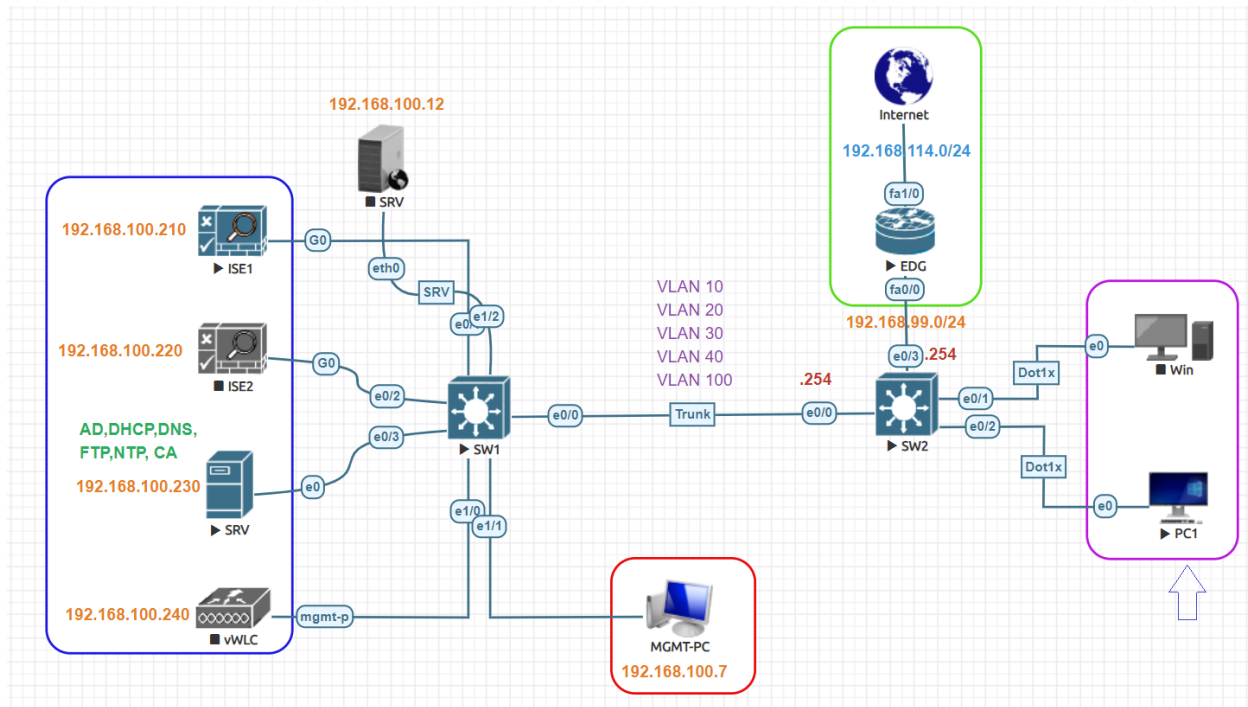


## Certificate-Based Authentication LAB:



|                                |                      |
|--------------------------------|----------------------|
| 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                  |

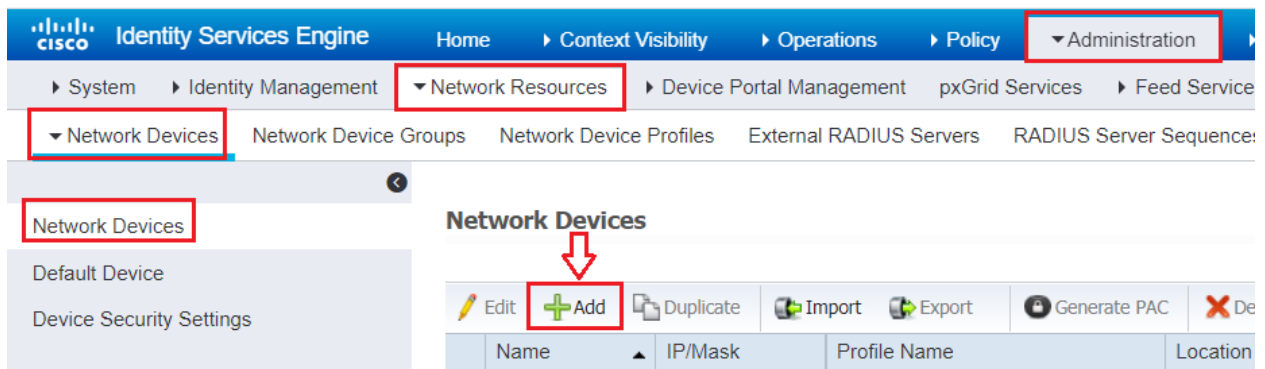
|   |
|---|
| <b>Dot1X Configuration</b>  |
| SW2(config)#aaa new-model   |
| SW2(config)#dot1x system-auth-control   |
| SW2(config)#radius server ISE1  |
| SW2(config-radius-server)# address ipv4 192.168.100.210 auth-port 1812 acct-port 1813 |
| SW2(config-radius-server)#key Test123   |
| SW2(config-radius-server)#radius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

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**

## 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.

The screenshot displays the Cisco ISE Administration console interface for creating a new Certificate Authentication Profile. The breadcrumb trail at the top indicates the navigation path: **Administration > Identity Management > External Identity Sources > Certificate Authentication Profile > Add**. The left sidebar shows the 'External Identity Sources' tree with 'Certificate Authentication Profile' selected. The main form fields are as follows:

- \* Name:** Test\_Certificate\_Auth
- Description:** (empty text field)
- Identity Store:** AD-Test\_Local
- Use Identity From:** Certificate Attribute
- Match Client Certificate Against Certificate In Identity Store:** Only to resolve identity ambiguity
- Buttons:** Submit, Cancel

A red arrow points to the Submit button.

## 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**

The screenshot shows the Cisco ISE Administration interface. The navigation pane on the left includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, and Feed Services. Under Identity Management, the path is Identity Source Sequences > AD\_Internal\_Store. The main content area shows the configuration for the AD\_Internal\_Store sequence. The Identity Source Sequence section has a Name field set to AD\_Internal\_Store and an empty Description field. The Certificate Based Authentication section has a checkbox for 'Select Certificate Authentication Profile' which is checked, and a dropdown menu set to 'Test\_Certificate\_Auth'. The Authentication Search List section has a description: 'A set of identity sources that will be accessed in sequence until first authentication succeeds'. It shows two lists: 'Available' with 'All\_AD\_Join\_Points' and 'Selected' with 'AD-Test.Local', 'Internal Users', 'Internal Endpoints', and 'Guest Users'. Arrows indicate the ability to move items between the lists.

Identity Source Sequences List > **AD\_Internal\_Store**

### Identity Source Sequence

▼ Identity Source Sequence

\* Name:

Description:

▼ Certificate Based Authentication

☒ Select Certificate Authentication Profile:

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

| Available          |   | Selected           |
|--------------------|---|--------------------|
| All_AD_Join_Points | > | AD-Test.Local      |
|                    | < | Internal Users     |
|                    |   | Internal Endpoints |
|                    |   | Guest Users        |


Click **Save** to apply the setting

▼ Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

☐ Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

☒ Treat as if the user was not found and proceed to the next store in the sequence



## 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**.

Allowed Protocols Services List > **EAP-TLS and MAB**

### Allowed Protocols

Name: **Allowed-EAP-TLS**

Description:

▼ Allowed Protocols

**Authentication Bypass**

☐ Process Host Lookup ⓘ

**Authentication Protocols**

☐ Allow PAP/ASCII

☐ Allow CHAP

☐ Allow MS-CHAPv1

☐ Allow MS-CHAPv2

☐ Allow EAP-MD5

☒ Allow EAP-TLS

☐ Allow LEAP

☒ Allow PEAP

☒ Allow EAP-FAST

▼ ☒ Allow EAP-TLS

☒ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy ⓘ

☒ Enable Stateless Session Resume

Session ticket time to live:

Proactive session ticket update will occur after  % of Time To Live has expired

## Configuring Downloadable ACL:

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

The screenshot shows the Cisco Identity Services Engine (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, showing 'Dictionary', 'Conditions', and 'Results'. The 'Results' menu is expanded, showing 'Authentication', 'Authorization', 'Profiling', and 'Posture'. The 'Authorization' menu is expanded, showing 'Authorization Profiles' and 'Downloadable ACLs'. The 'Downloadable ACLs' menu is expanded, showing a list of ACLs: 'DACL\_Test', 'DENY\_ALL\_IPV4\_TRAFFIC', 'DENY\_ALL\_IPV6\_TRAFFIC', 'PERMIT\_ALL\_IPV4\_TRAFFIC', and 'PERMIT\_ALL\_IPV6\_TRAFFIC'. The 'Add' button is highlighted with a red box and an arrow.

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.

The screenshot shows the 'New Downloadable ACL' configuration page in the Cisco Identity Services Engine (ISE) web interface. The left sidebar shows the navigation path: 'Authentication', 'Authorization', 'Downloadable ACLs', 'Profiling', 'Posture', and 'Client Provisioning'. The main content area is titled 'Downloadable ACL List > New Downloadable ACL'. The 'Downloadable ACL' form includes the following fields:

- Name:** **DACL\_Machine**
- Description:** (empty)
- IP version:** ☒ IPv4, ☐ IPv6, ☐ Agnostic
- \* DACL Content:**

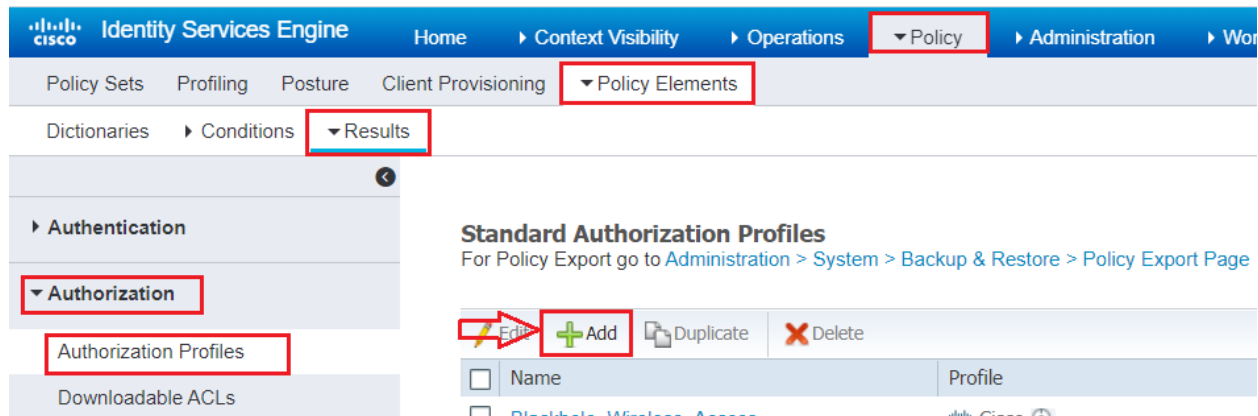
```
1234567 permit udp any any eq 53
8910111 permit udp any eq bootpc any eq bootps
2131415 permit ip any host 192.168.100.230
1617181 deny ip any any
9202122
2324252
6272829
3031323
3343536
3738394
```
- Check DACL Syntax:** (button)
- Submit:** (button)
- Cancel:** (button)

A red arrow points to the 'Submit' button.

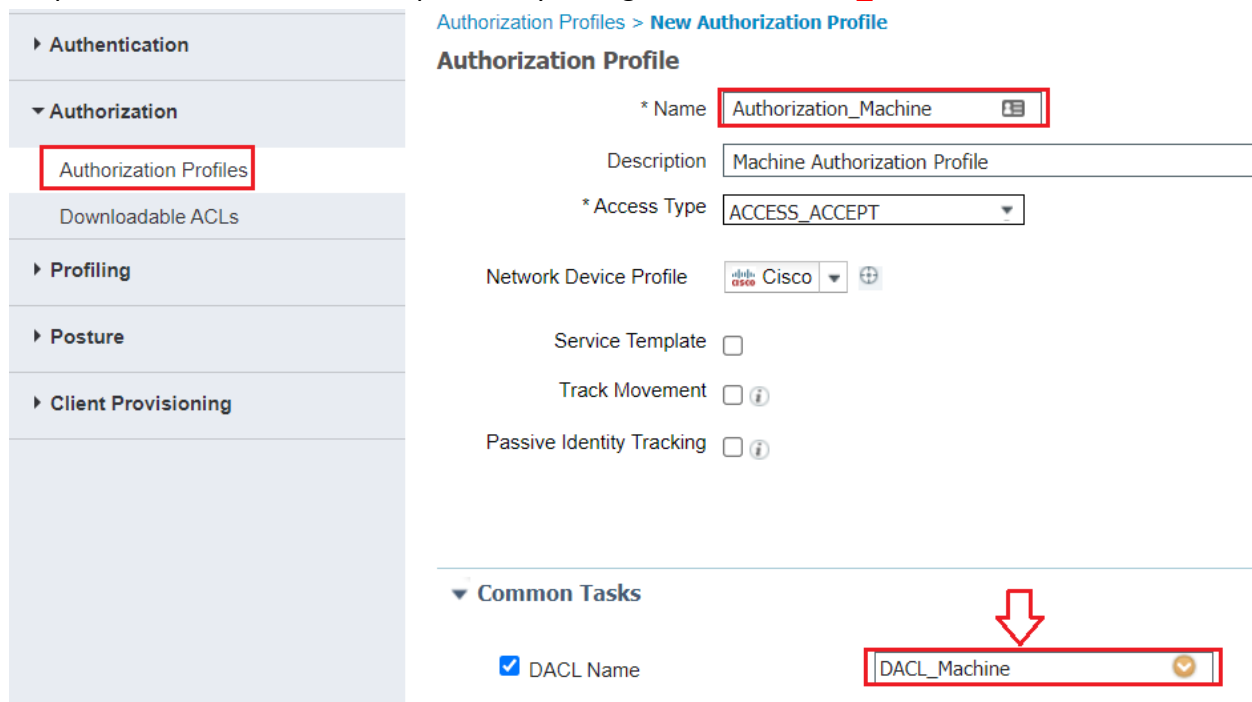


## Configuring DACL Profile:

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:


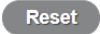

A policy set is a hierarchical container consisting of a single user-defined rule that indicates the allowed protocol or server sequence for network access, as well as authentication and authorization policies and policy exceptions, all also configured with user-defined condition-based rules. In order to create a Policy Set from ISE GUI, navigate to **Policy > Policy Set** and then click on plus (+) icon on the upper-left corner.

### Policy Sets

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

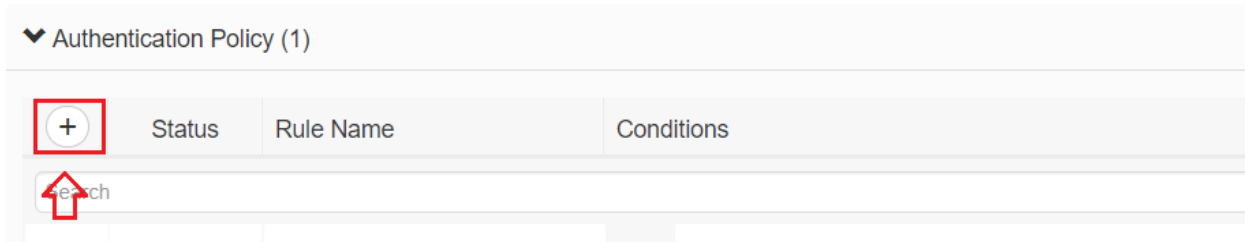
Name the Policy Set in this case **EAP-TLS Policy**, set the Conditions **Device: Device Type EQUALS All Device Types** and Set the **Allow Protocols** EAP-TLS protocols which created previously with Named Allowed-EAP-TLS. Click **Save** to apply the setting.

|   |        |                  |                         |   |  |
|---|--------|------------------|-------------------------|---|--|
|  | Status | Policy Set Name  | Description             | Conditions  | Allowed Protocols / Server Sequence  |
| ch  |        |                  |                         |   |  |
|  |        | EAP-TLS Policy   |                         |  DEVICE: Device Type EQUALS All Device Types | Allowed-EAP-TLS x         |
|  |        | Dot1x-Policy Set | Dot1 x Policy for Wired |  Wired_802.1X                                | Default Network Access x  |
|  |        | Default          | Default policy set      |   | Default Network Access x  |

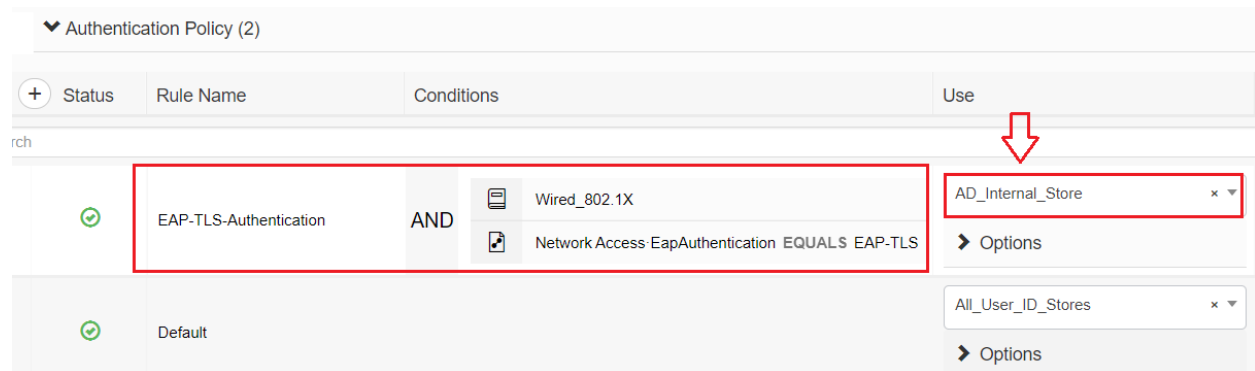
  
 

## 802.1x Authentication Policy:

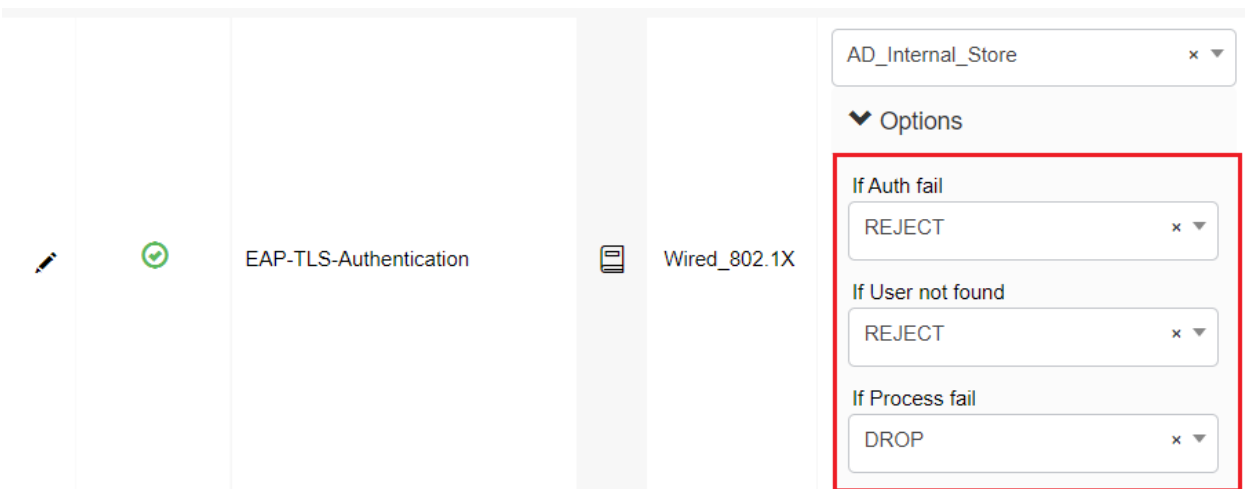
For network access policies, choose **Work Centers > Network Access > Policy Sets**. Navigate to Authentication Policy, click Add new authentication policy.



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 Policies:

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

Policy Sets

| Reset Policyset Hitcounts |        |                  |                         |              |                                     |      |          |      |
|---------------------------|--------|------------------|-------------------------|--------------|-------------------------------------|------|----------|------|
| Reset                     |        |                  |                         |              |                                     |      |          |      |
| Save                      |        |                  |                         |              |                                     |      |          |      |
| +                         | Status | Policy Set Name  | Description             | Conditions   | Allowed Protocols / Server Sequence | Hits | Actions  | View |
| Search                    |        |                  |                         |              |                                     |      |          |      |
|                           | ✓      | EAP-TLS Policy   |                         | Wired_802.1X | EAP-TLS and MAB                     | 0    | ⚙️ ➡️ ➡️ |      |
|                           | ✓      | Dot1x-Policy Set | Dot1 x Policy for Wired | Wired_802.1X | Default Network Access              | 0    | ⚙️ ➡️    |      |
|                           | ✓      | Default          | Default policy set      |              | Default Network Access              | 0    | ⚙️ ➡️    |      |

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.

| Authorization Policy (14) |        |           |            |
|---------------------------|--------|-----------|------------|
| +                         | Status | Rule Name | Conditions |
| Search                    |        |           |            |

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**

| +   | Status | Rule Name             | Conditions  | Results                      |
|-----|--------|-----------------------|---|------------------------------|
|     |        |                       |   | Profiles                     |
| rch |        |                       |   |                              |
| ✓   |        | Users-Authorization   | AND<br>AD-Test.Local-ExternalGroups EQUALS test.local/Users/Domain Users<br>Network Access-AuthenticationStatus EQUALS AuthenticationPassed | ⬇️<br>× PermitAccess +       |
| ✓   |        | Machine-Authorization | AD-Test.Local-ExternalGroups EQUALS test.local/Users/Domain Computers   | × Authorization_Machine ⬅️ + |
| ✓   |        | Default               |   | × DenyAccess +               |

## Verification:

Navigate to **Operations > RADIUS Livelog**.

Refresh


Reset Repeat Counts

Export To

| Time  | Status | Details | Repeat ... | Identity           | Endpoint ID       | Endpoint P... | Authenticat... |
|---|--------|---------|------------|--------------------|-------------------|---------------|----------------|
| <div> <div>x</div> <div></div> <div>Identity</div> <div>Endpoint ID</div> <div>Endpoint Profi</div> <div>Authenticator</div> </div> |        |         |            |                    |                   |               |                |
| 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: C0A864FE000000019018BF076
    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: C0A864FE000000019018BF076
    Acct Session ID: 0x00000000C
    Handle: 0x7B0000009
    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

```