

The diagram illustrates a network topology with the following components and connections:

- Fortinet** (192.168.100.253) is connected to **SW** (e1/2) via **port1**.
- PaloAlto** (192.168.100.252) is connected to **SW** (e1/3) via **mgmt**.
- Internet** is connected to **EDG** (192.168.114.0/24) via **fa1/0**. **EDG** is connected to **SW** (Gi0/2) via **fa0/0**.
- ISE1** (192.168.100.210) is connected to **SW** (e0/1) via **G0**.
- ISE2** (192.168.100.220) is connected to **SW** (e0/2) via **G0**.
- SRV** (AD,DHCP,DNS,FTP,NTP, 192.168.100.230) is connected to **SW** (e0/3) via **e0**.
- WLC** (192.168.100.240) is connected to **SW** (e1/0) via **mgmt-p**.
- MGMT-PC** (192.168.100.07) is connected to **SW** (e1/1) via **mgmt-p**.
- SW** (192.168.99.0/24) is connected to **SW** (Gi0/0) via **Trunk** (Gi0/0). **SW** (Gi0/0) is connected to **SW** (Gi0/2) via **.254**.
- SW** (Gi0/1) is connected to **PC1** via **e0**.
- SW** (Gi0/3) is connected to **PC2** via **e0**.

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**.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The navigation pane on the left shows the hierarchy: **System > Deployment > Deployment Nodes List > ise1**. The **Deployment** menu item is highlighted. The main content area shows the **Edit Node** configuration for node **ise1**. The **General Settings** tab is selected. The configuration includes the following details:

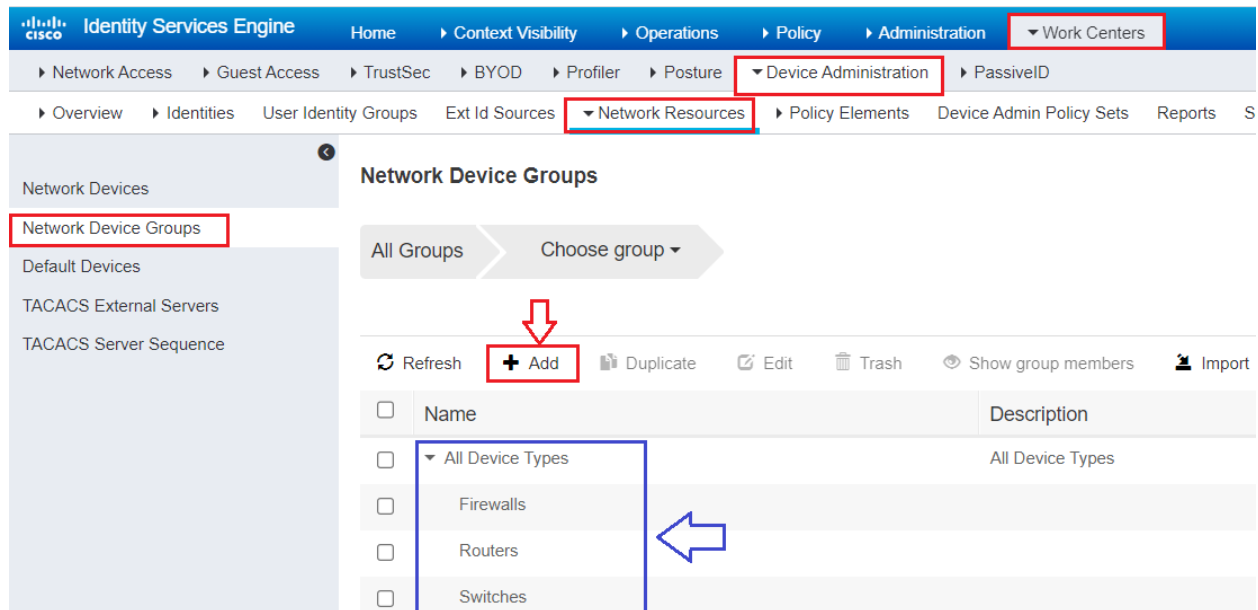
- Hostname: **ise1**
- FQDN: **ise1.test.local**
- IP Address: **192.168.100.210**
- Node Type: **Identity Services Engine (ISE)**

Below the configuration details, the **Role** is set to **PRIMARY**, and there is a **Make Standalone** button. The **Administration** checkbox is checked. The **Monitoring** checkbox is checked. The **Policy Service** checkbox is checked, and the **Enable Session Services** checkbox is checked. The **Include Node in Node Group** dropdown is set to **None**. The **Enable Profiling Service** checkbox is checked. The **Enable Threat Centric NAC Service** checkbox is unchecked. The **Enable SXP Service** checkbox is unchecked. The **Enable Device Admin Service** checkbox is checked and highlighted with a red box and an arrow. The **Enable Passive Identity Service** checkbox is unchecked. The **pxGrid** checkbox is checked.

At the bottom of the configuration area, there are **Save** and **Reset** buttons. The **Save** button is highlighted with a red box and an arrow.

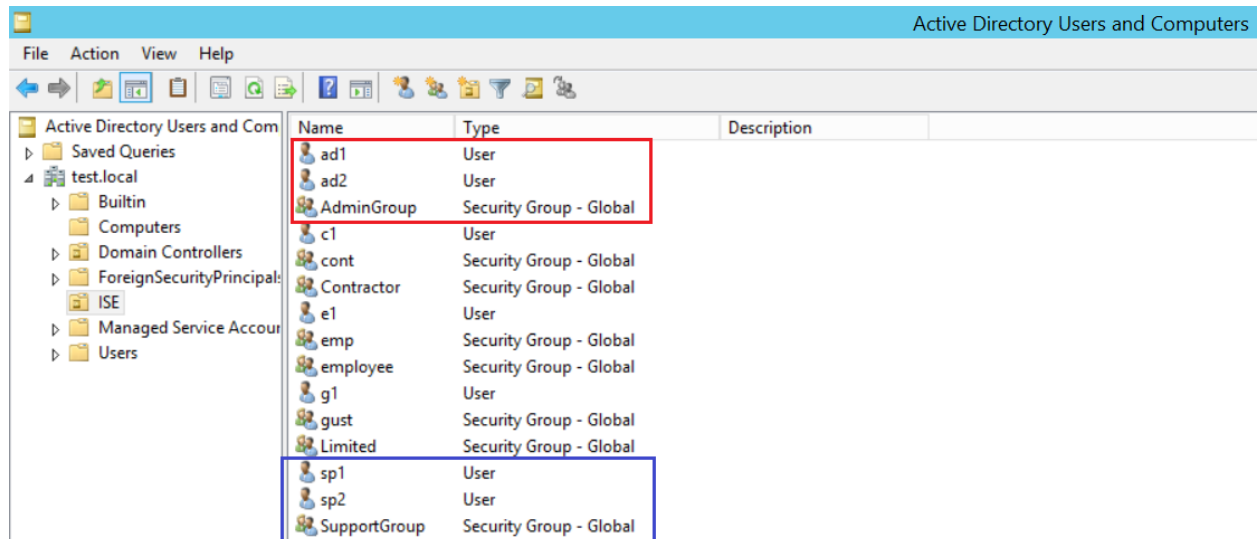
Create Device Groups:

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 **ad1** and **sp1**



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**.

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 left sidebar shows the navigation tree with Policy Elements expanded, and Dictionaries selected. The main content area shows the 'Dictionaries' page with a search bar and a list of dictionaries. The 'RADIUS Vendors' dictionary is selected. To the right, there is a section for importing a RADIUS Vendor. It includes a text box for the vendor file name, a 'Choose File' button, and 'Import' and 'Cancel' buttons. A red arrow points to the 'Import' button.

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

* Vendor file:

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.

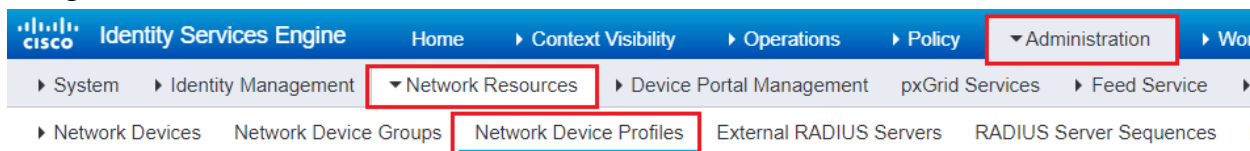
The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The left sidebar shows the navigation tree with Policy Elements expanded, and Dictionaries selected. The main content area shows the 'Dictionaries' page with a search bar and a list of dictionaries. The 'RADIUS Vendors' dictionary is selected. To the right, there is a section for the 'Dictionary Attributes' page. It includes a table with columns for Name, Number, Type, and Direction. The table lists four attributes: Fortinet-Access-Profile, Fortinet-Client-IP-Address, Fortinet-Group-Name, and Fortinet-Vdom-Name.

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:

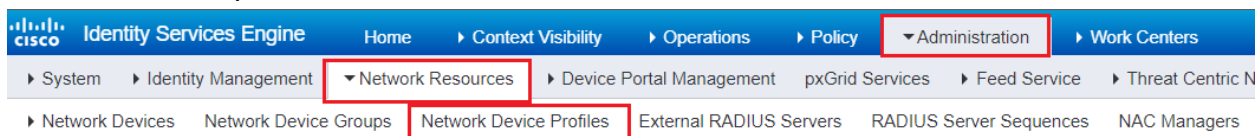
Navigate to **Administration > Network Resources > Network Device Profiles > Click +Add.**



Network Device Profiles

	<div> Add</div>	Duplicate	Import	Cisco Communities Import	Export Selected	Delete Selected
<input type="checkbox"/>	Name	Description	Vendor			
<input type="checkbox"/>	AlcatelWired	Profile for Alcatel switches	Alcatel			
<input type="checkbox"/>	ArubaWireless	Profile for Aruba wireless network access devices	Aruba			
<input type="checkbox"/>	BrocadeWired	Profile for Brocade switches	Brocade			
<input type="checkbox"/>	Cisco	Generic profile for Cisco network access devices	Cisco			
<input type="checkbox"/>	HPWired	Profile for HP switches	HP			
<input type="checkbox"/>	HPWired_SNMP_CoA	Profile for HP switches with no RADIUS CoA	HP			
<input type="checkbox"/>	HPWireless	Profile for HP wireless network access devices	HP			
<input type="checkbox"/>	MotorolaWireless	Profile for Motorola wireless network access devices	Motorola			
<input type="checkbox"/>	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 Profile List > [New Network Device Profile](#)

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.

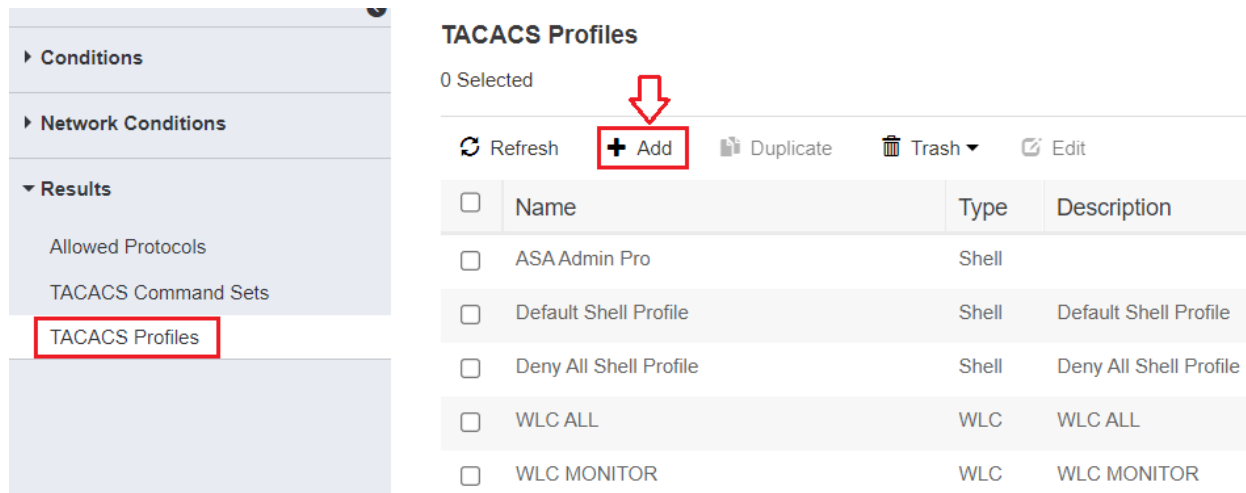
The screenshot shows the 'Add New Network Device' form in the Cisco ISE Administration console. The breadcrumb navigation is 'Work Centers > Device Administration > Network Resources > Network Devices'. The form is titled 'Network Devices' and includes a sidebar with 'Network Devices', 'Default Device', and 'Device Security Settings'. The main form fields are: Name (Fortigate), Description (Fortigate FW), IP Address (192.168.100.253), Device Profile (FortinetFG), Model Name, Software Version, Network Device Group (All Locations, Is IPSEC Device, All Device Types), RADIUS Authentication Settings (checked), TACACS Authentication Settings (checked), Shared Secret (masked), and Enable Single Connect Mode (unchecked).

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

The close-up screenshot shows the 'TACACS Authentication Settings' section. It includes a checkbox for 'TACACS Authentication Settings' (checked), a red arrow pointing to the header, the 'Shared Secret' field (masked with dots and highlighted with a red box), 'Show' and 'Retire' buttons, 'Enable Single Connect Mode' (unchecked), and radio buttons for 'Legacy Cisco Device' (selected) and 'TACACS Draft Compliance Single Connect Support' (unselected).

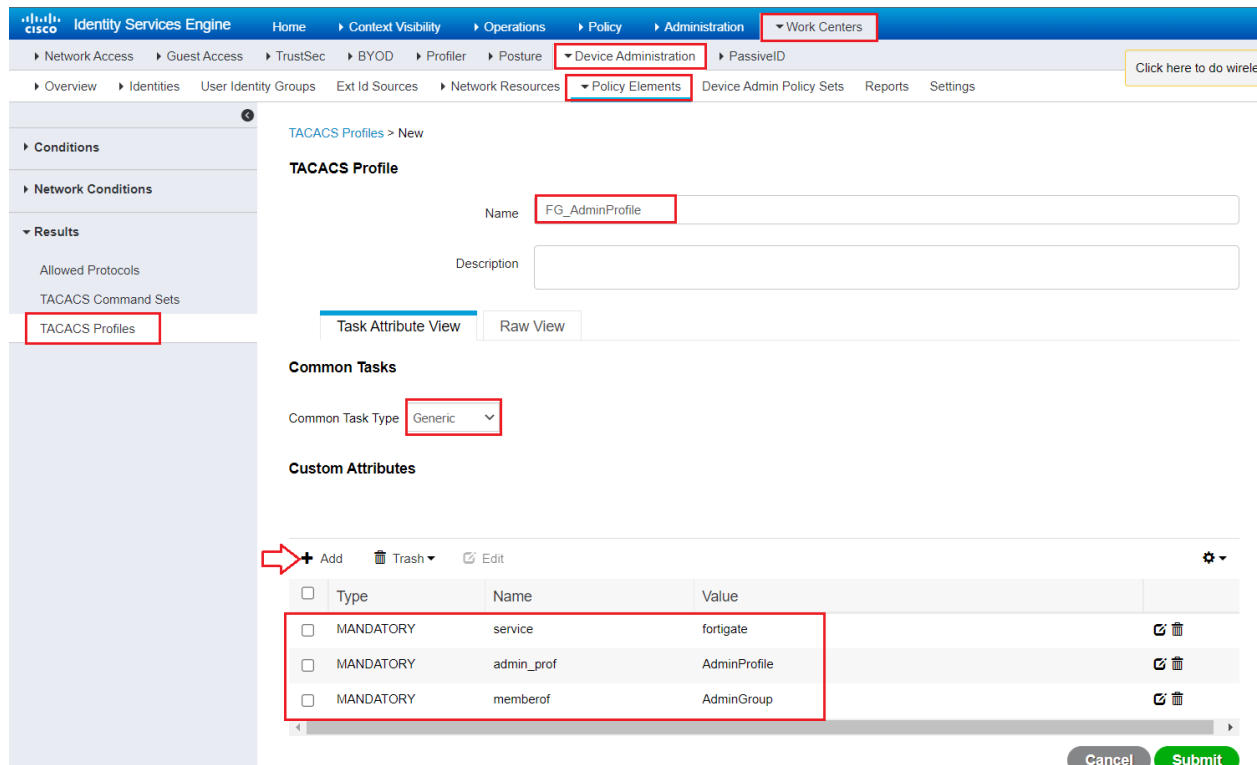
Create TACACS Profiles:

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**.



Name	Type	Description
ASAAdmin 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.



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:

Description:

Task Attribute View | Raw View

Common Tasks

Common Task Type:

Custom Attributes

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

Cancel Submit

MANDATORY service fortigate
 MANDATORY admin_prof SupportProfile
 MANDATORY memberof SupportGroup

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

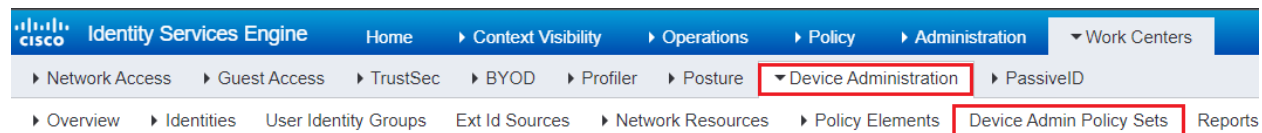
TACACS Profiles

Refresh + Add Duplicate Trash Edit

	Name	Type	Description
<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"/>	FG_AdminProfile	Generic	
<input type="checkbox"/>	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)

+	Status	Rule Name	Conditions	Results	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