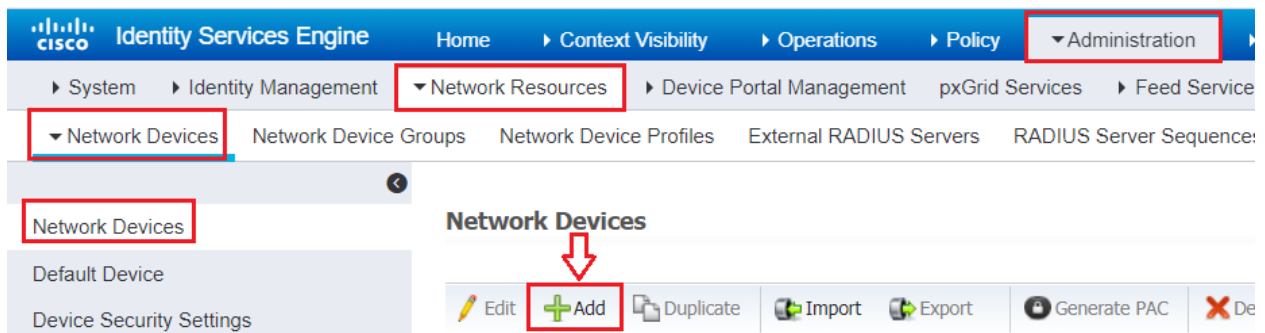


Add Network Device:

Go to **Administration > Network Resources > Network Devices** to add the Device (SW2).



Click on **Add** button to add Network Device like Cisco Wireless LAN Controller.



Configure **Name** of device, **IP address** configured. Scroll down to set Authentication settings.

Network Devices List > [New Network Device](#)

Network Devices

* Name

Description

IP Address / 32

* Device Profile

Model Name

Software Version

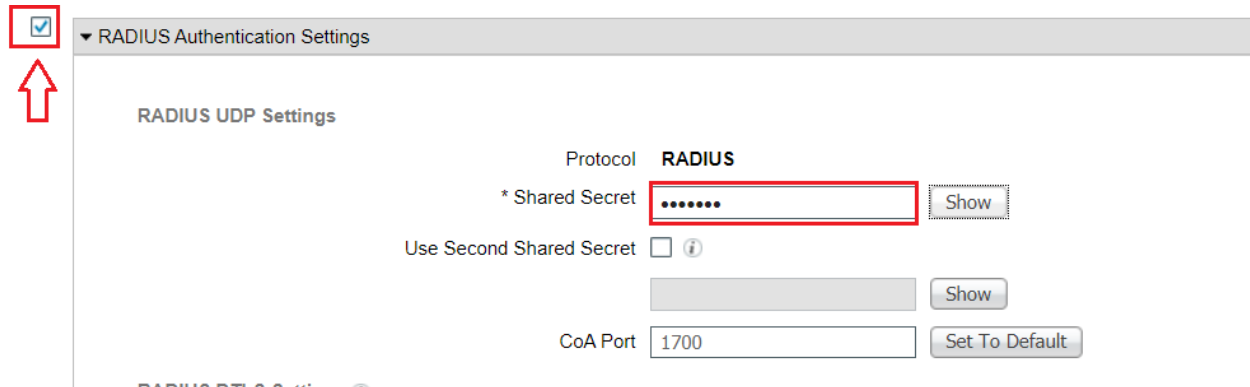
* Network Device Group

Location

IPSEC

Device Type

Scroll down to set Authentication settings. Set Password configured as Server key on Cisco Wireless LAN Controller device “Test123” and save settings.



☒ RADIUS Authentication Settings

RADIUS UDP Settings

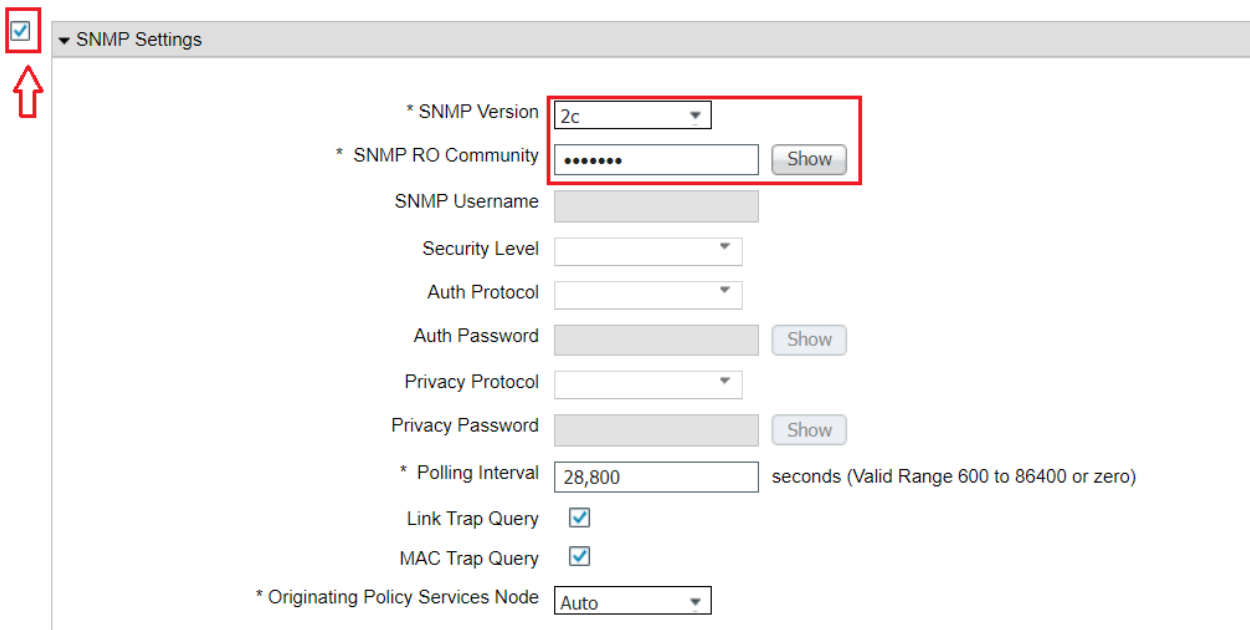
Protocol **RADIUS**

* Shared Secret

Use Second Shared Secret ☐

CoA Port

Scroll down to check **SNMP Settings** and set **SNMP RO Community** string settings, Click **Submit**.



☒ SNMP Settings

* SNMP Version

* SNMP RO Community

SNMP Username

Security Level

Auth Protocol

Auth Password

Privacy Protocol

Privacy Password

* Polling Interval seconds (Valid Range 600 to 86400 or zero)

Link Trap Query ☒

MAC Trap Query ☒






* Originating Policy Services Node

- ☒ RADIUS Authentication Settings
- ☐ TACACS Authentication Settings
- ☒ SNMP Settings
- ☐ Advanced TrustSec Settings

Policy Set:

In order to create a Policy Set from ISE GUI, navigate to **Policy > Policy Set** and then click on plus (+) icon on the upper-left corner.

Policy Sets










	Status	Policy Set Name	Description	Conditions
				
		Dot1x-Policy Set	Dot1 x Policy for Wired	 Wired_802.1X
		Default	Default policy set	

Name the Policy Set in this case **Wireless 802.1X**, set the Conditions **Radius-NAS-Port-Type EQUALS Wireless-IEEE 802.11** and Radius Service-Type EQUALS Framed, Set the **Allow Protocols Default Network Access** protocols. Click **Save** to apply the setting.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets

	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
		Wireless 802.1X		AND  Radius NAS-Port-Type EQUALS Wireless - IEEE 802.11  Radius Service-Type EQUALS Framed	Default Network Access x 
		EasyConnect-Policy	EasyConnect Policy	 Wired_MAB	Default Network Access x 

Radius-NAS-Port-Type

Equals Wireless - IEEE 802.11

AND

Radius-Service-Type

Equals Framed

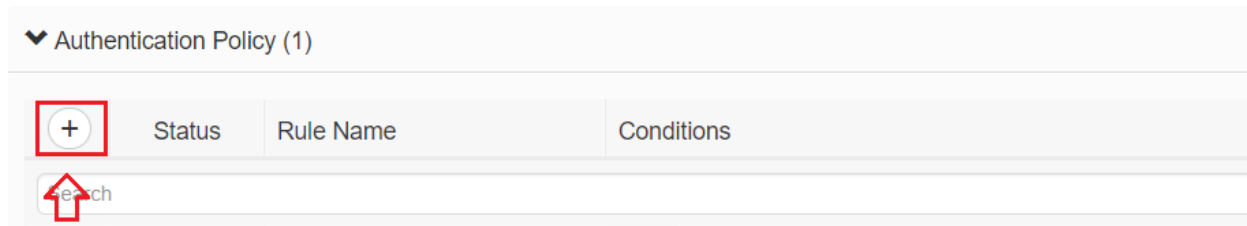
+ New AND OR

Set to 'Is not'

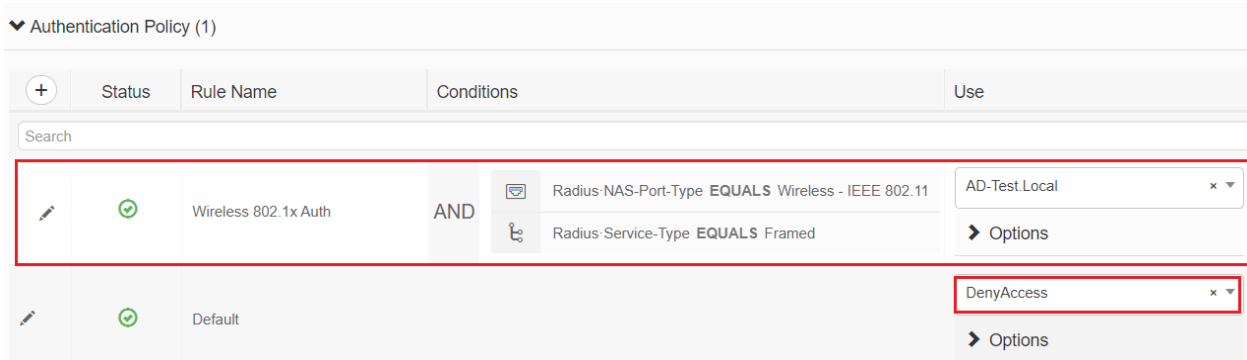
Duplicate Save

Authentication Policy:

For network access policies, choose **Work Centers > Network Access > Policy Sets**. Navigate to Authentication Policy, click Add new **authentication policy**.



Name Authentication Policy Rule in this case **Wireless 802.1x Auth** set the conditions to **Radius-NAS-Port-Type EQUALS Wireless-IEEE 802.11** and **Radius Service-Type EQUALS Framed** also change the default Identity store to **AD-Test.local**. Change the Default Rule Options to **DenyAccess**.



Leave the default **Options** settings and click **Save** to apply the changes.

Authorization Policies:

Navigate to **Policy>Policy Sets > click on Arrow Icon >**

Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Wireless 802.1X		AND Radius-NAS-Port-Type EQUALS Wireless - IEEE 802.11 Radius-Service-Type EQUALS Framed	Default Network Access x +	14	⚙️	➡️
EasyConnect-Policy	EasyConnect Policy	Wired_MAB	Default Network Access x +	0	⚙️	➡️

Navigate to **Authorization Policy** section click on **round circle Plus** icon to add new Authorization rules, name authorization Rules in this case **Employee-Wireless**. In **Conditions** click on **Plus** icon to set the conditions for authorization Rules.

▼ Authorization Policy (14)			
+	Status	Rule Name	Conditions
Search			

Set the conditions to **Wireless_802.1X** and **AD-Test.Local-ExternalGroups EQUALS test.local/SE-Groups/Employees local/users/Employees, Authorization_Employees** Set Results Profiles **Authorization_Employees**

▼ Authorization Policy (1)

<div><div>+</div></div>	Status	Rule Name	Conditions	Results	Profiles
<div>Search</div>					
<div><div><div></div></div></div>	<div><div></div></div>	Employee-Wireless	AND	<div><div><div></div></div><div>AD-Test.Local-ExternalGroups EQUALS test.local/ISE-Groups/Employees</div><div><div></div></div><div>Wireless_802.1X</div></div>	<div><div><div>× Authorization_Employees</div></div><div>+</div></div>
<div><div><div></div></div></div>	<div><div></div></div>	Default		<div><div><div>× DenyAccess</div></div><div>+</div></div>	

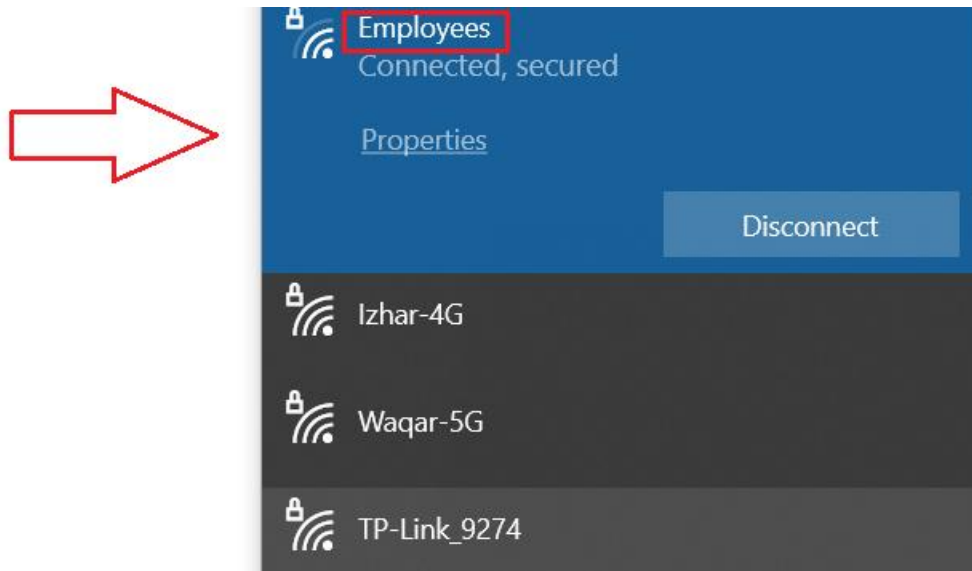
Click **Save** to apply the changes.

x Authorization_Employees +	Developers x +	4	⚙️
x DenyAccess +	Select from list ▾ +	0	⚙️

Reset Save

Verification:

Click on Wifi click on **Employees** SSID to connect it will connect automatically.



Navigate to **Operations > RADIUS LiveLog**.

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Center

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0

Refresh Reset Repeat Counts Export To

Time	Status	Details	Repeat ...	Identity	Endpoint ID
Aug 27, 2021 03:46:21.618 PM			0	e1@test.local	AC:67:5D:4B:82:41
Aug 27, 2021 03:46:21.360 PM				e1@test.local	AC:67:5D:4B:82:41
Aug 27, 2021 03:00:20.657 PM				e1@test.local	5A:48:98:C7:1A:2C

Overview

Event	5200 Authentication succeeded
Username	e1@test.local
Endpoint Id	AC:67:5D:4B:82:41 ⓘ
Endpoint Profile	
Authentication Policy	Wireless 802.1X >> Wireless 802.1x Auth
Authorization Policy	Wireless 802.1X >> Employee-Wireless
Authorization Result	Authorization_Employees

Go to **Policy > Policy Sets** and verify the Hits.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets

+	Status	Policy Set Name	Conditions	Allowed Protocols / Server Sequence	Hits
Search					
	✓	Wireless 802.1X	AND Radius-NAS-Port-Type EQUALS Wireless - IEEE 802.11 Radius-Service-Type EQUALS Framed	Default Network Access x +	6