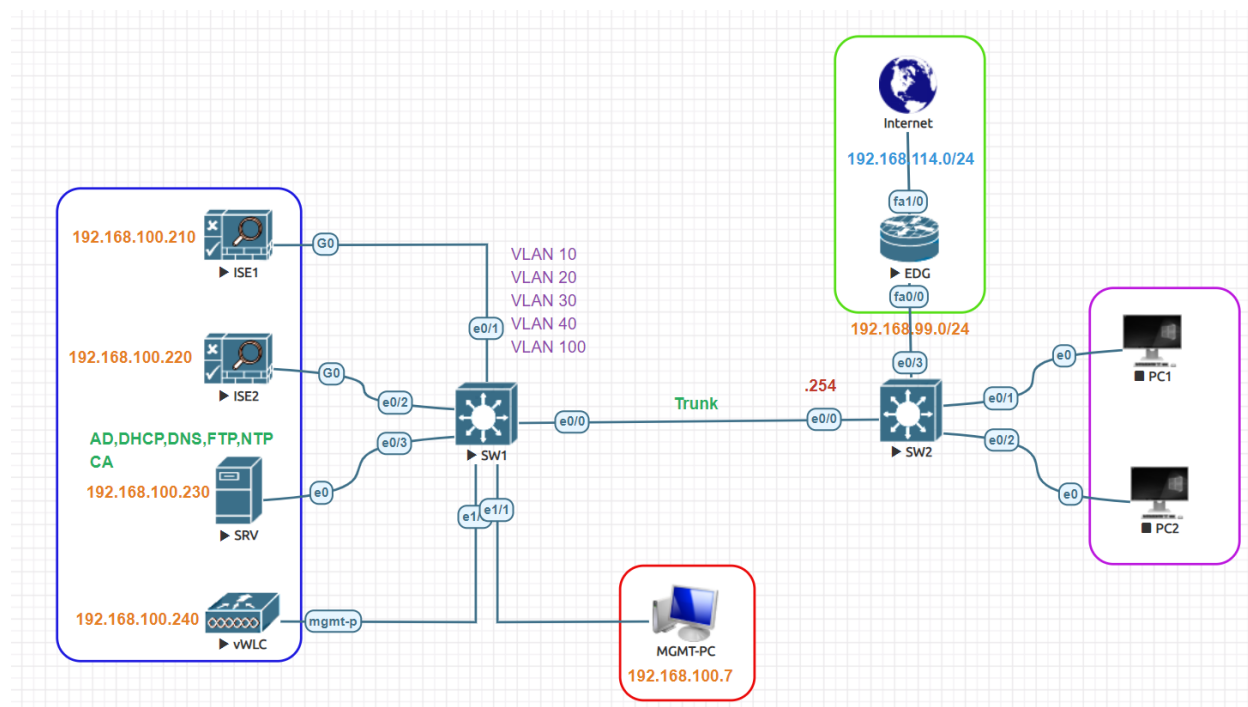


Dynamic VLAN Lab:



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
DACL Name	DACL_Test
Authorization Profile Name	Deny_ISE_AuthProfile
Dynamic VLAN	VLAN 40

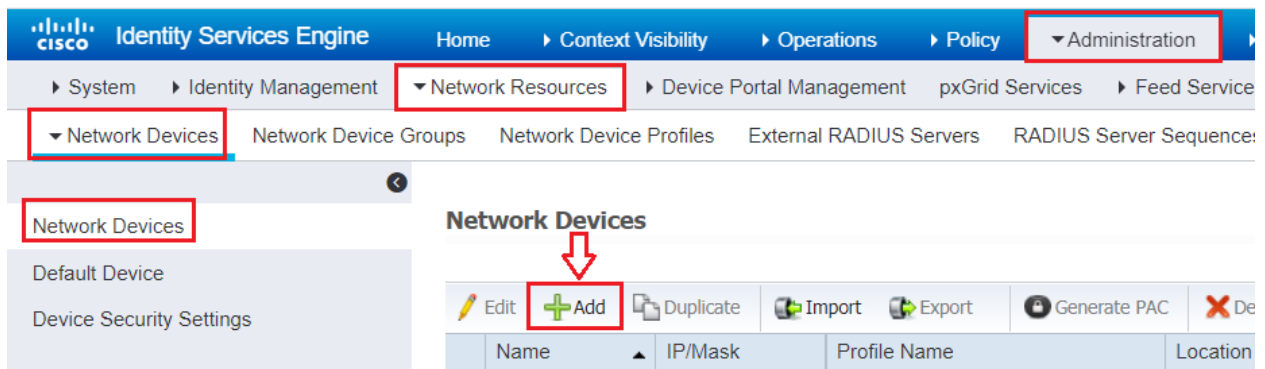
Dot1X Configuration
SW2(config)#aaa new-model
SW2(config)#dot1x system-auth-control
SW2(config)#radius server ISE1
SW2(config-radius-server)# address ipv4 192.168.100.210 auth-port 1812 acct-port 1813
SW2(config-radius-server)#key Test123
SW2(config-radius-server)#radius server ISE2
SW2(config-radius-server)# 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 form. The form fields are filled with:

- Name: SW2
- Description: SW2
- IP Address: 192.168.100.254
- Device Profile: Cisco
- Model Name: ADVENTERPRI
- Software Version: 15.2
- Network Device Group: All Locations
- Is IPSEC Device: Is IPSEC Device
- Device Type: All Device Types

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 ISE Policy Sets configuration page. The breadcrumb trail 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 ISE Policy Sets configuration page, 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

BYOD_is_Registered Catalyst_Switch_Local_Web_Authentication Compliance_Unknown_Devices MAC_in_SAN Network_Access_Authentication_Passed Non_Cisco_Profiled_Phones

Editor

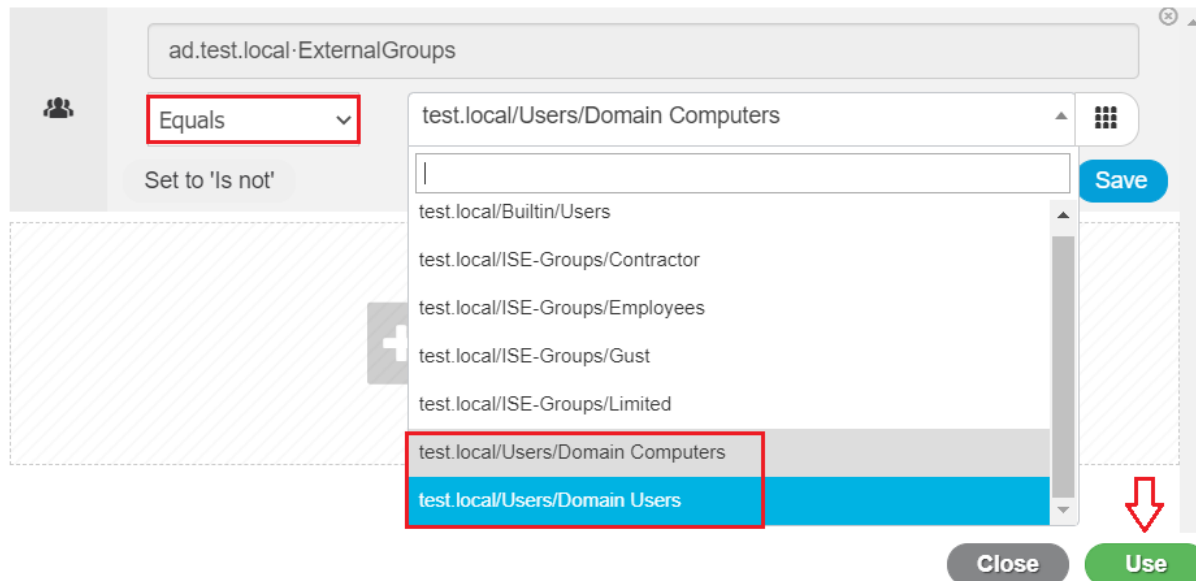
Click to add an attribute

Select attribute for condition

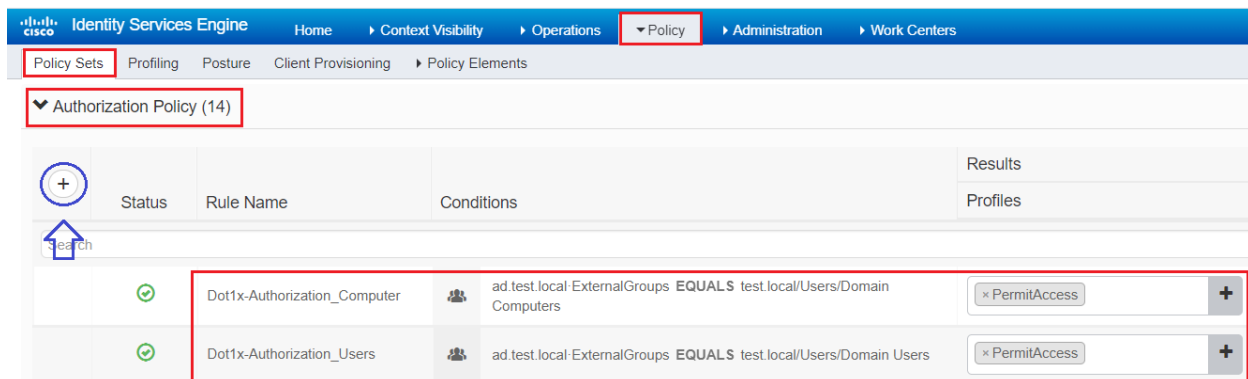
Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
WISPr	WISPr-Session-Terminate-Time	9	
ad.test.local	ExternalGroups		
ad.test.local	IdentityAccessRestricted		

Close Use

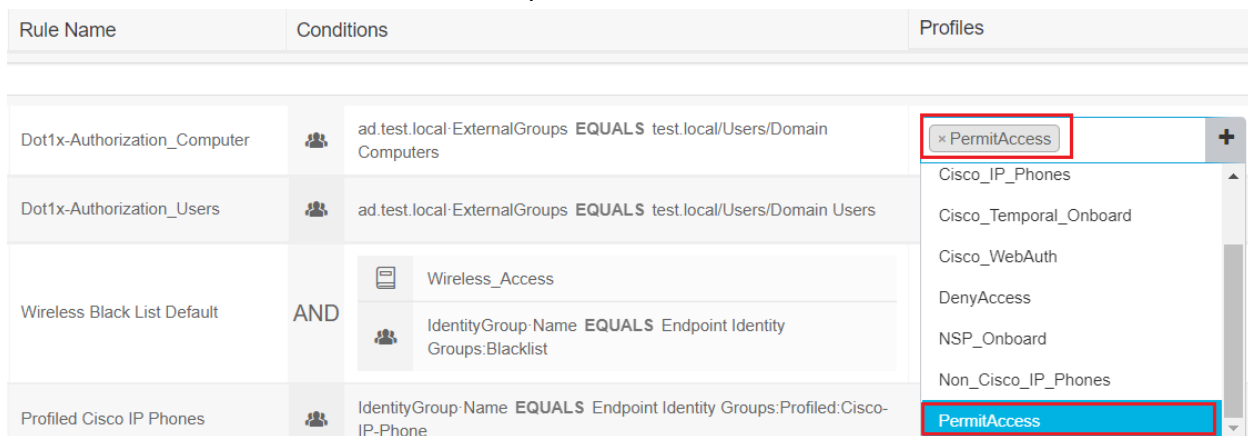
In **Editor > Equals > test.local/users/Domain Computers** also, create new same policy for **test.local/users/Domain Users**



Finally, two Authorization Polices are created for Dot1x Authorization.

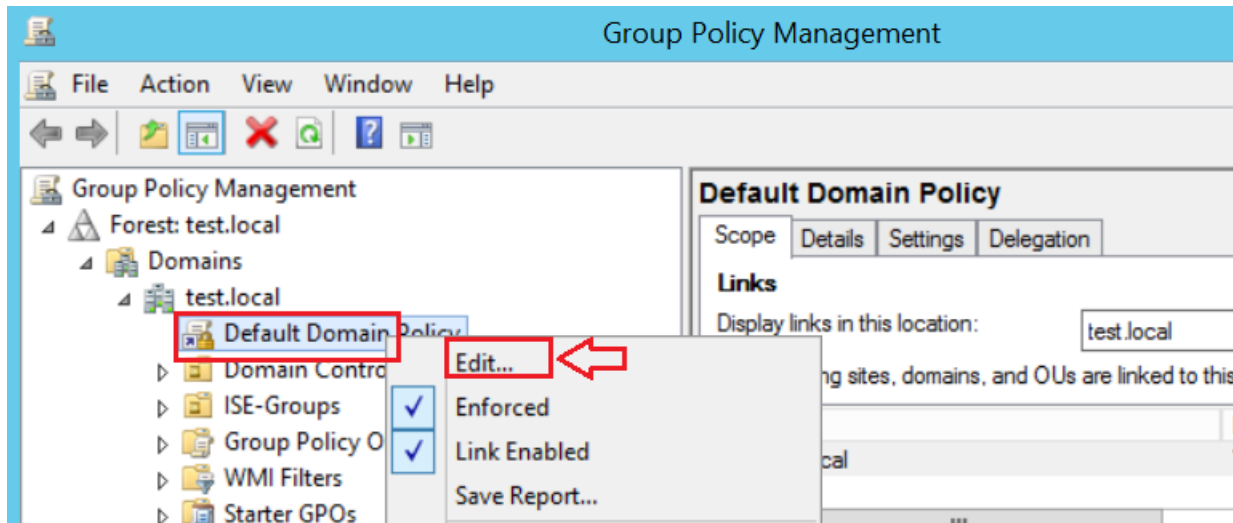


In **Profile** choose **PermitAccess** from dropdown and click **Save**.

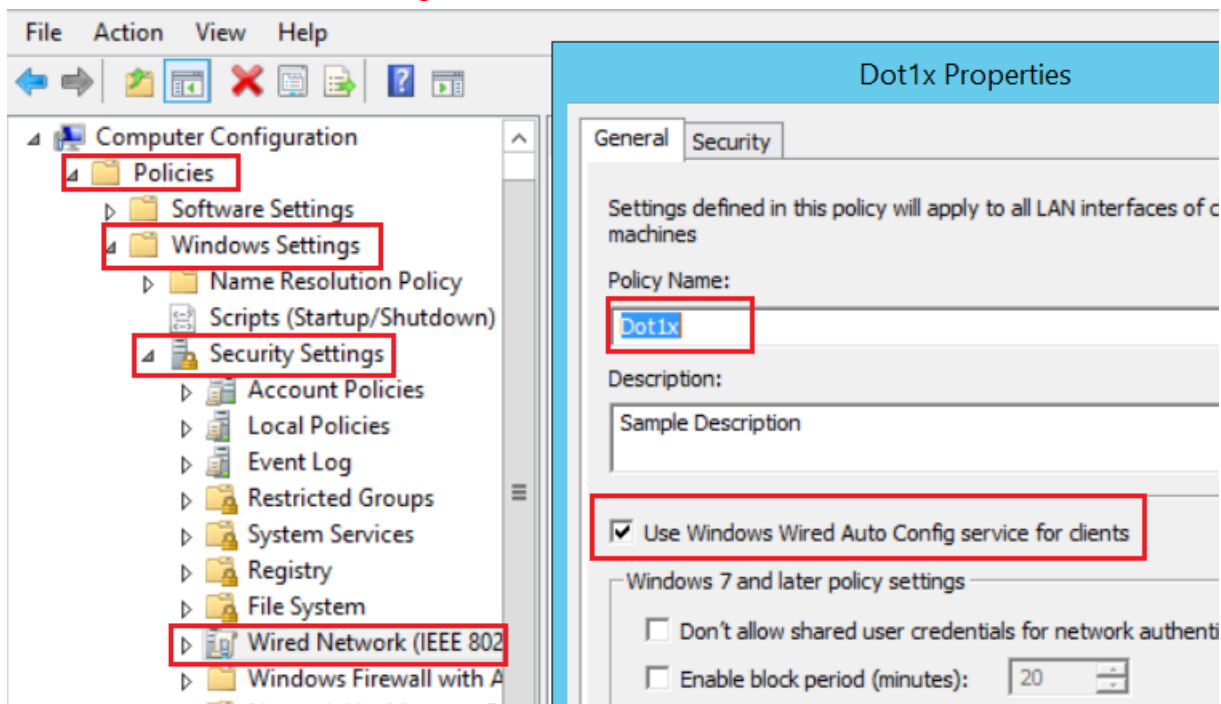


Dot1x Client Group Policy Creation:

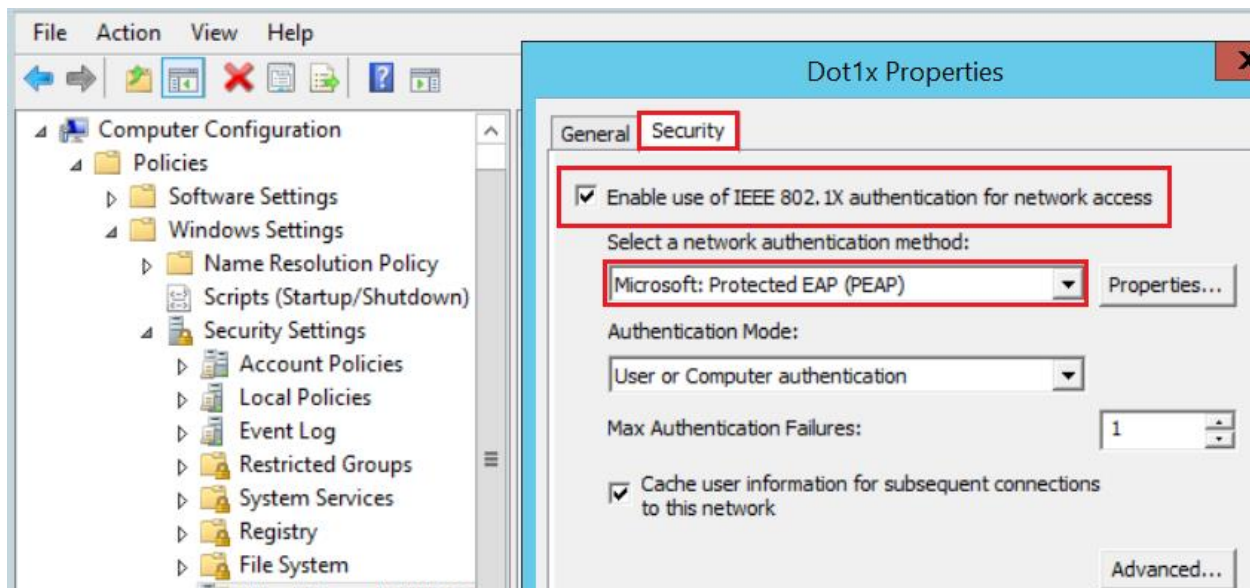
Let's create group policy to push down dot1x settings to clients. Open Group Policy Management. Highlight the domain and right-click on **Default Domain Policy** and click **Edit**.



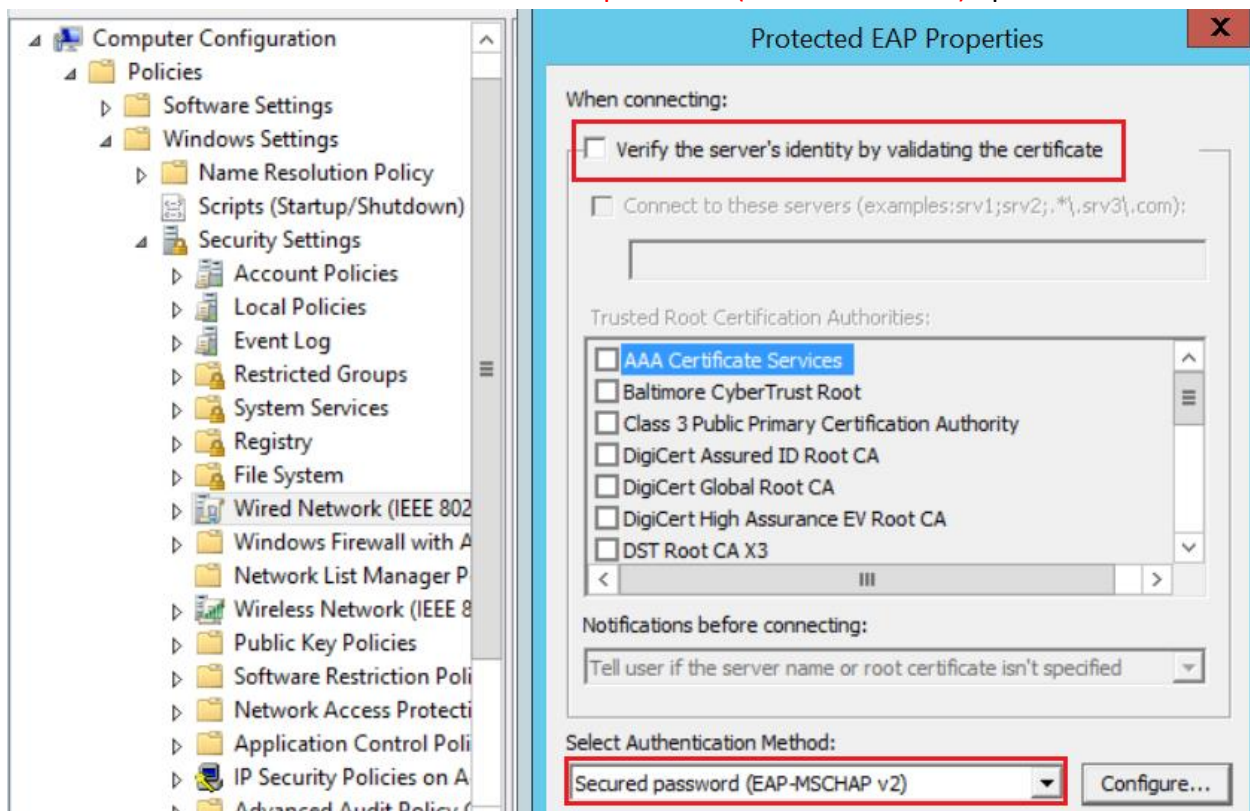
Navigate to **Computer Configuration > Windows Settings > Security Settings > Wired Network** and right-click on it. Choose **Create a New Wired Network Policy**. This will open the New Wired Network Policy Properties box. Name your policy whatever you'd like it to be and make sure the **Use Windows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



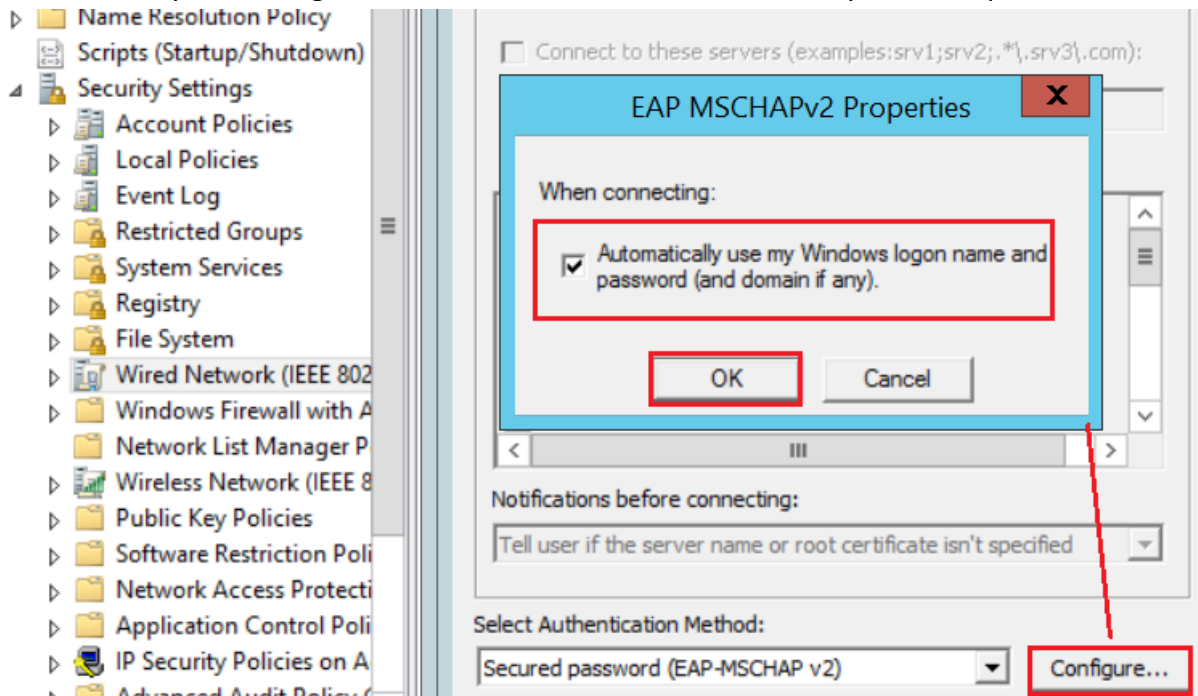
On the **Security** tab, ensure that the **Enable use of IEEE 802.1X authentication for network access** box is checked and from the Select a network authentication method drop-down, choose Microsoft: **Protected EAP (PEAP)**. Click on the Properties button to the right of it.



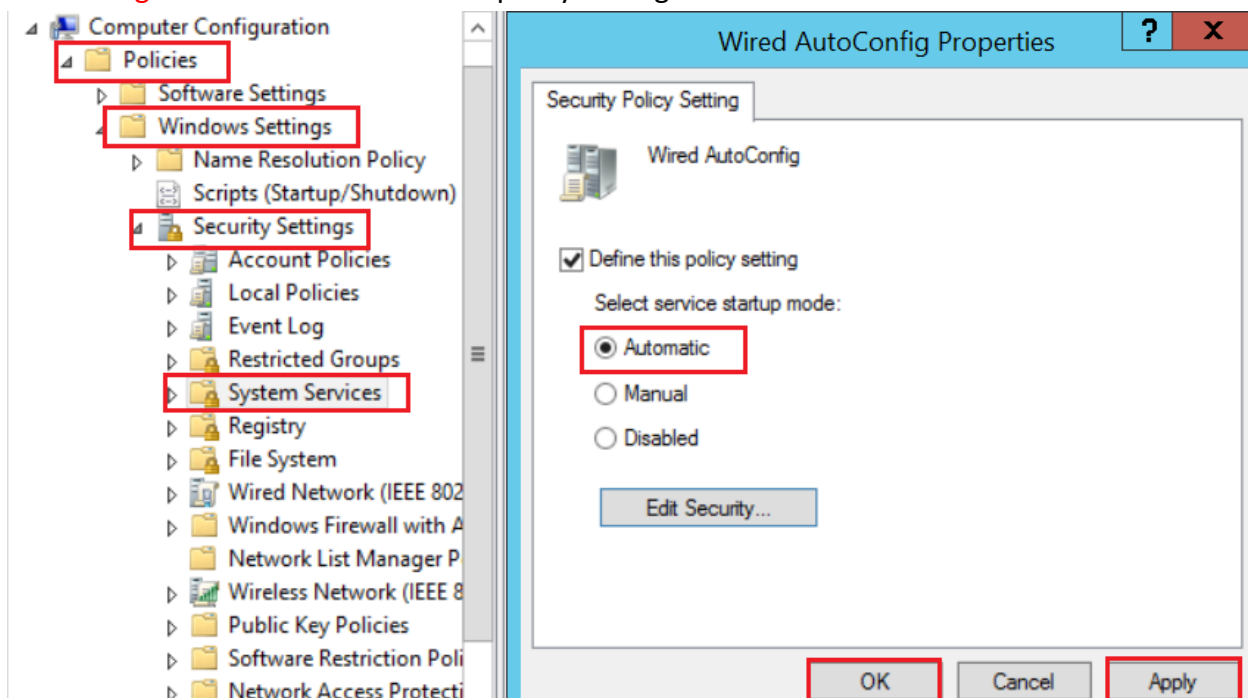
In the **Properties** box that pops up, uncheck the boxes next to **Verify the server's identity by validating the certificate**. Under the Select Authentication Method drop-down, this is where we will select our inner method. Choose **Secured password (EAP-MSCHAP v2)** options.



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**.



Configuring Downloadable ACL:

Navigate to **Policy > Policy Elements > Results > Authorization > Downloadable ACLs** click **Add**

The screenshot shows the Cisco ISE web interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', and 'Administration'. 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 expanded to show 'Authentication', 'Authorization', 'Profiling', and 'Posture'. The 'Authorization' menu is expanded to show 'Authorization Profiles' and 'Downloadable ACLs'. The 'Downloadable ACLs' page is displayed, showing a table of existing ACLs. A red box highlights the 'Add' button in the top left corner of the table.

Name	Description
DACL_Test	
DENY_ALL_IPV4_TRAFFIC	Deny all ipv4 traffic
DENY_ALL_IPV6_TRAFFIC	Deny all ipv6 traffic
PERMIT_ALL_IPV4_TRAFFIC	Allow all ipv4 Traffic
PERMIT_ALL_IPV6_TRAFFIC	Allow all ipv6 Traffic

Create a DACL with Name **DACL_Test**. Create the DACL deny ICMP to ISE 192.168.100.210 and permit ip any any Click **Save**

The screenshot shows the 'Downloadable ACL List > DACL_Test' page. The 'Downloadable ACL' section is visible. The 'Name' field is set to 'DACL_Test'. The 'Description' field is empty. The 'IP version' is set to 'IPv4'. The 'DACL Content' field contains the following text: 'deny icmp any host 192.168.100.210' and 'permit ip any any'. A red box highlights the 'Check DACL Syntax' button. Below the button are 'Save' and 'Reset' buttons.

Downloadable ACL List > **DACL_Test**

Downloadable ACL

* Name: **DACL_Test**

Description:

IP version: ☒ IPv4 ☐ IPv6 ☐ Agnostic

* DACL Content: deny icmp any host 192.168.100.210
permit ip any any

Check DACL Syntax

Save **Reset**

Now add this DACL to a new Authorization Profile. **Policy> Policy Elements> Results> Authorization> Authorization Profiles** Click **Add**

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 'Policy' menu is expanded, showing 'Policy Sets', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. The 'Policy Elements' menu is further expanded, showing 'Dictionaries', 'Conditions', and 'Results'. The 'Results' menu is expanded, showing 'Authentication', 'Authorization', and 'Downloadable ACLs'. The 'Authorization' menu is expanded, showing 'Authorization Profiles' and 'Downloadable ACLs'. The 'Authorization Profiles' menu is expanded, showing 'Add', 'Duplicate', and 'Delete' buttons. The 'Add' button is highlighted with a red box. Below the navigation bar, the 'Standard Authorization Profiles' section is visible, with a link to 'Administration > System > Backup & Restore > Policy Export Page'. A table with columns 'Name' and 'Profile' is shown, with a row for 'Blackhole_Wireless_Access'.

Name Authorization profile in this case **Deny_ISE_AuthProfile**. Select DACL Name from the drop-down list select the DACL previously configured called **DACL_Test**. Click **Save**.

The screenshot shows the 'Authorization Profiles > Deny_ISE_AuthProfile' configuration page. The 'Authorization Profile' section is visible, with fields for 'Name' (Deny_ISE_AuthProfile), 'Description', 'Access Type' (ACCESS_ACCEPT), 'Network Device Profile' (Cisco), 'Service Template', 'Track Movement', and 'Passive Identity Tracking'. The 'Common Tasks' section is visible, with a 'DACL Name' dropdown menu set to 'DACL_Test'. A red arrow points to the 'DACL_Test' dropdown.

Go to **Policy>Policy Sets** navigate to **Authorization Policy** section. Under Profiles of Dot1x rules from drop-down list choose previously configured Authorization Profiles **Deny_ISE_AuthProfile**.

The screenshot shows the 'Policy Sets' section of the Cisco Identity Services Engine (ISE) interface. The 'Authorization Policy' section is visible, with a table showing 'Dot1x-Authorization_Computer' and 'Dot1x-Authorization_Users' rules. The 'Profiles' column for these rules shows 'Deny_ISE_AuthProfile' selected. A red box highlights the 'Deny_ISE_AuthProfile' dropdown menu. A blue arrow points to the dropdown menu.

Dynamic VLAN Configuration:

Navigate to **Policy > Policy Elements > Results > Authorization > Authorization profiles** and click on already existing profile which created previously for DACL.

Standard Authorization Profiles
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

☐ Edit ☐ Add ☐ Duplicate ☐ Delete

<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco
<input type="checkbox"/>	Cisco_IP_Phones	Cisco
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco
<input type="checkbox"/>	Cisco_WebAuth	Cisco
<input checked="" type="checkbox"/>	Deny_ISE_AuthProfile	Cisco

Under the **Common Tasks** section, tick **VLAN**. Enter the VLAN ID in this case VLAN **40**.

Authorization Profile

* Name: Deny_ISE_AuthProfile

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: ☐

Track Movement: ☐

Passive Identity Tracking: ☐

Common Tasks

☒ VLAN

Tag ID: 1

Edit Tag ID/Name: 40

When done Click **Save** to apply the changes.

Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:40
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
DACL = DACL_Test

Save Reset

Go to **Policy>Policy Sets** navigate to **Authorization Policy** section. Under Profiles of Dot1x rules from drop-down list choose previously configured Authorization Profiles **Deny_ISE_AuthProfile**.

The screenshot shows the Cisco ISE Policy Sets configuration page. The 'Policy' tab is selected. Under 'Authorization Policy (14)', two rules are listed: 'Dot1x-Authorization_Computer' and 'Dot1x-Authorization_Users'. Both rules have a status of 'On' and are associated with the 'Deny_ISE_AuthProfile' profile. A blue arrow points to the 'Profiles' column header.

Status	Rule Name	Conditions	Profiles
On	Dot1x-Authorization_Computer	ad.test.local:ExternalGroups EQUALS test.local/Users/Domain Computers	Deny_ISE_AuthProfile
On	Dot1x-Authorization_Users	ad.test.local:ExternalGroups EQUALS test.local/Users/Domain Users	Deny_ISE_AuthProfile

The Profile has already applied in Downloadable Access Control List (DACL) Lab.

Verification:

Result

Class	CACS:C0A864FE0000000D002DC0AA:ise1/416482617/1
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) 40
EAP-Key-Name	19:60:fc:1d:bb:7a:74:43:90:82:79:ad:da:87:eb:22:f0:a2:3d:15:0c:4c:f8:83:3a:f2:de:91:75:ed:6d:2c:79:a8:90:4a:d2:87:87:4a:f9:7e:ed:c1:81:3a:16:9c:64:03:8f:14:50:94:06:4d:e5:9f:4f:1c:45:fd:bf:0d:b2
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-DACL_Test-60fb1f5a
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Base license consumed

```

SW2#show authentication session int e0/1 detail
    Interface: Ethernet0/1
    MAC Address: 5001.000a.0000
    IPv6 Address: Unknown
    IPv4 Address: 192.168.40.11 ←
    User-Name: host/PC1-WIN10.test.local
    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: 299s
    Session Uptime: 3309s
    Common Session ID: C0A864FE0000000D002DC0AA
    Acct Session ID: 0x00000002
    Handle: 0x32000001
    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:
    Vlan Group: Vlan: 40 ←
    ACS ACL: xACSACLx-IP-DACL_Test-60fb1f5a

Method status list:
    Method      State
    dot1x       Authc Success

```

```

SW2#show vlan br

```

VLAN	Name	Status	Ports
1	default	active	Et1/0, Et1/1, Et1/2, Et1/3
10	EMP	active	
20	CONT	active	Et0/2
30	GUST	active	
40	LMT	active	Et0/1 ←
100	MGMT	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

```

SW2# show authentication sessions interface ethernet 0/1
SW2# show authentication sessions interface ethernet 0/1 detail
SW2# show ip interface ethernet0/1
SW2# show vlan br
SW2#debug radius

```