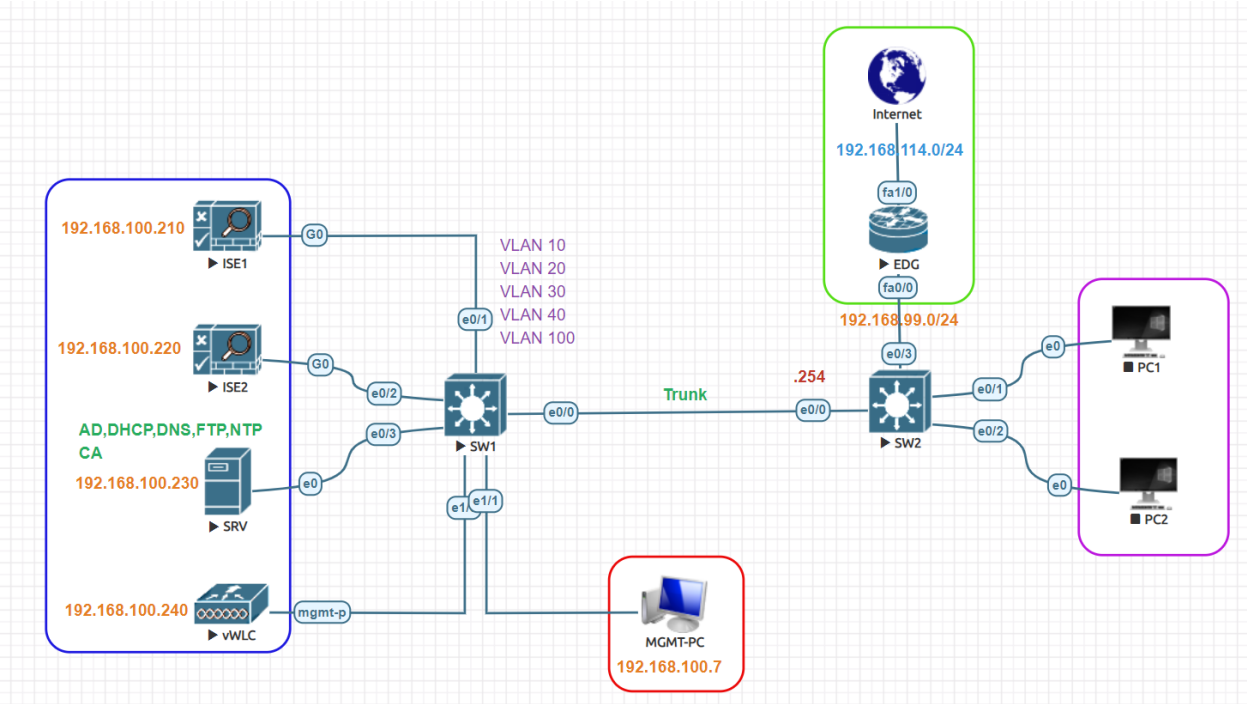
# Dynamic VLAN Lab:

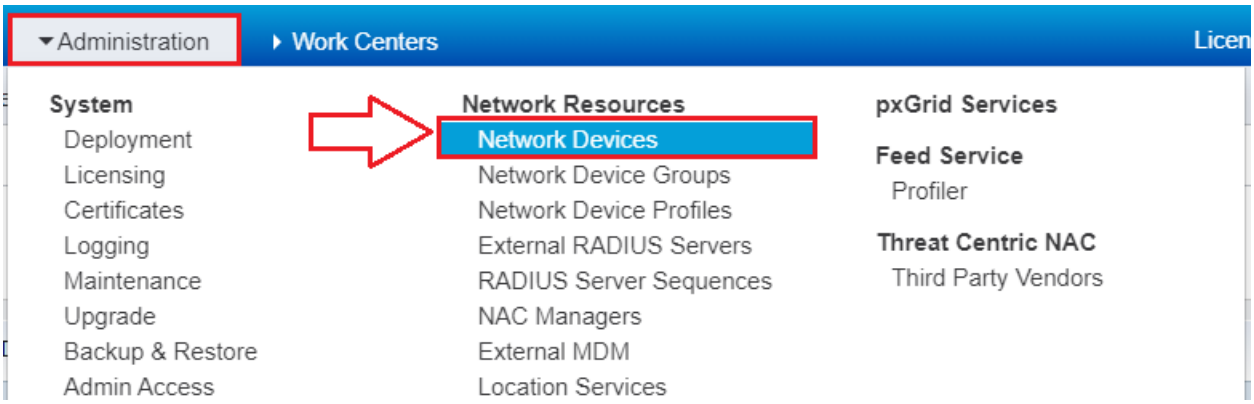



| | |
|---|---|
| Cisco ISE Primary IP Address | 192.168.100.210 |
| Cisco ISE Secondary IP Address | 192.168.100.220 |
| AD, DNS and CA Server IP Address | 192.168.100.230 |
| Domain Name: | test.local |
| Test User/Group | E1/Employee |
| Test VLAN | VLAN 20 |
| VLAN Subnet | 192.168.20.0/24 |
| VLAN 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 |

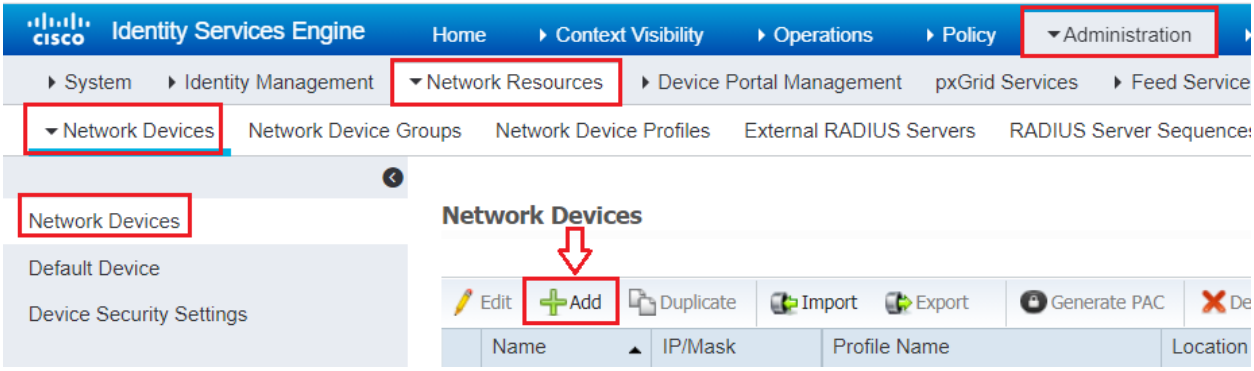
| Dot1X Configuration |
| --- |
| SW2(config)#aaa new-model |
| SW2(config)#dot1x system-auth-control |
| SW2(config)#radius server ISE1 |
| SW2(config-radius-server)# address ipv4 192.168.100.210 auth-port 1812 acct-port 1813 |
| SW2(config-radius-server)#key Test123 |
| SW2(config-radius-server)#radius 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:

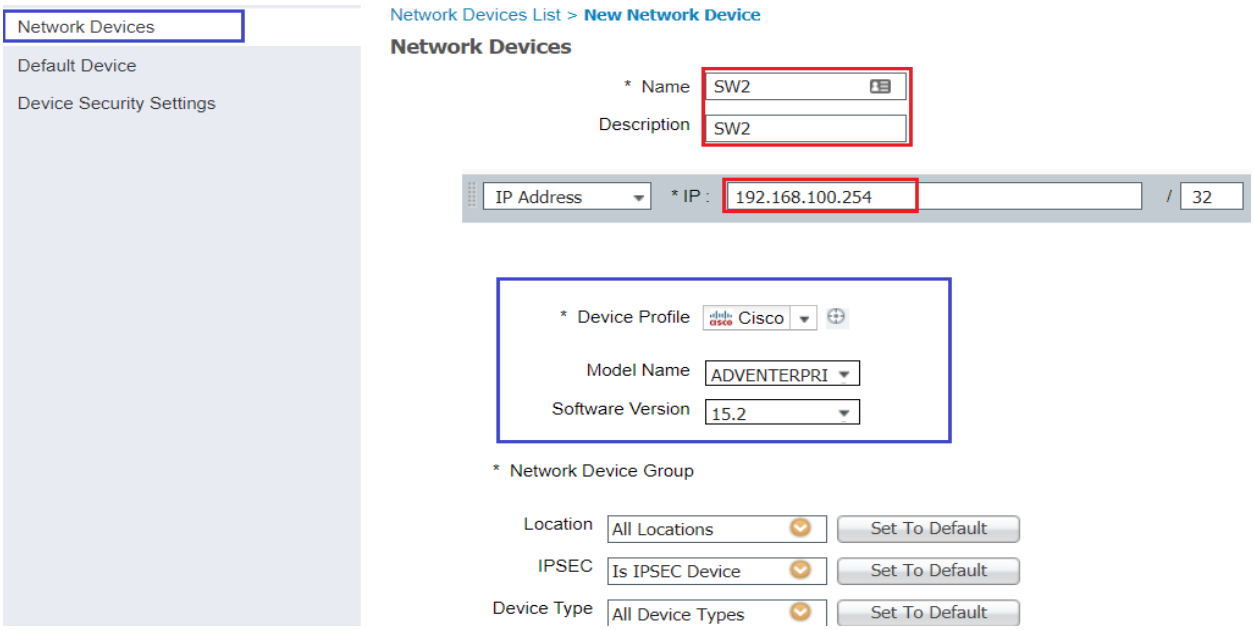
Go to Administration > Network Resources > Network Devices to add the Device (SW2).



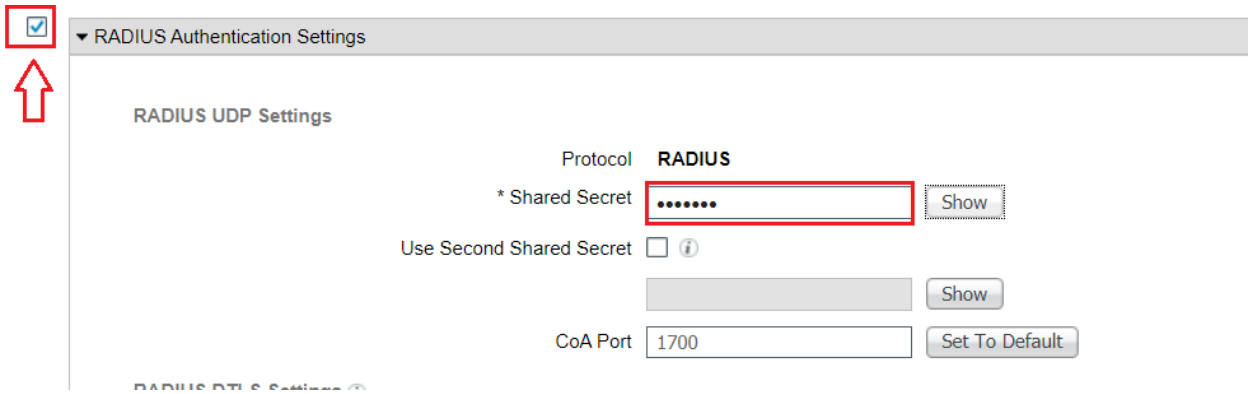

Click on Add button to add Network Device like Router and Switch.



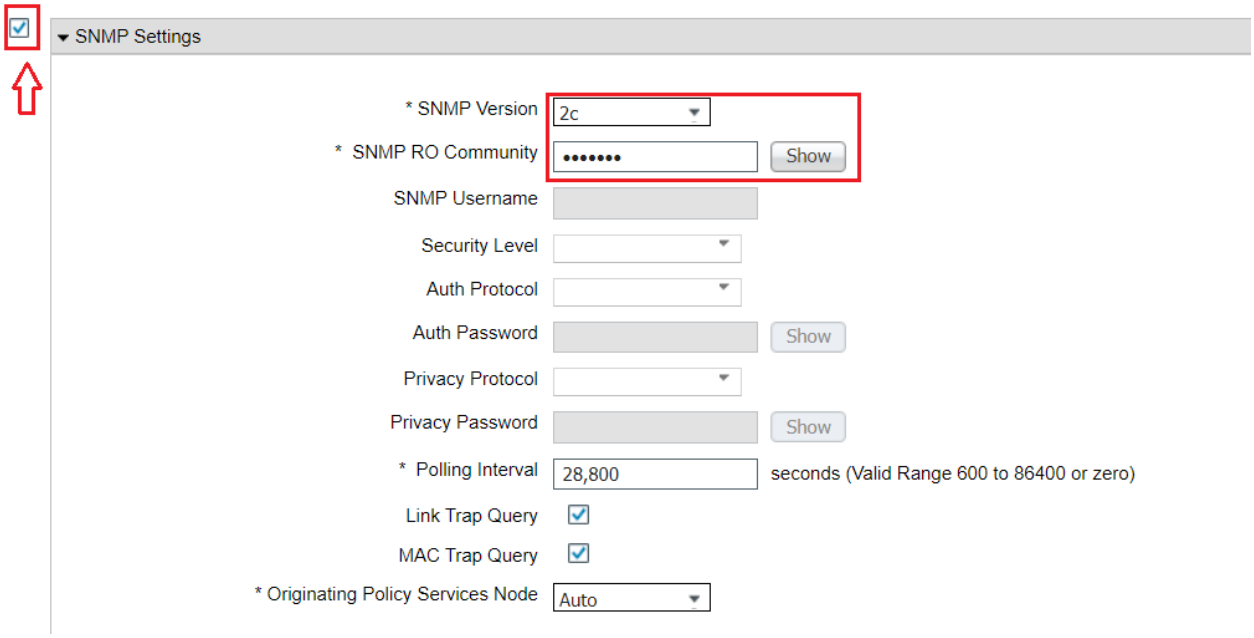

Configure **Name** of device, **IP address** configured. Scroll down to set Authentication settings.

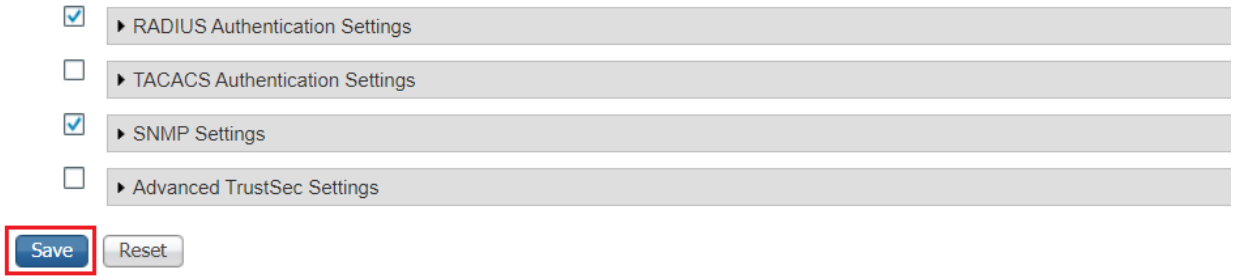


Scroll down to set Authentication settings. Set Password configured as Server key on Switch device “Test123” and save settings.



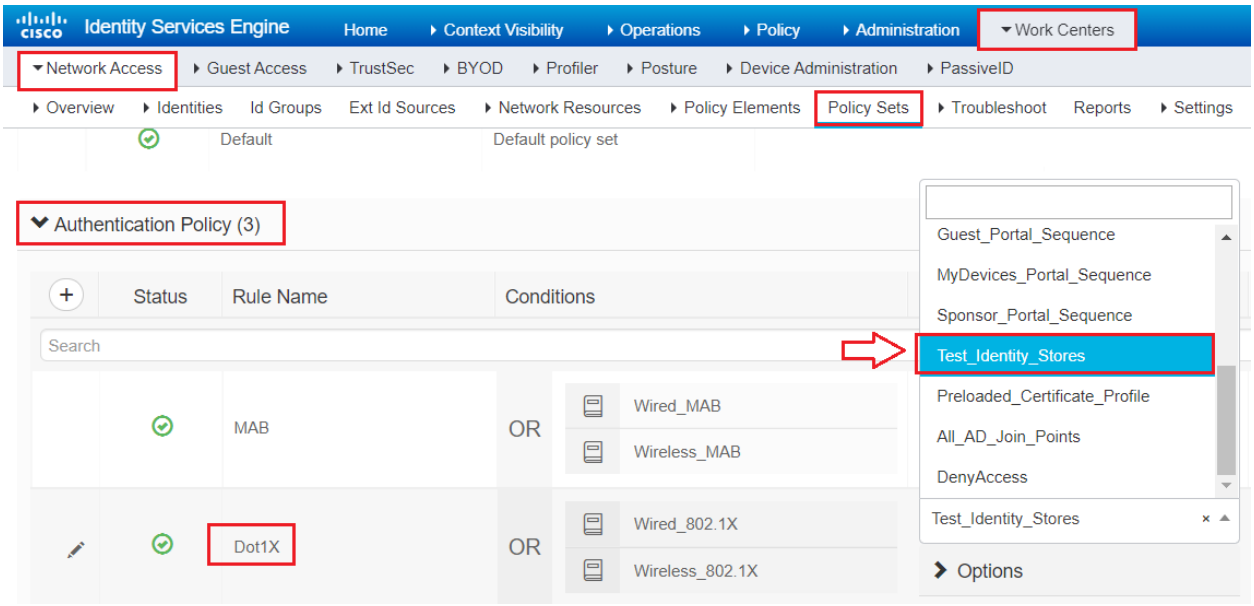

Scroll down to check SNMP Settings and set SNMP RO Community string settings, Click Submit.



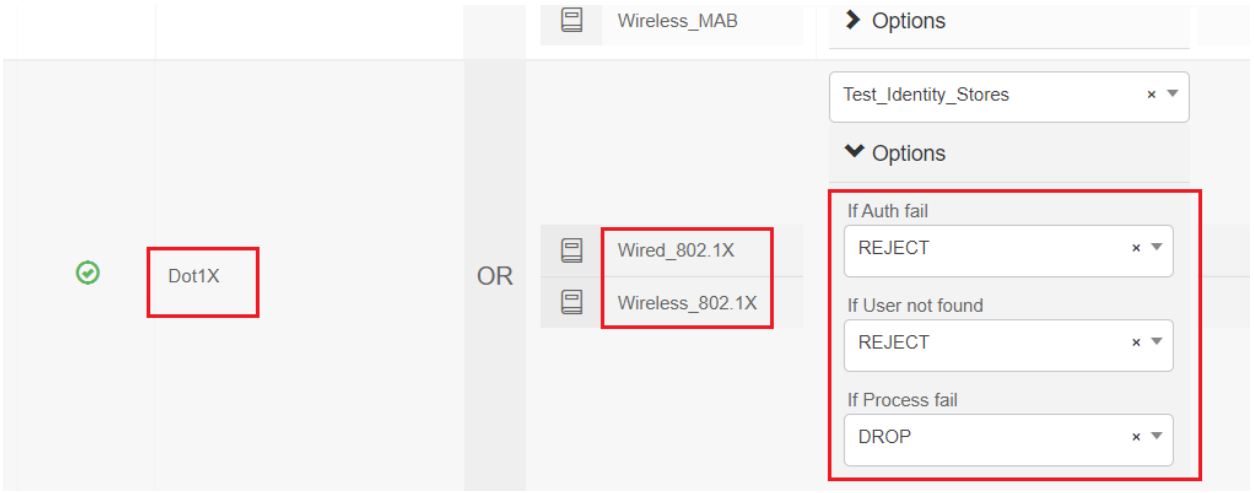



## 802.1x Authentication Polices:

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



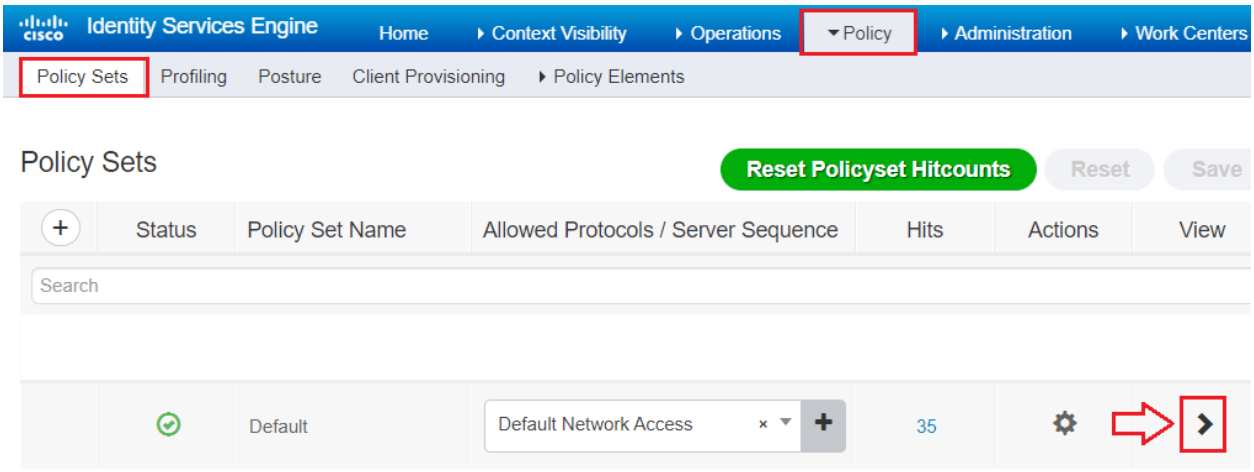

If the authentication fail the user will be Rejected, if user not found the user will be rejected, while if the process of Dot1x fail the user will be dropped.



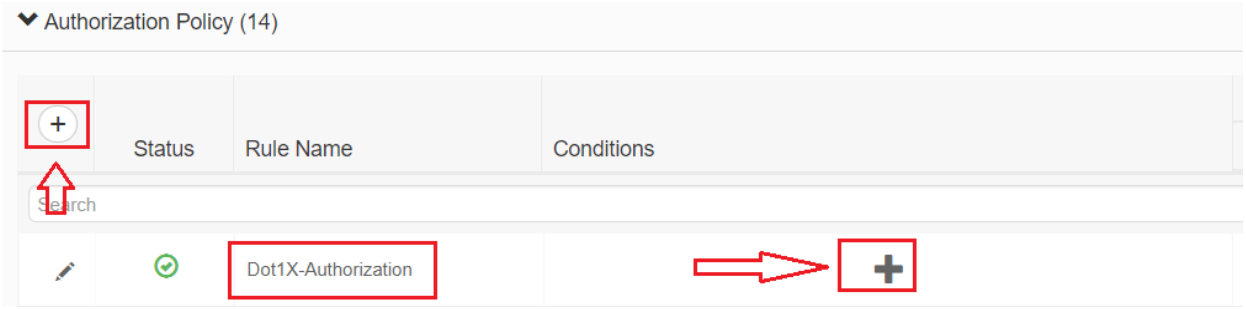

 Prepared By Ahmad Ali, Email: ahmadalimsc@gmail.com , Mobile# 0564303717

## 802.1x Authorization Polices:

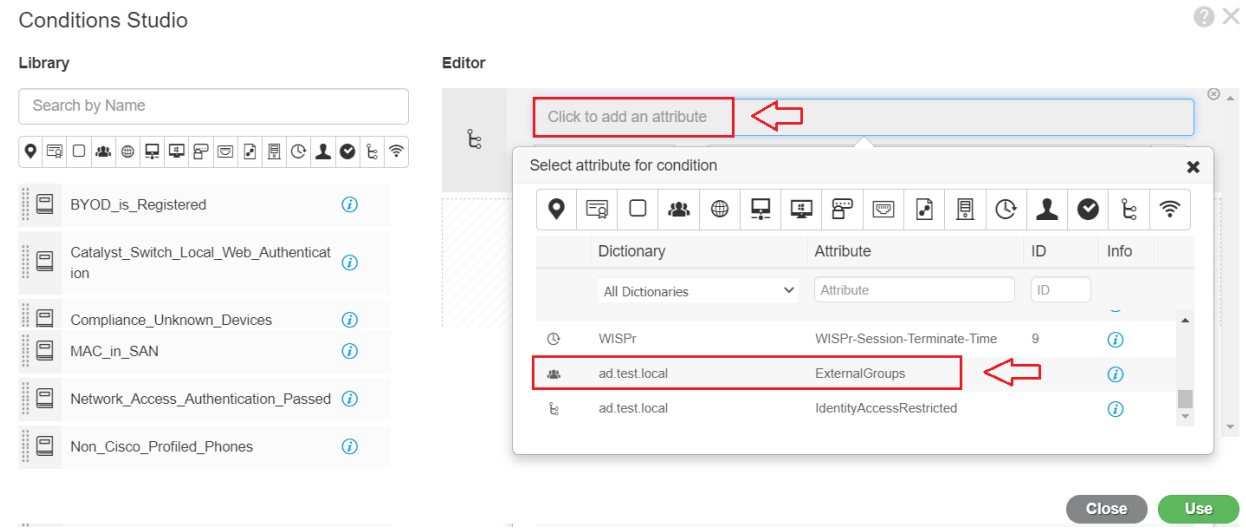
Navigate to Policy>Policy Sets > click on Arrow Icon >



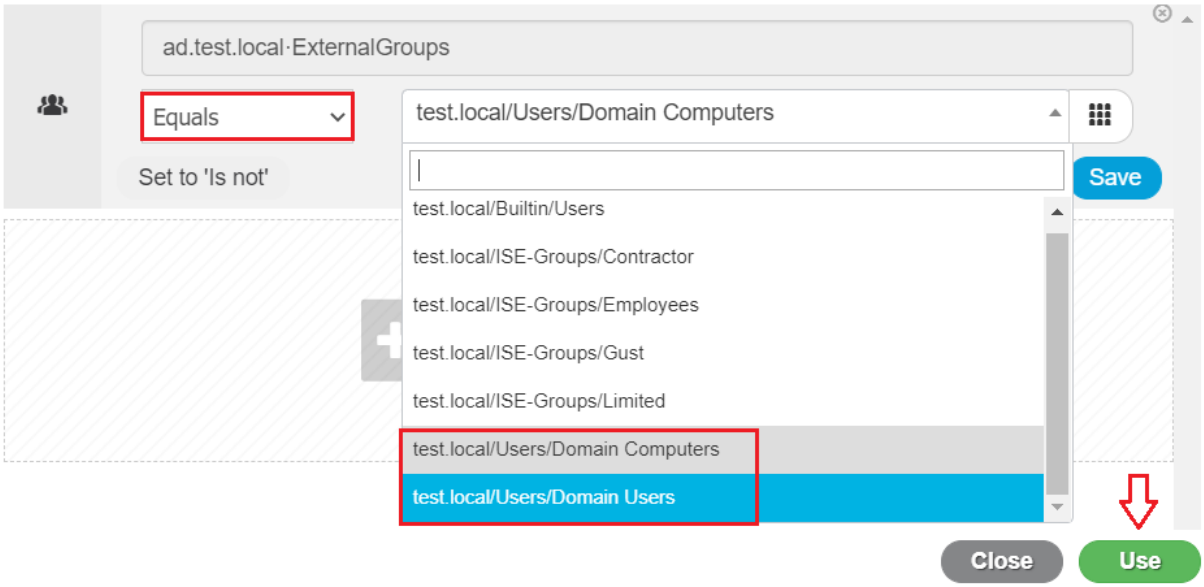

Navigate to Authorization Policy section click on round circle Plus icon to add new Authorization Policy, name the authorization policy in this case Dot1x-Authorization. In Conditions click on Plus icon to set the conditions for authorization policy.



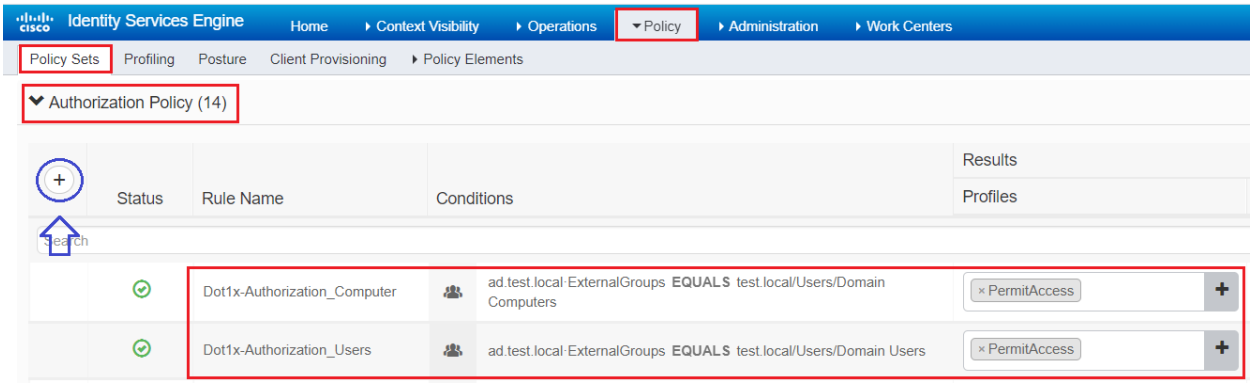

In Conditions Studio > Editor click to add an attribute choose ad.test.local



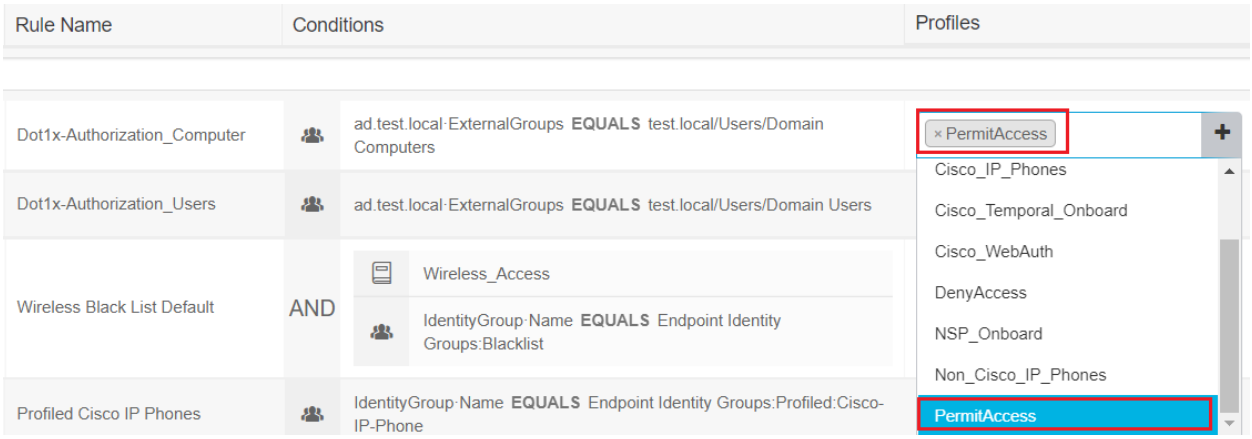
In Editor > Equals > test.local/users/Domain Computers also, create new same policy for test.local/users/Domain Users




Finally, two Authorization Polices are created for Dot1x Authorization.

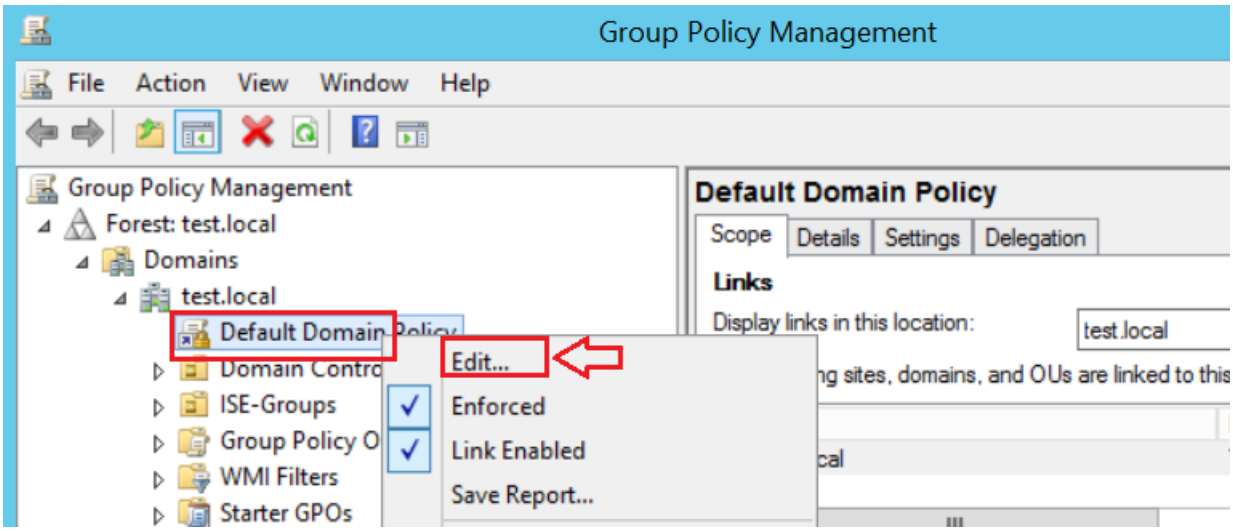



In Profile choose PermitAccess from dropdown and click Save.

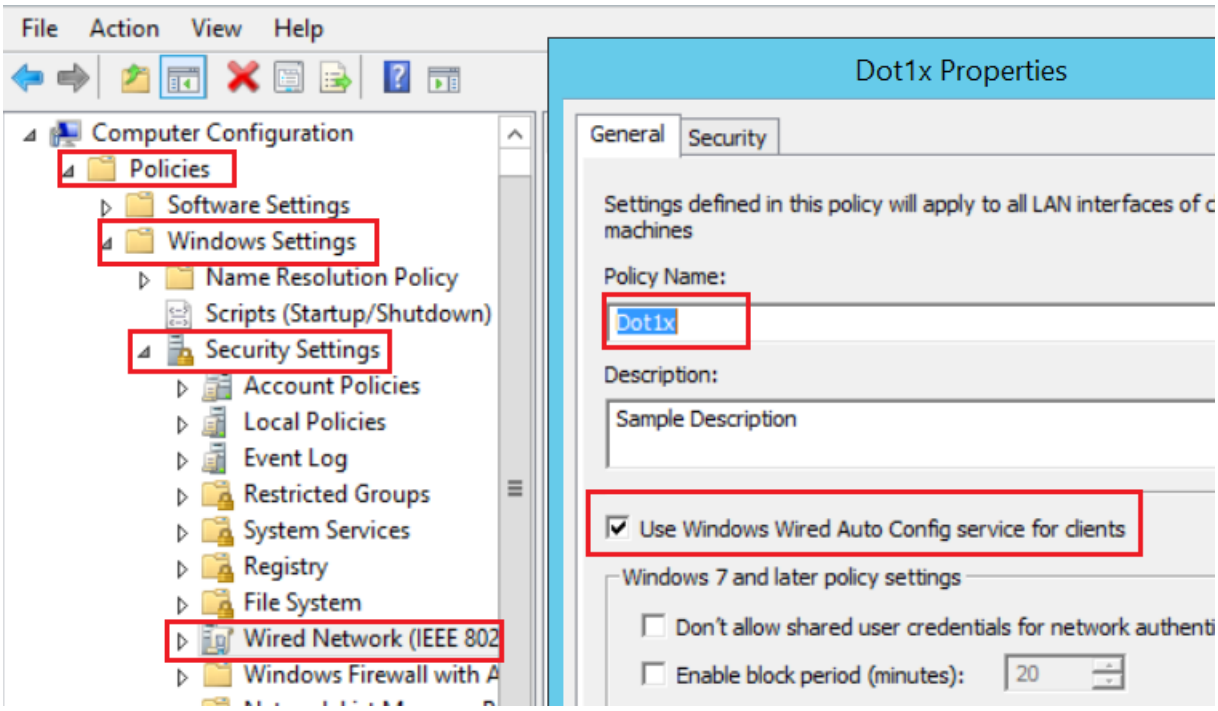


## Dot1x Client Group Policy Creation:

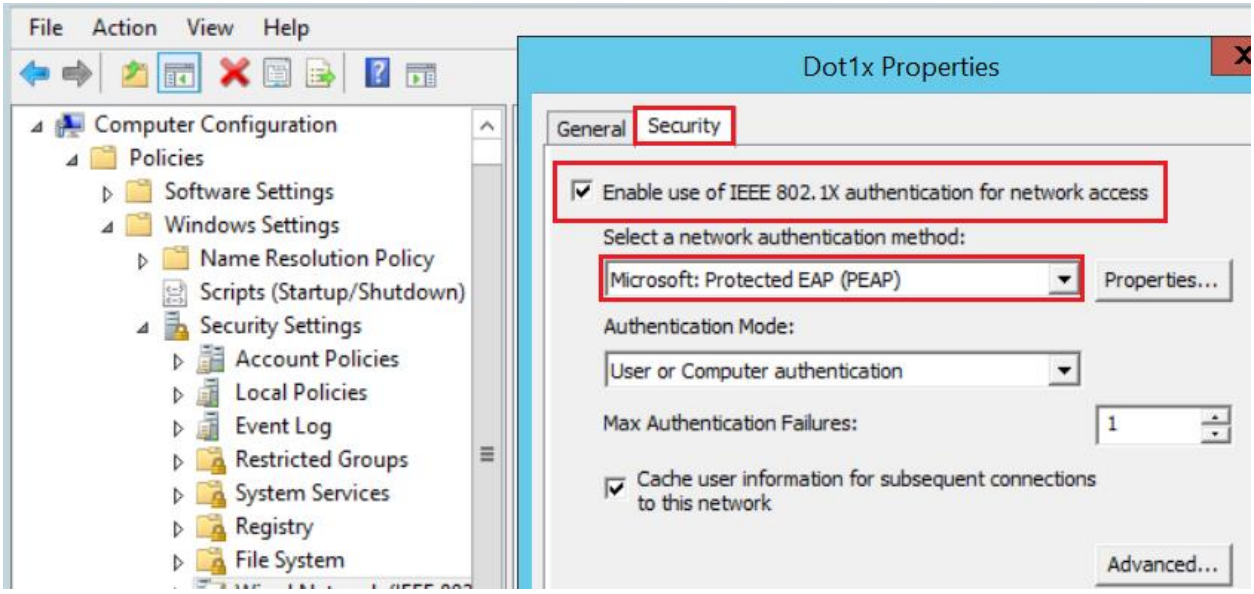
Let's create group policy to push down dot1x settings to clients. Open Group Policy Management. Highlight the domain and right-click on Default Domain Policy and click Edit.



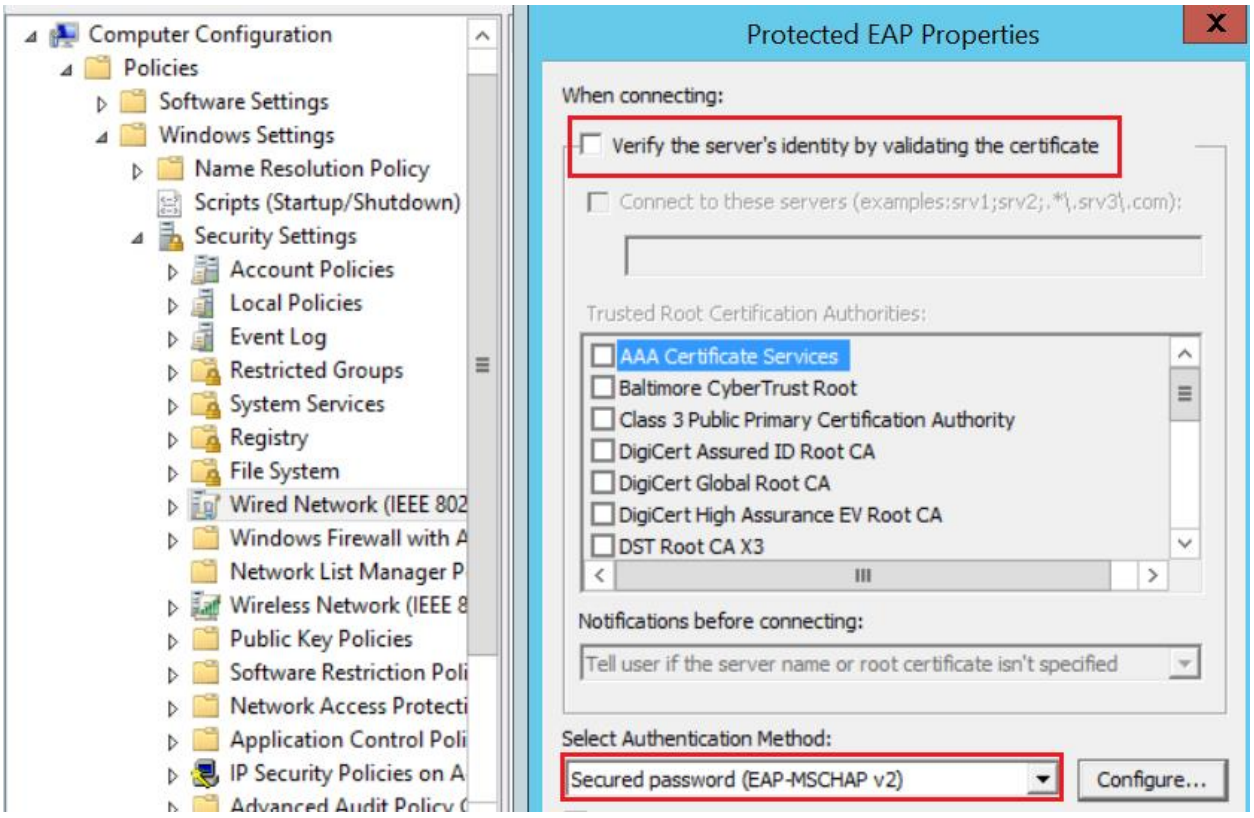

Navigate to Computer Configuration>Windows Settings>Security Settings>Wired Network and right-click on it. Choose Create a New Wired Network Policy. This will open the New Wired Network Policy Properties box. Name your policy whatever you'd like it to be and make sure the Use Windows Wired Auto Config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



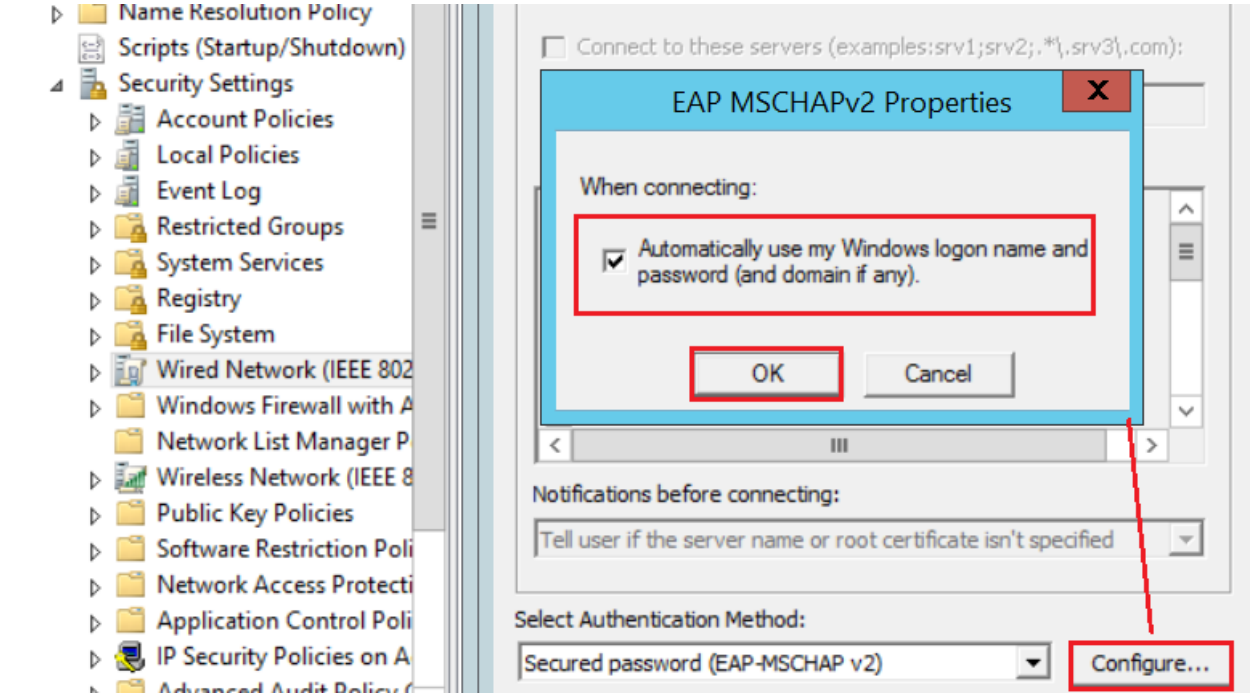
On the Security tab, ensure that the Enable use of IEEE 802.1X authentication for network access box is checked and from the Select a network authentication method drop-down, choose Microsoft: Protected EAP (PEAP). Click on the Properties button to the right of it.



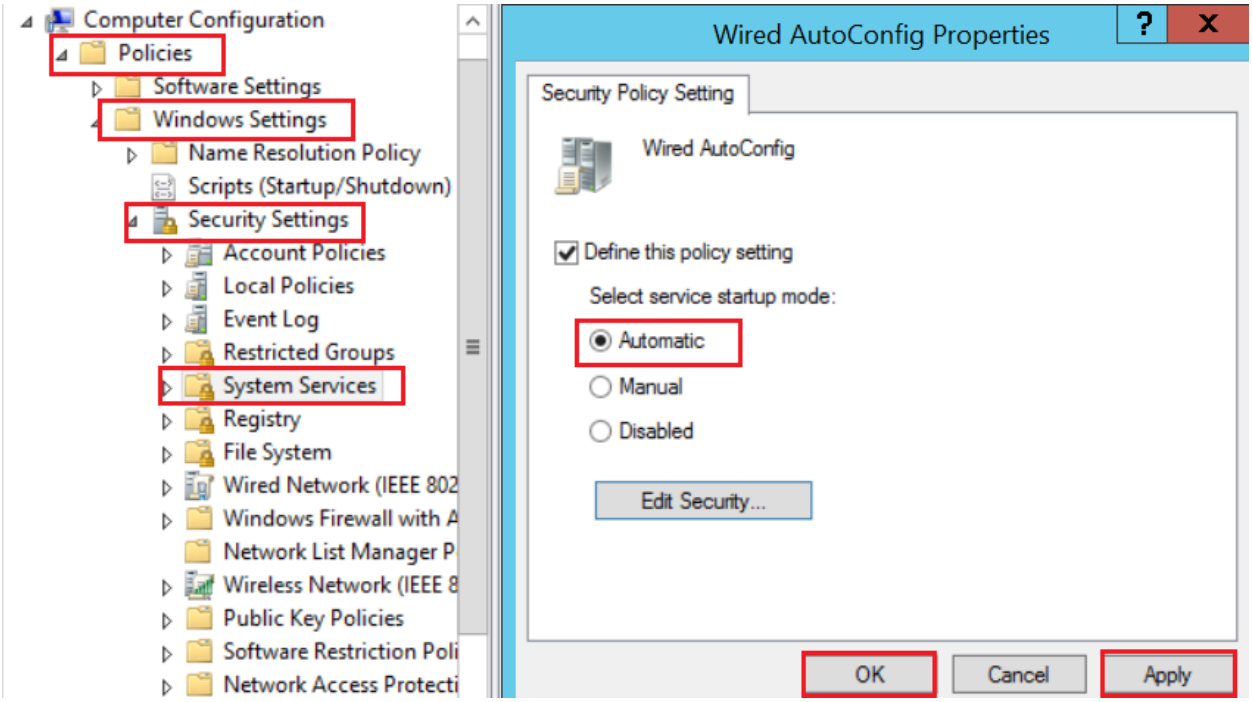

In the Properties box that pops up, uncheck the boxes next to Verify the server's identity by validating the certificate. Under the Select Authentication Method drop-down, this is where we will select our inner method. Choose Secured password (EAP-MSCHAP v2) options.



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.

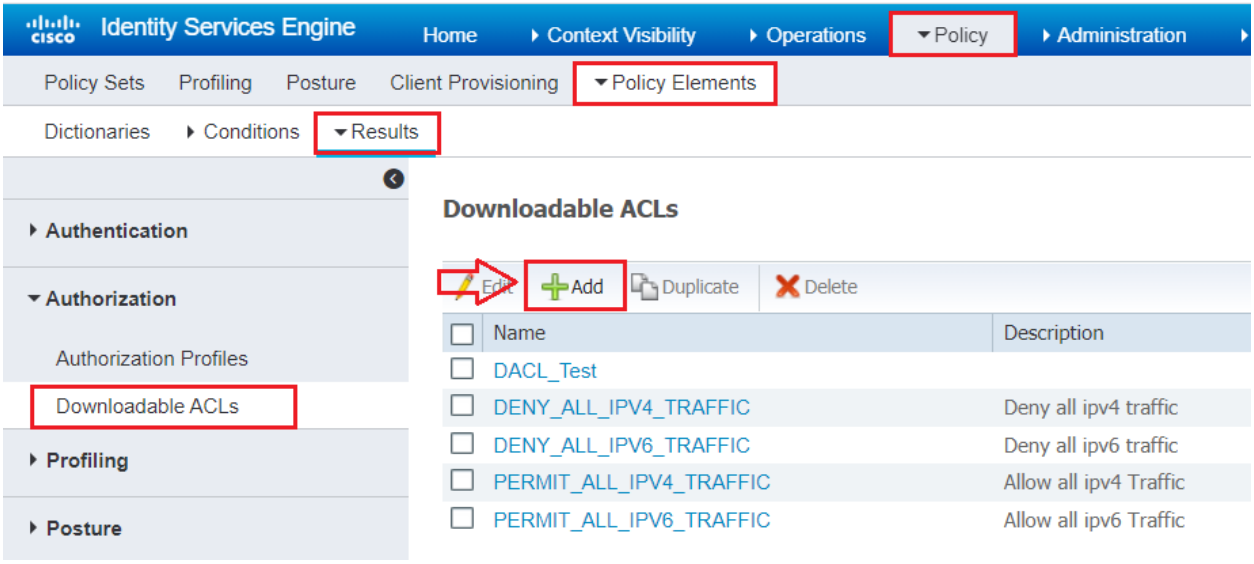



Wired Autoconfig service is not enabled by default on Windows machines. In order to get the dot1x wired settings to work, this should be enabled so let's create a group policy. Navigate to Computer Configuration>Policies>Windows Settings>Security Settings>System Settings>Wired Autoconfig. Check box for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

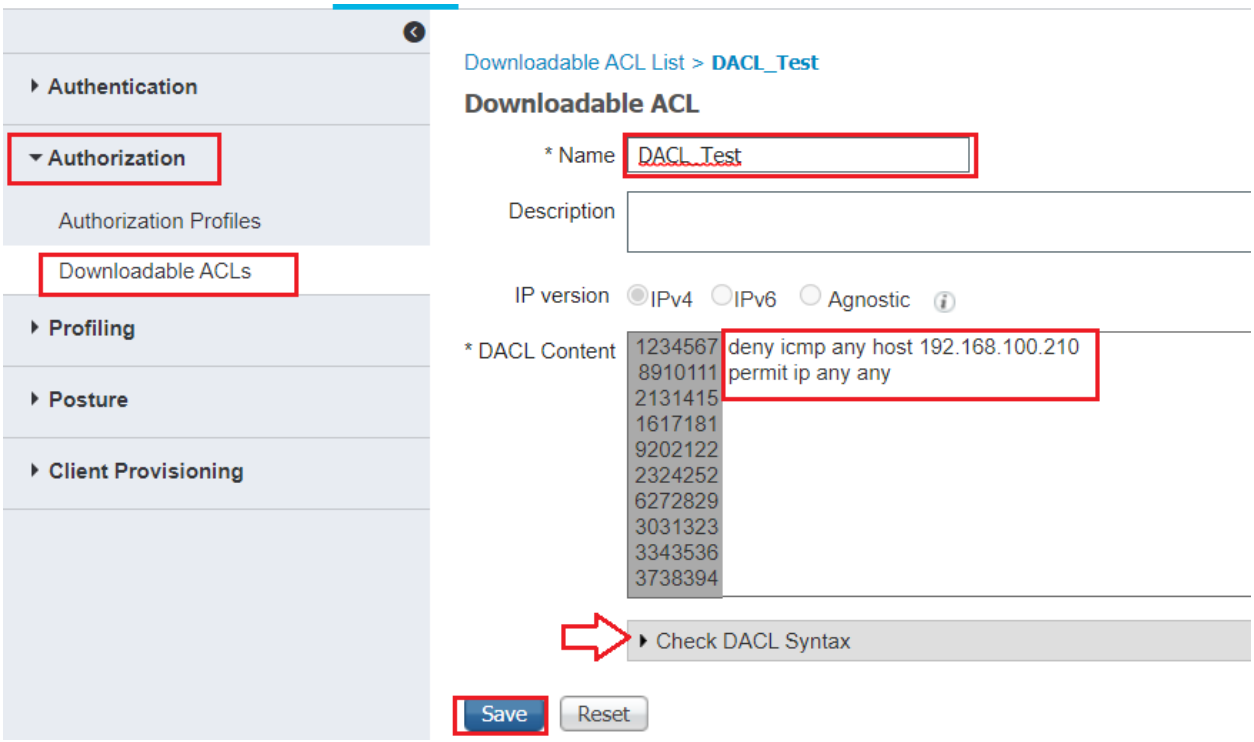


## Configuring Downloadable ACL:

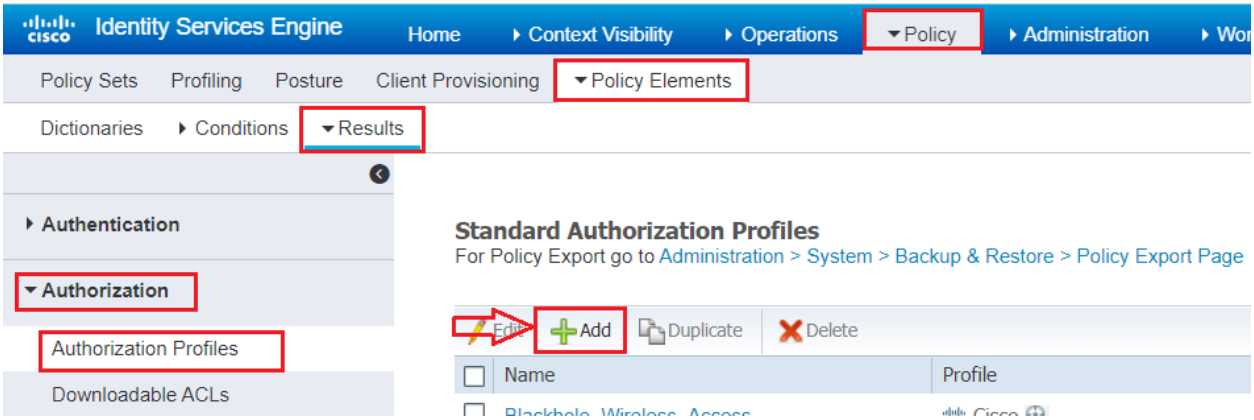
Navigate to Policy> Policy Elements> Results> Authorization> Downloadable ACLs click Add



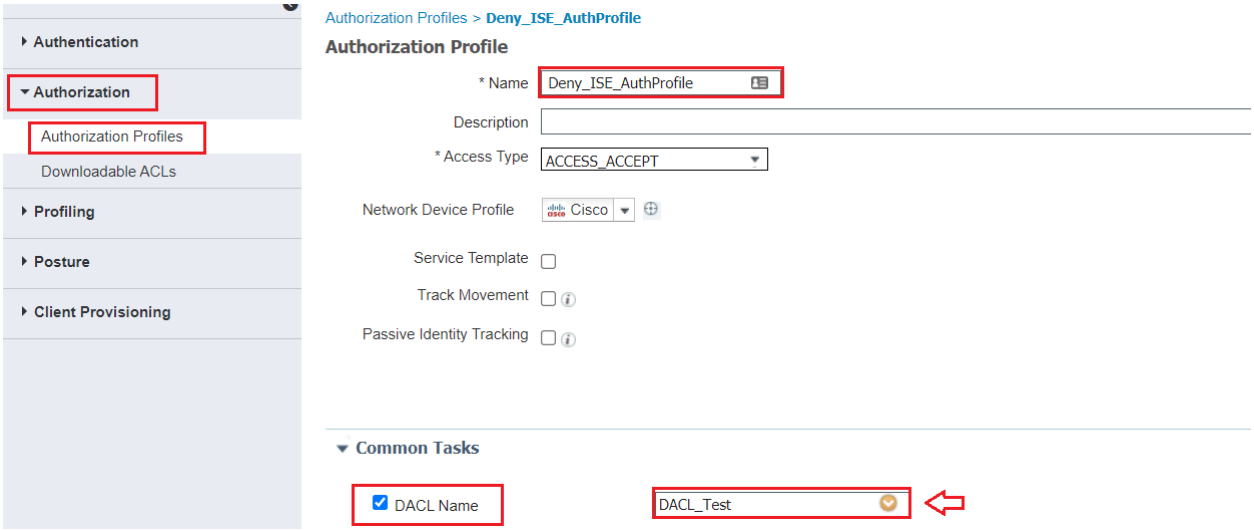

Create a DACL with Name DACL_Test. Create the DACL deny ICMP to ISE 192.168.100.210 and permit ip any any Click Save



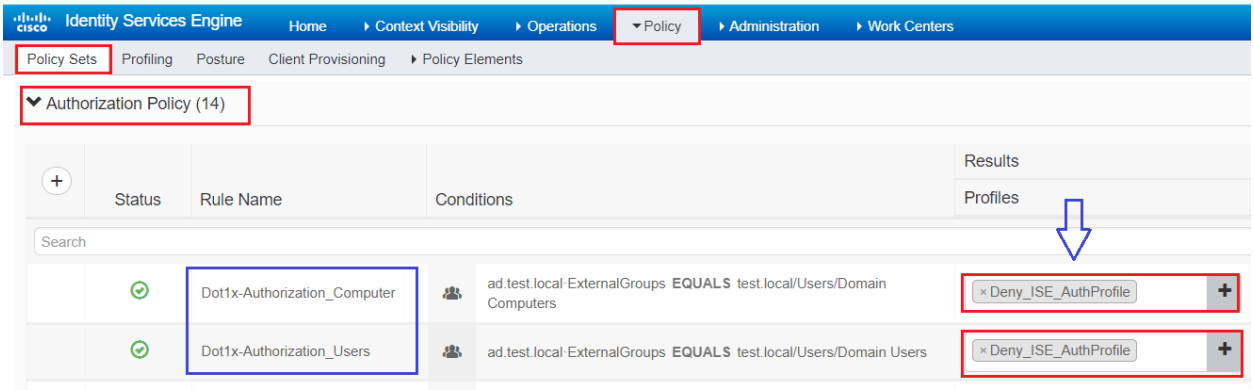
Now add this DACL to a new Authorization Profile. Policy> Policy Elements> Results> Authorization> Authorization Profiles Click Add




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.



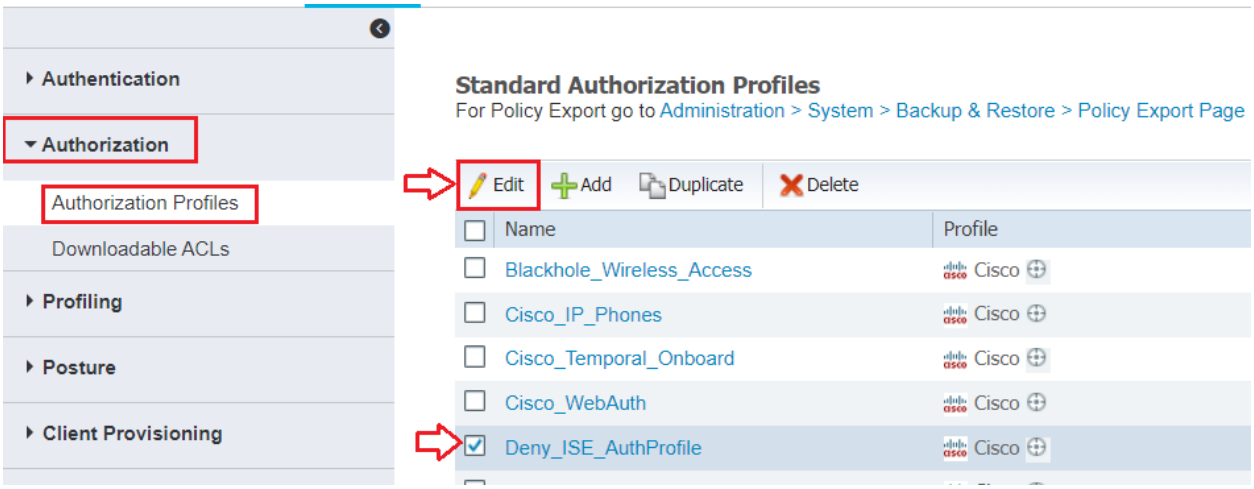

Go to Policy>Policy Sets navigate to Authorization Policy section. Under Profiles of Dot1x rules from drop-down list choose previously configured Authorization Profiles Deny_ISE_AuthProfile.



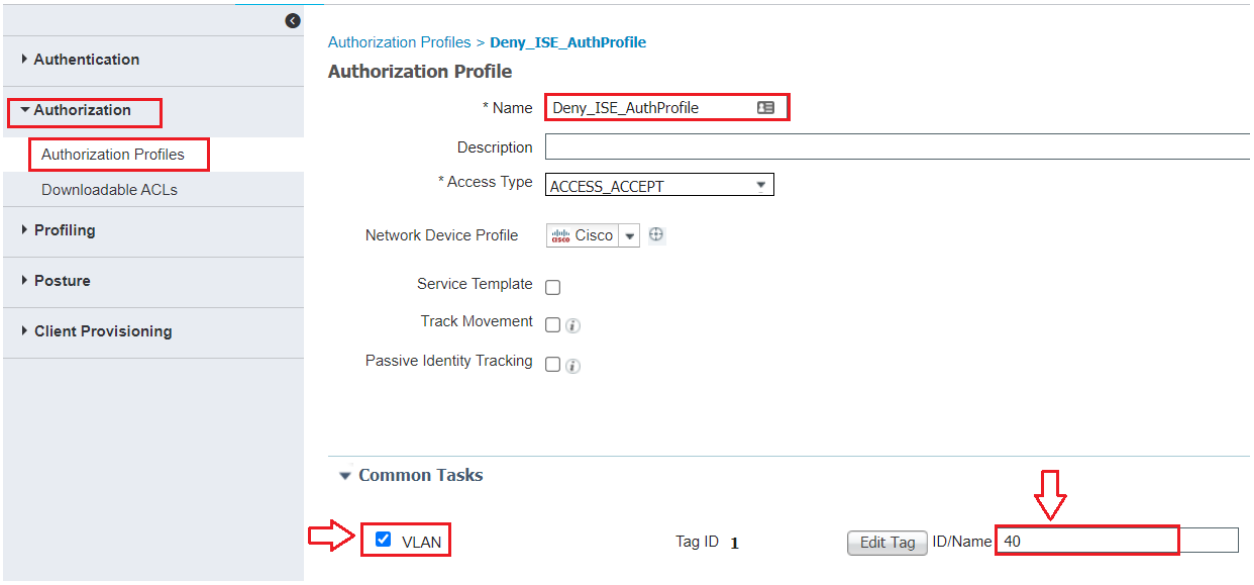

 Prepared By Ahmad Ali, Email: ahmadalimsc@gmail.com , Mobile# 0564303717

## Dynamic VLAN Configuration:

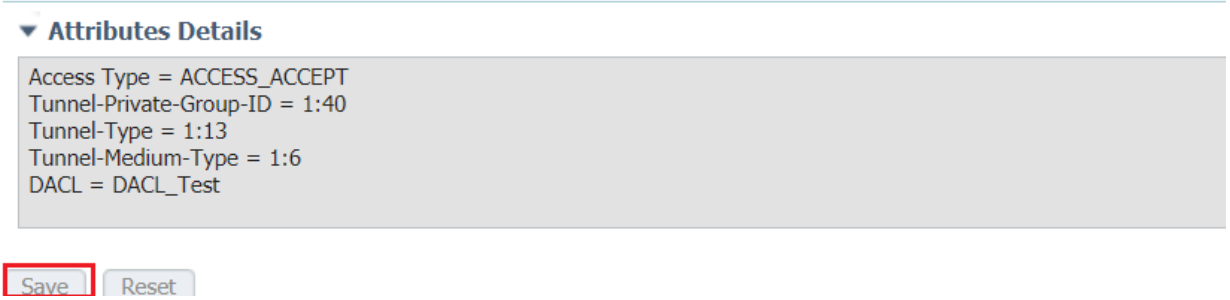
Navigate to Policy > Policy Elements > Results > Authorization > Authorization profiles and click on already existing profile which created previously for DACL.



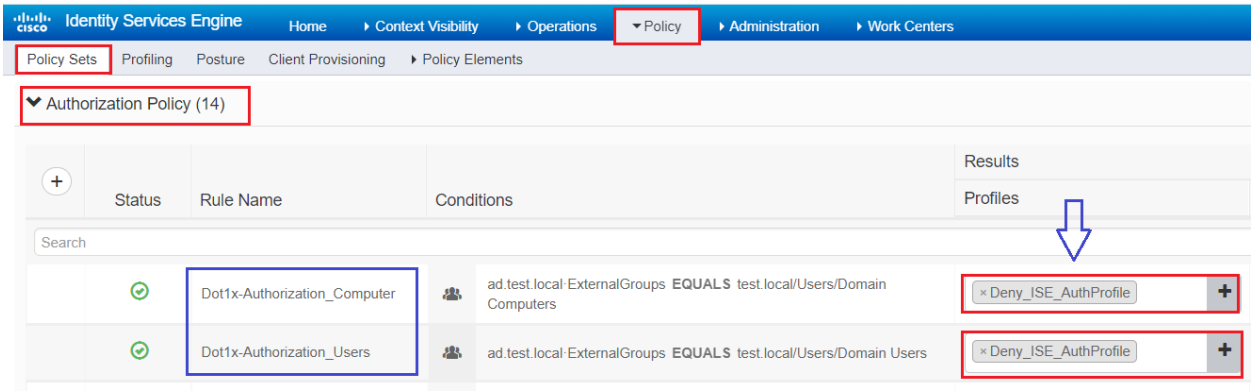

Under the Common Tasks section, tick VLAN. Enter the VLAN ID in this case VLAN 40.




When done Click Save to apply the changes.



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

## Verification:

```
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