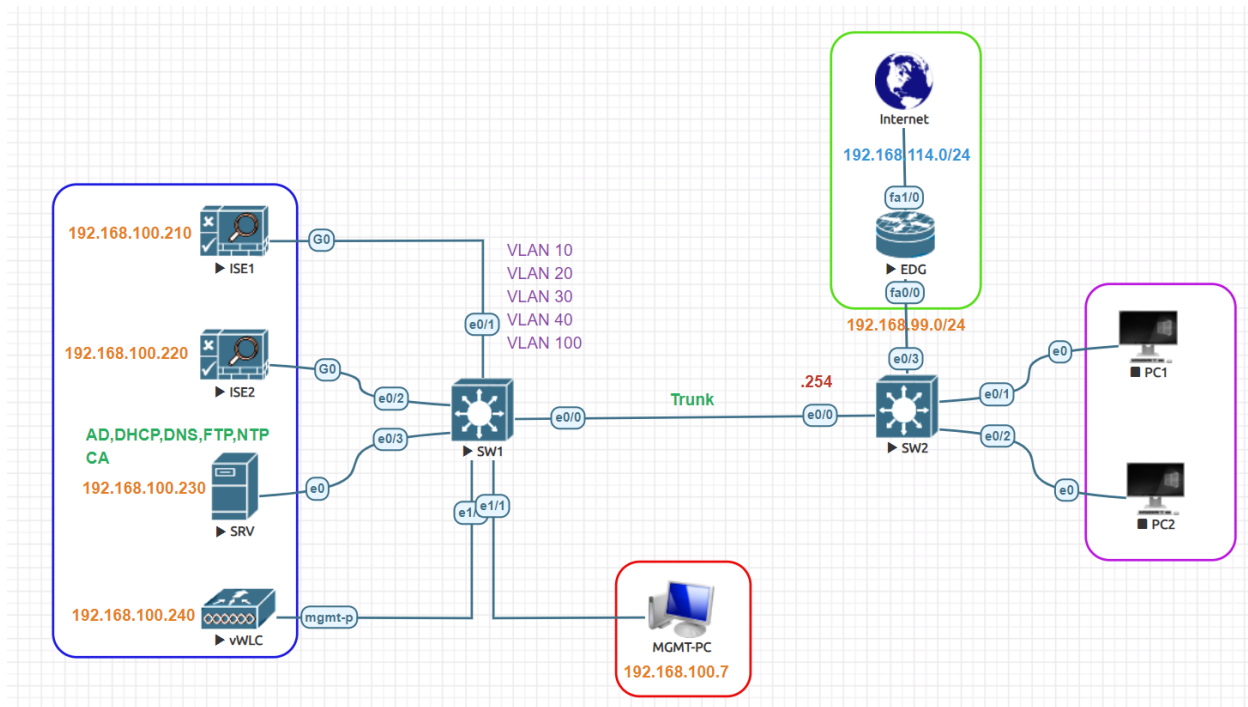


Dot1x LAB:



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
Test User/Group	E1/Employee
Test VLAN	VLAN 20
VLAN Subnet	192.168.20.0/24
VLAN 20 Gateway	192.168.20.1
Authenticator Switch	SW2
Authentication Switch MGMT IP	192.168.100.254
SW2 Dot1x interface	Ethernet 0/1

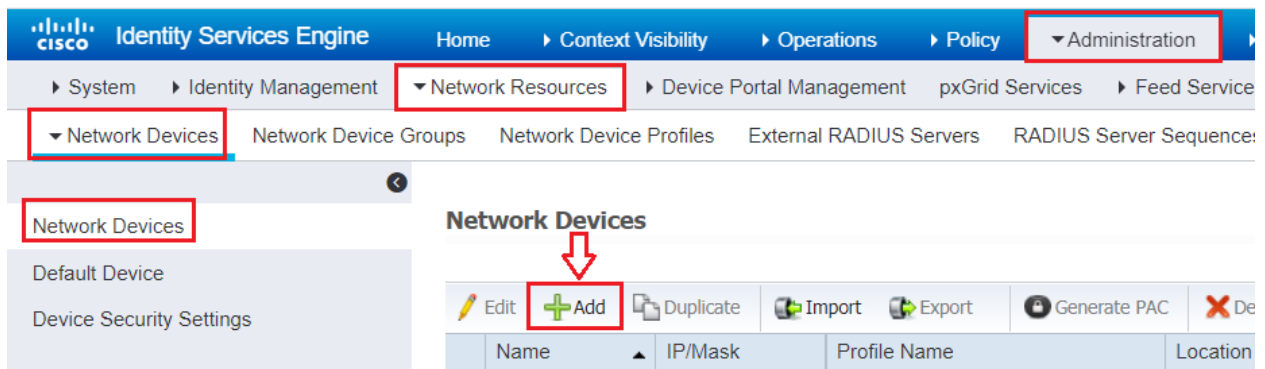
Dot1X Configuration
SW2(config)#aaa new-model
SW2(config)#dot1x system-auth-control
SW2(config)#radius server ISE1
SW2(config-radius-server)# address ipv4 192.168.100.210 auth-port 1812 acct-port 1813
SW2(config-radius-server)#key Test123
SW2(config-radius-server)#radius server ISE2
SW2(config-radius-server)# address ipv4 192.168.100.220 auth-port 1812 acct-port 1813
SW2(config-radius-server)#key Test123
SW2(config-radius-server)#radius-server attribute 6 on-for-login-auth
SW2(config)#radius-server attribute 8 include-in-access-req
SW2(config)#radius-server attribute 25 access-request include
SW2(config)#radius-server vsa send accounting
SW2(config)#radius-server vsa send authentication
SW2(config)#radius-server dead-criteria time 30 tries 3
SW2(config)#radius-server timeout 2
SW2(config)#aaa group server radius ISE-GROUP
SW2(config-sg-radius)#server name ISE1
SW2(config-sg-radius)#server name ISE2
SW2(config-sg-radius)#ip radius source-interface Vlan100
SW2(config-sg-radius)#aaa authentication dot1x default group ISE-GROUP
SW2(config)#aaa authorization network default group ISE-GROUP
SW2(config)#aaa accounting update periodic 5
SW2(config)#aaa accounting dot1x default start-stop group ISE-GROUP
SW2(config)#aaa server radius dynamic-author
SW2(config-locsvr-da-radius)#client 192.168.100.210 server-key Test123
SW2(config-locsvr-da-radius)#client 192.168.100.220 server-key Test123
SW2(config-locsvr-da-radius)#snmp-server community Test123 RO
SW2(config)#interface Ethernet0/1
SW2(config-if)#description win10 node
SW2(config-if)#switchport access vlan 20
SW2(config-if)#switchport mode access
SW2(config-if)#authentication host-mode multi-auth
SW2(config-if)#authentication port-control auto
SW2(config-if)#mab
SW2(config-if)#dot1x pae authenticator
SW2(config-if)#dot1x timeout tx-period 10
SW2(config-if)#spanning-tree portfast edge
SW2(config-if)#authentication event fail action next-method
SW2(config-if)#authentication order dot1x mab

Add Network Device:

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



Click on **Add** button to add Network Device like Router and Switch.



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

The screenshot shows the Cisco ISE New Network Device configuration page. The 'Name' field is set to 'SW2', the 'Description' field is set to 'SW2', the 'IP Address' field is set to '192.168.100.254', and the 'Device Profile' is set to 'Cisco'. The 'Model Name' is set to 'ADVENTERPRI' and the 'Software Version' is set to '15.2'. The 'Network Device Group' section is also visible.

Scroll down to set Authentication settings. Set Password configured as Server key on Switch 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 ☒

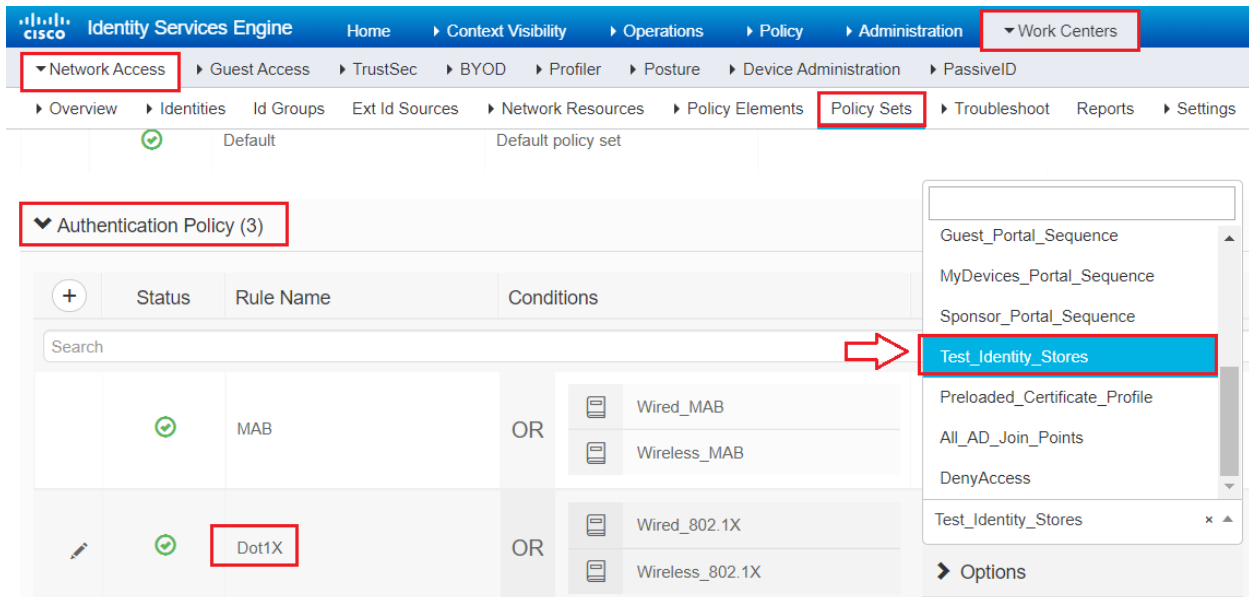
MAC Trap Query ☒

* Originating Policy Services Node

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

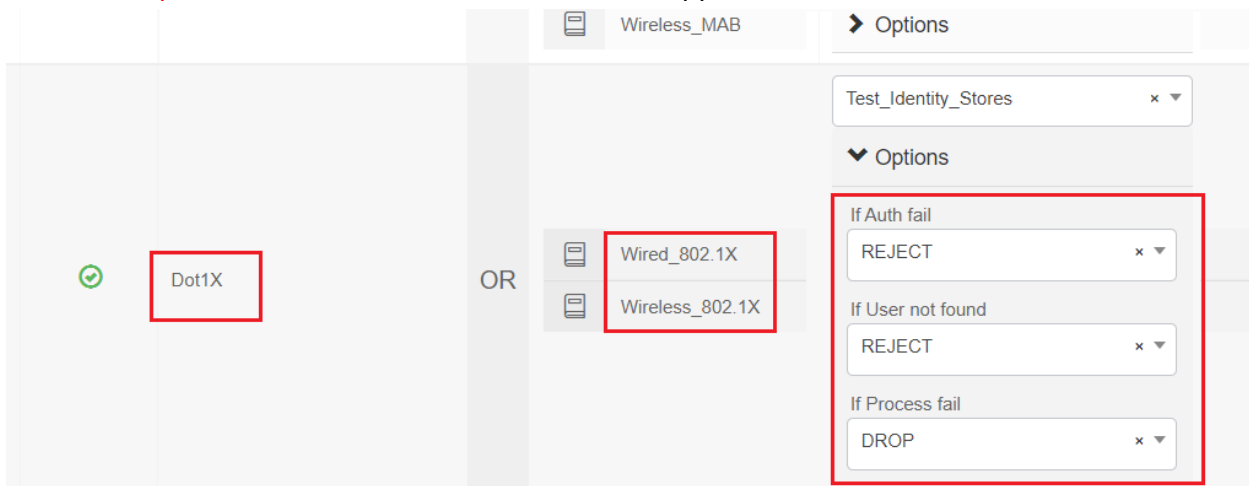
802.1x Authentication Policies:

For network access policies, choose **Work Centers > Network Access > Policy Sets**. Change the default Identity store to **Test_Identity_Stores** which we created earlier.



The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is **Work Centers > Network Access > Policy Sets**. The **Policy Sets** tab is selected. Under **Authentication Policy (3)**, there are three policies: **MAB**, **Dot1X**, and **Wired_802.1X**. The **Dot1X** policy is highlighted with a red box. A red arrow points from the **Dot1X** policy to the **Test_Identity_Stores** dropdown menu, which is also highlighted with a red box. The dropdown menu shows a list of identity stores, with **Test_Identity_Stores** selected.

If the **authentication fail** the user will be Rejected, if **user not found** the user will be rejected, while if the **process** of Dot1x fail the user will be dropped.



The screenshot shows the Cisco Identity Services Engine (ISE) interface, specifically the **Options** section for the **Dot1X** policy. The **Test_Identity_Stores** dropdown is selected. The **Options** section shows three conditions: **If Auth fail** with **REJECT**, **If User not found** with **REJECT**, and **If Process fail** with **DROP**. Each condition is highlighted with a red box.

802.1x Authorization Policies:

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

Policy Sets

Reset Policyset Hitcounts Reset Save

+	Status	Policy Set Name	Allowed Protocols / Server Sequence	Hits	Actions	View
Search						
	✓	Default	Default Network Access x +	35	⚙️ ➡️	

Navigate to **Authorization Policy** section click on **round circle Plus** icon to add new Authorization Policy, name the authorization policy in this case **Dot1x-Authentication**. In **Conditions** click on **Plus** icon to set the conditions for authorization policy.

Authorization Policy (14)

+	Status	Rule Name	Conditions
Search			
✎️	✓	Dot1X-Authentication	+

In **Conditions Studio > Editor** click to add an attribute choose **ad.test.local**

Conditions Studio

Library

Search by Name

Editor

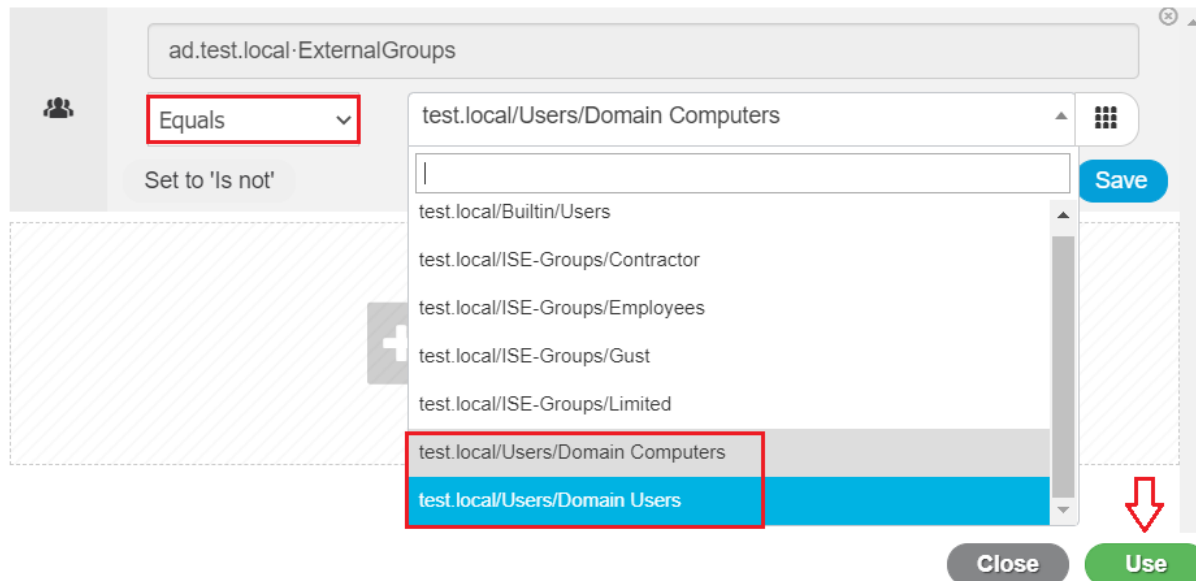
Click to add an attribute

Select attribute for condition

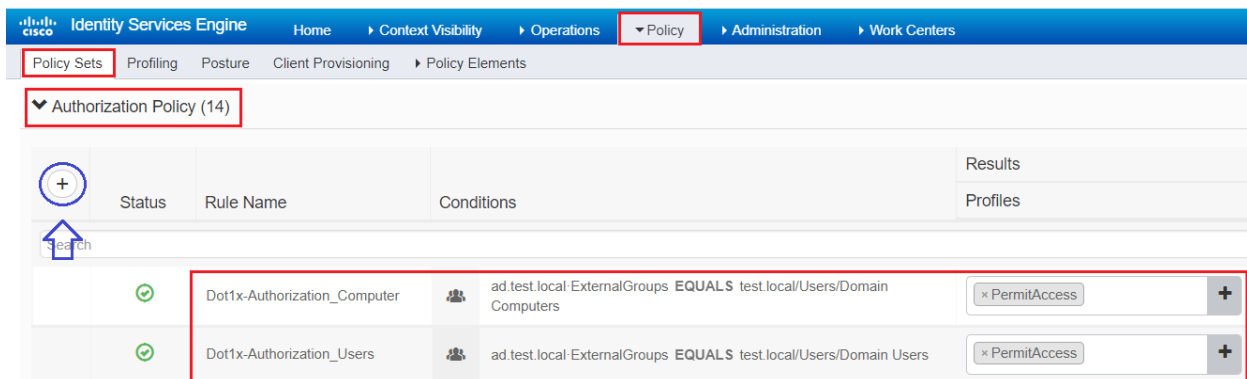
Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
WISPr	WISPr-Session-Terminate-Time	9	
ad.test.local	ExternalGroups		
ad.test.local	IdentityAccessRestricted		

Close Use

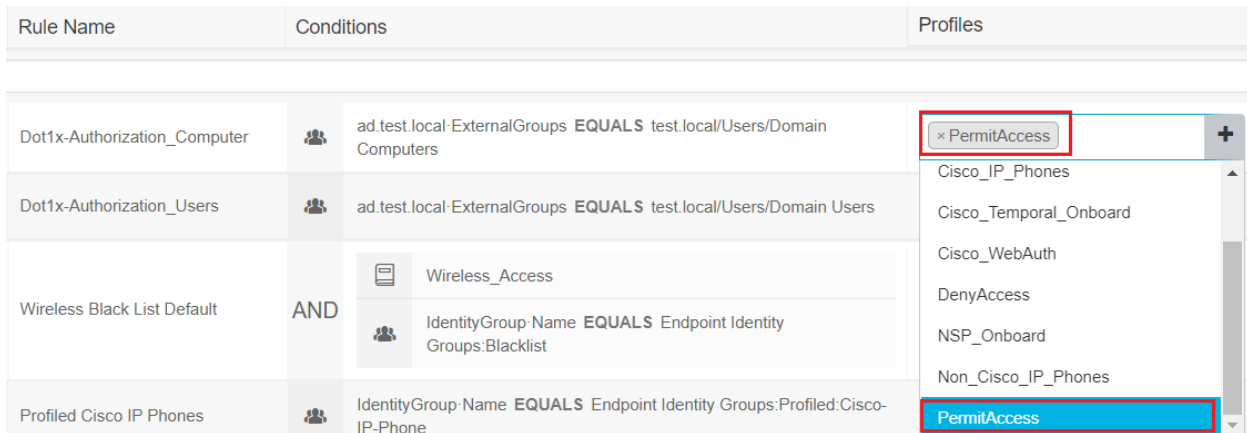
In **Editor > Equals > test.local/users/Domain Computers** also, create new same policy for **test.local/users/Domain Users**



Finally, two Authorization Polices are created for Dot1x Authorization.

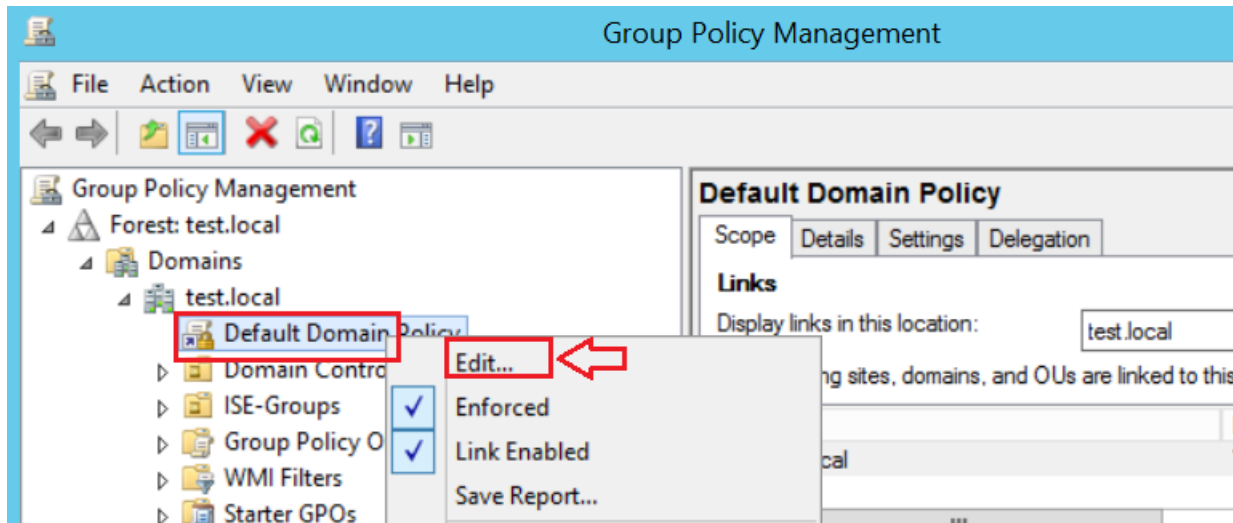


In **Profile** choose **PermitAccess** from dropdown and click **Save**.

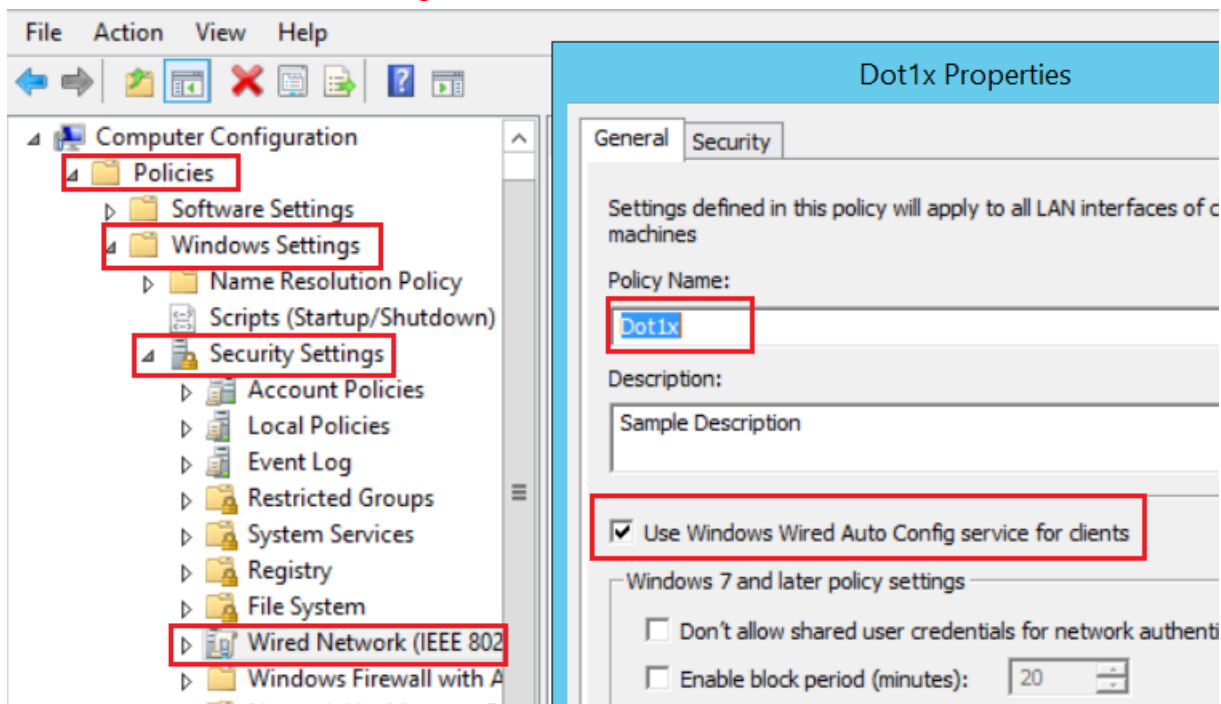


Dot1x Client Group Policy Creation:

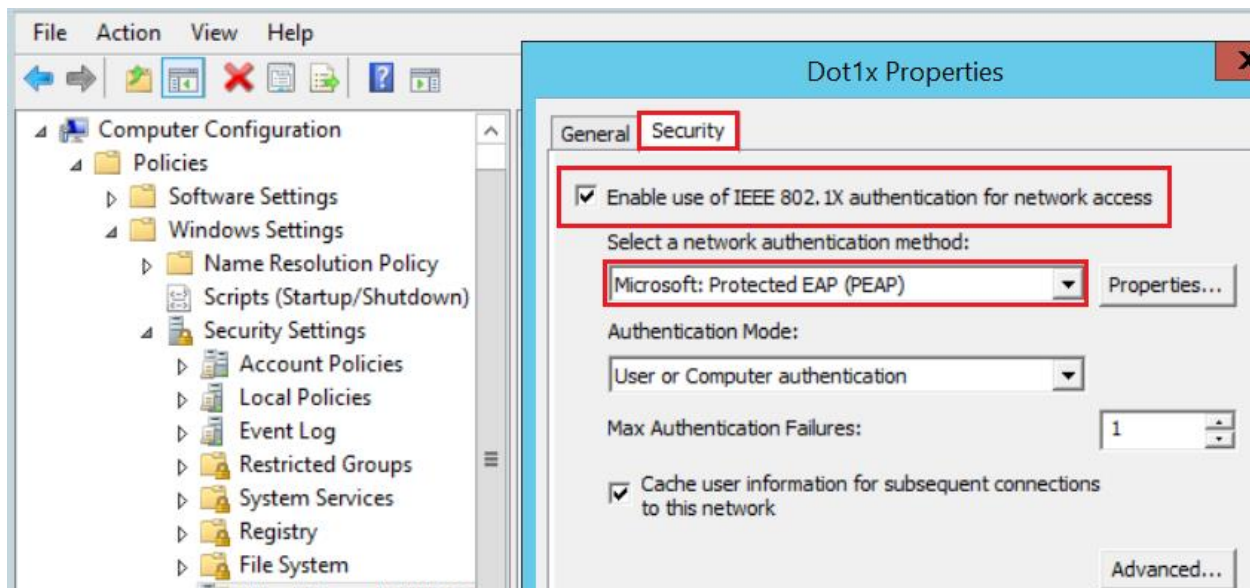
Let's create group policy to push down dot1x settings to clients. Open Group Policy Management. Highlight the domain and right-click on **Default Domain Policy** and click **Edit**.



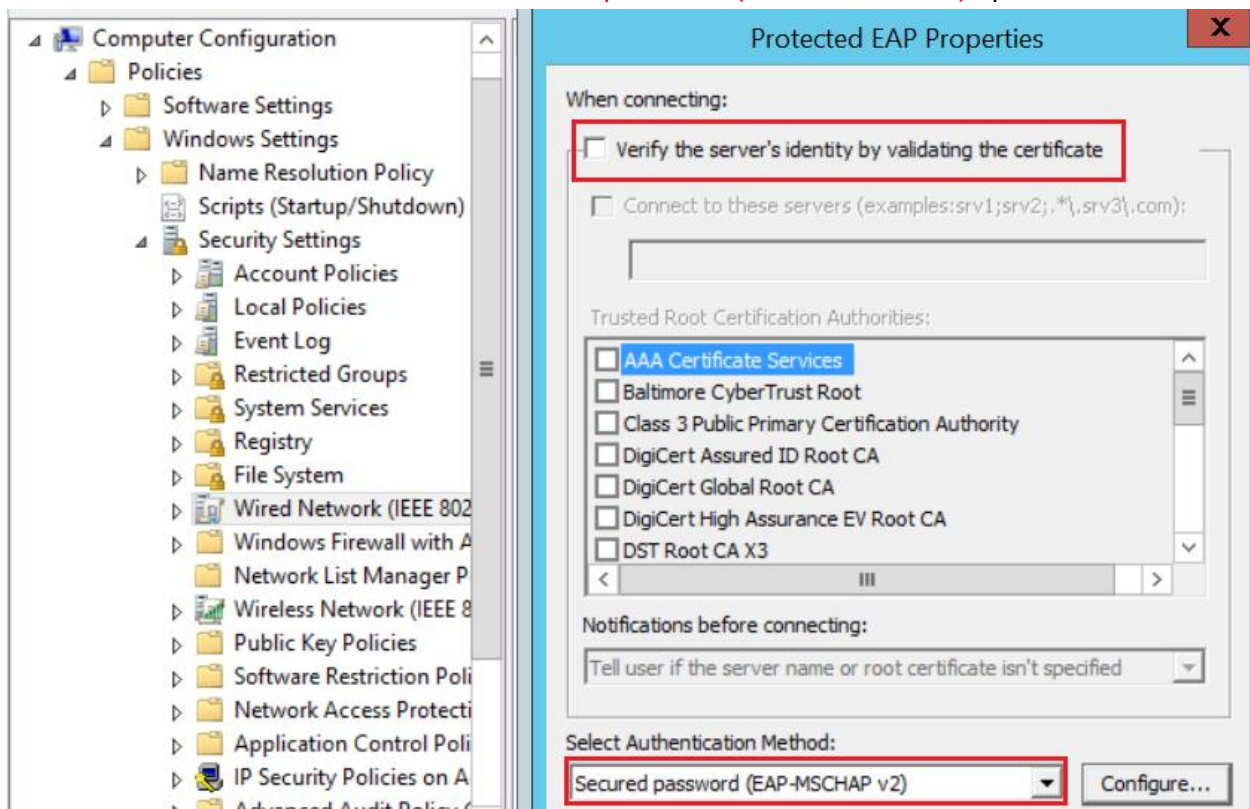
Navigate to **Computer Configuration > Windows Settings > Security Settings > Wired Network** and right-click on it. Choose **Create a New Wired Network Policy**. This will open the New Wired Network Policy Properties box. Name your policy whatever you'd like it to be and make sure the **Use Windows Wired Auto Config service for clients** box is checked.



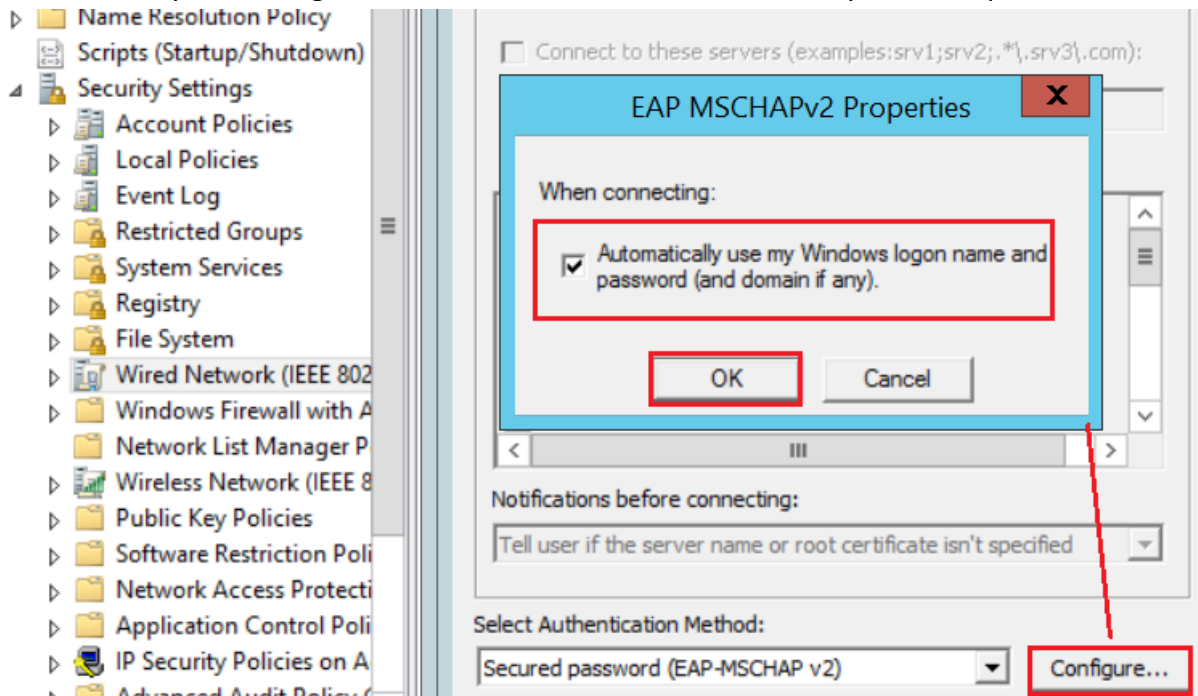
On the **Security** tab, ensure that the **Enable use of IEEE 802.1X authentication for network access** box is checked and from the Select a network authentication method drop-down, choose Microsoft: **Protected EAP (PEAP)**. Click on the Properties button to the right of it.



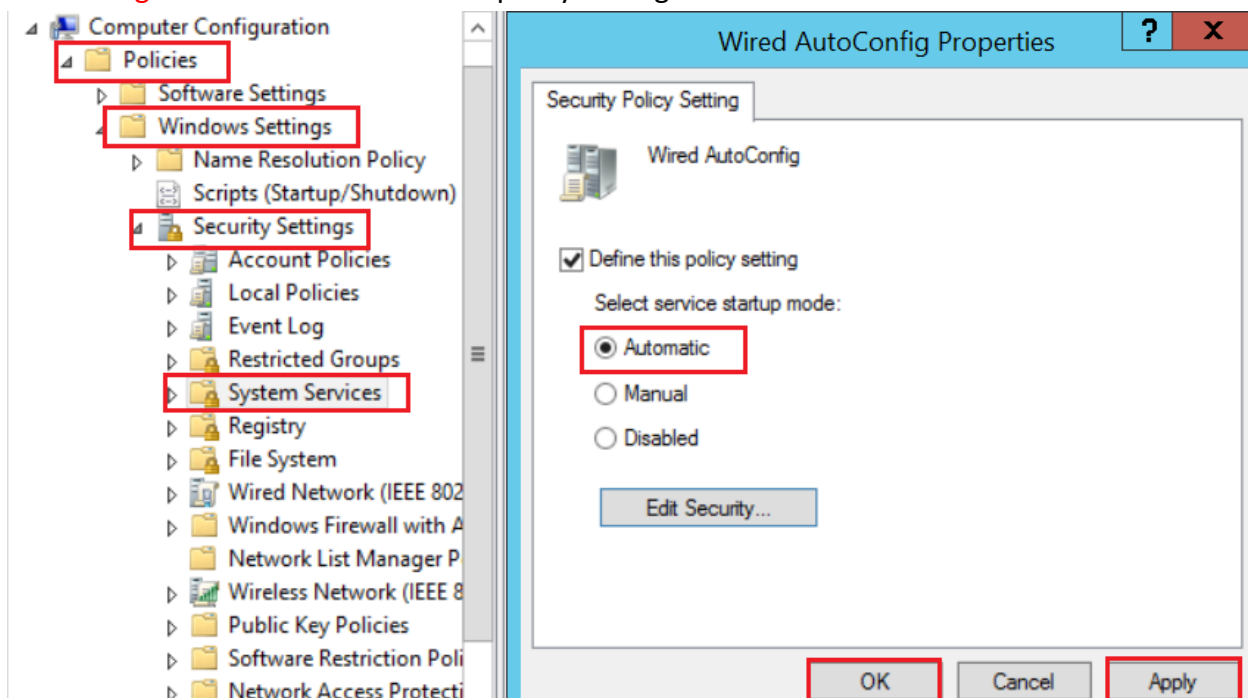
In the **Properties** box that pops up, uncheck the boxes next to **Verify the server's identity by validating the certificate**. Under the Select Authentication Method drop-down, this is where we will select our inner method. Choose **Secured password (EAP-MSCHAP v2)** options.



Click on the **Configure...** box next to it. EAP MSCHAPv2 box should pop up. Check the boxes and click **OK** to save your settings. Do the same for the rest of the boxes you have open.



Wired Autoconfig service is not enabled by default on Windows machines. In order to get the dot1x wired settings to work, this should be enabled so let's create a group policy. Navigate to **Computer Configuration>Policies>Windows Settings>Security Settings>System Settings>Wired Autoconfig**. Check box for Define this policy setting and choose the radio button for **Automatic**.



Verification:

Navigate to **Operations > RADIUS Livelog**.

Refresh Reset Repeat Counts Export To

Time	Status	Details	Repeat ...	Identity	Endpoint ID
Jul 21, 2021 05:17:24.705 PM	Auth		0	TESTe1	50:01:00:0A:00:00
Jul 21, 2021 04:17:50.686 PM	Auth			TESTe1	50:01:00:0A:00:00
Jul 21, 2021 04:17:18.672 PM	Auth			host/PC1-WIN10.t...	50:01:00:0A:00:00
Jul 21, 2021 02:37:09.868 PM	Auth			TESTe1	50:01:00:0A:00:00

Verification commands on Cisco Switch

SW2# show dot1x interface ethernet 0/1
SW2# show dot1x all
SW2# Show authentication sessions
SW2# Show authentication sessions interface ethernet 0/1 details

SW2#show authentication sessions

Interface	Identifier	Method	Domain	Status	Fg	Session ID
Et0/1	5001.000a.0000	dot1x	DATA	Auth		C0A864FE000000120188C7C8

Session count = 1

Key to Session Events Blocked Status Flags:

- A - Applying Policy (multi-line status for details)
- D - Awaiting Deletion
- F - Final Removal in progress
- I - Awaiting IIF ID allocation
- N - Waiting for AAA to come up
- P - Pushed Session
- R - Removing User Profile (multi-line status for details)
- U - Applying User Profile (multi-line status for details)
- X - Unknown Blocker

```
SW2#show authentication sessions interface e0/1 details
```

```
Interface: Ethernet0/1
MAC Address: 5001.000a.0000
IPv6 Address: Unknown
IPv4 Address: 192.168.20.11
User-Name: TEST\e1
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: 300s (local), Remaining: 229s
Session Uptime: 3981s
Common Session ID: C0A864FE000000120188C7C8
Acct Session ID: 0x00000007
Handle: 0x1B000003
Current Policy: POLICY_Et0/1
```

Local Policies:

```
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
Security Status: Link Unsecure
```

Server Policies:

Method status list:

Method	State
dot1x	Authc Success

```
SW2#show dot1x all
```

```
Sysauthcontrol Enabled
Dot1x Protocol Version 3
```

Dot1x Info for Ethernet0/1

```
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 10
```