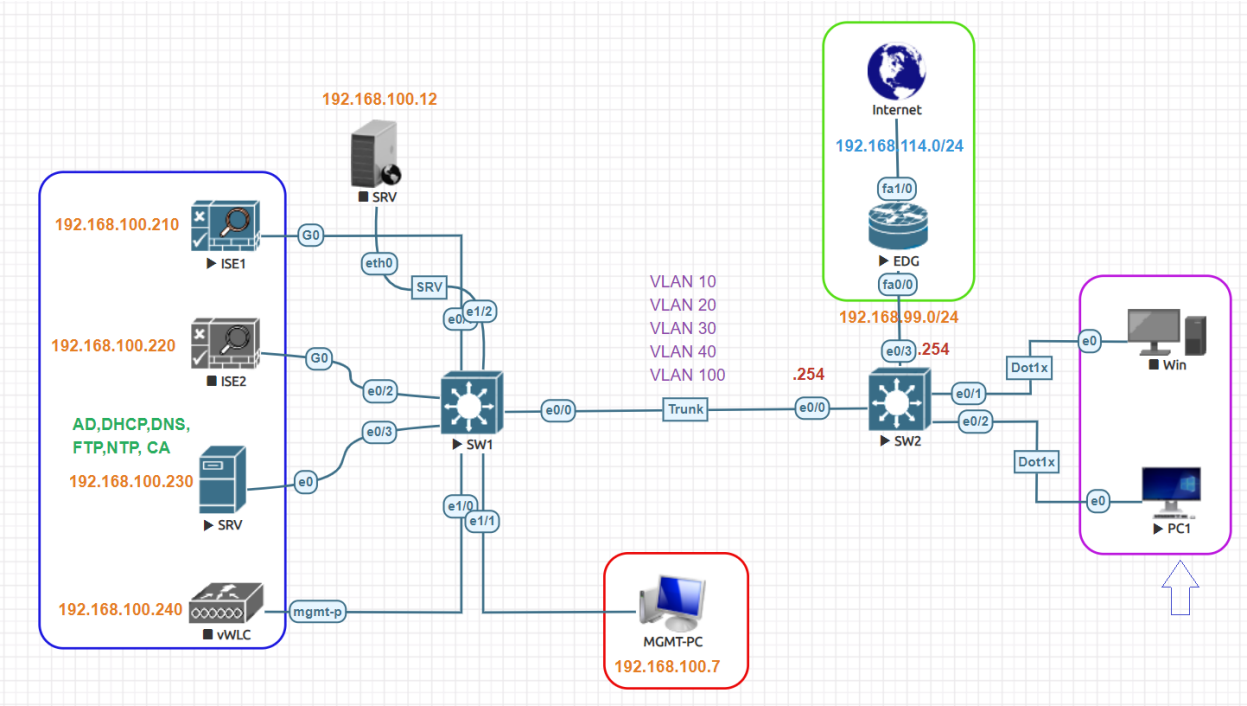
Certificate-Based Authentication LAB:

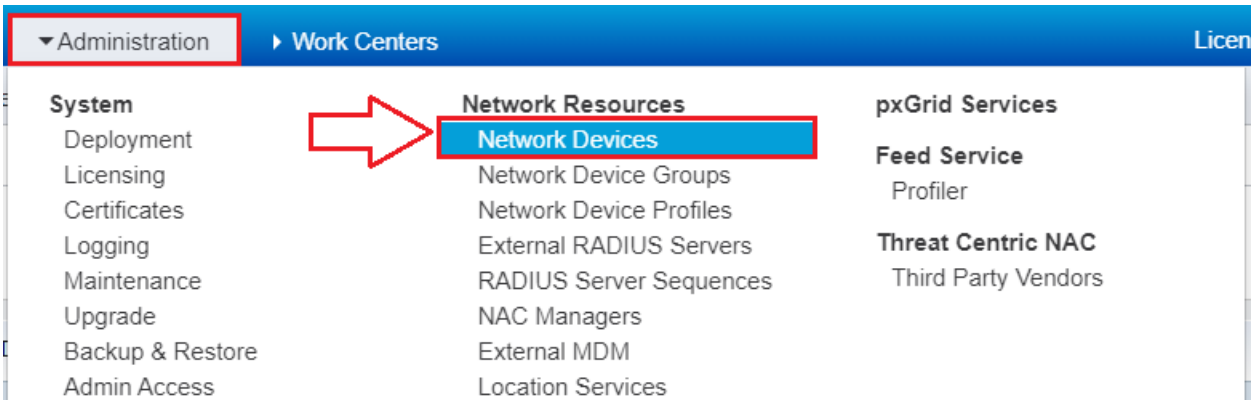


Cisco ISE Primary IP Address	192.168.100.210
Cisco ISE Secondary IP Address	192.168.100.220
AD and DNS IP Address	192.168.100.230
CA Server IP Address	192.168.100.230
Domain Name:	test.local
Test User/Group	E1/Employee
Test VLAN	VLAN 20
VLAN Subnet	192.168.20.0/24
VLAN 20 Gateway	192.168.20.1
Authenticator Switch	SW2
Authentication Switch MGMT IP	192.168.100.254
SW2 Dot1x interface	Ethernet 0/2
Certificate Authentication	Computer and User
Certificate Template	User and Workstation
Computer Hostname	PC1-Win10
Computer Name	PC1

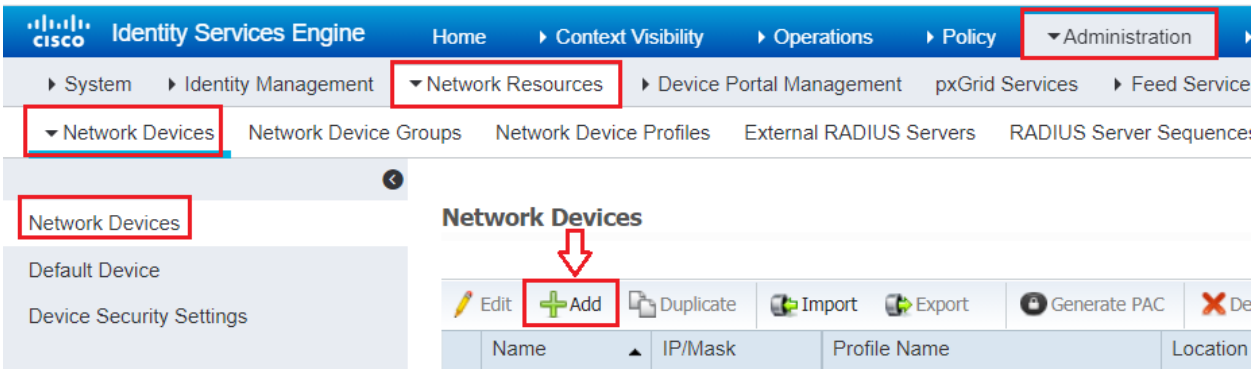
Dot1X Configuration
SW2(config)#aaa new-model
SW2(config)#dot1x system-auth-control
SW2(config)#radius server ISE1
SW2(config-radius-server)# address ipv4 192.168.100.210 auth-port 1812 acct-port 1813
SW2(config-radius-server)#key Test123
SW2(config-radius-server)#radius server ISE2
SW2(config-radius-server)# 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 Ethernet0/2
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:

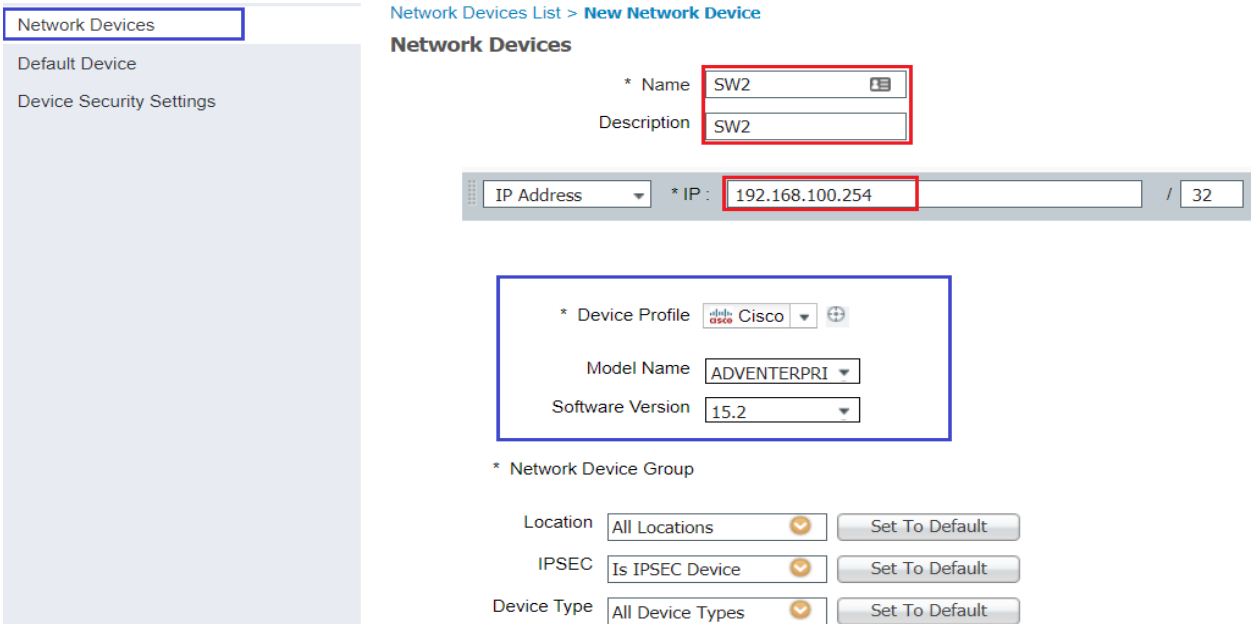
Go to Administration > Network Resources > Network Devices to add the Device (SW2).



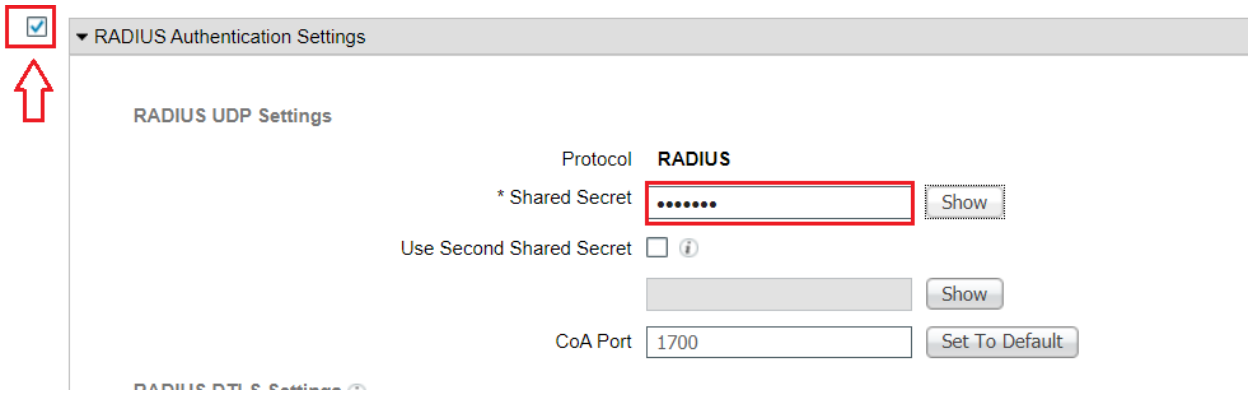
Click on Add button to add Network Device like Router and Switch.



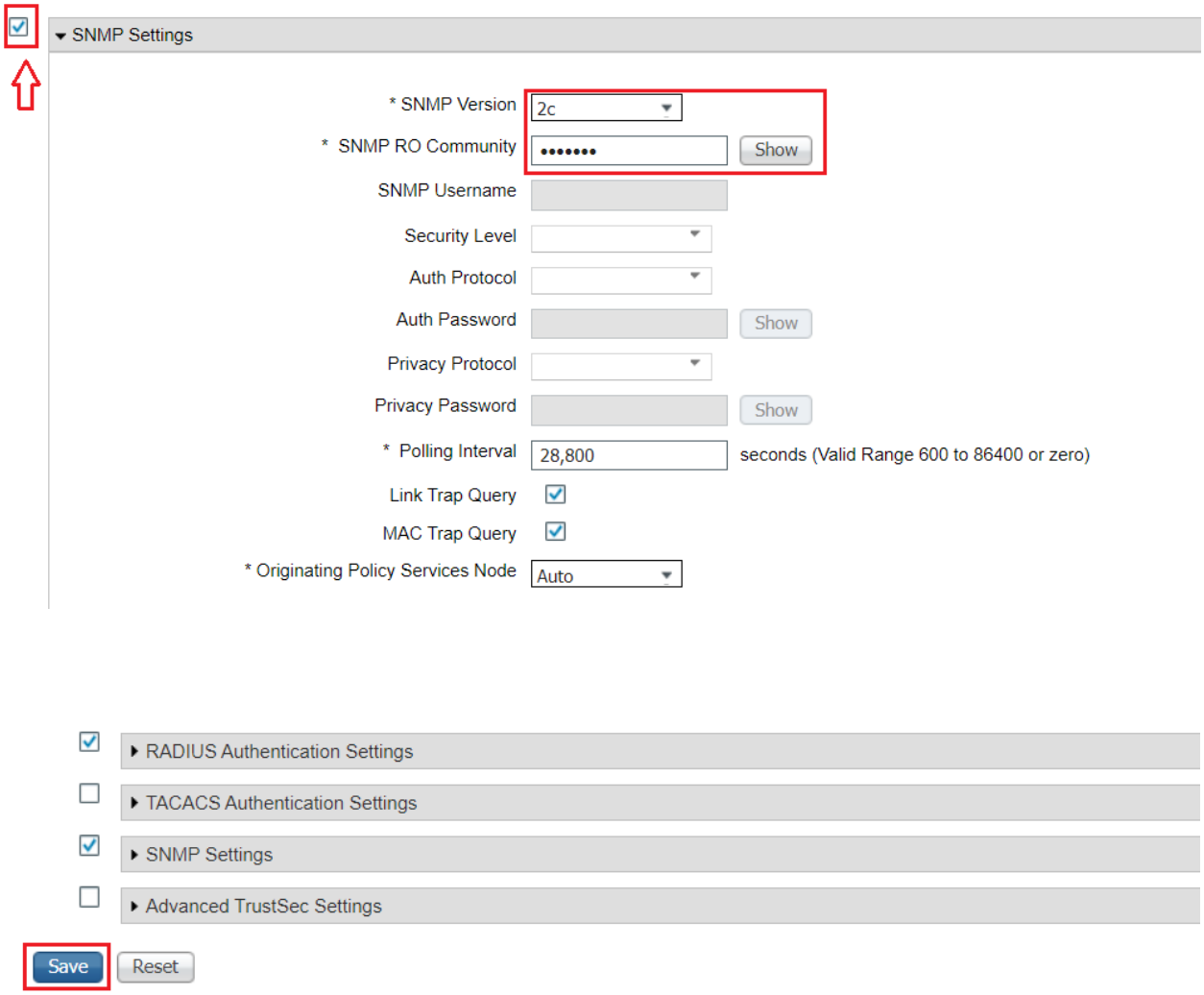
Configure **Name** of device, **IP address** configured. Scroll down to set Authentication settings.



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.

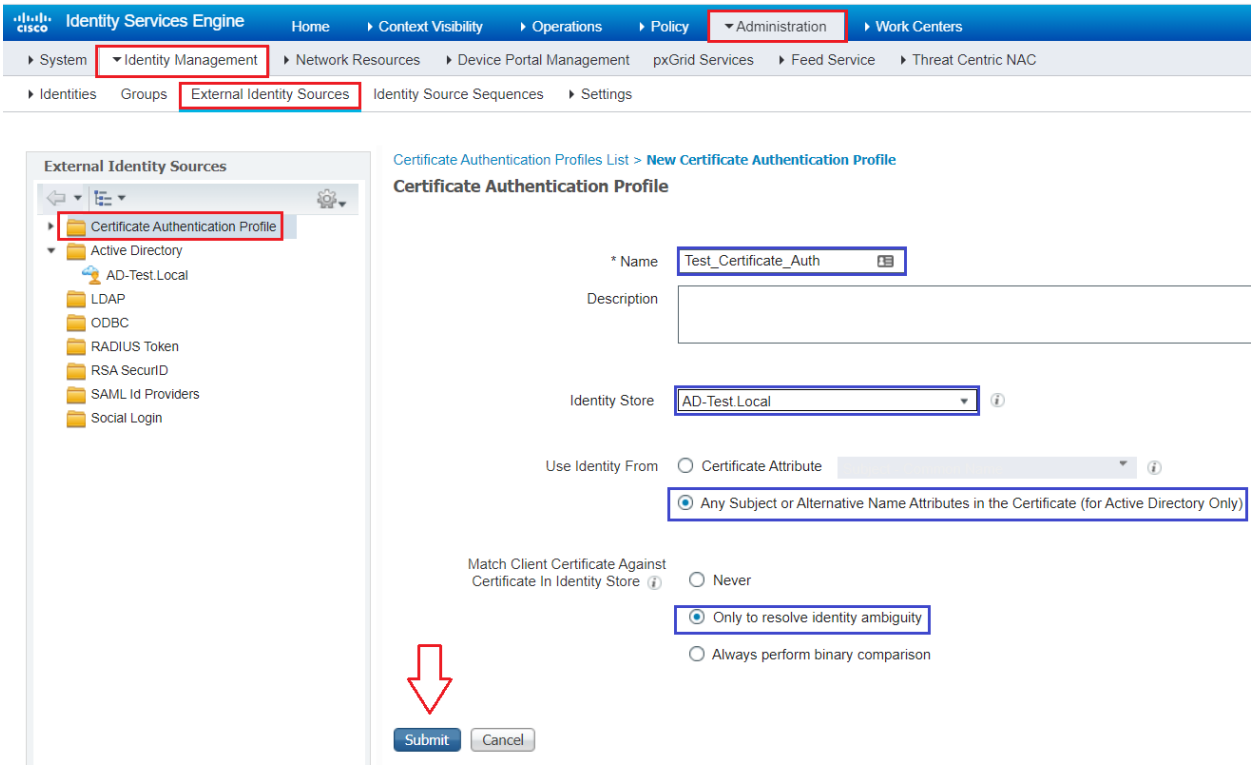


Certificate Profile:

You must create a certificate authentication profile in ISE if you want to use the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) certificate-based authentication method. Instead of authenticating via the traditional username and password method, Cisco ISE compares a certificate received from a client with one in the server to verify the authenticity of a user. EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) provides client and server authentication. It is often used for wireless networking and one of the stronger forms of authentication since both wireless client & server are authenticated with certificates.

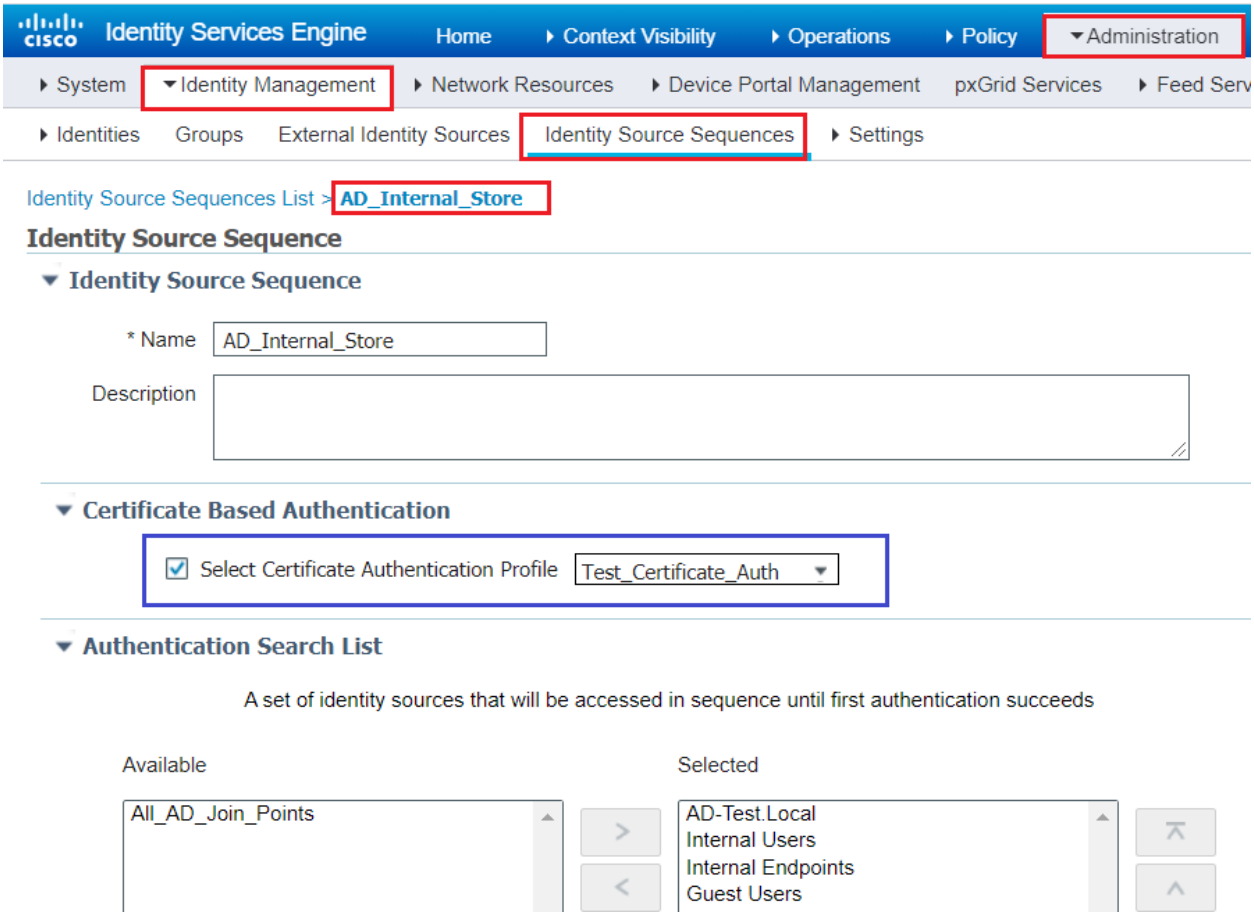
Create Certificate Profile:

Choose Administration > Identity Management > External Identity Sources > Certificate Authentication Profile > Add. Enter the name and an optional description for the certificate authentication profile. Select an identity store from the drop-down list. Any Subject or Alternative Name Attributes in the Certificate. Choose when you want to Match Client Certificate Against Certificate In Identity Store. Only to resolve identity ambiguity—This option performs the binary comparison of client certificate to certificate on account in Active Directory only if ambiguity is encountered. Click Submit to add the certificate authentication profile.

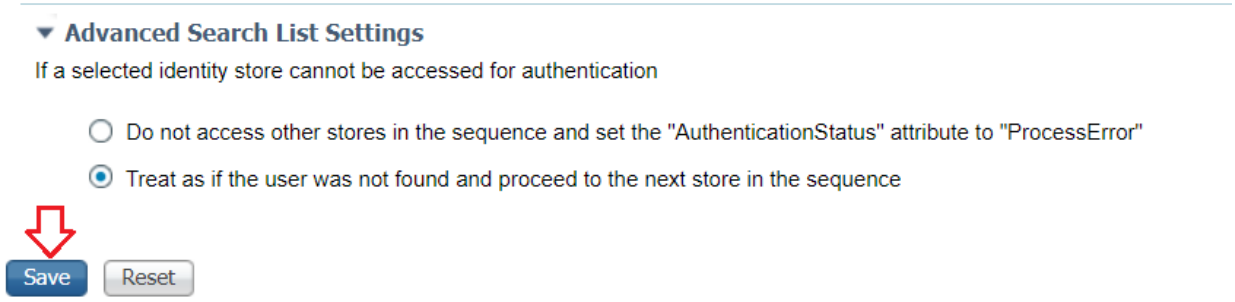


Identity Source Sequence:

The next step is to modify the Identity Source Sequence. This will tell ISE what order of databases to search for a user account when authenticating to a device. Navigate to Administration -> Identity Management -> Identity Source Sequences click on AD_Internal_Store which we created previously. In Certificate Based Authentication check Select Certificate Authentication Profile from drop down choose Test_Certificate_Auth



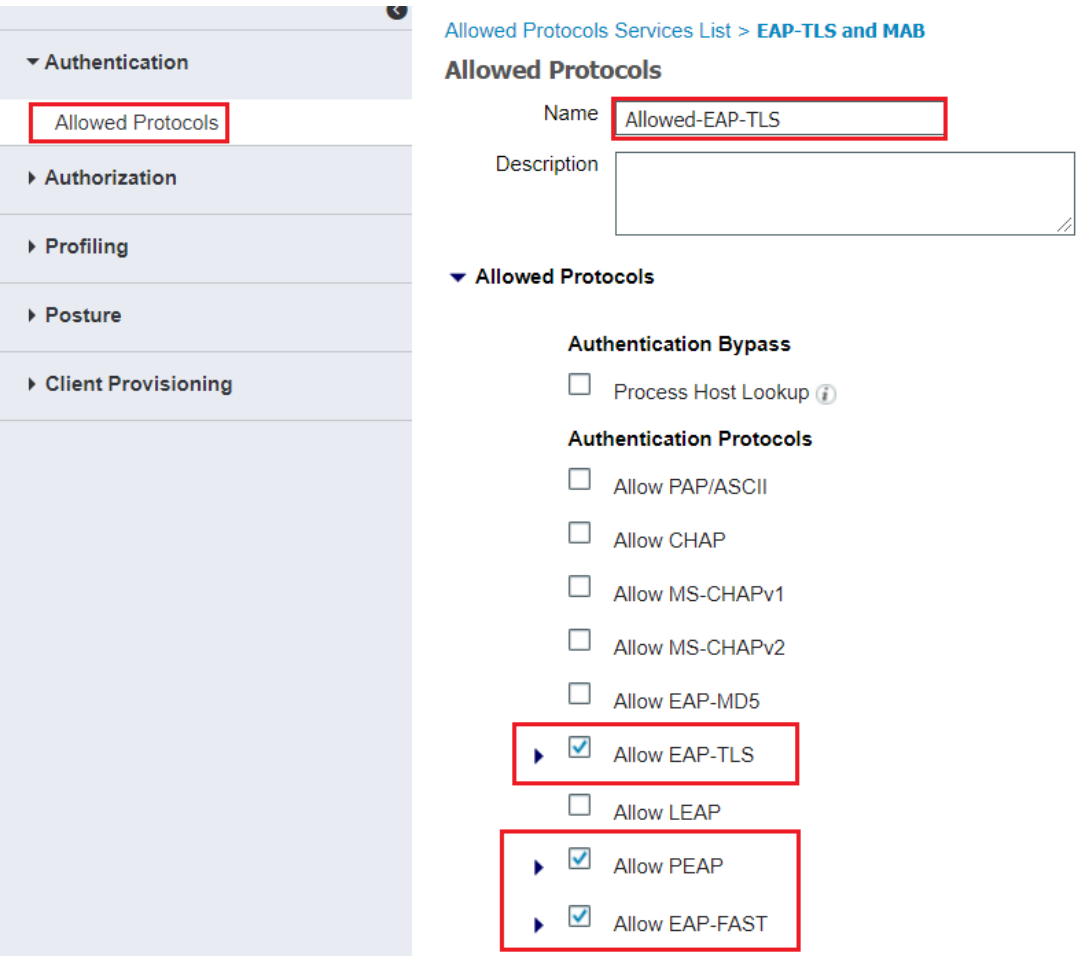
Click Save to apply the setting

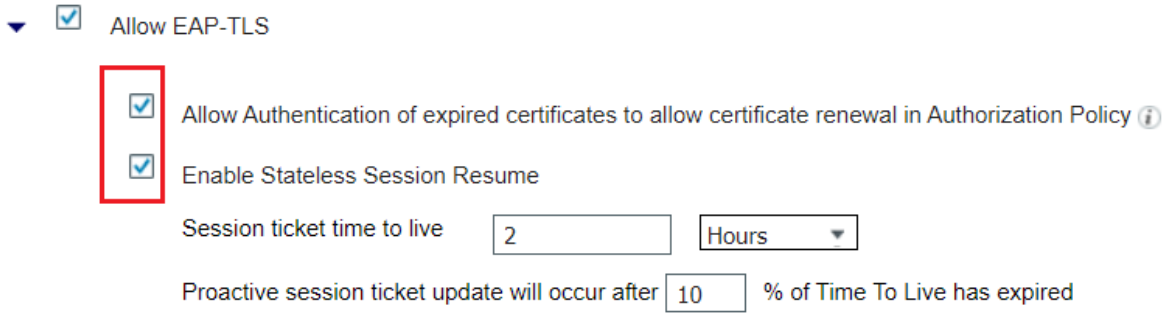


Define Allowed Protocols Service.

The Allowed Protocols Service enables only that authentication methods/protocols which ISE supports during Radius Authentication. In order to configure from Cisco ISE GUI.

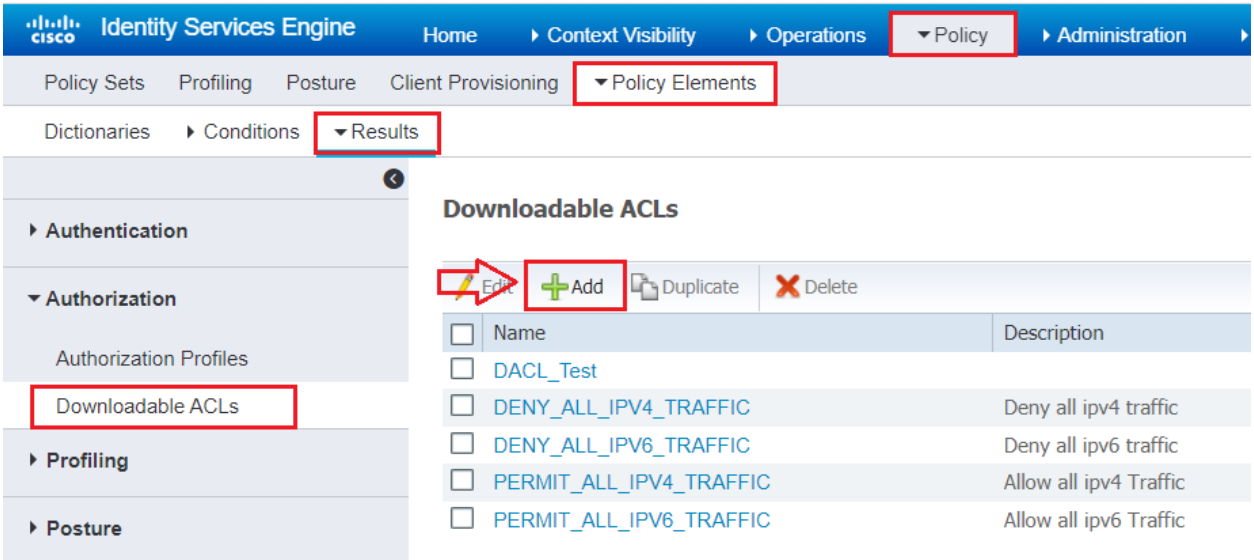
Navigate to Policy > Policy Elements: Results > Authentication > Allowed Protocols and then it binds as an element to the Authentication Policy. Enable EAP-TLS since ISE and our supplicant authenticates via EAP-TLS also unchecked Process Host Lookup and click Submit.



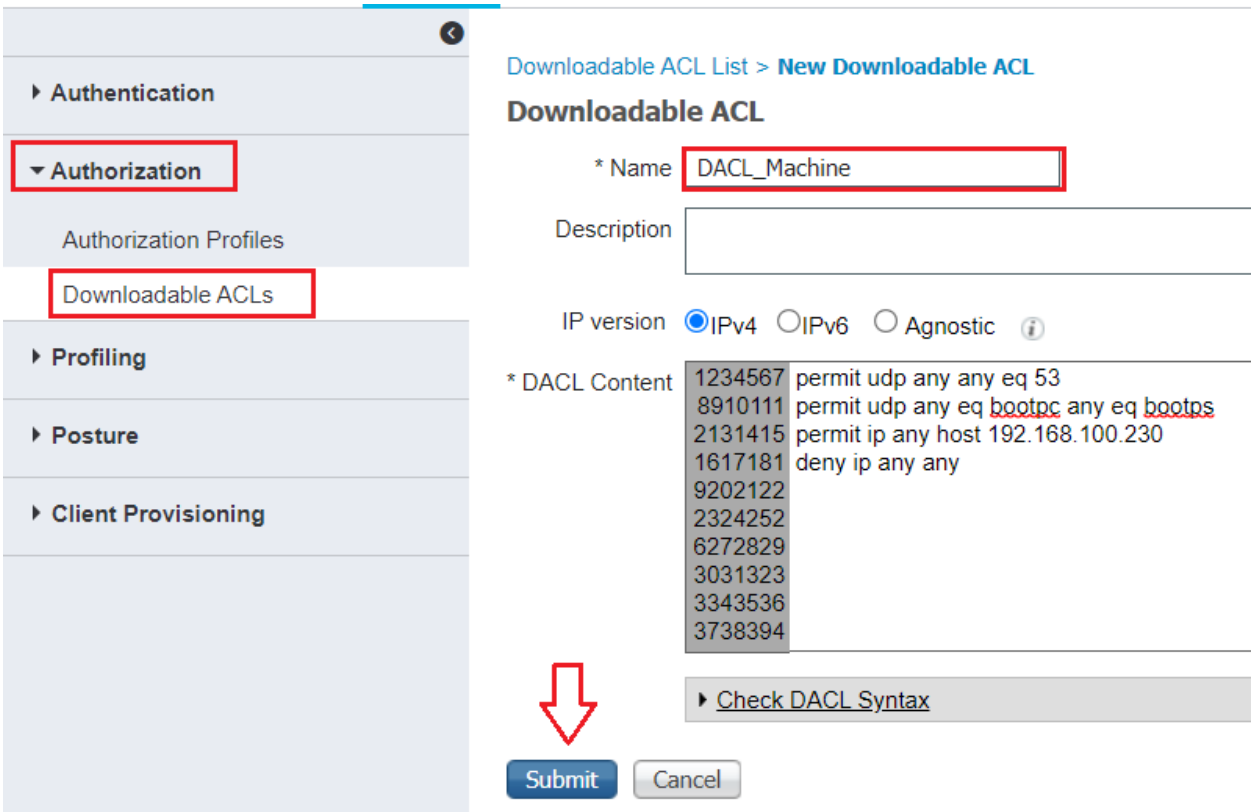


Configuring Downloadable ACL:

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

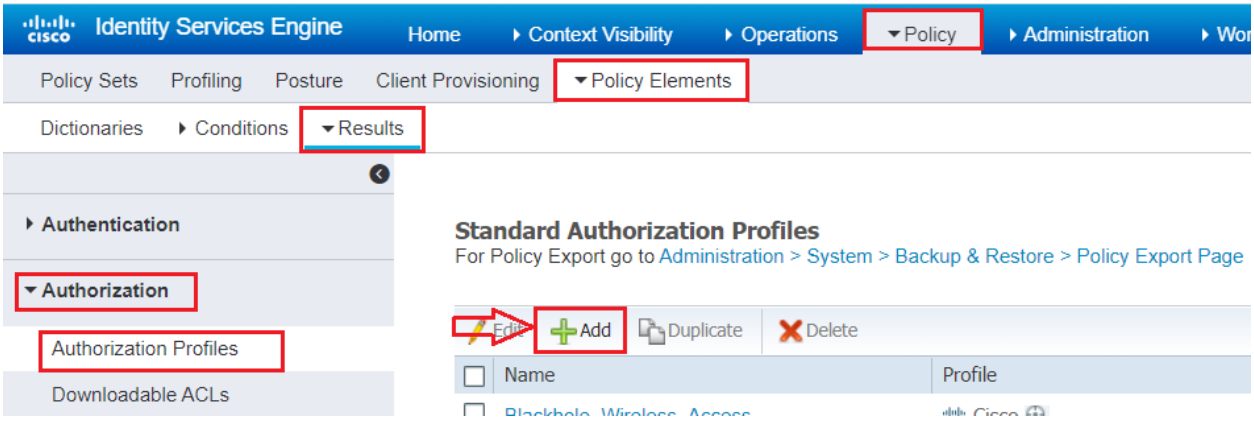


Create a DACL with Name DACL_Machine. Allow DNS, DHCP other traffic to Active Directory which IP address is 192.168.100.230 and deny everything else.

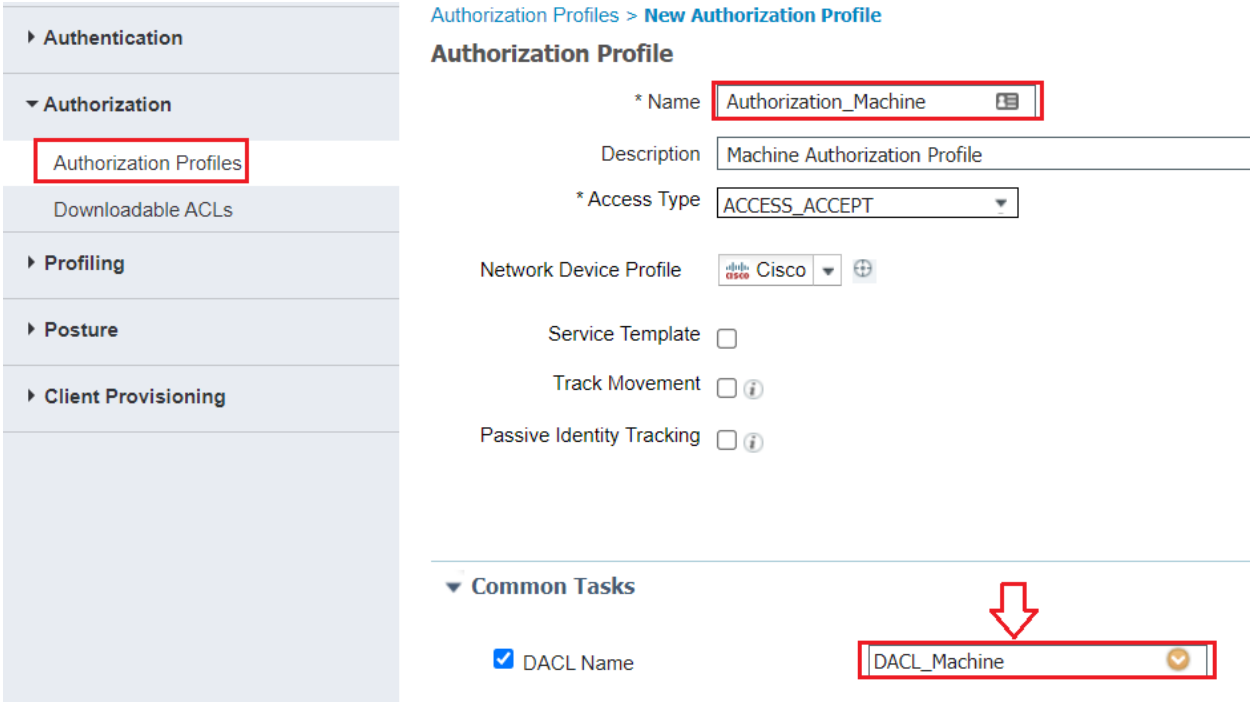


Configuring DACL Profile:

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

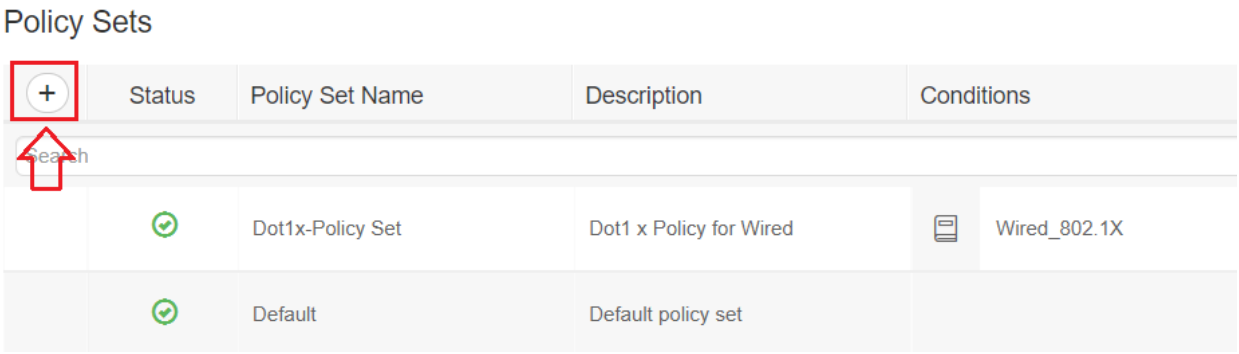


Name Authorization profile in this case Authorization_Machine. Select DACL Name from the drop-down list select the DACL previously configured called DACL_Machine. Click Save.

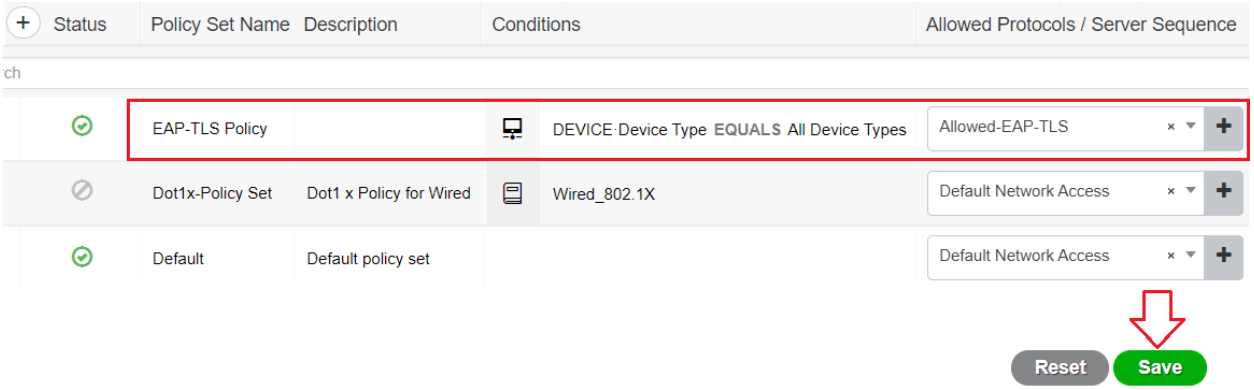


Policy Set:

A policy set is a hierarchical container consisting of a single user-defined rule that indicates the allowed protocol or server sequence for network access, as well as authentication and authorization policies and policy exceptions, all also configured with user-defined condition-based rules. 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.

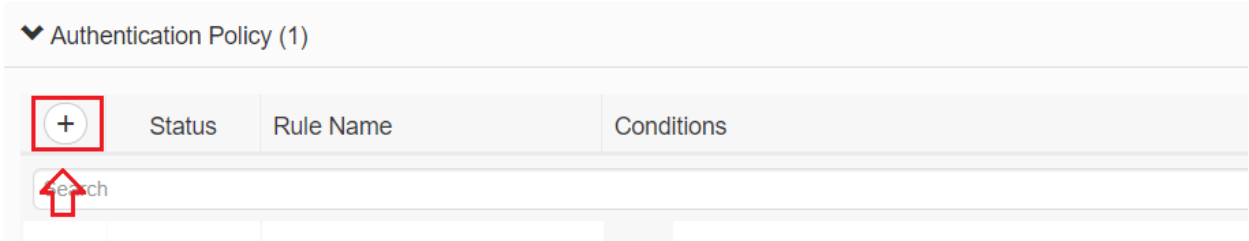


Name the Policy Set in this case EAP-TLS Policy, set the Conditions Device: Device Type EQUALS All Device Types and Set the Allow Protocols EAP-TLS protocols which created previously with Named Allowed-EAP-TLS. Click Save to apply the setting.

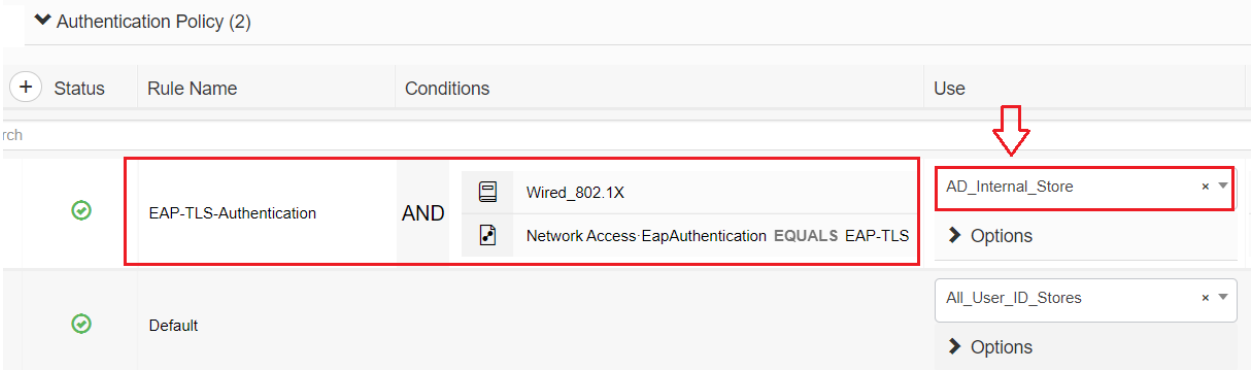


802.1x Authentication Policy:

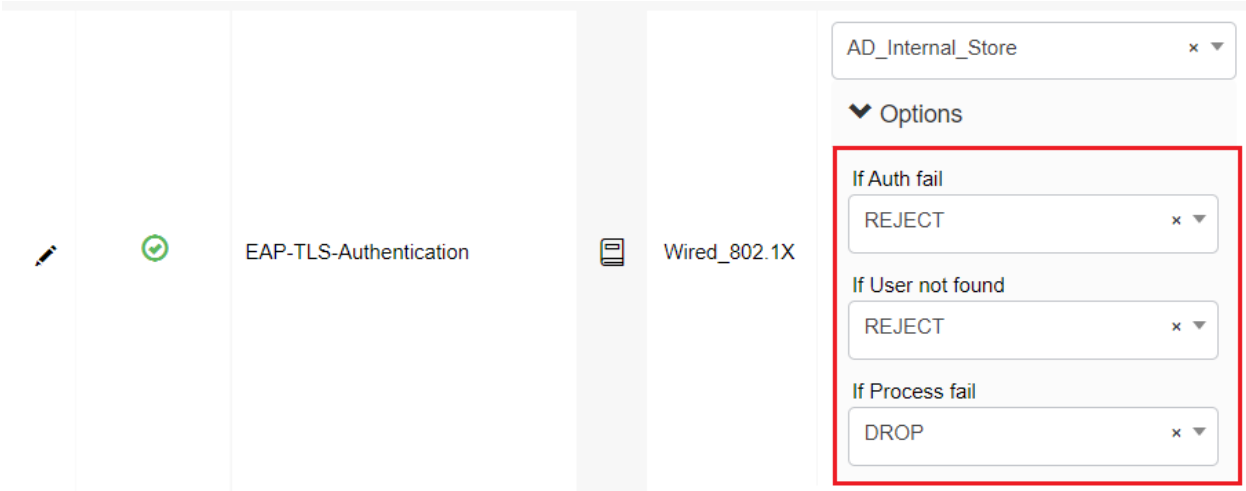
For network access policies, choose Work Centers > Network Access > Policy Sets. Navigate to Authentication Policy, click Add new authentication policy.



Name Authentication Policy Rule in this case EAP-TLS-Authentication set the conditions to Wired_8021X and Network Access EapAuthentication EQUALS EAP-TLS also change the default Identity store to AD_Internal_Store which we created earlier.

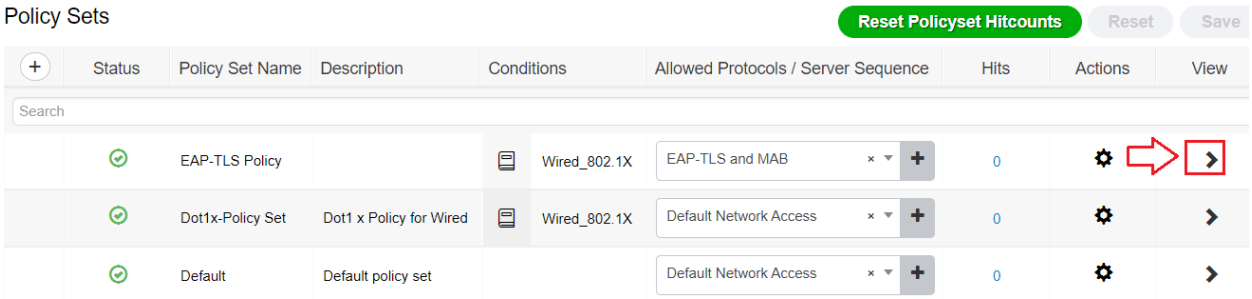


Leave the default Options settings and click Save to apply the changes.

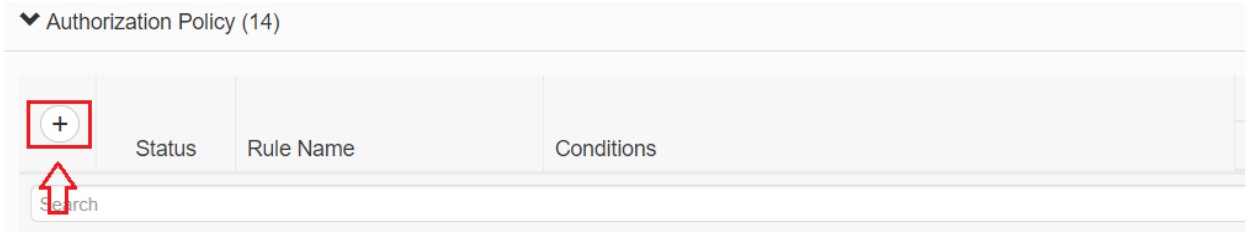


802.1x Authorization Polices:

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

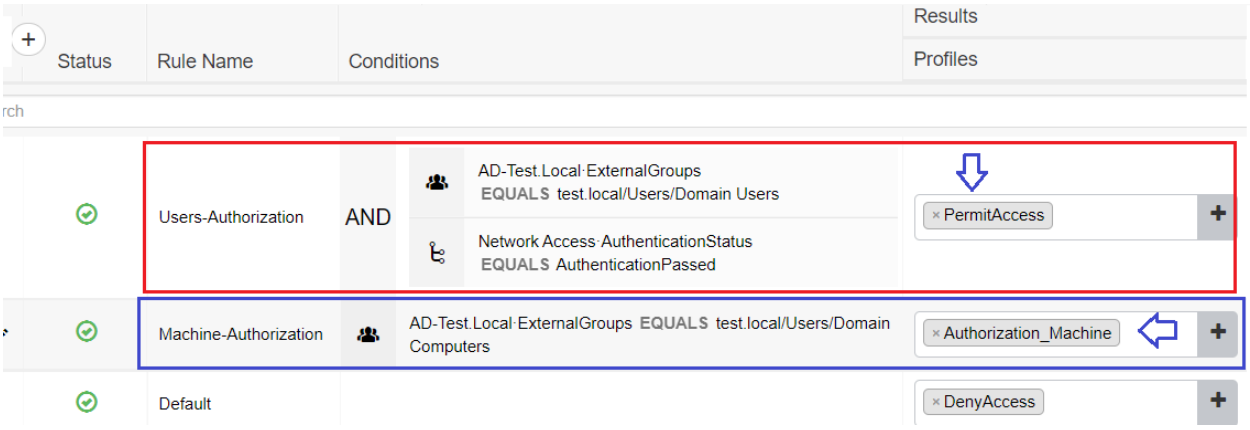


Navigate to Authorization Policy section click on round circle Plus icon to add new Authorization Policy, name authorization policy in this case Users-Authorization and Machine-Authorization. In Conditions click on Plus icon to set the conditions for authorization policy.



In Users-Authorization AD-Test.Local·ExternalGroups EQUALS test.local/users/Domain Users AND Network Access·AuthenticationStatus EQUALS AuthenticationPass Assign Profiles: PermitAccess

Machine-Authorization AD-Test.Local·ExternalGroups EQUALS test.local/users/Domain Computers Assign Profiles: Authorizaiton_Machine



Verification:

Navigate to Operations > RADIUS Livelog.

Refresh | Reset Repeat Counts | Export To

Time	Status	Details	Repeat …	Identity	Endpoint ID	Endpoint P…	Authenticat…
				Identity	Endpoint ID	Endpoint Profi	Authenticatior
Aug 21, 2021 04:17:15.398 PM			0	e1@test.local	50:01:00:0A:00:00	FreeBSD-W…	EAP-TLS Po…
Aug 21, 2021 02:29:38.594 PM				e1@test.local	50:01:00:0A:00:00	FreeBSD-W…	EAP-TLS Po…
Aug 21, 2021 02:27:04.721 PM				PC1-WIN10$@tes…	50:01:00:0A:00:00	FreeBSD-W…	EAP-TLS Po…
Aug 21, 2021 02:26:57.331 PM					50:01:00:0A:00:00		

Event	5200 Authentication succeeded
Username	PC1-WIN10$@test.local
Endpoint Id	50:01:00:0A:00:00
Endpoint Profile	FreeBSD-Workstation
Authentication Policy	EAP-TLS Policy >> EAP-TLS-Authentication
Authorization Policy	EAP-TLS Policy >> Machine-Authorization
Authorization Result	PermitAccess

Event	5200 Authentication succeeded
Username	PC1-WIN10$@test.local
Endpoint Id	50:01:00:0A:00:00
Calling Station Id	50-01-00-0A-00-00
Endpoint Profile	FreeBSD-Workstation
IPv4 Address	169.254.96.167
Authentication Identity Store	AD-Test.Local
Identity Group	Workstation
Audit Session Id	C0A864FE00000019018BF076
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	SW2
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.168.100.254

Overview

Event	5200 Authentication succeeded
Username	e1@test.local
Endpoint Id	50:01:00:0A:00:00
Endpoint Profile	FreeBSD-Workstation
Authentication Policy	EAP-TLS Policy >> EAP-TLS-Authentication
Authorization Policy	EAP-TLS Policy >> Users-Authorization
Authorization Result	PermitAccess

Event	5200 Authentication succeeded
Username	e1@test.local
Endpoint Id	50:01:00:0A:00:00
Calling Station Id	50-01-00-0A-00-00
Endpoint Profile	FreeBSD-Workstation
IPv4 Address	192.168.20.12
Authentication Identity Store	AD-Test.Local
Identity Group	Workstation
Audit Session Id	C0A864FE00000019018BF076
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	SW2
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.168.100.254

Verification commands on Cisco Switch

SW2# show dot1x interface ethernet 0/2
SW2# show dot1x all
SW2# Show authentication sessions
SW2# Show authentication sessions interface ethernet 0/2 details

```
SW2#show authentication sessions interface e0/2 details
            Interface:  Ethernet0/2
          MAC Address:  5001.000a.0000
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.20.12
            User-Name:  e1@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: 155s
       Session Uptime:  6937s
    Common Session ID:  C0A864FE00000019018BF076
      Acct Session ID:  0x00000009
               Handle:  0x7B000009
       Current Policy:  POLICY_Et0/2

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

```
SW2#show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            3

Dot1x Info for Ethernet0/2
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 10
```

```
SW2#show authentication sessions interface e0/2 details
            Interface:  Ethernet0/2
          MAC Address:  5001.000a.0000
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.20.12
            User-Name:  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: 191s
       Session Uptime:  7503s
    Common Session ID:  C0A864FE00000019018BF076
      Acct Session ID:  0x0000000C
               Handle:  0x7B000009
       Current Policy:  POLICY_Et0/2

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

Server Policies:
              ACS ACL:  xACSACLx-IP-DACL_Machine-611fc10a
```

```
SW2#show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            3

Dot1x Info for Ethernet0/2
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 10
```