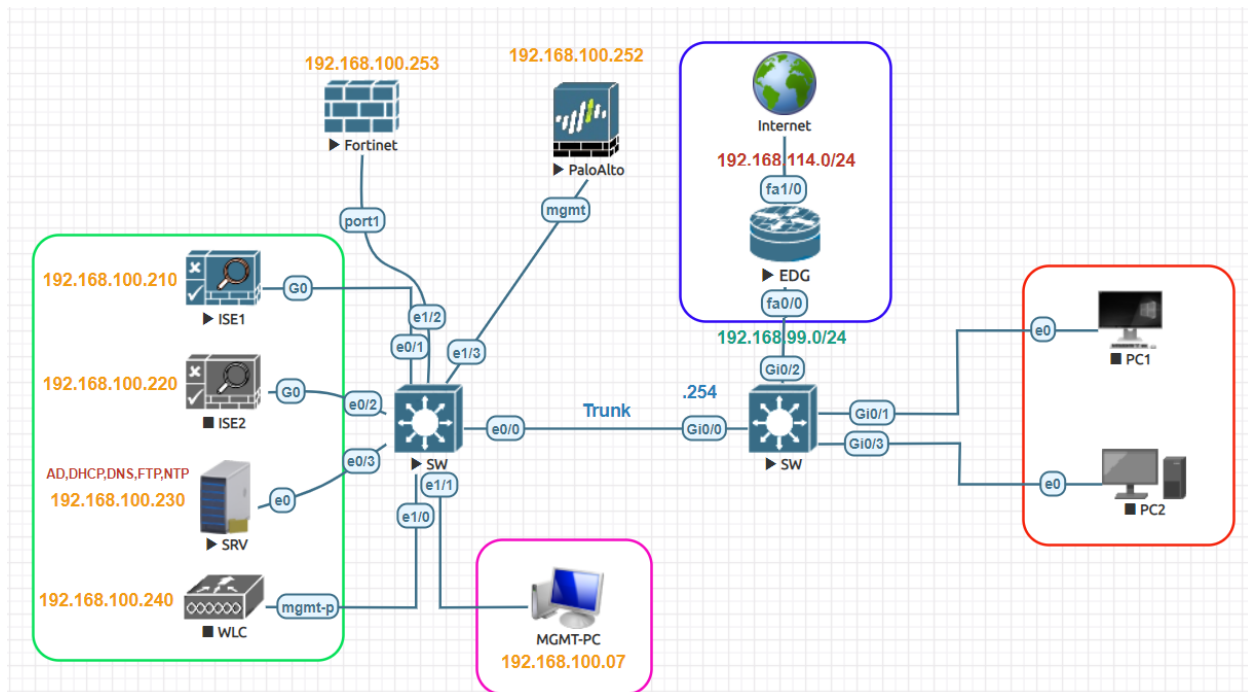


## Palo Alto FW Device Administration Lab:



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	Palo Alto Firewall
Authentication Switch MGMT IP	192.168.100.254
Palo Alto Firewall Interface	MGMT
Network Device IP Address	192.168.100.252

## 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 the 'System' menu (highlighted with a red box) with sub-items like 'Deployment' (highlighted with a red box) and 'PAN Failover'. The main content area is titled 'Deployment Nodes List > ise1' and shows the 'Edit Node' configuration for 'ise1'. The 'General Settings' tab is selected (highlighted with a red box). The configuration details include:

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

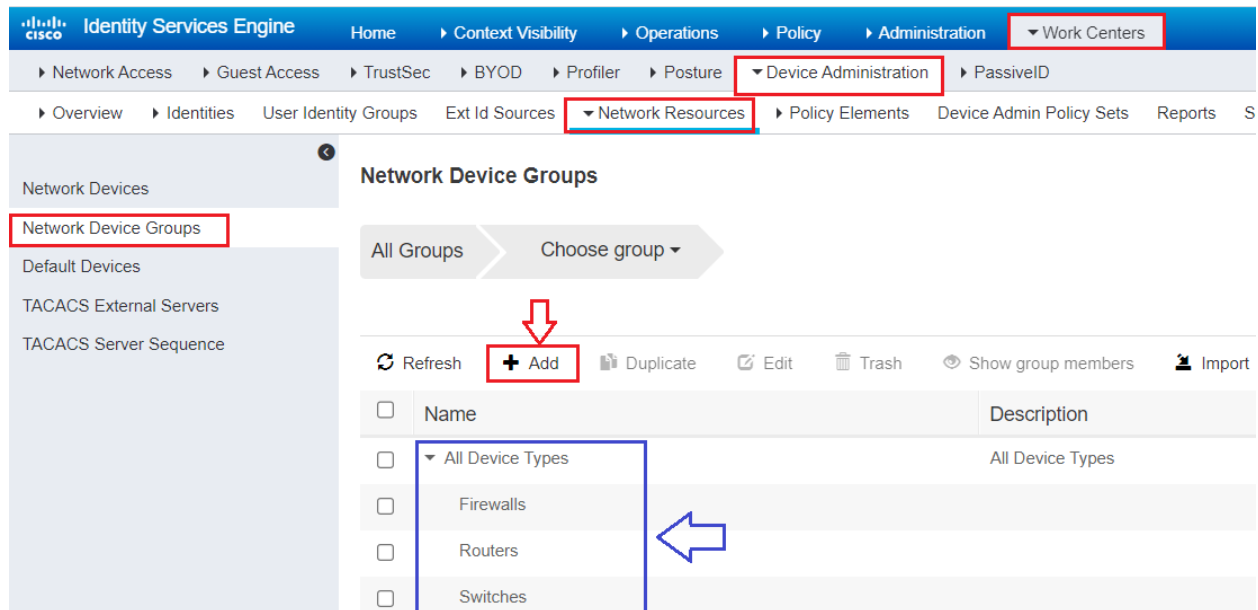
Below the configuration details, the 'Role' is set to 'PRIMARY', and there is a 'Make Standalone' button. The 'Administration' checkbox is checked. The 'Monitoring' checkbox is checked. The 'Policy Service' checkbox is checked, and its sub-items are expanded:

- ☒ Enable Session Services (info icon)
- Include Node in Node Group: None (dropdown menu, info icon)
- ☒ Enable Profiling Service (info icon)
- ☐ Enable Threat Centric NAC Service (info icon)
- ☐ Enable SXP Service (info icon)
- ☒ Enable Device Admin Service (info icon) (highlighted with a red box and an arrow)
- ☐ Enable Passive Identity Service (info icon)

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.

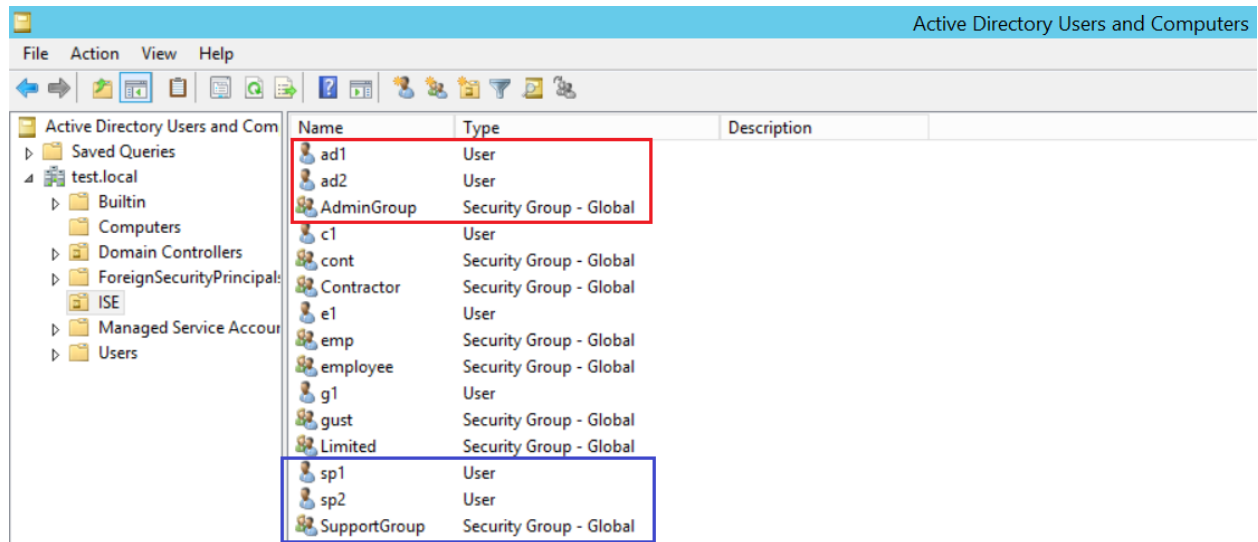
## Create Device Groups:

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 **ad1** and **sp1**



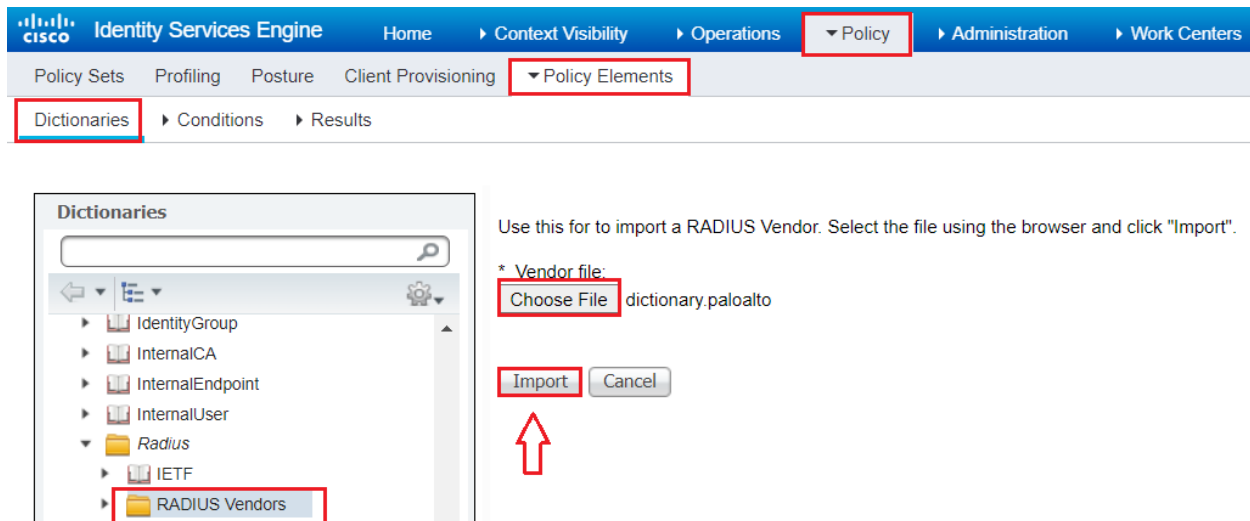
Choose **Administration > Identity Management > External Identity Sources > Active Directory**. Click the **Groups** Tab. Click on Add and then Select Groups from Directory.

## Palo Alto RADIUS Dictionary:

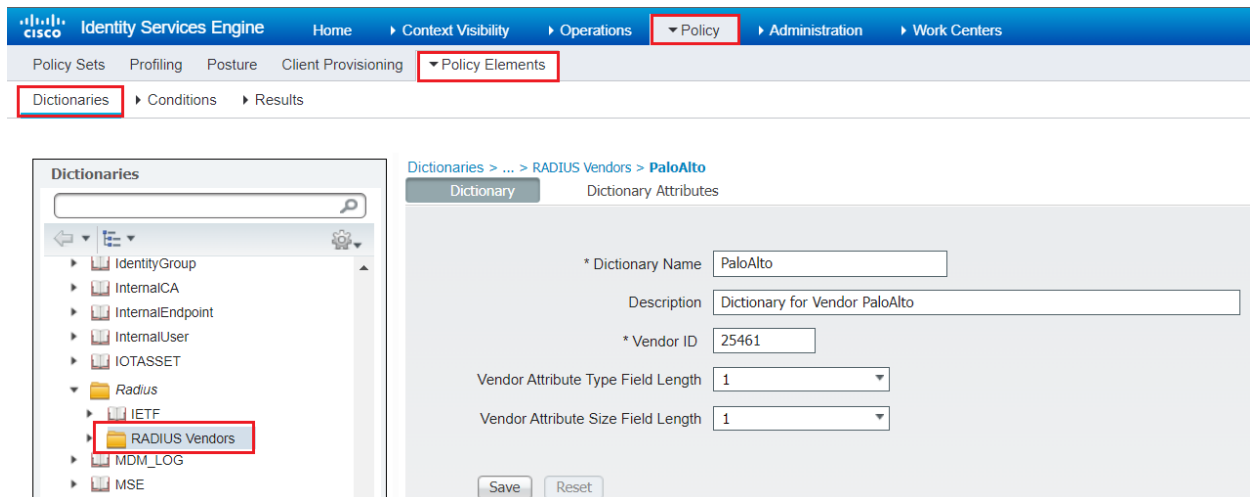
Palo Alto Radius dictionary defines the authentication attributes needed for communication between a PA and Cisco ISE server. You can download the dictionary from here:

<https://docs.paloaltonetworks.com/resources/radius-dictionary.html>

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



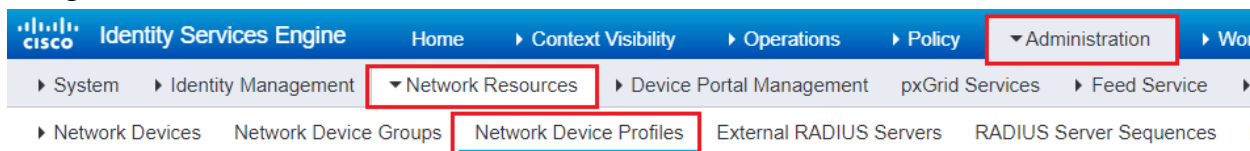
To verify Dictionary, go to **Policy >Policy Elements > Dictionary System -> RADIUS -> RADIUS Vendors** click on Dictionary to check and verify it.



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.

## Network Device Profiles:

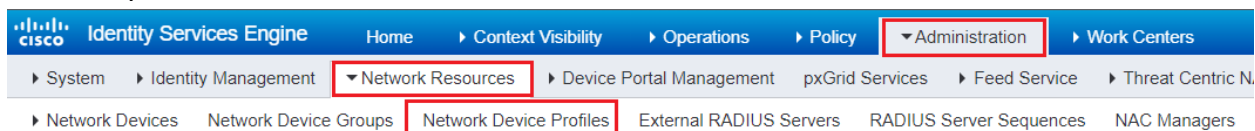
Navigate to **Administration > Network Resources > Network Device Profiles > Click +Add.**



### Network Device Profiles

	<div></div>					
<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 PaloAlto, Vender, Support Protocols and choose RADIUS Dictionary and **submit**.



## 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 Cisco Identity Services Engine (ISE) interface for adding a new network device. The breadcrumb navigation is **Work Centers > Device Administration > Network Resources > Network Devices**. The **Add** button is highlighted. The form fields are as follows:

- Name:** PaloAltoFW
- Description:** PaloAlto FW
- IP Address:** 192.168.100.252
- Device Profile:** PaloAlto
- Model Name:** (empty)
- Software Version:** (empty)
- Network Device Group:** (empty)
- RADIUS Authentication Settings:** (checked)
- RADIUS UDP Settings:**
  - Protocol:** RADIUS
  - \* Shared Secret:** (masked with dots)
  - Use Second Shared Secret:** (unchecked)
  - CoA Port:** 1700

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

This close-up view of the **RADIUS Authentication Settings** section shows the following details:

- The **RADIUS Authentication Settings** checkbox is checked (indicated by a red arrow).
- The **RADIUS UDP Settings** section is expanded.
- The **Protocol** is set to **RADIUS**.
- The **\* Shared Secret** field contains a masked value (dots) and is highlighted with a red box. A **Show** button is next to it.
- The **Use Second Shared Secret** checkbox is unchecked.
- The **CoA Port** is set to **1700**.

## Authorization Profile:

Let's create two authorization profiles which we will use later in the policy. Use two of the predefined roles. (superuser, superreader). Please make sure that you select the 'Palo' Network Device Profile. If you want to use custom Admin Roles, the names must match on the PA and Cisco ISE.

Navigate to **Policy > Policy Elements > Results**. Navigate to **Authorization > Authorization Profiles** and click + **Add**. Name: Provide valid name. Access Type: ACCESS ACCEPT. Network Device Profile: Select the profile you created for Radius in this case PaloAlto. In advanced Attributes Settings choose **PaloAlto: PaloAlto-Admin-Role** and type **superuser**. Click on **Submit**

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' menu is expanded, showing 'Policy Sets', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. The 'Policy Elements' menu is further expanded to show 'Dictionary', 'Conditions', and 'Results'. The 'Results' menu is selected, and the 'Authorization Profiles' link is highlighted in the left sidebar. The main content area is titled 'Authorization Profiles > New Authorization Profile'. It contains a form for creating a new authorization profile. The form fields are: 'Name' (PA-AdminGroup), 'Description' (empty), 'Access Type' (ACCESS\_ACCEPT), and 'Network Device Profile' (PaloAlto). Below the form is a section for 'Advanced Attributes Settings' which contains a table with one row: 'PaloAlto:PaloAlto-Admin-Role' equals 'superuser'. A red arrow points to the 'superuser' value. At the bottom of the form are 'Submit' and 'Cancel' buttons.

Authorization Profiles > New Authorization Profile

**Authorization Profile**

\* Name: PA-AdminGroup

Description:

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: PaloAlto

**Common Tasks**

**Advanced Attributes Settings**

PaloAlto:PaloAlto-Admin-Role	=	superuser	+
------------------------------	---	-----------	---

**Attributes Details**

Access Type = ACCESS\_ACCEPT  
PaloAlto-Admin-Role = superuser

Submit Cancel

Navigate to **Policy > Policy Elements > Results**. Navigate to **Authorization > Authorization Profiles** and click + **Add**. Name: Provide valid name. Access Type: ACCESS ACCEPT. Network Device Profile: Select the profile you created for Radius in this case PaloAlto. In advanced Attributes Settings choose **PaloAlto: PaloAlto-Admin-Role** and type **superreader**. Click on **Submit**.

**Identity Services Engine** Home Context Visibility Operations **Policy** Administration Work

Policy Sets Profiling Posture Client Provisioning **Policy Elements**

Dictionaries Conditions **Results**

**Authorization Profiles > New Authorization Profile**

**Authorization Profile**

\* Name **PA-SupportGroup**

Description

\* Access Type **ACCESS\_ACCEPT**

Network Device Profile **PaloAlto**

**Common Tasks**

**Advanced Attributes Settings**

PaloAlto:PaloAlto-Admin-Role = **superreader**

**Attributes Details**

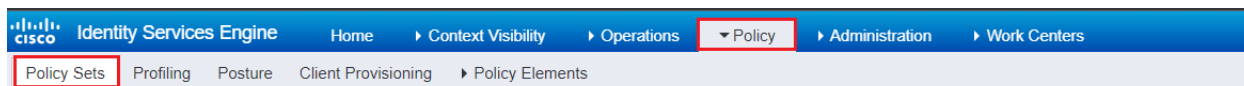
Access Type = ACCESS\_ACCEPT  
PaloAlto-Admin-Role = superreader

**Submit** Cancel



## Device Administration Policy:

Navigate to **Policy > 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 / Server Sequence
Search				
		PaloAlto-Policy	Network Access Device IP Address EQUALS 192.168.100.252	Default Network Access x ▾ +
		Default		Default Network Access x ▾ +

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

		PaloAlto-Policy	Network Access Device IP Address EQUALS 192.168.100.252	
▼ Authentication Policy (1)				
	Status	Rule Name	Conditions	Use
Search				
		PA-Auth	Network Access Device IP Address EQUALS 192.168.100.252	AD-TEST ➤ Options
		Default		All_User_ID_Stores ➤ Options

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

▼ Authorization Policy (1)				
	Status	Rule Name	Conditions	Results Profiles
Search				
		PA-SupportGroup	AD-TEST:ExternalGroups EQUALS test.local/ISE/SupportGroup	× PA-SupportGroup
		PA-AdminGroup	AD-TEST:ExternalGroups EQUALS test.local/ISE/AdminGroup	× PA-AdminGroup
		Default		× DenyAccess