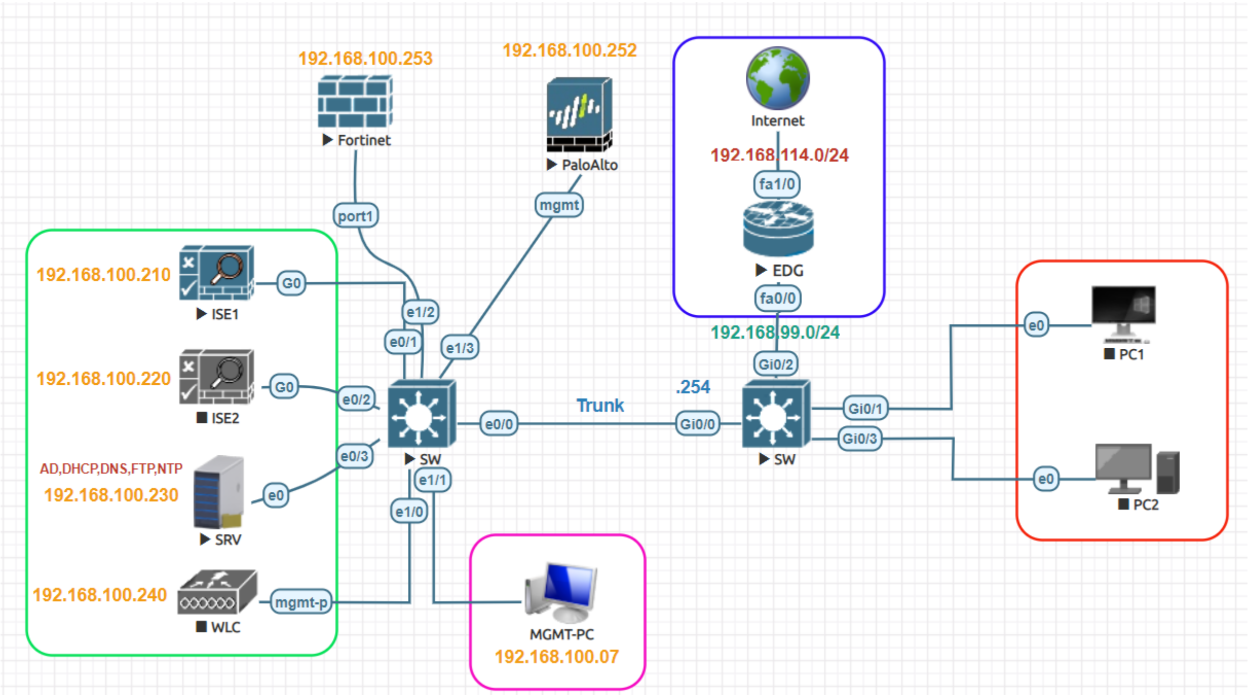
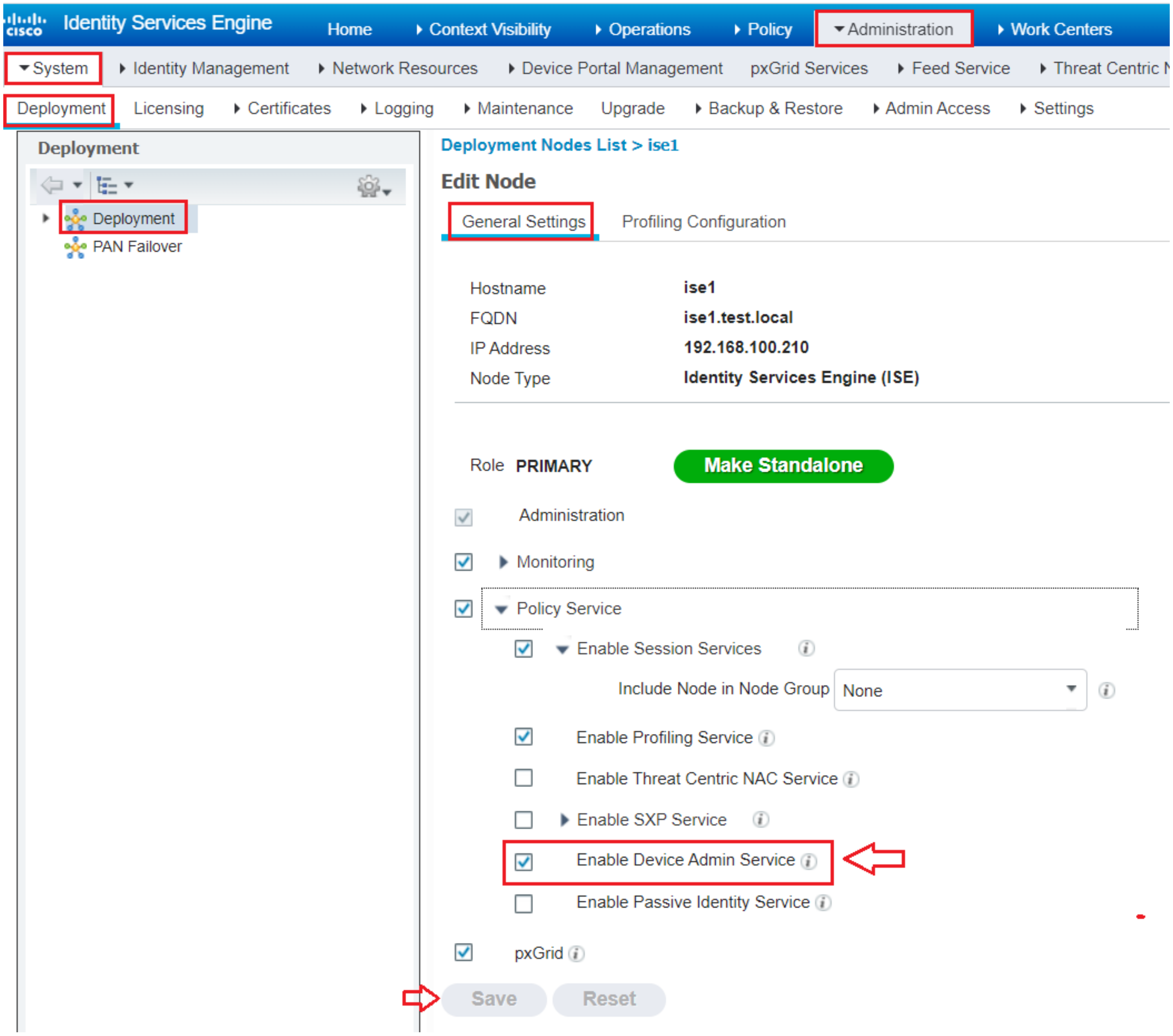
Fortigate FW Device Administration Lab:



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	Fortigate Firewall
Authentication Switch MGMT IP	192.168.100.254
Fortigate Firewall Interface	Port1
Network Device IP Address	192.168.100.253

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

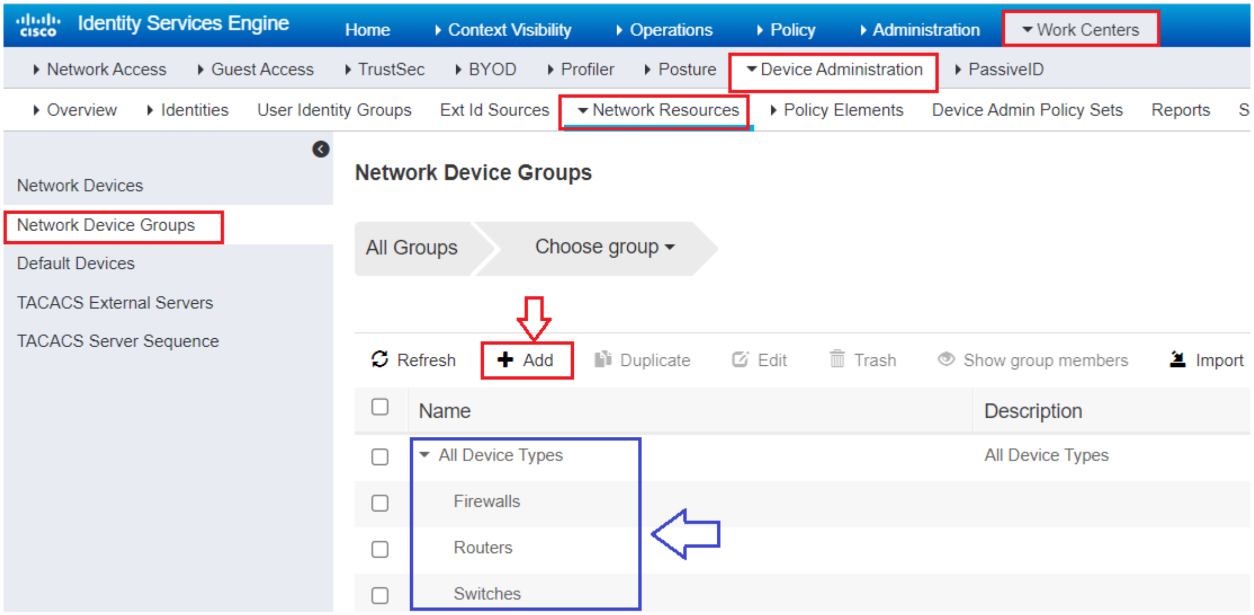
☑ Policy Service

- ☑ 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:

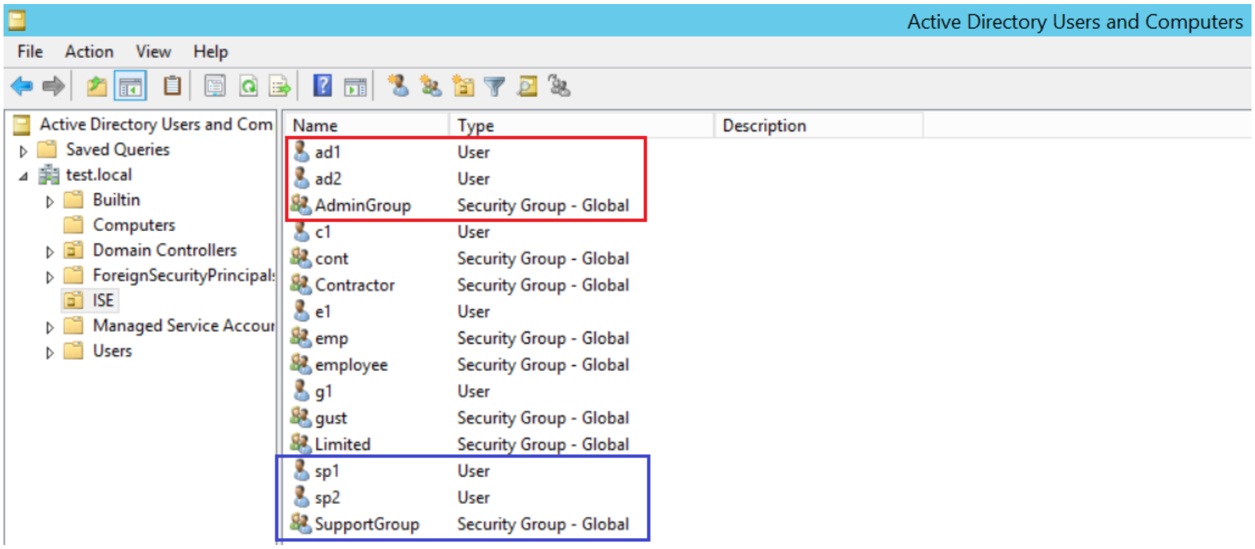
Create device groups. We can group devices based on type or location. Work Centers> Device Administration > Network Resources > Network Device Groups



	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 ad1 and sp1



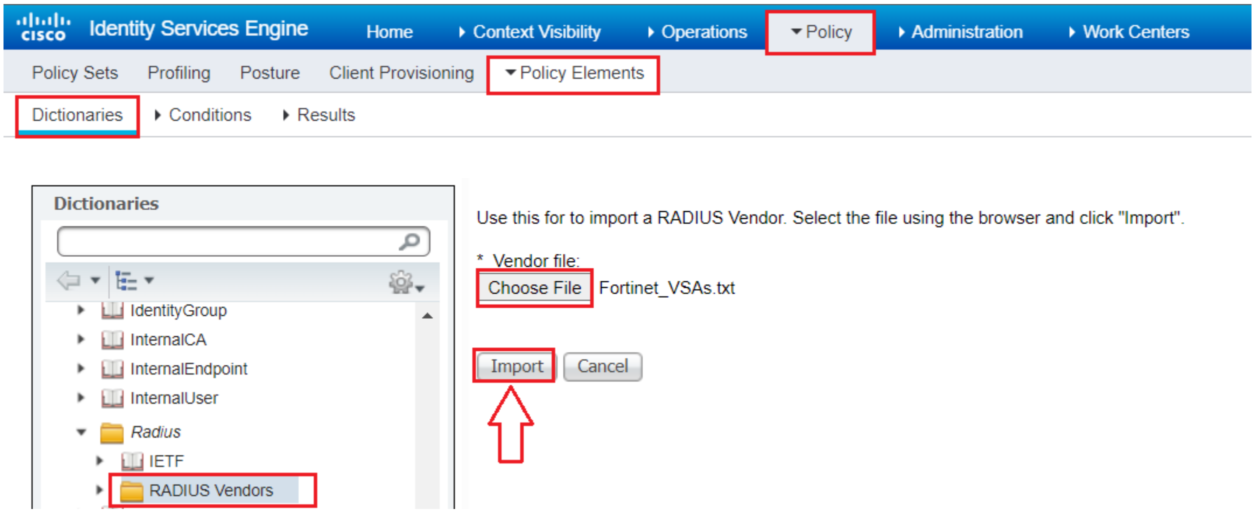
Name	Type	Description
ad1	User	
ad2	User	
AdminGroup	Security Group - Global	
c1	User	
cont	Security Group - Global	
Contractor	Security Group - Global	
e1	User	
emp	Security Group - Global	
employee	Security Group - Global	
g1	User	
gust	Security Group - Global	
Limited	Security Group - Global	
sp1	User	
sp2	User	
SupportGroup	Security Group - Global	

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

Fortigate Firewall RADIUS Dictionary:

Fortigate Firewall Radius dictionary defines the authentication attributes needed for communication between a Fortigate Firewall & Cisco ISE server. You can download dictionary from here: https://community.cisco.com/kxiwq67737/attachments/kxiwq67737/discussions-network-access-control/538562/1/Fortinet_VSAs.txt.zip

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

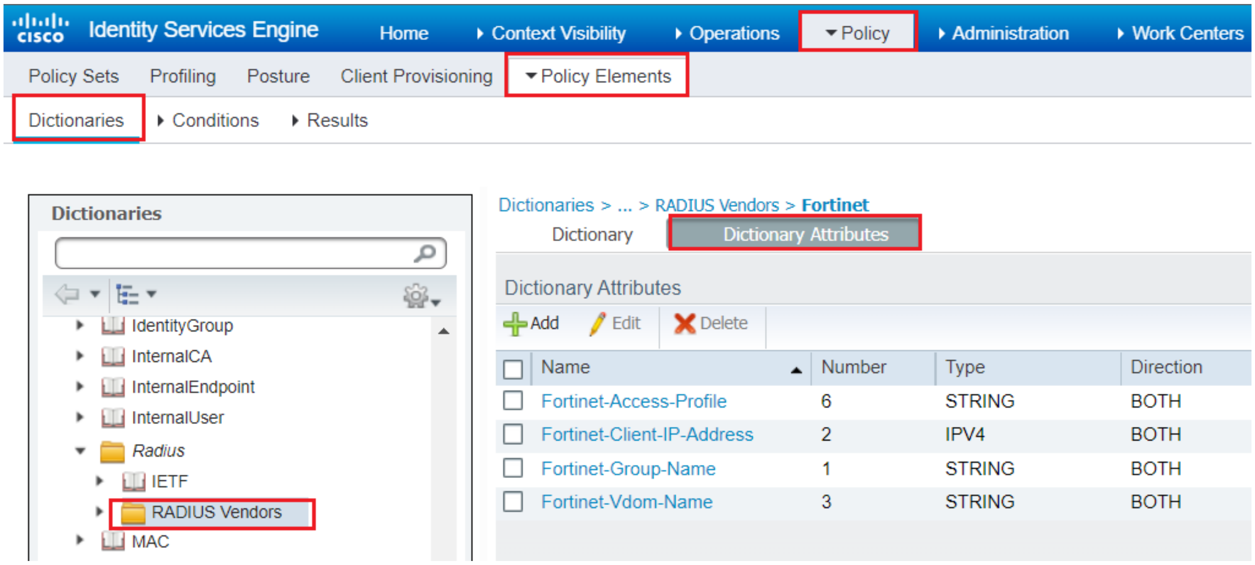


Use this for to import a RADIUS Vendor. Select the file using the browser and click "Import".

* Vendor file: Fortinet_VSAs.txt

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.

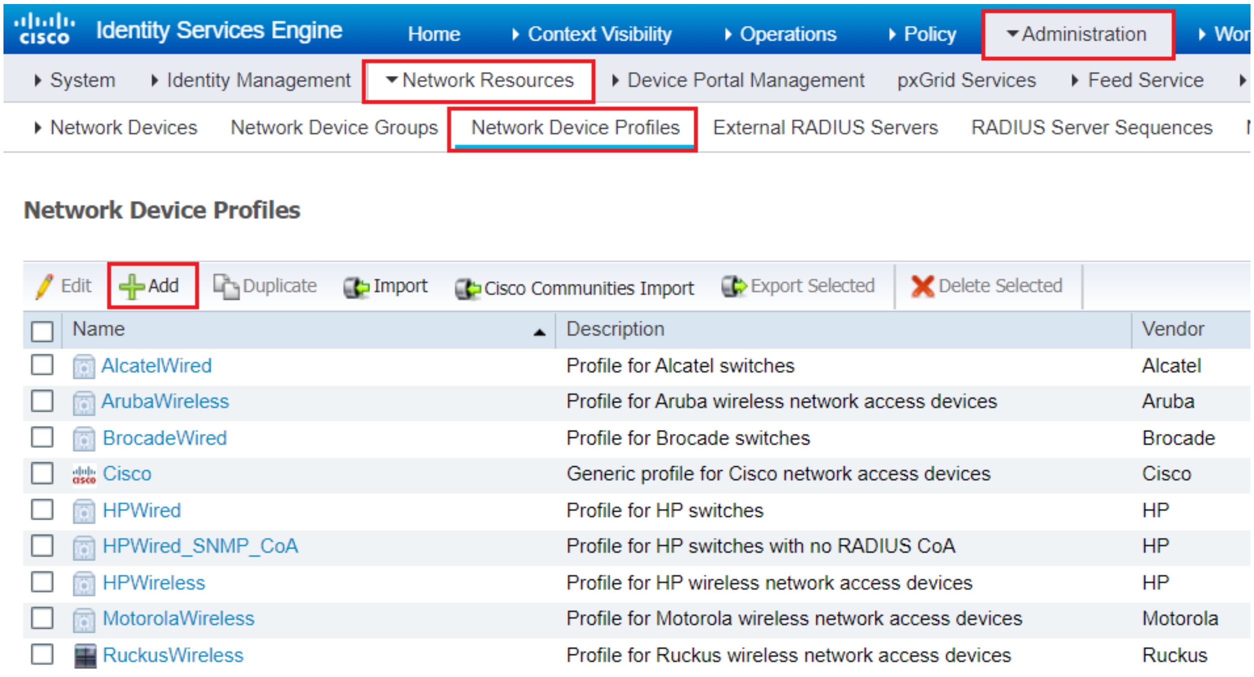


Dictionary Attributes

□	Name	Number	Type	Direction
□	Fortinet-Access-Profile	6	STRING	BOTH
□	Fortinet-Client-IP-Address	2	IPV4	BOTH
□	Fortinet-Group-Name	1	STRING	BOTH
□	Fortinet-Vdom-Name	3	STRING	BOTH

Network Device Profiles:

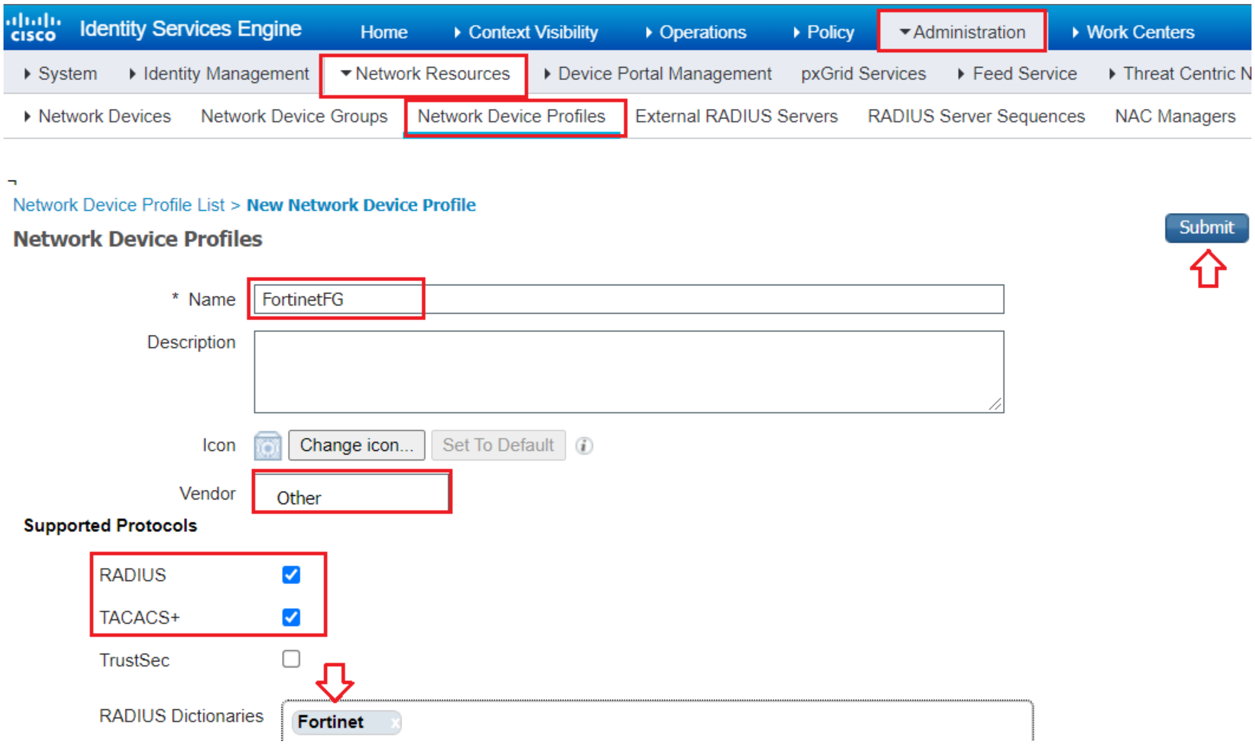
Navigate to Administration > Network Resources > Network Device Profiles > Click +Add.



Network Device Profiles

	Name	Description	Vendor
□	AlcatelWired	Profile for Alcatel switches	Alcatel
□	ArubaWireless	Profile for Aruba wireless network access devices	Aruba
□	BrocadeWired	Profile for Brocade switches	Brocade
□	Cisco	Generic profile for Cisco network access devices	Cisco
□	HPWired	Profile for HP switches	HP
□	HPWired_SNMP_CoA	Profile for HP switches with no RADIUS CoA	HP
□	HPWireless	Profile for HP wireless network access devices	HP
□	MotorolaWireless	Profile for Motorola wireless network access devices	Motorola
□	RuckusWireless	Profile for Ruckus wireless network access devices	Ruckus

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



Network Device Profiles

* Name	FortinetFG
Description	
Icon	
Vendor	Other

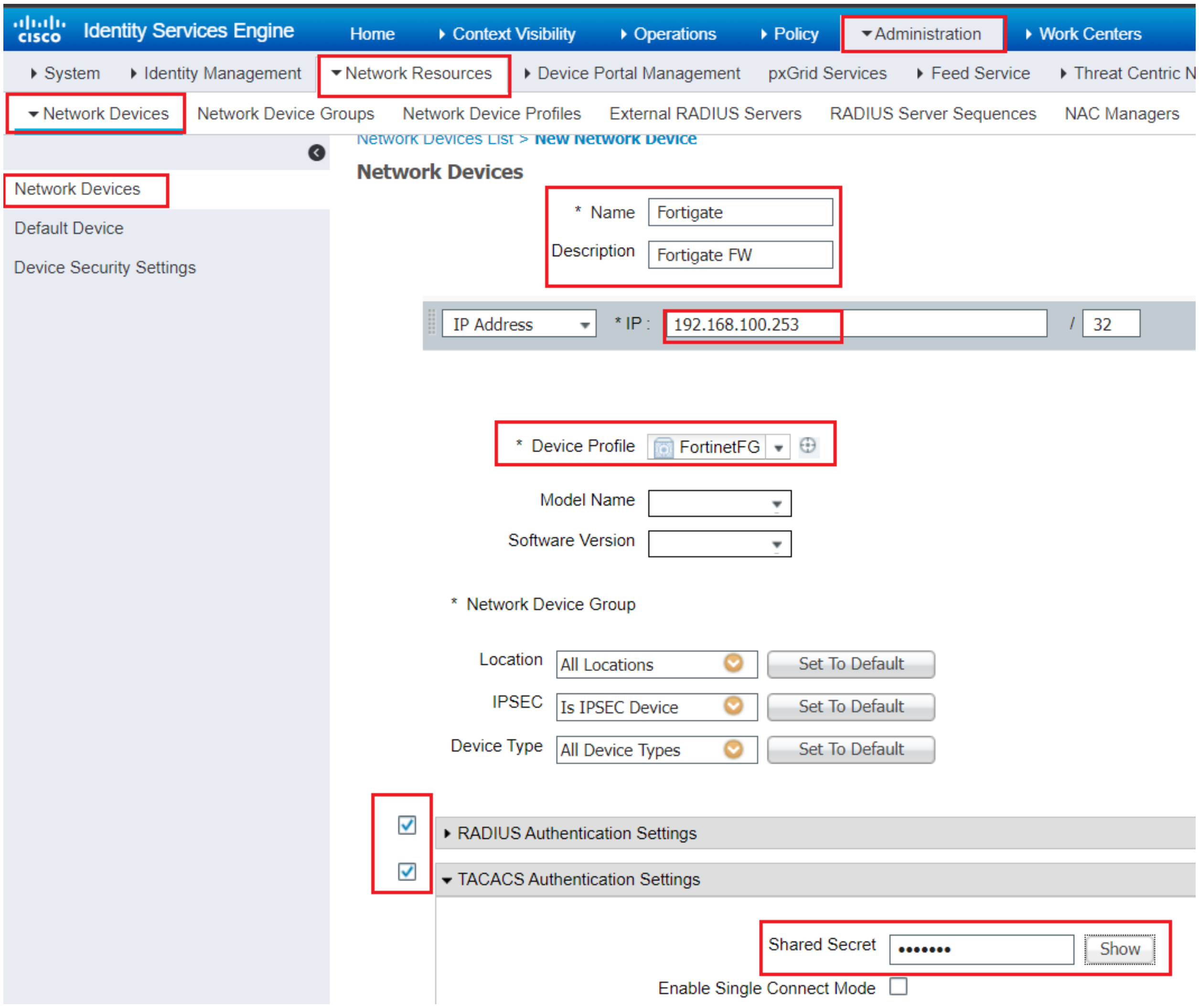
Supported Protocols

RADIUS	☑
TACACS+	☑
TrustSec	□
RADIUS Dictionaries	Fortinet

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: Fortigate

Description: Fortigate FW

IP Address * IP : 192.168.100.253 / 32

* Device Profile: FortinetFG

Model Name:

Software Version:

* Network Device Group

Location: All Locations

IPSEC: Is IPSEC Device

Device Type: All Device Types

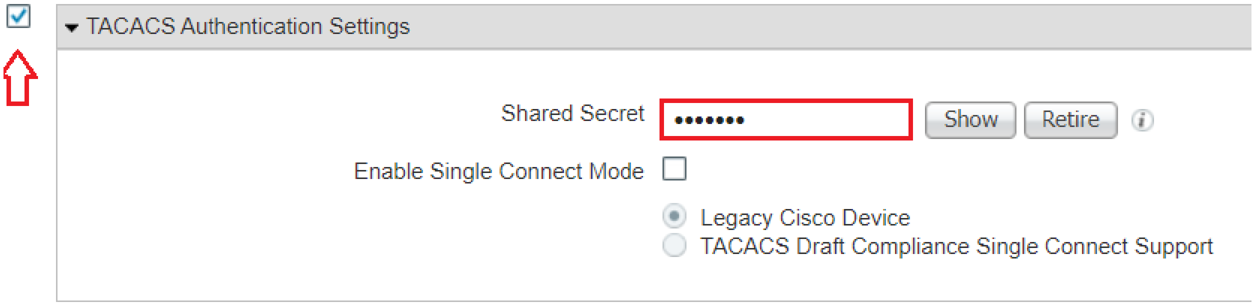
☑ RADIUS Authentication Settings

☑ TACACS Authentication Settings

Shared Secret: •••••••

Enable Single Connect Mode □

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



☑ TACACS Authentication Settings

Shared Secret: •••••••

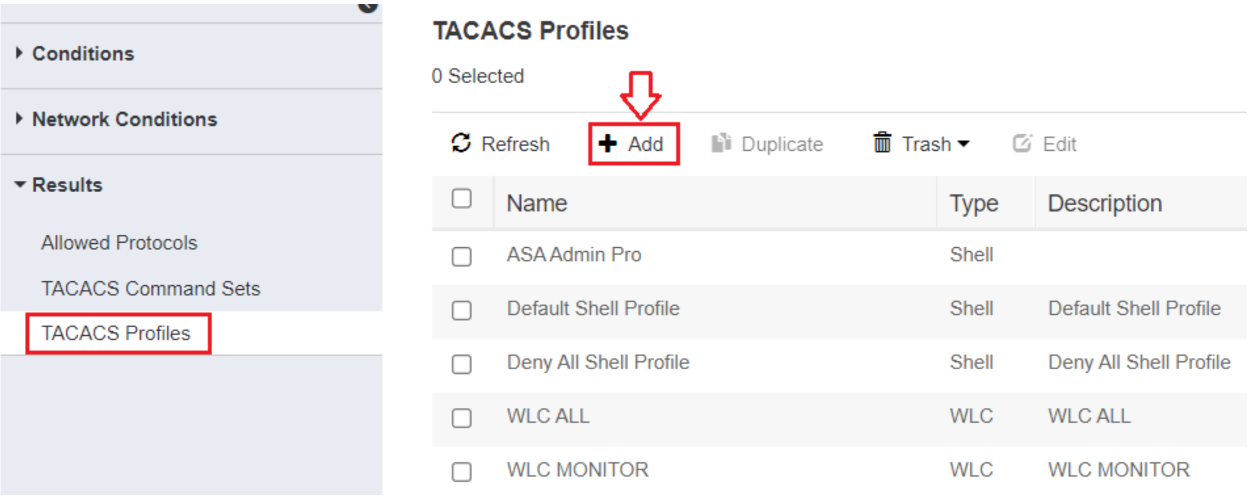
Enable Single Connect Mode □

● Legacy Cisco Device

○ TACACS Draft Compliance Single Connect Support

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.

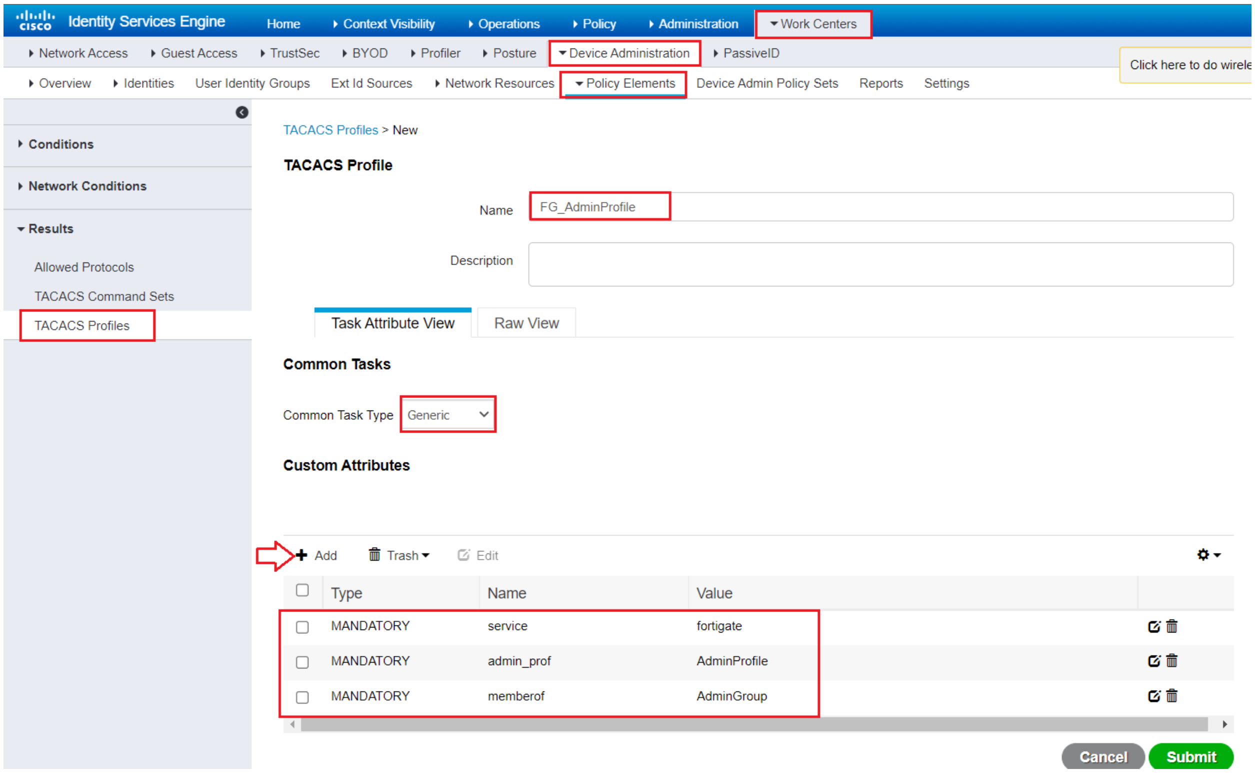


TACACS Profiles

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

Provide Name in this case FG_AdminProfile change Common Task Type to Generic in Custom Attributes Click add and supply the Attributes and finally Click Submit button.



TACACS Profiles > New

TACACS Profile

Name: FG_AdminProfile

Description:

Common Tasks

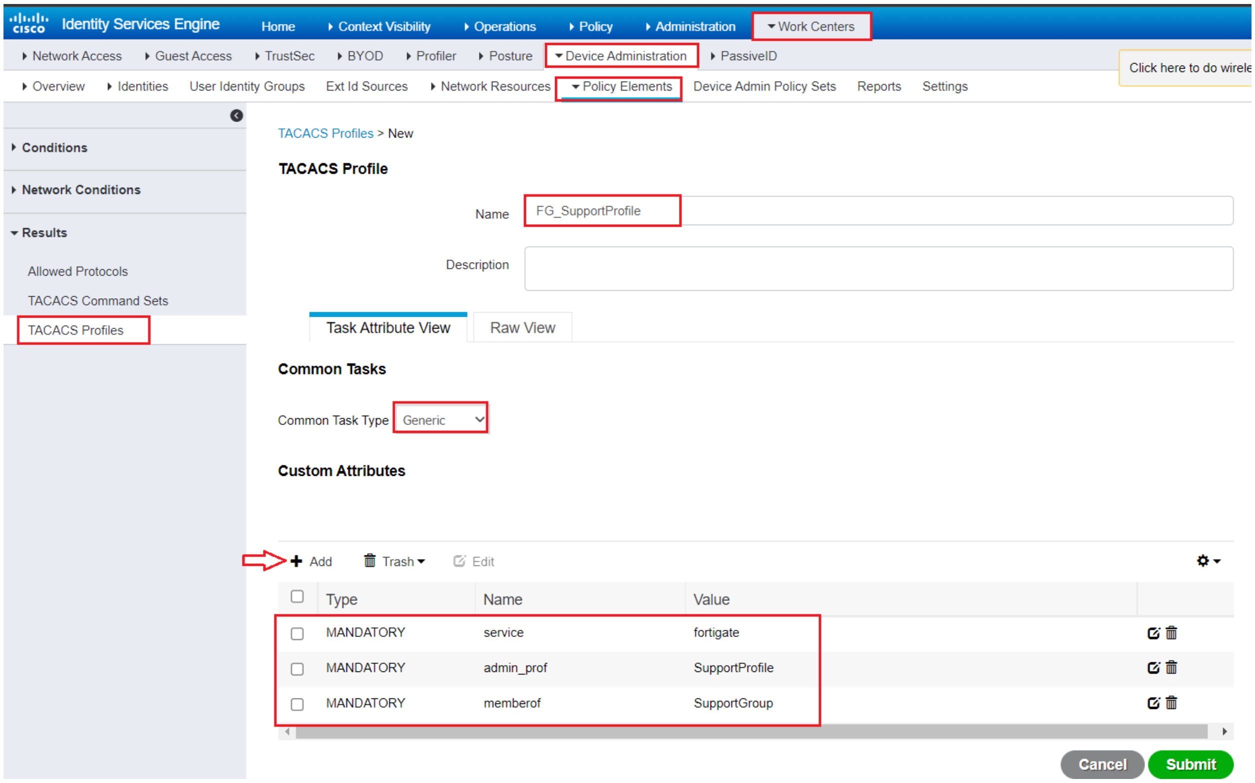
Common Task Type: Generic

Custom Attributes

□	Type	Name	Value
□	MANDATORY	service	fortigate
□	MANDATORY	admin_prof	AdminProfile
□	MANDATORY	memberof	AdminGroup

MANDATORY	service	fortigate
MANDATORY	admin_prof	AdminProfile
MANDATORY	memberof	AdminGroup

Let’s create another TACACS Profile for Support Users.



TACACS Profiles > New

TACACS Profile

Name: FG_SupportProfile

Description:

Common Tasks

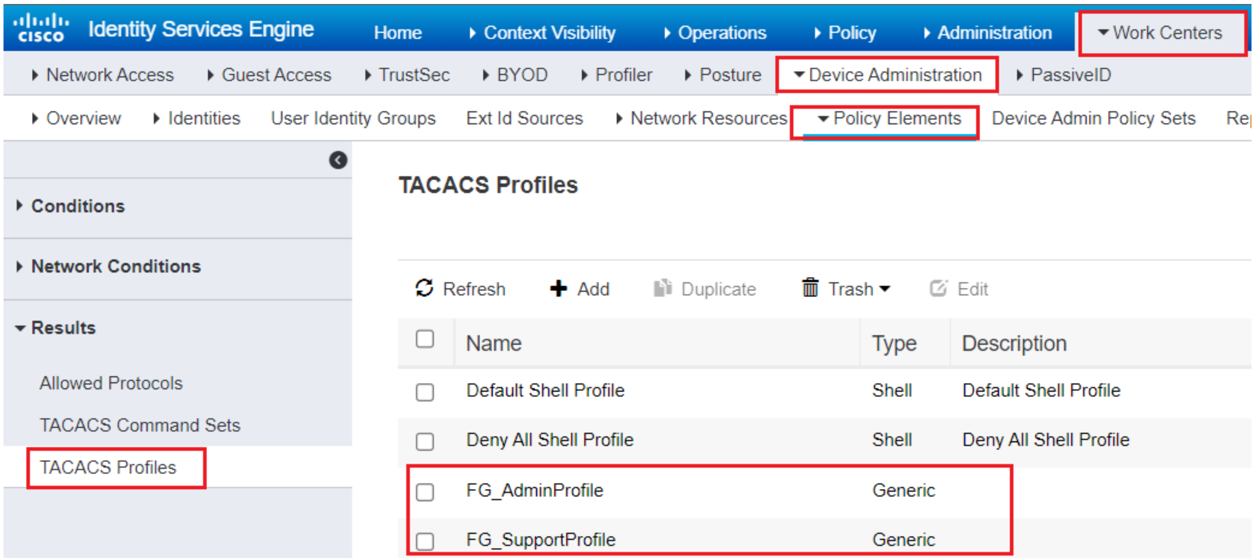
Common Task Type: Generic

Custom Attributes

□	Type	Name	Value
□	MANDATORY	service	fortigate
□	MANDATORY	admin_prof	SupportProfile
□	MANDATORY	memberof	SupportGroup

MANDATORY	service	fortigate
MANDATORY	admin_prof	SupportProfile
MANDATORY	memberof	SupportGroup

Now we have two TACACS Profiles one for Admin Group second for Support Group.

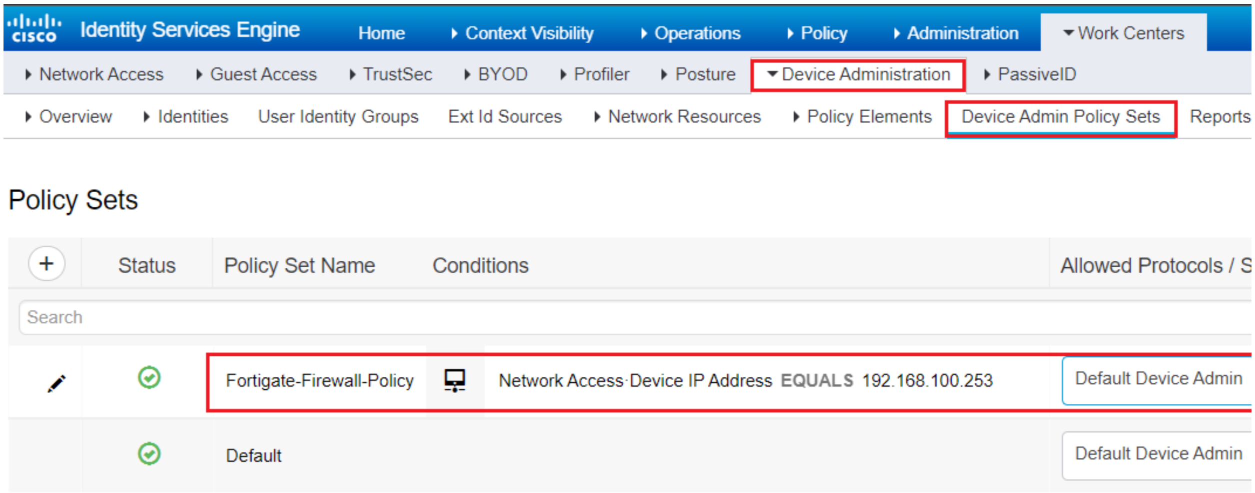


TACACS Profiles

□	Name	Type	Description
□	Default Shell Profile	Shell	Default Shell Profile
□	Deny All Shell Profile	Shell	Deny All Shell Profile
□	FG_AdminProfile	Generic	
□	FG_SupportProfile	Generic	

Device Administration Policy:

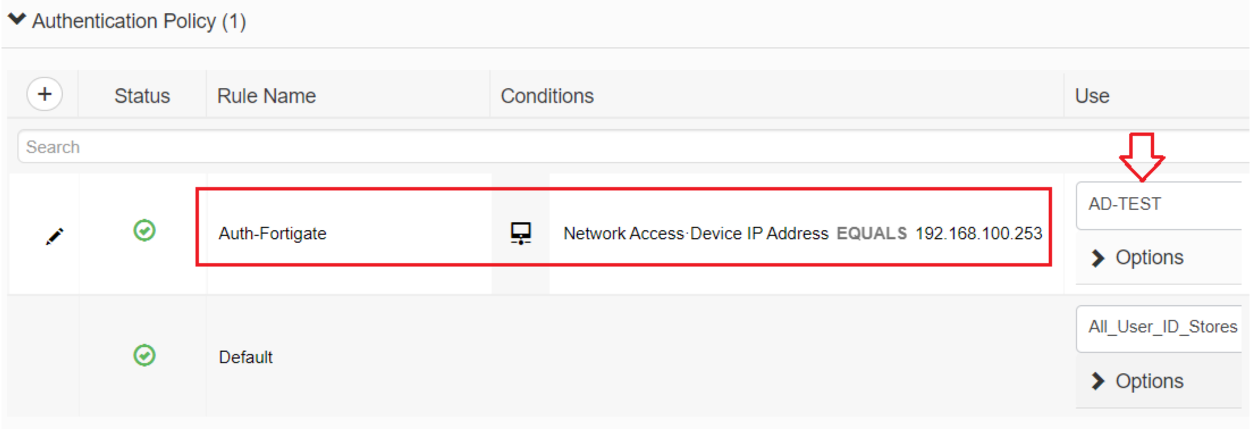
Here we will call all the items configured earlier. Navigate to Work Centers > Device Administration > Device Admin Policy Sets and add new policy or use default. Click small arrow button on right side of policy to expand.



Policy Sets

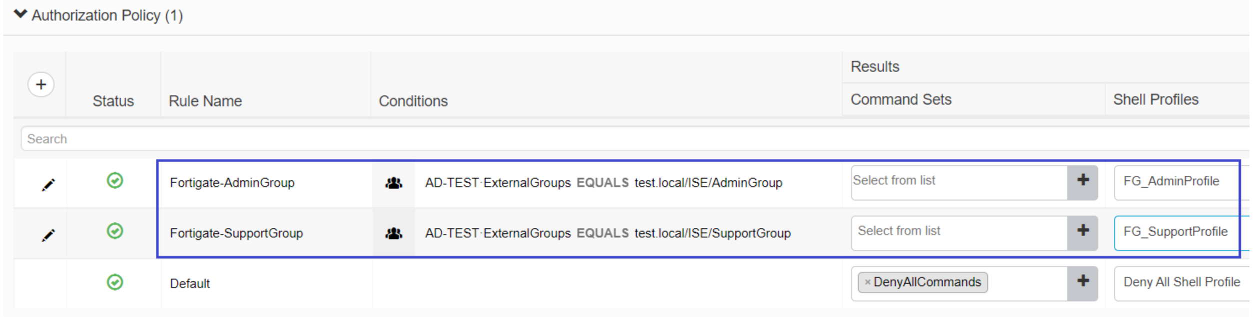
+	Status	Policy Set Name	Conditions	Allowed Protocols / S
Search				
✎	✓	Fortigate-Firewall-Policy	Network Access·Device IP Address EQUALS 192.168.100.253	Default Device Admin
	✓	Default		Default Device Admin

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


⌄ Authentication Policy (1)

+	Status	Rule Name	Conditions	Use
Search				
✎	✓	Auth-Fortigate	Network Access·Device IP Address EQUALS 192.168.100.253	AD-TEST › Options
	✓	Default		All_User_ID_Stores › Options

Then, configure authorization Policies under 'Authorization Policy'.


⌄ Authorization Policy (1)

				Results	
+	Status	Rule Name	Conditions	Command Sets	Shell Profiles
Search					
✎	✓	Fortigate-AdminGroup	AD-TEST·ExternalGroups EQUALS test.local/ISE/AdminGroup	Select from list +	FG_AdminProfile
✎	✓	Fortigate-SupportGroup	AD-TEST·ExternalGroups EQUALS test.local/ISE/SupportGroup	Select from list +	FG_SupportProfile
	✓	Default		× DenyAllCommands +	Deny All Shell Profile