

ISE Configuration for EAP-TLS Server

(Supplement to the Common Criteria Operational User
Guidance

And Preparative Procedures for ISEv3.1)

Version 0.2

April 14, 2023



1 Introduction

This document describes the configuration of Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) Authentication with Cisco Identity Services Engine (ISE) for wired connections.

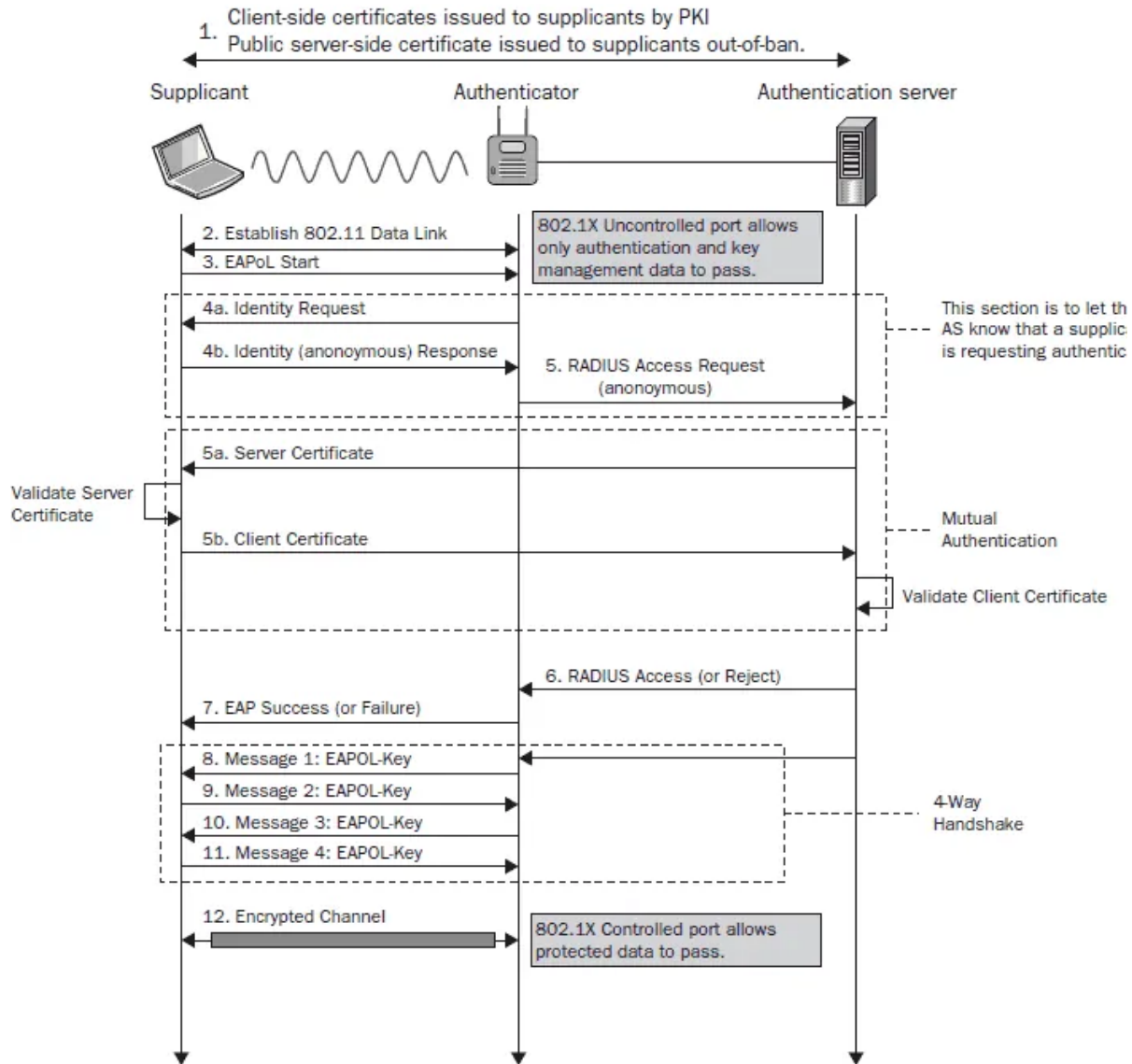
For the scope of this guide, it is important to understand these phases of the ISE (RADIUS) Authentication flow:

Authentication - Identify and validate the end-identity (machine, user, and so on) that requests network access.

Authorization - Determine what permissions/access the end-identity will be granted on the network.

Accounting - Report and track the end-identity's network activity after network access is achieved.

EAP-TLS Flow



2 Prerequisites

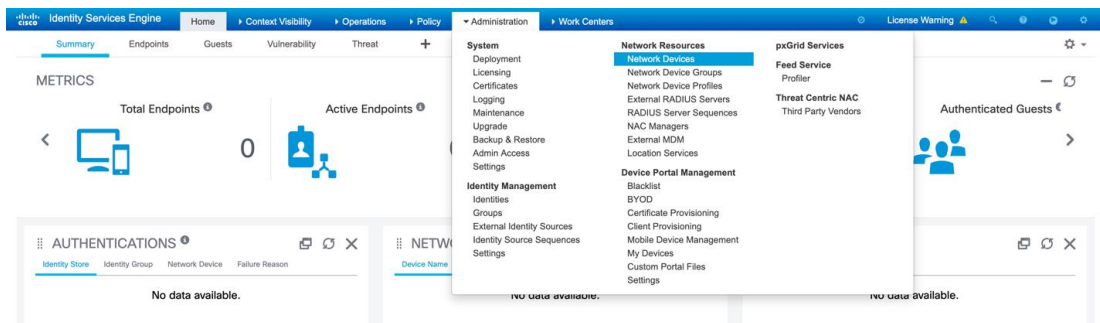
- Make sure that all the IP's of Supplicant (Test Laptop), Authenticator (Switch) and Authentication server (TOE) are reachable to each other.
- Make sure the Supplicant and Authentication server are directly connected to the Switch

- We also need a bridge between the Authentication server and the Authenticator to capture the traffic between them.

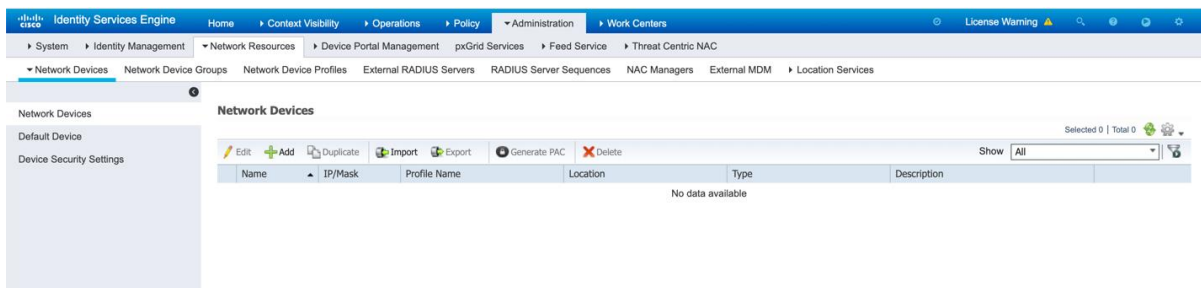
3 ISE Configuration Steps: ISE EAP-TLS Server

3.1 Add the Network Access Device in ISE

- Login to the ISE Administration User Interface (UI) as a SuperAdmin role user.
- The Network Access Device (Authenticator) that an endpoint is connected to is also configured in ISE so that RADIUS/TACACS+ (Device Admin) communication can take place. Between the NAD and ISE, a shared secret/password is used for trust purposes.
- To add a NAD via the ISE GUI, navigate to **Administration > Network Resources: Network Devices > Network Devices**, which is shown in this image.



- Click the Add button to add a new Network Device



- Complete the RADIUS Network Access Device relevant fields:


- Complete Name field.
- Complete IP Address(es) for the Network Access Device
- Check the checkbox for the RADIUS Authentication Settings
- Enter the RADIUS Shared Secret



Network Devices List > [New Network Device](#)

Network Devices

* Name

Description


IP Address * IP: / 32 


* Device Profile  Cisco 


Model Name

Software Version

* Network Device Group

Location 

IPSEC 


Device Type 

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Use Second Shared Secret 

CoA Port

- Click the Submit button to persist the changes.

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Use Second Shared Secret ⓘ

CoA Port

RADIUS DTLS Settings ⓘ

DTLS Required ⓘ

Shared Secret ⓘ

CoA Port

Issuer CA of ISE Certificates for CoA ⓘ

DNS Name

General Settings

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

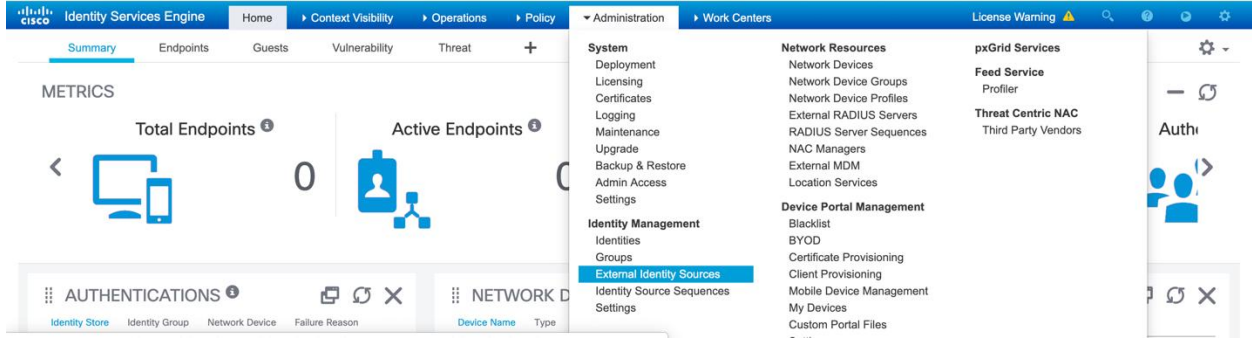
Advanced TrustSec Settings

More information can be found in *Cisco Identity Services Engine Administrator Guide, Release 3.1 > Chapter: Secure Access > [Defining Network Devices in Cisco ISE](#)*.

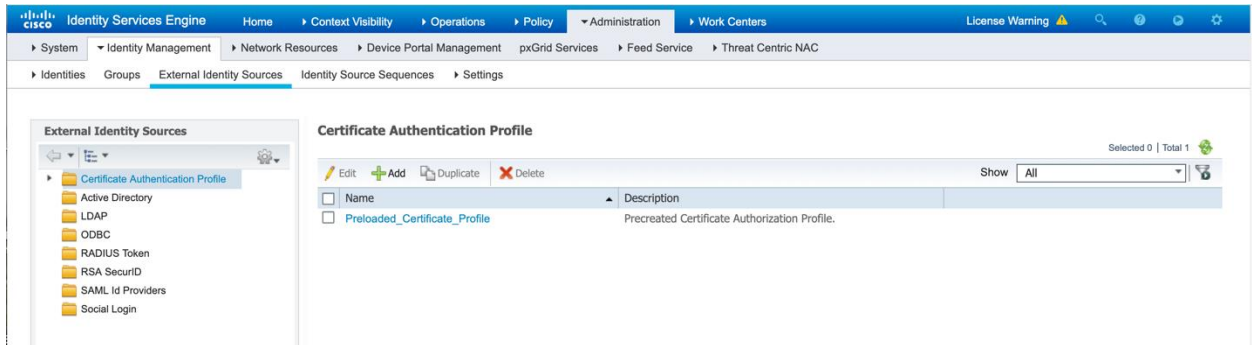
3.2 Configure How ISE Extracts the Identity from the EAP-TLS X.509 client certificate

- The purpose of the Certificate Authentication Profile is to inform ISE which certificate field the identity (machine or user) can be found on the client certificate (end-identity certificate) presented to ISE during EAP-TLS (also during other certificate-based authentication methods).
- From ISE GUI, navigate to the Menu: **Administration > Identity Management > External Identity Sources**

ISE Configuration for EAP-TLS Server



- In the Left-Side Navigation, click on **Certificate Authentication Profile** folder



- Add a new Certificate Authentication Profile by clicking on the **Add** button

Certificate Authentication Profiles List > [New Certificate Authentication Profile](#)

Certificate Authentication Profile

* Name

Description

Identity Store ⓘ

Use Identity From Certificate Attribute ⓘ
 Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only) ⓘ

Match Client Certificate Against Certificate In Identity Store ⓘ Never
 Only to resolve identity ambiguity
 Always perform binary comparison

- Complete the following fields:
 - Name
 - Use Identity From: selected radio button for Certificate Attribute, pull down the selection where the identity will be obtained from in the EAP-TLS Client certificate.
 - Optionally: Add a Description
 - Leave Identity Store as default value of [not applicable]
 - Match Client Certificate Against Certificate in Identity Store: Keep default value with selected radio button for **“Never”**.
- Click the **Submit** button save the Certificate Authentication Profile.

Use Identity From is used to choose the certificate attribute from which a specific field the identity can be found. The choices are:

Subject - Common Name
Subject Alternative Name
Subject - Serial Number
Subject
Subject Alternative Name - Other Name
Subject Alternative Name - EMAIL
Subject Alternative Name - DNS

EXAMPLE: EAP-TLS Client Certificate Identity is in the Subject Alternative Name – Other Name User Principal Name.

Certificate Authentication Profiles List > [New Certificate Authentication Profile](#)

Certificate Authentication Profile

* Name

Description

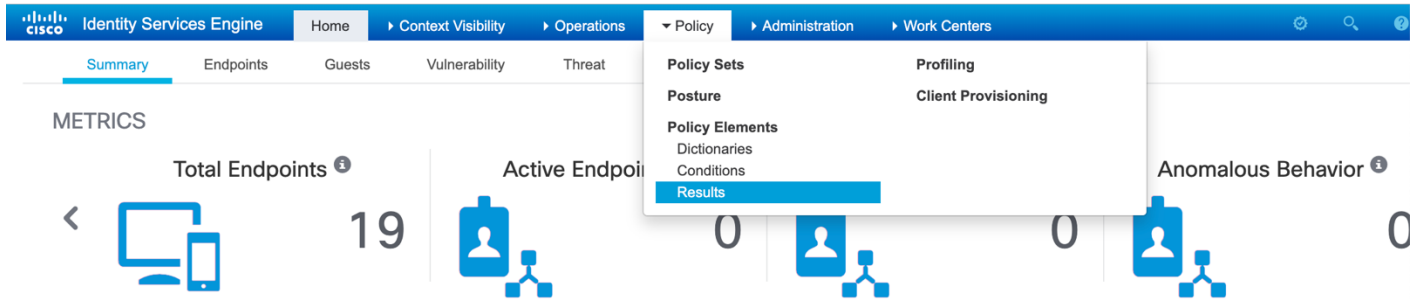
Identity Store

Use Identity From Certificate Attribute Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

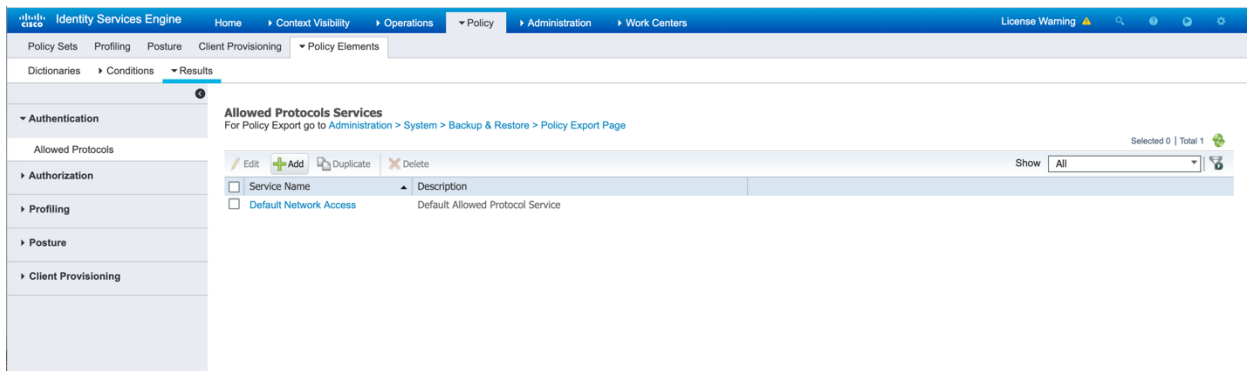
Match Client Certificate Against Certificate In Identity Store Never Only to resolve identity ambiguity Always perform binary comparison

3.3 Configure ISE EAP Server to only support EAP-TLS and require the RADIUS Message-Authenticator

- Authentication and Authorization Policies are created from the ISE GUI, choose **Policy > Policy Sets**. These are enabled by default on ISE 3.x.
- When you install ISE, there is always one Policy Set defined, which is the default Policy Set.
- The default Policy Set contains predefined and default authentication, authorization, and exception policy rules.
- Navigate to the Menu: **Policy > Policy Elements > Results**




- On the Left-Side Navigation, select Authentication > Allowed Protocols
- The Allowed Protocols Service enables only that authentication methods/protocols which ISE supports during RADIUS Authentication.









- Add a new Allowed Protocols services profile by clicking the 'Add' button

Allowed Protocols Services

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

Selected 0 | Total 1 

 Edit	 Add	 Duplicate	 Delete	Show	All 	
<input type="checkbox"/>	Service Name					Description

- Fill in the following mandatory fields: Name, check the checkbox EAP-TLS only protocol, and check the checkbox Require Message-Authenticator for all RADIUS Requests.
- All other checkboxes are unchecked.
- Optionally add a Description
- Click the 'Submit' button to persist the changes. NOTE: When editing an Allowed Protocols page, click the 'Save' button to persist the changes.
- NOTE: When editing an Allowed Protocols page, click the 'Save' button to persist the changes.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Allowed Protocols Services List > **New Allowed Protocols Service**

Allowed Protocols

Name: EAP_TLS_only

Description: Only allow EAP-TLS Authentication method and require Message-Authenticator

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 Authentication of expired certificates to allow certificate renewal in Authorization Policy

Enable Stateless Session Resume

Session ticket time to live: 2 Hours

Proactive session ticket update will occur after 10 % of Time To Live has expired

Allow LEAP

Allow PEAP

Allow EAP-FAST

Allow EAP-TTLS

Preferred EAP Protocol: LEAP

EAP-TLS L-bit

Allow weak ciphers for EAP





Require Message-Authenticator for all RADIUS Requests



Submit Cancel

- Before continuing, wait until you see the green confirmation notification message in the lower right corner

Allowed Protocols Services

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

 Edit	 Add	 Duplicate	 Delete
<input type="checkbox"/> Service Name	Description		
<input type="checkbox"/> Default Network Access	Default Allowed Protocol Service		
<input type="checkbox"/> EAP_TLS_only	Only allow EAP-TLS Authentication method and require Message-Authe...		

 Server Response
EAP_TLS_only was successfully created 

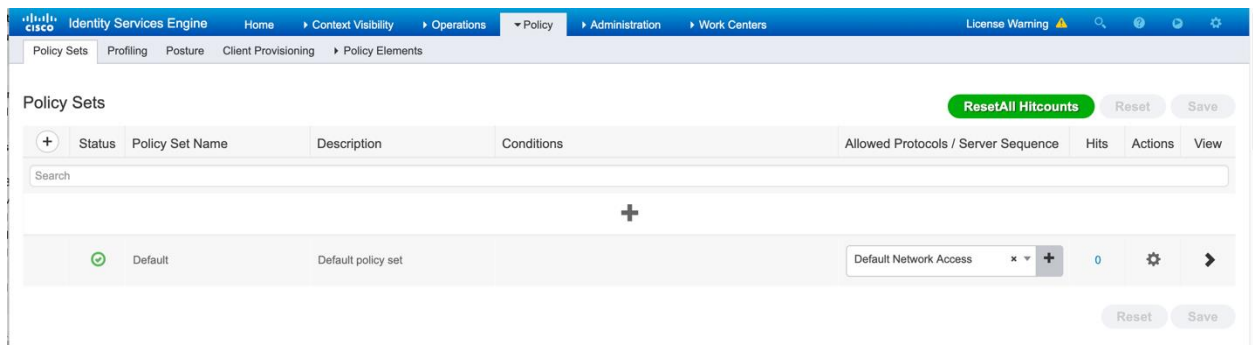
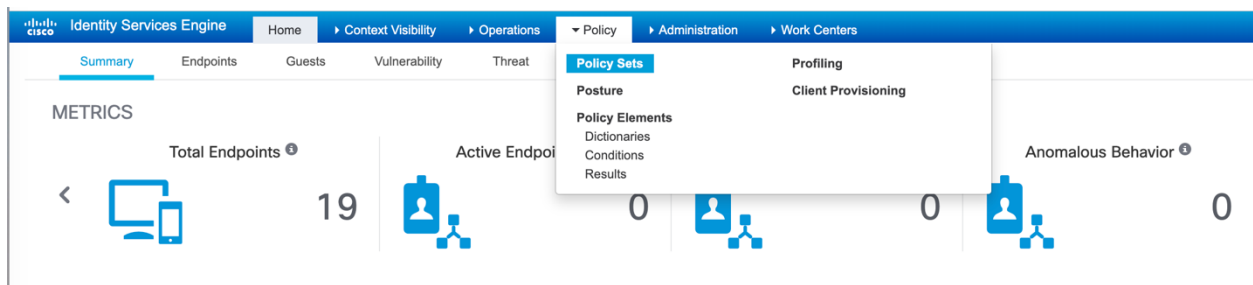
3.4 Apply the settings into the Authentication Policy and Authorization.

ISE groups the Authentication Policy and Authorization Policy into Policy Sets.

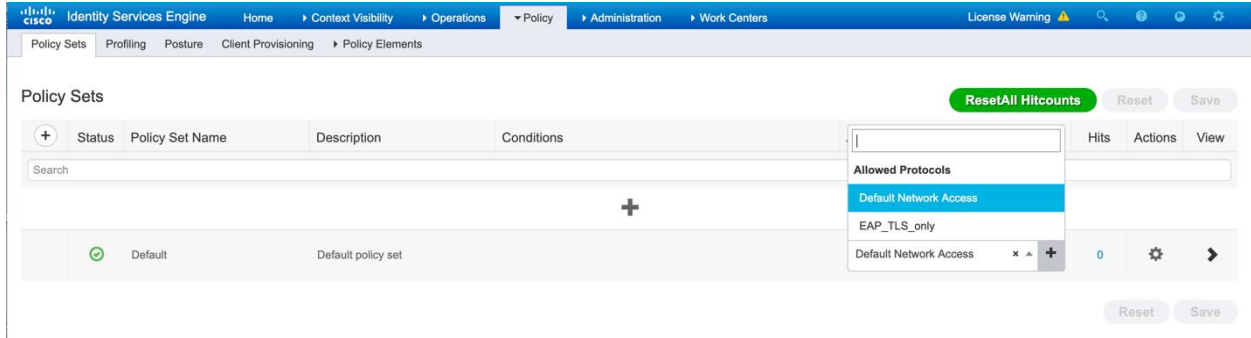
Authentication and Authorization Policies are created from the ISE GUI, choose Policy > Policy Sets. These are enabled by default on ISE 3.x.

When you install ISE, there is always one Policy Set defined, which is the default Policy Set. The default Policy Set contains predefined and default authentication, authorization, and exception policy rules.

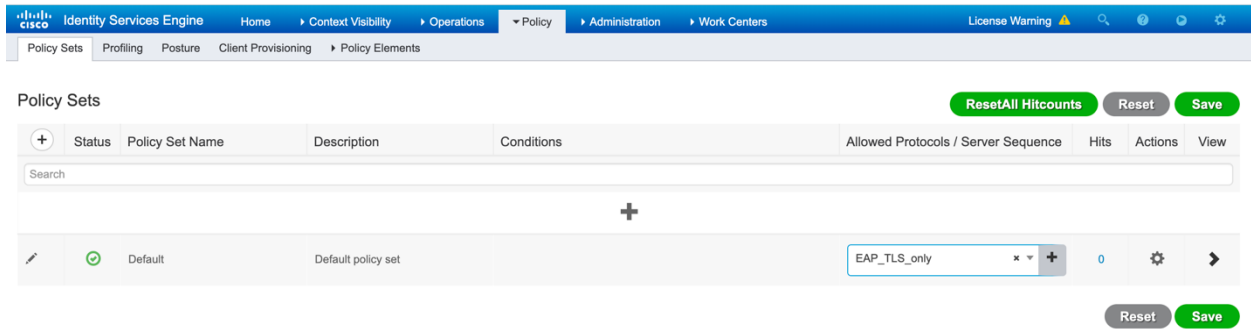
- In order to create a Policy Set from the ISE GUI, navigate to Policy > Policy Set and then click the plus (+) icon in the upper-left corner, as shown in this image.



- For the Default Policy Set, replace the Allowed Protocols pulldown menu with the value created in steps above
- Click on the Allowed Protocols Pulldown arrow.



- Select the Allowed Protocols pulldown and select the name of the Allowed Protocols setting created



- Click on the Save button to persist the changes.

3.5 Add Authentication Policy Rule for EAP-TLS

Inside the Policy Set, the Authentication Policy will bind/combine these policy elements previously configured to be used with conditions to determine when an Authentication Rule is to be matched.

- At the end of step in the Policy > Policy Sets page
- Click on the > button in the Default policy set row

ISE Configuration for EAP-TLS Server

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Default	Default policy set		EAP_TLS_only	0	⚙️	➔

- The Authentication Policy and Authorization Policy rules are now present.

Policy Sets → Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
+	Default	Default policy set		EAP_TLS_only	0

➤ Authentication Policy (3)

➤ Authorization Policy - Local Exceptions

➤ Authorization Policy - Global Exceptions

➤ Authorization Policy (12)

- Click the > Authentication Policy to expand the rules.

Policy Sets → Default

Status	Rule Name	Conditions	Use	Hits	Actions
+	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints	0	⚙️
+	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores	0	⚙️
+	Default		All_User_ID_Stores	0	⚙️



- For the Row with Rule Name Dot1X click the gear icon on the far right then select the Insert new row above

The screenshot displays the Cisco ISE Policy Sets configuration interface. At the top, there are navigation tabs for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Below the navigation, the 'Policy Sets' section is active, showing a table of Authentication Policies. The table has columns for Status, Rule Name, Conditions, Use, Hits, and Actions. The 'Dot1X' rule is selected, and a context menu is open over its 'Actions' column, with 'Insert new row above' highlighted. The table lists rules: MAB (Wired_MAB, Wireless_MAB), Dot1X (Wired_802.1X, Wireless_802.1X), and Default (All_User_ID_Stores). The 'Use' column shows 'Internal Endpoints' for MAB, 'All_User_ID_Stores' for Dot1X, and 'All_User_ID_Stores' for Default. The 'Hits' column shows 0 for all rules. The 'Actions' column shows a gear icon for each rule.

- A new rule named “Authentication Rule 1” is created above the Rule name Dot1X as shown in the below screenshot.

ISE Configuration for EAP-TLS Server

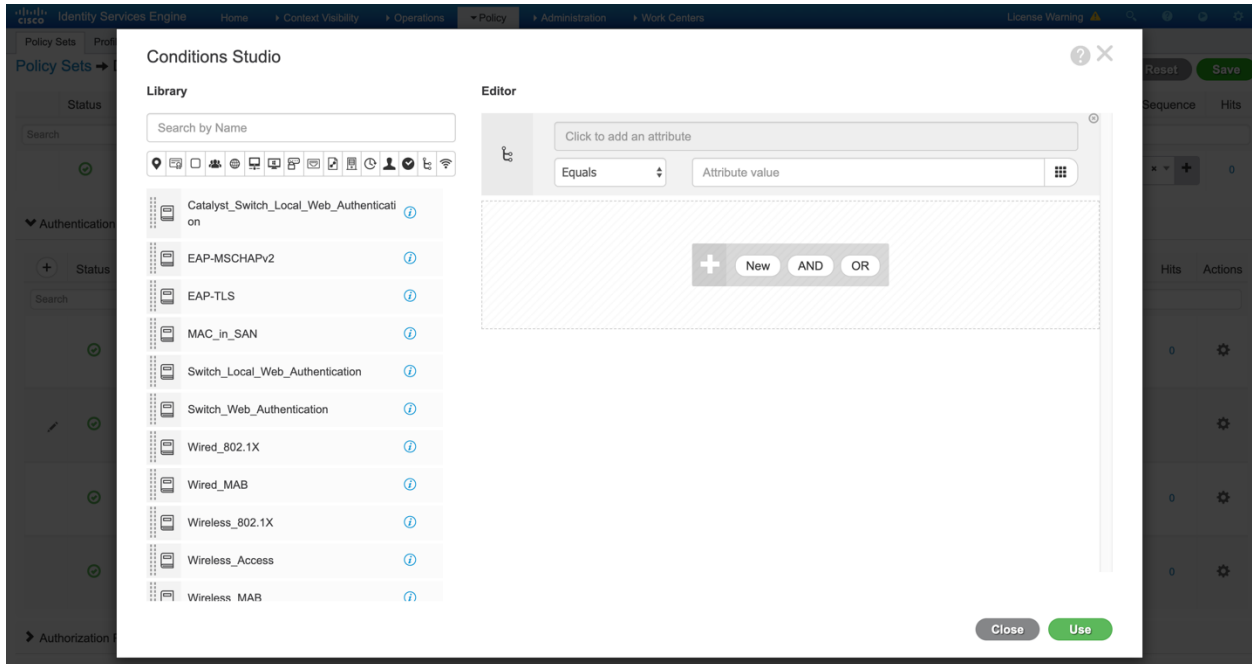
The screenshot shows the ISE configuration interface for Policy Sets. The top navigation bar includes "Policy Sets", "Profiling", "Posture", "Client Provisioning", and "Policy Elements". The main heading is "Policy Sets → Default". On the right, there are buttons for "ResetAll Hitcounts", "Reset", and "Save". Below this is a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. A search bar is present above the table. The table lists a "Default" policy set. Below this, the "Authentication Policy (4)" section is expanded, showing a table with columns: Status, Rule Name, Conditions, Use, Hits, and Actions. The table contains four rows: "MAB" with conditions "Wired_MAB" and "Wireless_MAB"; "Authentication Rule 1" with a plus sign in the Conditions column; "Dot1X" with conditions "Wired_802.1X" and "Wireless_802.1X"; and "Default". Each row has a "Use" dropdown menu and an "Options" link.

- Edit the name of the Authentication Rule: Click on the “Authentication Rule 1” text and edit it to a descriptive name as shown below.

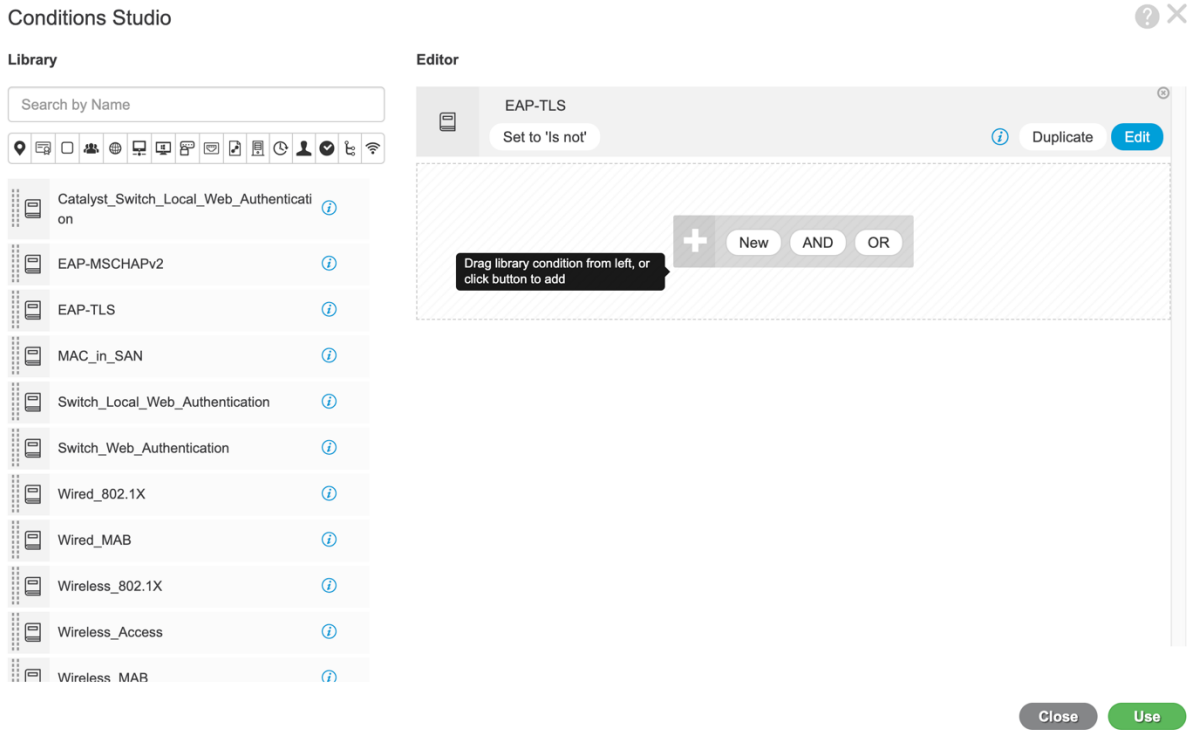
This screenshot is similar to the previous one, but the rule name in the "Authentication Policy" table has been updated to "EAP_TLS_Dot1X". The "Conditions" column for this rule now contains a plus sign (+) instead of the text "Authentication Rule 1". The rest of the interface, including the navigation bar, buttons, and other table rows, remains the same.

- Add a condition to the EAP-TLS Authentication Rule by clicking the + icon in the Conditions column.

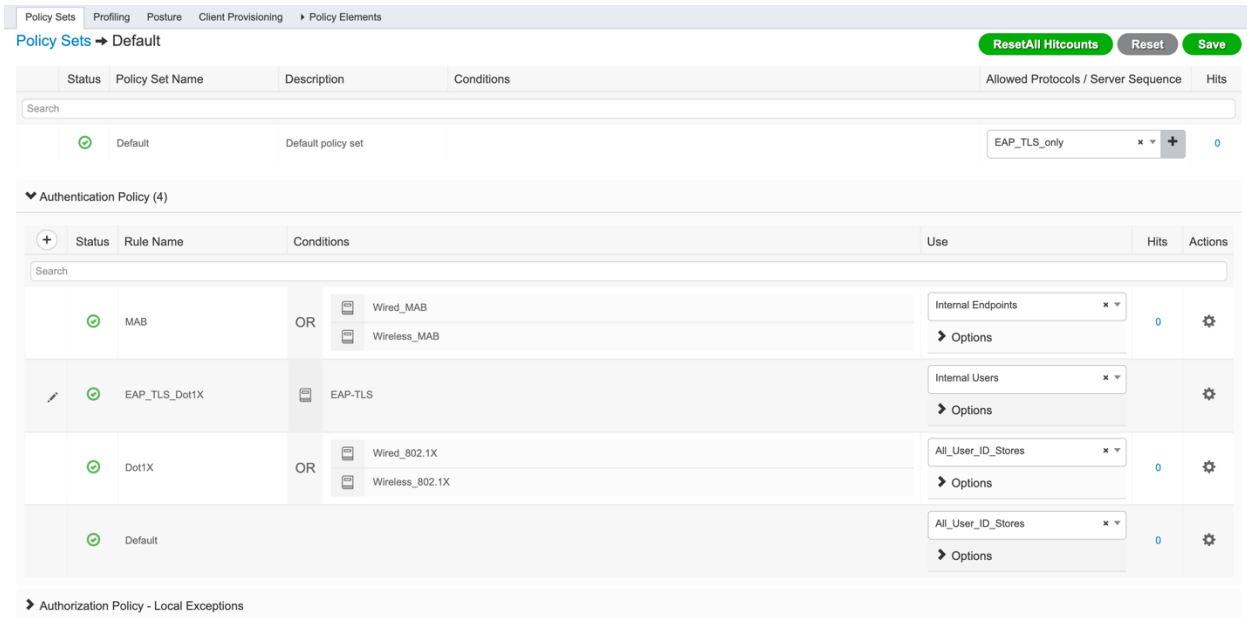
- The Conditions Studio window appears as shown below.



- Set the rule to match when EAP-TLS authentications occur by dragging the EAP-TLS item under the Library column into the Editor.



- Click the Use button to save the condition
- The Policy Set rule now contains the Rule Name and Condition.

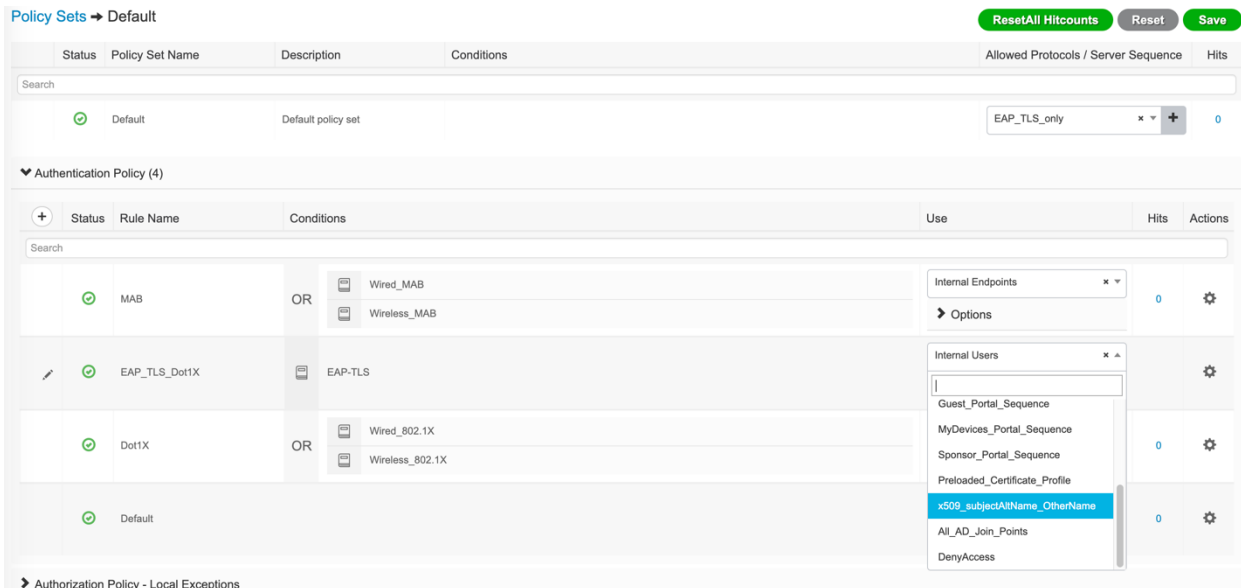


- Modify the Use column to specify where to extract the X.509 Certificate Identity from for the EAP-TLS authentication.

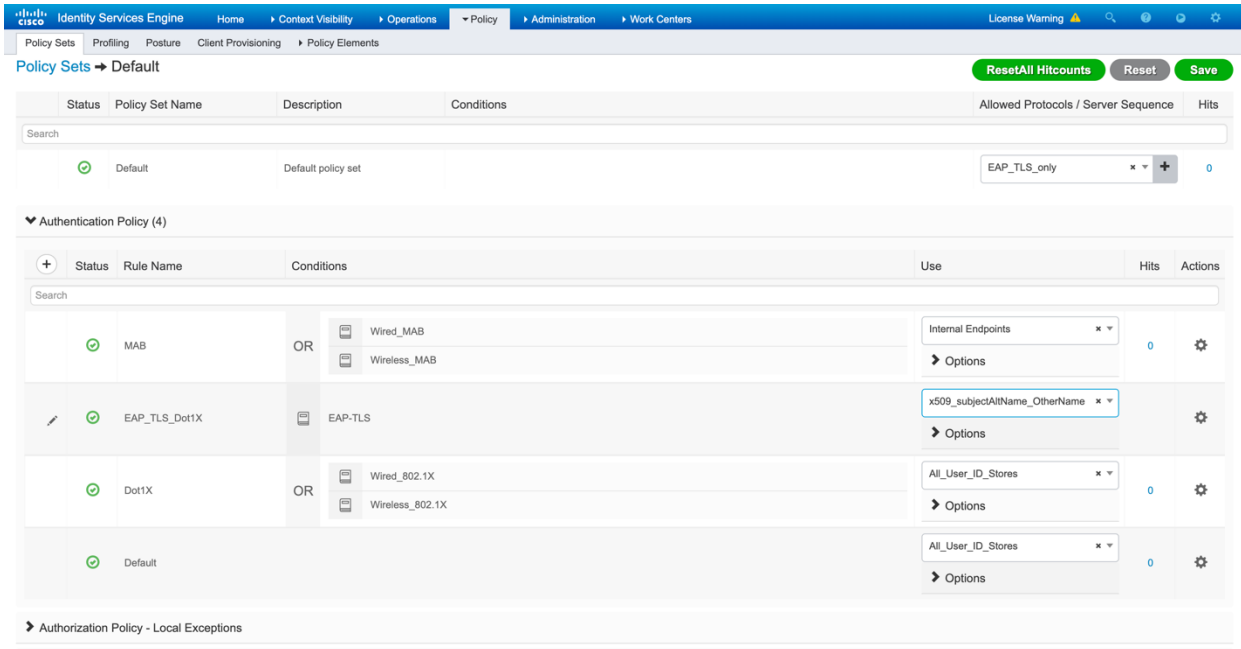
Under the Use column for the Rule Name EAP_TLS_Dot1X click on the triangle to the right of the Internal Users value



- Then pull down, scroll down, and select the name of the Certificate Authentication Profile name created at the end of Step 3.2.

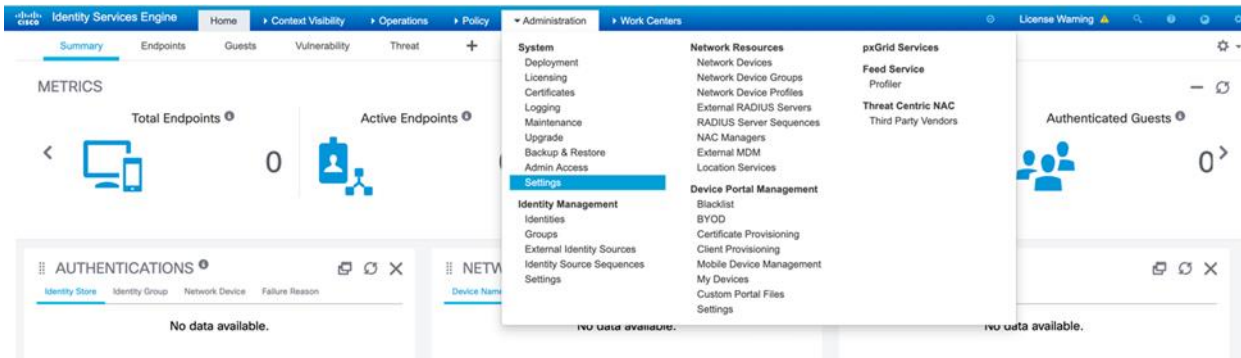


- Click the name of the Certificate Authentication Profile x509_subjectAltName_OtherName to select the value.
- The page will appear as follows.
- Click the Save button in the upper right corner to persist the changes.

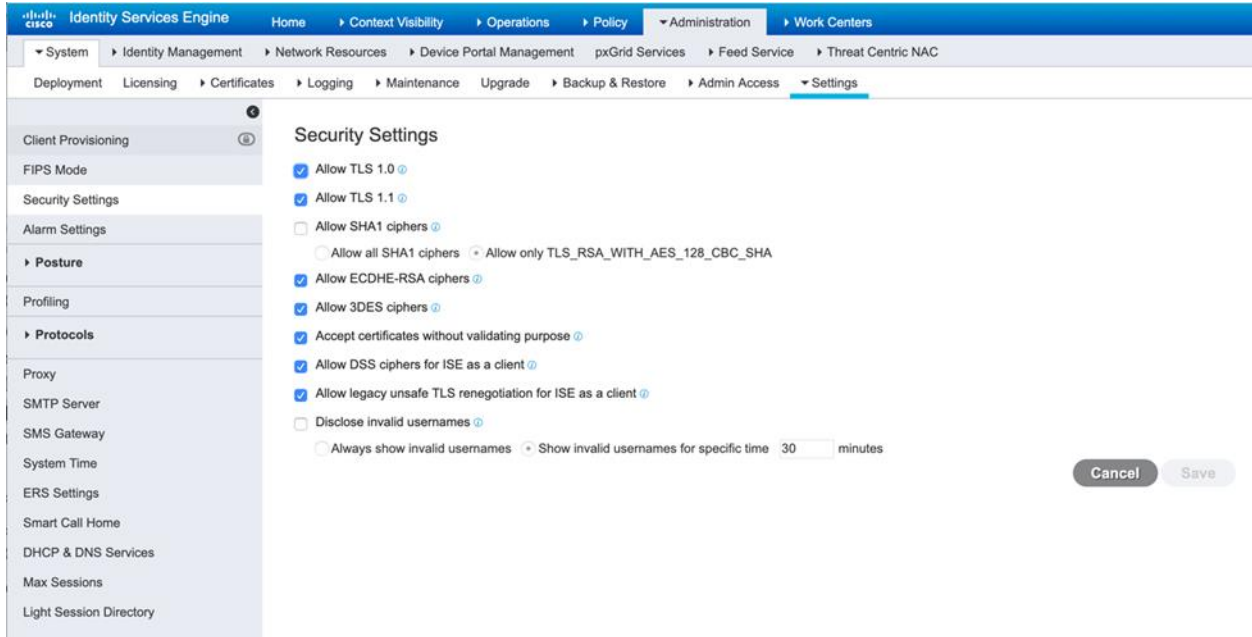


3.6 Security Settings hardening to restrict support only for TLS version 1.2, and support the strongest security cipher suites as described in our claims.

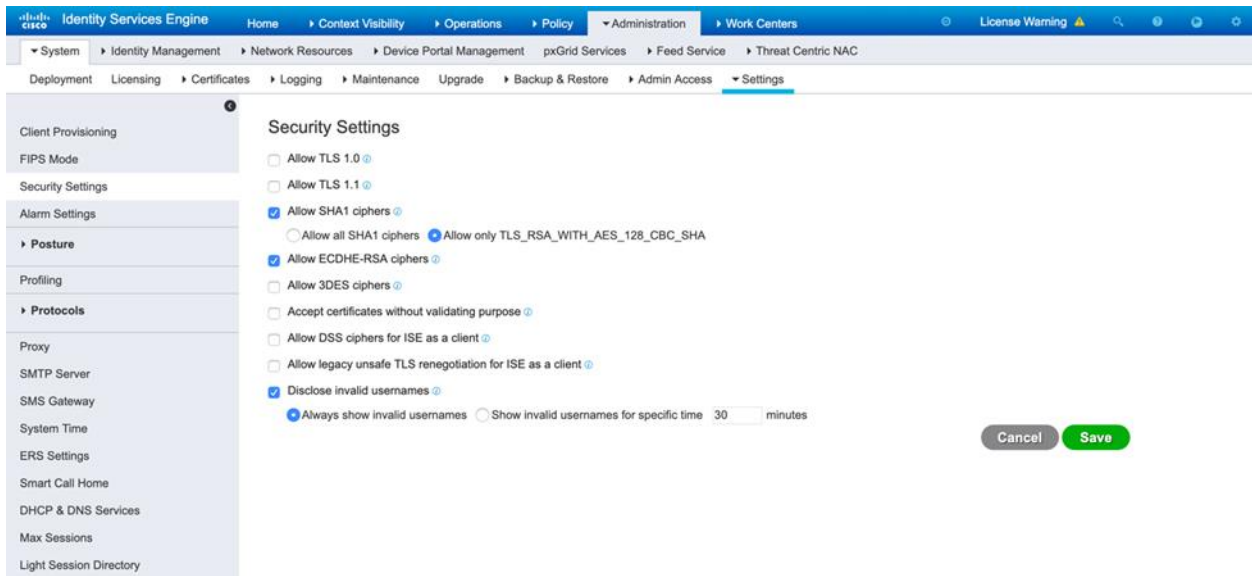
- Navigate to Menu: Administration > System > Settings



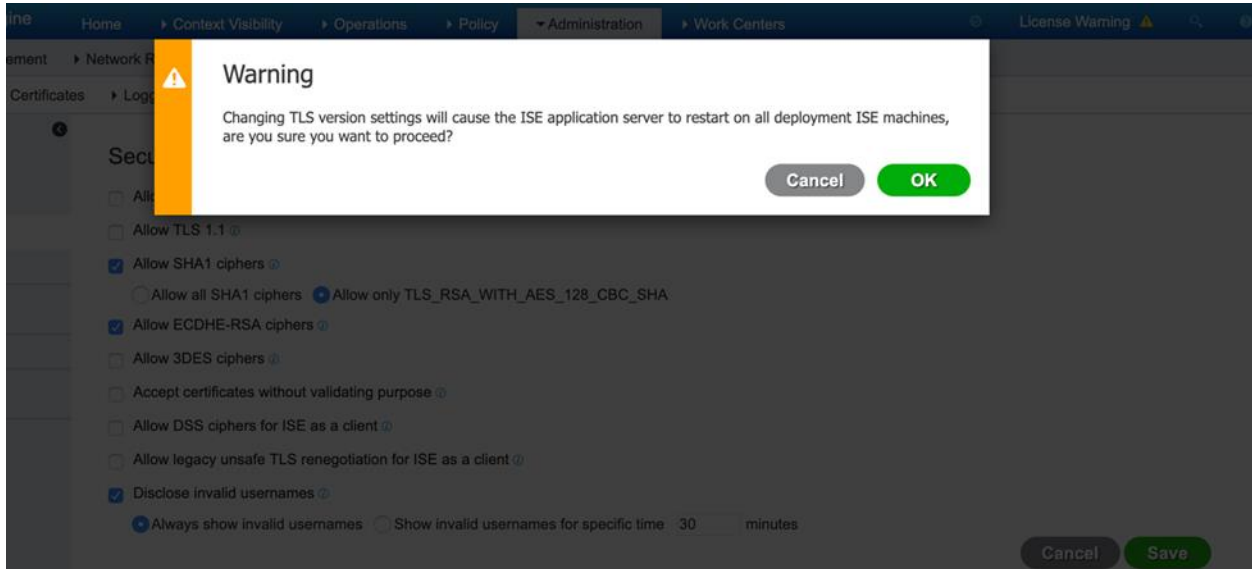
- Click on the Security Settings. The default values are shown below.



- Modify the security settings to match the Security Target claims
 - Uncheck all checkboxes as shown in the below image.
 - Check all checkboxes and radio buttons as shown in the below image.
- Click the Save button to persist the changes.



- Click the OK button for the warning box that notifies that the ISE services will restart because of the changes requested.



- Wait for the ISE Application Server service to restart.
- To monitor whether ISE Application Server has restarted, login to the ISE command line interface (CLI) as an admin-role user.
- Run the command: show application status ise

ise-vnd/foobar# **show application status ise**

```
-----
Database Listener      running      1945
Database Server       running      73 PROCESSES
Application Server     initializing
.
.
.
```

- When the Application Server is in the running state, the service has come back up after the automatic restart.
- This restart will take approximately 5-10 minutes.
- The output of the show application status ise will appear similar to the following when all services are up.

```
ise-vnd/foobar# show application status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	1945
Database Server	running	94 PROCESSES
Application Server	running	2525
Profiler Database	running	3704
ISE Indexing Engine	running	4619
AD Connector	running	13210
M&T Session Database	running	3483
M&T Log Processor	running	29242
Certificate Authority Service	running	12940
EST Service	running	21106
SXP Engine Service	disabled	
Docker Daemon	running	4580
TC-NAC Service	disabled	

Wifi Setup Helper Container	disabled	
pxGrid Infrastructure Service	disabled	
pxGrid Publisher Subscriber Service	disabled	
pxGrid Connection Manager	disabled	
pxGrid Controller	disabled	
PassiveID WMI Service	disabled	
PassiveID Syslog Service	disabled	
PassiveID API Service	disabled	
PassiveID Agent Service	disabled	
PassiveID Endpoint Service	disabled	
PassiveID SPAN Service	disabled	
DHCP Server (dhcpd)	disabled	
DNS Server (named)	disabled	
ISE Messaging Service	running	5271

4 X509 Certificate Configuration

Below sections describe how the X.509 certificates are configured for the Test VM and TOE.

4.1 X509 certificate for TOE

- **Create a self-signed CA certificate with the help of XCA application**

Open the certificate tab and click the “New Certificate” button on the right.

For each tab:

- Source:
 - Select “Create a self-signed certificate”
 - Change the Signature Algorithm to SHA256
 - Click “Apply All”.
- Subject
 - Fill the distinguished name as per the requirement
 - Click “Generate a new key”. Create the key.
- Extension
 - Select “Type” as Certificate Authority
 - Select “Key identifier” as Subject Key Identifier
 - Select “Key identifier” as Authority Key Identifier
 - Make sure the dates are acceptable.
 - Add the X509v3 Key Usage for Digital Signature, Certificate Sign and Key Agreement

- Add the Extended X509v3 Key Usage for TLS Web Server Authentication and TLS Web Client Authentication
- Add Netscape Cert Type for SSL Client, SSL Server, SSL CA, S/MIME CA, Object Signing CA

Click “OK” to create the certificate.

When it prompts for a response about the certificate being valid for longer than the signer, click “adjust data and continue”.

- **Create intermediate CA certificate signed by the above CA with the help of XCA application**

Open the certificate tab and click the “New Certificate” button on the right.

For each tab:

- Source:
 - Select “Use this certificate for signing” and choose “CA
 - Change the Signature Algorithm to SHA256
 - Click “Apply All”.
- Subject
 - Fill the distinguished name as per the requirement
 - Click “Used keys too”. Select the key generated for CA
- Extension
 - Select “Type” as Certificate Authority
 - Select “Key identifier” as Subject Key Identifier
 - Select “Key identifier” as Authority Key Identifier
 - Make sure the dates are acceptable.
 - Add the X509v3 Key Usage for Digital Signature, Certificate Sign and Key Agreement

- Add the Extended X509v3 Key Usage fo TLS Web Server Authentication and TLS Web Client Authentication
- Add Netscape Cert Type for SSL Client, SSL Server, SSL CA, S/MIME CA, Object Signing CA

Click “OK” to create the certificate.

When it prompts for a response about the certificate being valid for longer than the signer, click “adjust data and continue”.

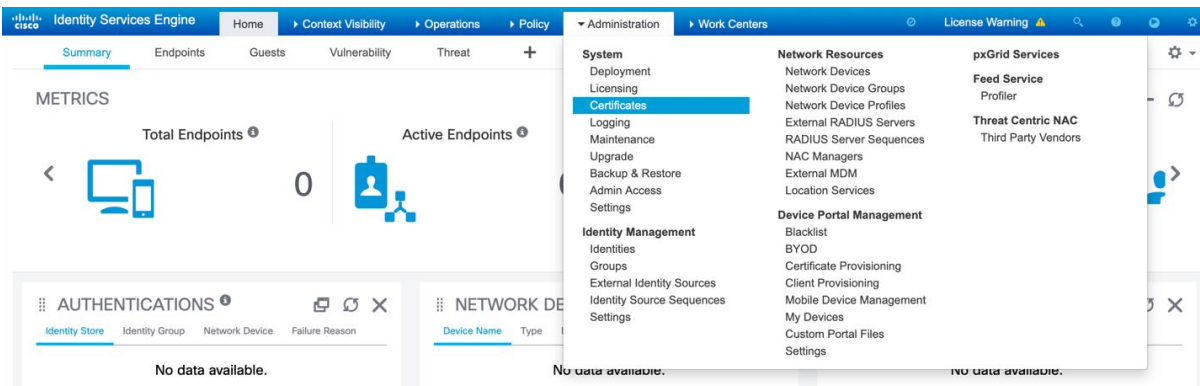
• **Generate a Certificate Signing Request from ISE**

The first step is to generate a Certificate Signing Request (CSR) from ISE and submit it to the CA (server) in order to obtain the signed certificate issued to ISE, as a System Certificate.

This certificate will be presented as a Server Certificate by ISE during EAP-TLS authentication.

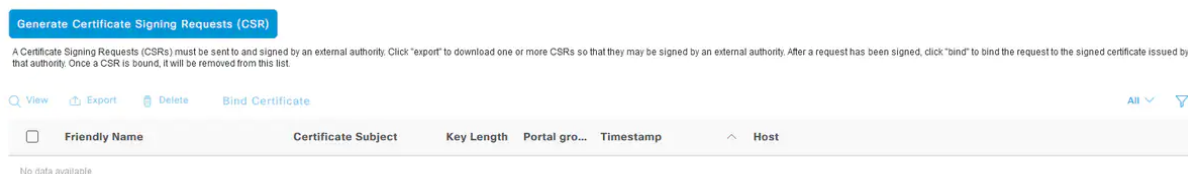
This is performed in the ISE GUI.

Navigate to Administration > System: Certificates > Certificate Management > Certificate Signing Requests.



Under Certificate Signing Requests, click Generate Certificate Signing Requests (CSR) as shown in this image.

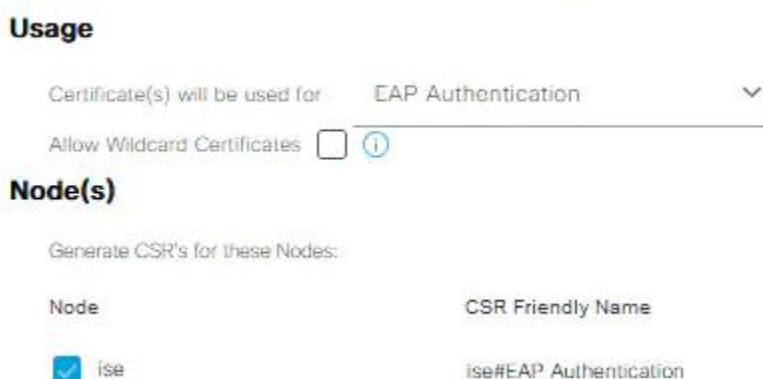
Certificate Signing Requests



On the Certificate Signing Request (CSR) form, choose these options in order to complete the CSR and obtain its contents:

Certificate Usage, for this configuration example choose EAP Authentication.

This is an example of a completed CSR form, created using a wildcard statement.



If you plan to utilize a wildcard statement in the certificate, *.example.com, then you must also check the Allow Wildcard Certificate check box.

The best location is the Subject Alternative Name (SAN) certificate field for compatibility for any usage and across multiple different type of endpoint operating systems that might be present in the environment.

Subject: This includes the Common Name (CN), Organizational Unit (OU), Organization (O), City (L), State (ST), and Country (C) certificate fields.

The \$FQDN\$ variable is the value that represents the management Fully Qualified Domain Name (hostname + domain name) associated with each ISE node.

Subject

Common Name (CN)
\$FQDN\$ ⓘ

Organizational Unit (OU)
ⓘ

Organization (O)
Example Company ⓘ

City (L)
San Jose

State (ST)
California

Country (C)
US

The Subject Alternative Name (SAN) fields are also to be completed in order to include any required and desired information to be used to establish trust. As a requirement, you will need to define the DNS Entry that points to the FQDN of the ISE node(s) which will be associated to this certificate, after the certificate has been signed.

Subject Alternative Name (SAN)

⋮	DNS Name	ise.example.com	-	+	
⋮	DNS Name	ise2.example.com	-	+	
⋮	DNS Name	ise3.example.com	-	+	ⓘ

Ensure that the define the appropriate "Key Type", "Key Length", and "Digest to Sign With" that conforms to the capabilities of the CA Server(s) and with good security practices in mind. Default values are: RSA, 4096 bits, and SHA-384, respectively. Available choices and compatibility will be displayed in this page within the ISE Admin UI.

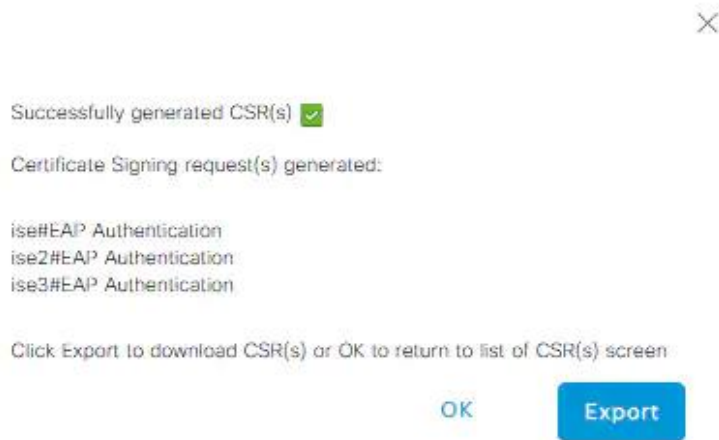
* Key type
RSA ▼ ⓘ

* Key Length
4096 ▼ ⓘ

* Digest to Sign With
SHA-384 ▼

Certificate Policies

In order to save the CSR, click Generate. Click Export, located at the bottom right-hand side, in order to export the CSR file(s) from this prompt:



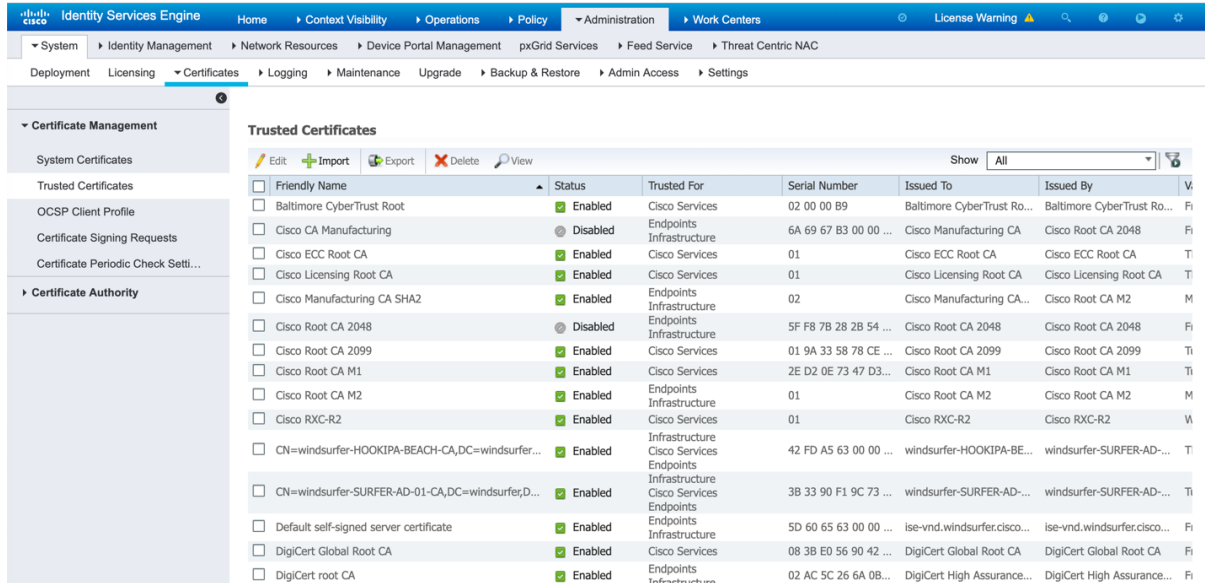
Sign the CSR using the intermediate CA created above and export the file in .pem format

- **Import CA Certificates into ISE**

After the CA returns the signed certificate, it will also include the full CA chain comprised of a root certificate and one/multiple intermediary certificates.

The ISE Admin UI will enforce you to import all certificates in the CA chain first, prior to association or upload of any system certificates.

In order to import the root certificate into ISE GUI, navigate to Administration > System: Certificates > Certificate Management



Click Import button, Browse to the Certificate Authority Certificate in PEM or DER format

Import a new Certificate into the Certificate Store

* Certificate File No file chosen

Friendly Name

Trusted For: ⓘ

Trust for authentication within ISE

Trust for client authentication and Syslog

Trust for authentication of Cisco Services

Validate Certificate Extensions

Description

- Check the following check boxes:
 - Trust for authentication within ISE
 - Trust for client authentication and syslog
- Validate Certificate Extensions
- Optionally enter a Friendly Name and Description

Import a new Certificate into the Certificate Store

* Certificate File TrustAnchorRo...tificate.crt

Friendly Name ⓘ

Trusted For: ⓘ

Trust for authentication within ISE

Trust for client authentication and Syslog

Trust for authentication of Cisco Services

Validate Certificate Extensions

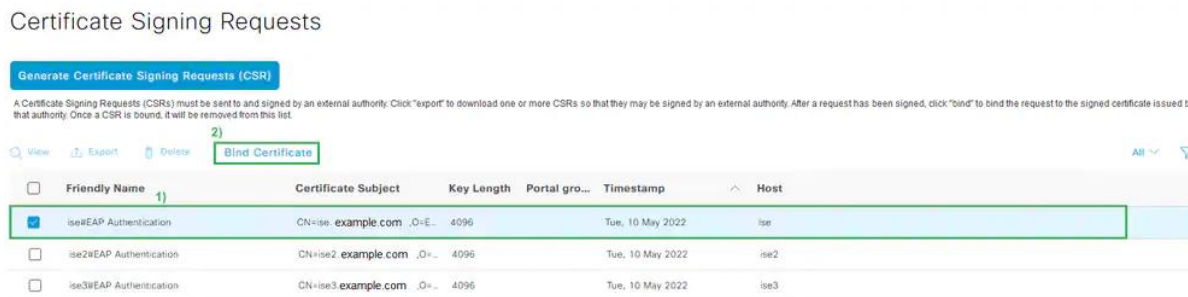
Description

Click on the Submit button to persist the changes.

Repeat the previous step for each Intermediary Certificate(s) as part of the CA certificate chain.

Once all certificates, as part of the full CA chain, are imported into the Trusted Certificates store in ISE, return to the ISE GUI and navigate to Administration > System: Certificates > Certificate Management: Certificate Signing Requests.

Locate the CSR entry under Friendly Name that corresponds to the signed certificate, click the certificate's check box, and then click Bind Certificate.



On the next page, click Browse and choose the signed certificate file, define a desired Friendly Name, and choose the Certificate Usage(s). Submit to save the changes.

Bind CA Signed Certificate

* Certificate File EXAMPLE_ISE.cer

Friendly Name ⓘ

Validate Certificate Extensions ⓘ

Usage

EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

At this time, the signed certificate is moved to the ISE GUI. Navigate to Administration > System: Certificates > Certificate Management: System Certificates and assign to the same node which the CSR was created for.

4.2 X509 certificate for VM

- **Create a End Entity certificate for VM using XCA application**

Open the certificate tab and click the “New Certificate” button on the right.

For each tab:

- Source:
 - Select “Use this certificate for signing” and choose “CA”
 - Change the Signature Algorithm to SHA256
 - Click “Apply All”.
- Subject
 - Fill the distinguished name as per the requirement
 - Click “Generate a new key”. Create the key.
- Extension
 - Select “Type” as End Entity
 - Select “Key identifier” as Subject Key Identifier
 - Make sure the dates are acceptable.
 - Select X509v3 Subject Alternate Name as IP Address or FQDN
 - Add the X509v3 Key Usage for Digital Signature, Certificate Sign and Key Agreement
 - Add the Extended X509v3 Key Usage fo TLS Web Server Authentication and TLS Web Client Authentication
 - Add Netscape Cert Type for SSL Client and SSL Server

Click “OK” to create the certificate.

When it prompts for a response about the certificate being valid for longer than the signer, click “adjust data and continue”.

Note: Sign the certificate with the same CA certificate which we used to sign the TOE certificate

5 Configuration of the Authenticator (Switch)

Global Configuration Settings for Classic IOS and IOS 15.x Switches

- **Set the DNS domain name on the switch.**

Cisco IOS does not allow for certificates, or even self-generated keys, to be created and installed without first defining a DNS domain name on the device.

Type **ip domain-name** domain-name at the global configuration prompt.

- **Enable AAA on the access switch(es).**

By default, the AAA subsystem of the Cisco switch is disabled. Prior to enabling the AAA subsystem, none of the required commands are available in the configuration. Enable AAA as follows:

```
C3560X(config)# aaa new-model
```

- **Create an authentication method for 802.1X.**

An authentication method is required to instruct the switch to use a particular group of RADIUS servers for 802.1X authentication requests. Create the authentication method as follows:

```
C3560X(config)# aaa authentication dot1x default group radius
```

- **Create an authorization method for 802.1X.**

The method created enables the user/device identity (username/password or certificate) to be validated by the RADIUS Server. However, simply having valid credentials is not enough. An authorization is also required. The authorization is what defines that the user or device is actually allowed to access the network, and what level of access is actually permitted. Create the authorization method as follows:

```
C3560X(config)# aaa authorization network default group radius
```

- **Create an accounting method for 802.1X.**

RADIUS accounting packets are extremely useful, and in many cases are required. These types of packets ensure that the RADIUS server (Cisco ISE) knows the exact state of the switch port and endpoint.

Create the accounting method as follows:

```
C3560X(config)# aaa accounting dot1x default start-stop group radius
```

```
C3560X(config)# aaa accounting exec default start-stop group ISE
```

```
C3560X(config)# aaa accounting system default start-stop group ISE
```

- **Configure periodic RADIUS accounting updates**

Periodic RADIUS accounting packets allow Cisco ISE to track which sessions are still active on the network. The following command configures periodic updates to be sent whenever there is new information, as well as a periodic update once per 24 hours (1440 minutes) to show ISE that the session is still alive:

```
C3560X(config)# aaa accounting update newinfo periodic 1440
```

- **Configure a user**

Within global configuration mode, add a username and password for the RADIUS keepalive, which is proactively checking the online status of the RADIUS server.

```
C3560X(config)# username username password password
```

- **Add the Cisco ISE servers to the RADIUS group.**

```
Cat3560X(config)# aaa group server radius server-name
```

```
Cat3560X(config-radius-server)# server-private ise_ip address auth-port 1812
```


acct-port 1813 key shared-secret

```
Cat3560X(config-radius-server)# ip radius source-interface name
```

- **Set the dead criteria**

```
Cat3560X(config)# radius-server dead-criteria time 5 tries 3
```

```
Cat3560X(config)# radius-server deadtime 15
```

- **Enable Change of Authorization (CoA)**

```
C3560X(config)# aaa server radius dynamic-author
```

```
C3560X(config-locsvr-da-radius)# client ise_ip_address server-key
shared_secret
```

```
C3560X(config-locsvr-da-radius)# auth-type any
```

- **Configure the switch to use the Cisco vendor-specific attributes (VSA).**

```
C3560X(config)# radius-server vsa send authentication
```

```
C3560X(config)# radius-server vsa send accounting
```

```
C3560X(config)# radius-server attribute 6 on-for-login-auth
```

```
C3560X(config)# radius-server attribute 8 include-in-access-req
```

```
C3560X(config)# radius-server attribute 25 access-request include
```

```
C3560X(config)# radius-server attribute 4 switch_ip address
```

```
C3560X(config)# radius-server attribute 2 length maximum 240
```

- **Enable 802.1X globally on the switch.**

```
C3560X(config)# dot1x system-auth-control
```

```
C3560X(config)# dot1x critical eapol
```

- **Enable syslog on the switch**

```
C3560X(config)# Logging console
```

- **Configure Interfaces as Switch Ports**

```
Cisco3560X(config)#interface name
```

```
Cisco 3560X(config-if)#switchport access vlan name
```

```
Cisco 3560X(config-if)# switchport mode access
```

- **Set the port for Open Authentication**

```
C3560X(config-if-range)# authentication open
```

- **Set the host mode of the port.**

```
C3560X(config-if-range)# authentication host-mode multi-auth
```

- **Configure the authentication method priority on the switch ports.**

```
C3560X(config-if-range)# authentication priority dot1x
```

- **Configure the authentication method order on the switch ports**

```
C3560X(config-if-range)# authentication order dot1x
```

- **Enable the port to perform IEEE 802.1X authentication**

```
C3560X(config-if-range)# dot1x pae authenticator
```

- **Configure Authentication Timers**

```
C3560X(config-if-range)# dot1x timeout tx-period 10
```

- **Enable authentication (Optional)**

```
C3560X(config-if-range)# authentication port-control auto
```

```
C3650X(config-if-range)# authentication periodic
```

```
C3650X(config-if-range)# authentication timer reauthenticate server
```

```
C3650X(config-if-range)# authentication timer inactivity server dynamic
```

6 Configuration of the Supplicant (Test laptop)

- Create a folder and copy all the certificates (.crt) and their respective RSA keys in (.pem) format to it.
- WPA supplicant configuration file

Create a eap-tls.conf file and copy paste the following commands in it with the changes highlighted as per one's setup

```
#
=====
==
# wpa_supplicant configuration file
#
# EAP-TLS specific
#
=====
==

openssl_ciphers=AES128-SHA (Supported Ciphersuite)

update_config=1

ctrl_interface=/var/run/wpa_supplicant

# -----
# IEEE 802.1X/EAPOL version
# wpa_supplicant is implemented based on IEEE Std 802.1X-2004 which defines
# EAPOL version 2. However, there are many APs that do not handle the new
# version number correctly (they seem to drop the frames completely). In order
# to make wpa_supplicant interoperate with these APs, the version number is set
```

```
# to 1 by default. This configuration value can be used to set it to the new  
# version (2).
```

```
# to 1 by default. This configuration value can be used to set it to the new  
# version (2).
```

```
# -----
```

```
eapol_version=2
```

```
# EAP fast re-authentication
```

```
# By default, fast re-authentication is enabled for all EAP methods that  
# support it. This variable can be used to disable fast re-authentication.
```

```
# Normally, there is no need to disable this.
```

```
fast_reauth=0
```

```
network={  
    key_mgmt=IEEE8021X  
    eap=TLS  
    identity="SAN as specified in the certificate"  
    ca_cert="location of CA certificate"  
    client_cert="location of client certificate"  
    private_key="location of CA's private key"  
    eapol_flags=3  
}
```

7 Commands to execute the test

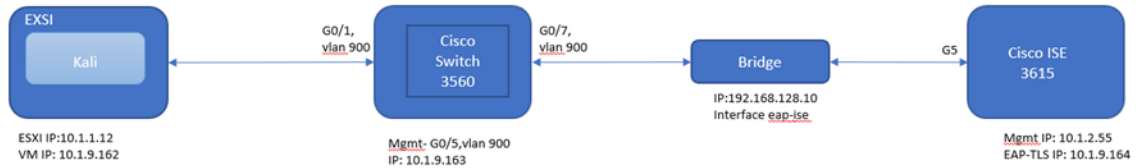
- Run the command in the directory where the conf file is saved.

```
(root@rupal)-[~/home/acumensec/Desktop]# wpa_supplicant -t -dd -Dwired -iens33 -ceap tls.conf
```

- Interpretation of the command
 - t = include timestamp in debug messages
 - d = increase debugging verbosity (-dd even more)
 - D = driver name (can be multiple drivers: nl80211,wext)
 - wired = Wired Ethernet driver
 - i = interface name
 - c = Configuration file

8 Example

- Testbed Diagram



Name	OS Version	Function	IP address	MAC Address
Cisco Switch (3560X)	IOS 15.2	Authenticator	10.1.9.163	D0:D0:FD:EF:3B:00
Bridge	Raspbian GNU/Linux 11 (bullseye) Kernel: Linux 5.15.32-v7+	Bridge	192.168.128.10	00:50:b6:e1:51:7e
Cisco ISE	3.1.0.135	Authentication Server (TOE)	10.1.9.164	b4:96:91:42:d3:93
			10.1.1.52 port 3015	
User workstation (Kali)	Linux 5.18.0-kali5-amd64	Supplicant	10.1.9.162	00:50:56:8b:04:e4
			10.1.1.12	

8.1 Configuration of the Authentication server (TOE)

ISE Configuration for EAP-TLS Server

The screenshot displays the Cisco ISE Administration console for configuring a Network Device. The breadcrumb navigation shows 'Administration > Network Resources'. The main navigation tabs include 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', and 'RADIUS Server Sequences'. The left sidebar contains 'Network Devices', 'Default Device', and 'Device Security Settings'. The configuration form includes the following fields:

- Description: [Empty text field]
- IP Address: * IP: 10.1.9.163 / 32 [Gear icon]
- Device Profile: Cisco [Dropdown arrow]
- Model Name: [Dropdown arrow]
- Software Version: [Dropdown arrow]
- Network Device Group: [Empty text field]
- Device Type: All Device Types [Dropdown arrow] [Set To Default](#)
- IPSEC: No [Dropdown arrow] [Set To Default](#)
- Location: All Locations [Dropdown arrow] [Set To Default](#)
- RADIUS Authentication Settings
 - RADIUS UDP Settings
 - Protocol: RADIUS
 - Shared Secret: [Masked] [Show](#)

ISE Configuration for EAP-TLS Server

The screenshot shows the Cisco ISE Administration console under 'External Identity Sources'. The 'Certificate Authentication Profile' configuration page is displayed for the profile named 'X509_subject_name'. The configuration includes:

- Name:** X509_subject_name
- Description:** (Empty text box)
- Identity Store:** [not applicable]
- Use Identity From:** Certificate Attribute (Selected), Subject Alternative Name
- Match Client Certificate Against Certificate In Identity Store:** Never (Selected)

The screenshot shows the Cisco ISE Administration console under 'Policy - Policy Elements'. The 'Results' tab is active, showing the configuration for the 'EAP-TLS_ONLY' policy element. The configuration includes:

- Name:** EAP-TLS_ONLY
- Description:** Only Allow EAP-TLS Authentication
- Allowed Protocols:**
 - Some protocols and options are disabled due to FIPS compliance
 - 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 Authentication of expired certificates to allow certificate renewal in Authorization Policy
 - Enable Stateless Session Resume
 - Session ticket time to live: 2 Hours
 - Proactive session ticket update will occur after: 10 % of Time To Live has expired
 - Allow LEAP
 - Allow PEAP
 - Allow EAP-FAST
 - Allow EAP-TTLS
 - Allow TEAP
 - Preferred EAP Protocol: EAP-TLS
 - EAP-TLS L-bit
 - Allow weak ciphers for EAP
 - Require Message-Authenticator for all RADIUS Requests

ISE Configuration for EAP-TLS Server

Cisco ISE Policy - Policy Sets

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	Default	Default policy set		EAP-TLS_ONLY	0		

Reset Save

Cisco ISE Policy - Policy Sets

Policy Sets -> Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions
●	Default	Default policy set		EAP-TLS_ONLY	0	

Authentication Policy (4)

Status	Rule Name	Conditions	Use	Hits	Actions
●	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	
●	EAP-TLS_DOT1X	EAP-TLS	X509_subject_name > Options	1	
●	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	0	

Authorization Policy (13)

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
●	EAP-TLS_DOT1X	EAP-TLS	PermitAccess		Select from list	1	
●	Wireless Black List Default	AND Wireless_Access IdentityGroup-Name EQUALS Endpoint Identity Groups Blacklist	Blackhole_Wireless_Ac...		Select from list	0	

ISE Configuration for EAP-TLS Server

Security Settings

- Allow TLS 1.0
- Allow TLS 1.1
- Allow SHA1 ciphers
- Allow all SHA1 ciphers Allow only TLS_RSA_WITH_AES_128_CBC_SHA
- Allow ECDHE-RSA ciphers
- Allow 3DES ciphers
- Accept certificates without validating purpose
- Allow DSS ciphers for ISE as a client
- Allow legacy unsafe TLS renegotiation for ISE as a client
- Disclose invalid usernames
- Always show invalid usernames Show invalid usernames for specific time minutes

Cancel Save

System Certificates

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
Default self-signed saml server certificate - CN=SAML_ISE3615.acumensec.local	SAML		SAML_ISE3615.acumensec.local	SAML_ISE3615.acumensec.local	Tue, 12 Oct 2021	Sun, 11 Oct 2026	Active
CN=ISE3615.acumensec.local, OU=ISE Messaging ServicesCertificate Services Endpoint Sub CA - ISE3615#00001	ISE Messaging Service		ISE3615.acumensec.local	Certificate Services Endpoint Sub CA - ISE3615	Mon, 11 Oct 2021	Mon, 12 Oct 2026	Active
CN=ISE3615.acumensec.local, OU=Certificate Services System Certificate Services Endpoint Sub CA - ISE3615#00002	pxGrid		ISE3615.acumensec.local	Certificate Services Endpoint Sub CA - ISE3615	Mon, 11 Oct 2021	Mon, 12 Oct 2026	Active
Default self-signed server certificate	Admin, Portal, RADIUS DTLS	Default Portal Certificate Group	ISE3615.acumensec.local	ISE3615.acumensec.local	Thu, 17 Feb 2022	Sat, 17 Feb 2024	Active
EAP-TLS	EAP Authentication		ISE3615.acumensec.local	EAP-TLS_I_CA	Wed, 17 Aug 2022	Tue, 25 Jul 2023	Active

ISE Configuration for EAP-TLS Server

Administration - System

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates**
- OCSP Client Profile
- Certificate Signing Request
- Certificate Periodic Check Se...

Certificate Authority

Trusted Certificates

For disaster recovery it is recommended to export and backup all your trusted certificates.

Edit Import Export Delete View

<input type="checkbox"/>	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
<input type="checkbox"/>	1#ISS-ca	Infrastructure Endpoints	0D 99 DA 6F ...	CA-ROOT	CA-ROOT	Sun, 31 Jul 2...	Mon, 31 Jul 2...	Enabled
<input type="checkbox"/>	1#ISS-ica	Infrastructure Endpoints	34 66 61 4B 8...	ICA-ROOT	CA-ROOT	Sun, 31 Jul 2...	Mon, 31 Jul 2...	Enabled
<input type="checkbox"/>	1#Bundle	Infrastructure Endpoints	3F 3D DE 11 ...	CA-Root	CA-Root	Wed, 3 Feb 2...	Mon, 3 Feb 2...	Enabled
<input type="checkbox"/>	1#Bundles	Infrastructure Endpoints	7D 3B C5 89 ...	CA-Roots	CA-Roots	Wed, 3 Feb 2...	Mon, 3 Feb 2...	Enabled
<input type="checkbox"/>	1#ICA-CERT	Infrastructure Endpoints	2A CE 2F 14 ...	ICA-Root	CA-Root	Wed, 3 Feb 2...	Mon, 3 Feb 2...	Enabled
<input type="checkbox"/>	1#EAP-TLS	Infrastructure Cisco Services Endpoints	76 6F 2C 56 2...	EAP-TLS_ICA	EAP-TLS_CA	Mon, 25 Jul 2...	Tue, 25 Jul 20...	Enabled
<input type="checkbox"/>	1#ECDSA-ICA	Infrastructure Endpoints	73 24 09 8D ...	ICA-ROOT	ICA-ROOT	Sun, 31 Jan 2...	Wed, 28 Jan ...	Enabled
<input type="checkbox"/>	1#OCSP	Infrastructure Endpoints	66 07 C7 F1 2...	ICA-OCSP-CRL	CA-OCSP-CRL	Thu, 17 Feb 2...	Fri, 17 Feb 20...	Enabled
<input type="checkbox"/>	1#OCSP-ICA-TEST	Infrastructure Endpoints	6F 45 48 D6 5...	OCSP-ICA	OCSP-ROOT	Thu, 17 Feb 2...	Fri, 17 Feb 20...	Enabled
<input type="checkbox"/>	1#SECP-CA	Infrastructure Endpoints	48 2C ED E8 ...	ECDSA-ICA	ECDSA-CA	Mon, 21 Feb ...	Tue, 21 Feb 2...	Enabled
<input type="checkbox"/>	2#Bundle	Infrastructure Endpoints	54 22 5A 1B ...	ICA-ROOT	CA-Root	Wed, 3 Feb 2...	Mon, 3 Feb 2...	Enabled
<input type="checkbox"/>	2#Bundles	Infrastructure Endpoints	5F 32 CD 18 ...	ICA-Roots	CA-Roots	Wed, 3 Feb 2...	Mon, 3 Feb 2...	Enabled
<input type="checkbox"/>	2#ICA-CERT	Infrastructure Endpoints	77 56 CA 4C ...	CA-Root	CA-Root	Wed, 3 Feb 2...	Mon, 3 Feb 2...	Enabled
<input type="checkbox"/>	2#EAP-TLS	Infrastructure Cisco Services Endpoints	10 D0 98 8D ...	EAP-TLS_CA	EAP-TLS_CA	Mon, 25 Jul 2...	Tue, 25 Jul 20...	Enabled

8.2 Configuration of the Authenticator

```
switch3560#sh run
```

```
Building configuration...
```

```
Current configuration : 6839 bytes
```

```
!
```

```
! Last configuration change at 08:35:33 UTC <date> by tester
```

```
!
```

```
version 15.2
```

```
no service pad
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
service password-encryption
```

```
!
```

```
hostname switch3560
```

```
!  
boot-start-marker  
boot-end-marker  
!  
!  
!  
username acumensec privilege 15 secret 5 $1$cvrn$nW38pMU9jkldfSgK2a/l./  
aaa new-model  
aaa local authentication attempts max-fail 3  
aaa local authentication default authorization default  
!  
!  
aaa group server radius ISE  
server-private 10.1.9.164 key 7 1543595F302F38107B6164  
ip radius source-interface Vlan900  
!  
aaa authentication login default local  
aaa authentication login console local  
aaa authentication enable default none  
aaa authentication dot1x default group ISE  
aaa authorization console  
aaa authorization config-commands  
aaa authorization exec default if-authenticated  
aaa authorization network default group ISE  
aaa accounting update newinfo periodic 2880  
aaa accounting dot1x default start-stop group ISE  
aaa accounting exec default start-stop group ISE
```

```
aaa accounting system default start-stop group ISE
!
!
!
!
!
aaa server radius dynamic-author
client 10.1.9.164 server-key 7 091D1C5A2D000426585E55
auth-type any
!
dot1x system-auth-control
dot1x critical eapol
!
interface GigabitEthernet0/1
switchport access vlan 900
switchport mode access
authentication host-mode multi-auth
authentication open
authentication order dot1x
authentication priority dot1x
authentication port-control auto
authentication periodic
authentication timer reauthenticate server
authentication timer inactivity server dynamic
dot1x pae authenticator
dot1x timeout tx-period 10
!
```

```
!  
interface Vlan900  
 ip address 10.1.9.163 255.255.255.0  
!  
!  
radius-server attribute 6 on-for-login-auth  
radius-server attribute 8 include-in-access-req  
radius-server attribute 25 access-request include  
radius-server attribute 4 10.1.9.163  
radius-server attribute 2 length maximum 240  
radius-server dead-criteria time 10 tries 3  
radius-server deadtime 15  
radius-server key 7 00554155305E18325C731D
```

8.3 Configuration of the Supplicant


```

[root@rupal] ~ /home/acumensec/Desktop/eap-tls
# ls -ltr
total 12
-rw-r--r-- 1 acumensec acumensec 2696 Aug 17 09:47 EAP-TLS_ICA.pem
-rw-r--r-- 1 acumensec acumensec 1679 Aug 17 11:42 EAP-TLS_CA_key.pem
-rw-r--r-- 1 acumensec acumensec 1399 Aug 24 13:09 acumensec.crt

[root@rupal] ~ /home/acumensec/Desktop/eap-tls
# cd /home/acumensec/Desktop

[root@rupal] ~ /home/acumensec/Desktop
# cat eap-tls.conf
# =====
# wpa_supplicant configuration file
#
# EAP-TLS specific
# =====

openssl_ciphers=AES128-SHA

update_config=1
ctrl_interface=/var/run/wpa_supplicant

# -----
# IEEE 802.1X/EAPOL version
# wpa_supplicant is implemented based on IEEE Std 802.1X-2004 which defines
# EAPOL version 2. However, there are many APs that do not handle the new
# version number correctly (they seem to drop the frames completely). In order
# to make wpa_supplicant interoperate with these APs, the version number is set
# to 1 by default. This configuration value can be used to set it to the new
# version (2).

# to 1 by default. This configuration value can be used to set it to the new
# version (2).
# -----

eapol_version=2

# EAP fast re-authentication
# By default, fast re-authentication is enabled for all EAP methods that
# support it. This variable can be used to disable fast re-authentication.
# Normally, there is no need to disable this.

fast_reauth=0

network={
    key_mgmt=IEEE8021X
    eap=TLS
    identity="10.1.9.162, rupal.acumensec.local"
    ca_cert="/home/acumensec/Desktop/eap-tls/EAP-TLS_ICA.pem"
    client_cert="/home/acumensec/Desktop/eap-tls/acumensec.crt"
    private_key="/home/acumensec/Desktop/eap-tls/EAP-TLS_CA_key.pem"
    eapol_flags=3
}

[root@rupal] ~ /home/acumensec/Desktop
#

```

8.4 Results

```

root@rupal: /home/acumensec/Desktop
# wpa_supplicant -t -dd -Dwired -ish2 -c eap-tls.conf
1661564076.540787: wpa_supplicant v2.10
1661564076.540963: random: getrandom() support available
1661564076.541116: Successfully initialized wpa_supplicant
1661564076.541241: Initializing interface 'eth2' conf 'eap-tls.conf' driver 'wired' ctrl_interface 'N/A' bridge 'N/A'
1661564076.541324: Configuration file 'eap-tls.conf' -> '/home/acumensec/Desktop/eap-tls.conf'
1661564076.541397: Reading configuration file '/home/acumensec/Desktop/eap-tls.conf'
1661564076.541487: openssl_ciphers='AES128-SHA'
1661564076.541559: update_config=1
1661564076.541621: ctrl_interface='/var/run/wpa_supplicant'
1661564076.541683: eapol_version=2
1661564076.541743: fast_reauth=0
1661564076.541803: Line: 35 - start of a new network block
1661564076.541870: key_mgmt: 0x0
1661564076.541939: eap_methods - hexdump(len=16): 00 00 00 00 0d 00 00 00 00 00 00 00 00 00 00 00
1661564076.542006: identity - hexdump_ascii(len=33):
 31 30 2e 31 2e 39 2e 31 36 32 2c 20 72 75 70 61 10.1.9.162, rupa
 6c 2e 61 63 75 6d 65 6e 73 65 63 2e 6c 6f 63 61 1.acumensec.local
 6c 1
1661564076.542247: ca_cert - hexdump_ascii(len=47):
 2f 68 6f 6d 65 2f 61 63 75 6d 65 6e 73 65 63 2f /home/acumensec/
 44 65 73 6b 74 6f 70 2f 65 61 70 2d 74 6c 73 2f Desktop/eap-tls/
 45 41 50 2d 54 4c 53 5f 49 43 41 2e 70 65 6d EAP-TLS_ICA.pem
1661564076.542488: client_cert - hexdump_ascii(len=45):
 2f 68 6f 6d 65 2f 61 63 75 6d 65 6e 73 65 63 2f /home/acumensec/
 44 65 73 6b 74 6f 70 2f 65 61 70 2d 74 6c 73 2f Desktop/eap-tls/
 61 63 75 6d 65 6e 73 65 63 2e 63 72 74 acumensec.crt
1661564076.542730: private_key - hexdump_ascii(len=50):
 2f 68 6f 6d 65 2f 61 63 75 6d 65 6e 73 65 63 2f /home/acumensec/
 44 65 73 6b 74 6f 70 2f 65 61 70 2d 74 6c 73 2f Desktop/eap-tls/
 45 41 50 2d 54 4c 53 5f 43 41 5f 6b 65 79 2e 70 EAP-TLS_CA_key.p
 65 6d em
1661564076.543042: Priority group 0
1661564076.543105: id=0 said=""
1661564076.543352: driver_wired_init_common: Added multicast membership with packet socket
1661564076.543431: Add interface eth2 to a new radio N/A
1661564076.553138: eth2: Own MAC address: 00:50:56:b8:04:e4
1661564076.553229: eth2: RSN: flushing PMKID list in the driver
1661564076.553291: eth2: Setting scan request: 0.100000 sec
1661564076.565091: TDLS: TDLS operation not supported by driver
1661564076.565233: TDLS: Driver uses internal link setup
1661564076.565339: TDLS: Driver does not support TDLS channel switching
1661564076.567683: eth2: WPS: UUID based on MAC address: 4df7d647-4c78-5cd3-aa08-4391f2b6d948
1661564076.569892: ENGINE: Loading builtin engines
1661564076.570517: ENGINE: Loading builtin engines
1661564076.570691: EAPOL: SUPP_PAE entering state DISCONNECTED
1661564076.570771: EAPOL: Supplicant port status: Unauthorized
1661564076.570863: EAPOL: KEY_RX entering state NO_KEY_RECEIVE
1661564076.570922: EAPOL: SUPP_BE entering state INITIALIZE
1661564076.570982: EAP: EAP entering state DISABLED
1661564076.571188: MBO: Update non-preferred channels, non_pref_chan=N/A
1661564076.571277: eth2: Added interface eth2
1661564076.571345: eth2: State: DISCONNECTED -> DISCONNECTED
1661564076.653463: eth2: Using wired authentication - overriding ap_scan configuration
1661564076.653616: EAPOL: External notification - EAP success=0
1661564076.653726: EAPOL: External notification - EAP fail=0
1661564076.653831: EAPOL: External notification - portControl=Auto
1661564076.653937: eth2: Already associated with a configured network - generating associated event
1661564076.654046: eth2: Event ASSOC (0) received

```



```

switch3560#sh authentication sessions mac 0050.568b.04e4

Interface      MAC Address      Method  Domain  Status Fg Session ID
-----
Gi0/1          0050.568b.04e4  dot1x   DATA   Auth    000000000000001B05C22DB6

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

switch3560#sh authentication sessions mac 0050.568b.04e4 details
      Interface: GigabitEthernet0/1
      MAC Address: 0050.568b.04e4
      IPv6 Address: Unknown
      IPv4 Address: 10.1.9.162
      User-Name: rupal.acumensec.local
      Status: Authorized
      Domain: DATA
      Oper host mode: multi-auth
      Oper control dir: both
      Session timeout: N/A
      Common Session ID: 000000000000001B05C22DB6
      Acct Session ID: 0x00000007
      Handle: 0xE8000004
      Current Policy: POLICY_Gi0/1

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

switch3560#
switch3560#

```

- Verify via packet capture

ISE Configuration for EAP-TLS Server

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
1	0.000000000	Cisco_ef:3b:01				EAP	62	Request, Identity
2	10.286627812	Cisco_ef:3b:01				EAP	62	Request, Identity
3	19.428895400	Cisco_ef:3b:01				EAP	62	Request, Identity
4	19.429090618	Whware_8b:04:e4				EAP	58	Response, Identity
5	19.455600352	Cisco_ef:3b:01				EAP	62	Request, TLS EAP (EAP-TLS)
6	19.463266441	Whware_8b:04:e4				TLSv1.2	140	Client Hello
7	19.573242882	Cisco_ef:3b:01				EAP	1032	Request, TLS EAP (EAP-TLS)
8	19.575014707	Whware_8b:04:e4				EAP	26	Response, TLS EAP (EAP-TLS)
9	19.591005261	Cisco_ef:3b:01				EAP	1028	Request, TLS EAP (EAP-TLS)
10	19.592426384	Whware_8b:04:e4				EAP	26	Response, TLS EAP (EAP-TLS)
11	19.607323949	Cisco_ef:3b:01				EAP	1028	Request, TLS EAP (EAP-TLS)
12	19.608338895	Whware_8b:04:e4				EAP	26	Response, TLS EAP (EAP-TLS)
13	19.624185142	Cisco_ef:3b:01				TLSv1.2	124	Server Hello, Certificate, Certificate Request, Server Hello Done
14	19.640838716	Whware_8b:04:e4				EAP	1428	Response, TLS EAP (EAP-TLS)
15	19.654219189	Cisco_ef:3b:01				EAP	62	Request, TLS EAP (EAP-TLS)
16	19.655785042	Whware_8b:04:e4				EAP	1424	Response, TLS EAP (EAP-TLS)
17	19.672729666	Cisco_ef:3b:01				EAP	62	Request, TLS EAP (EAP-TLS)
18	19.678464789	Whware_8b:04:e4				TLSv1.2	766	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
19	19.710814002	Cisco_ef:3b:01				TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
20	19.711833040	Whware_8b:04:e4				EAP	26	Response, TLS EAP (EAP-TLS)
21	20.606482621	Cisco_ef:3b:01				EAP	62	Request, Identity
22	20.607044671	Cisco_ef:3b:01				EAP	62	Success


```

version: v3 (2)
serialNumber: 0b01abed40f0bac67d
  > signature (sha256withRSAEncryption)
  > issuer: rdnSequence (0)
  > validity
  > subject: rdnSequence (0)
  > subjectPublicKeyInfo
  > extensions: 8 items
    > Extension (id-ce-basicConstraints)
    > Extension (id-ce-subjectKeyIdentifier)
    > Extension (id-ce-authorityKeyIdentifier)
    > Extension (id-ce-keyUsage)
    > Extension (id-ce-extendedKeyUsage)
    > Extension (id-ce-subjectAltName)
      Extension Id: 2.5.29.17 (id-ce-subjectAltName)
        > GeneralNames: 2 items
          > GeneralName: dNSName (2)
            > dNSName: rupal.acumsec.local
            > GeneralName: IPAddress (7)
          > Extension (ns_cert_exts.cert_type)
          > Extension (ns_cert_exts.comment)
        > algorithmIdentifier (sha256withRSAEncryption)
        > padding: 0
        encrypted: 3be7b6268365721f5aaa66bcb071efc86231af8efb0ad20ecbc9660d1a391dc071e06822...
        Certificate Length: 955
      > Certificate: 308203b73882029fa0030201020208756f2c562777c3c9300d06092a864886f70d01010b... (id-at-commonName=EAP-TLS_ICA,id-at-organizationalUnitName=CC,id-at-organizationName=Acumen,id-at-countryName=US)
  
```

ISE Configuration for EAP-TLS Server

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
6	7.268654	10.1.9.163	1645	10.1.9.164	1645	RADIUS	347	Access-Request id=203
7	7.278143	10.1.9.164	1645	10.1.9.163	1645	RADIUS	163	Access-Challenge id=203
8	7.301957	10.1.9.163	1645	10.1.9.164	1645	RADIUS	504	Access-Request id=204
9	7.311208	10.1.9.164	1645	10.1.9.163	1645	RADIUS	1175	Access-Challenge id=204
10	7.415022	10.1.9.163	1645	10.1.9.164	1645	RADIUS	390	Access-Request id=205
11	7.421373	10.1.9.164	1645	10.1.9.163	1645	RADIUS	1171	Access-Challenge id=205
12	7.431890	10.1.9.163	1645	10.1.9.164	1645	RADIUS	390	Access-Request id=206
13	7.437931	10.1.9.164	1645	10.1.9.163	1645	RADIUS	1171	Access-Challenge id=206
14	7.448666	10.1.9.163	1645	10.1.9.164	1645	RADIUS	390	Access-Request id=207
15	7.453989	10.1.9.164	1645	10.1.9.163	1645	RADIUS	261	Access-Challenge id=207
17	7.481163	10.1.9.163	1645	10.1.9.164	1645	RADIUS	322	Access-Request id=208
18	7.486854	10.1.9.164	1645	10.1.9.163	1645	RADIUS	163	Access-Challenge id=208
20	7.503482	10.1.9.163	1645	10.1.9.164	1645	RADIUS	318	Access-Request id=209
21	7.509458	10.1.9.164	1645	10.1.9.163	1645	RADIUS	163	Access-Challenge id=209
22	7.518501	10.1.9.163	1645	10.1.9.164	1645	RADIUS	1134	Access-Request id=210
23	7.542402	10.1.9.164	1645	10.1.9.163	1645	RADIUS	242	Access-Challenge id=210
24	7.551179	10.1.9.163	1645	10.1.9.164	1645	RADIUS	390	Access-Request id=211
25	7.576754	10.1.9.164	1645	10.1.9.163	1645	RADIUS	344	Access-Accept id=211
27	8.444342	10.1.9.163	1646	10.1.9.164	1646	RADIUS	340	Accounting-Request id=36
28	8.452939	10.1.9.164	1646	10.1.9.163	1646	RADIUS	62	Accounting-Response id=36


```

> Frame 24: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits)
> Ethernet II, Src: Cisco_ef:3b:43 (d0:d0:fd:ef:3b:43), Dst: IntelCor_42:d3:93 (b4:96:91:42:d3:93)
> Internet Protocol Version 4, Src: 10.1.9.163, Dst: 10.1.9.164
> User Datagram Protocol, Src Port: 1645, Dst Port: 1645
  v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0xd3 (211)
    Length: 348
    Authenticator: 13ea646bcb8c8b8c5edc574bfe0388a3
    [The response to this request is in frame 25]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=35 val=10.1.9.162, rupal.acumensec.local
    > AVP: t=Service-Type(6) l=6 val=Framed(2)
    > AVP: t=Vendor-Specific(26) l=27 vnd=ciscoSystems(9)
    > AVP: t=Framed-MTU(12) l=6 val=1500
    > AVP: t=Called-Station-Id(30) l=19 val=D0-D0-FD-EF-3B-01
    > AVP: t=Calling-Station-Id(31) l=19 val=00-50-56-8B-04-E4
    > AVP: t=EAP-Message(79) l=8 Last Segment[1]
    > AVP: t=Message-Authenticator(80) l=18 val=9024692fef774448dbb15cab1f4962de
    > AVP: t=EAP-Key-Name(102) l=2 val=
    > AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
    > AVP: t=Framed-IP-Address(8) l=6 val=10.1.9.162
    > AVP: t=NAS-IP-Address(4) l=6 val=10.1.9.163
    > AVP: t=NAS-Port-Id(87) l=20 val=GigabitEthernet0/1
    > AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
  
```

- Verify via logs

ISE Configuration for EAP-TLS Server

Operations - RADIUS

License Warning

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 0 Repeat Counter 0

Refresh Never Show Latest 100 records Within Last 12 hours

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...
Aug 27, 2022 01:44:02.3...	●		0	rupal.acumensec...	00:50:56:8B:04:E4	VMWare...	Default >>	Default >>	PermitAcc...	10.1.9.162	switch3550	GigabitEth...	Profiled	
Aug 27, 2022 01:44:01.5...	■			rupal.acumensec...	00:50:56:8B:04:E4	VMWare...	Default >>	Default >>	PermitAcc...	10.1.9.162	switch3550	GigabitEth...	Profiled	
Aug 27, 2022 01:41:32.3...	■			rupal.acumensec...	00:50:56:8B:04:E4	VMWare...	Default >>	Default >>	PermitAcc...	10.1.9.162	switch3550	GigabitEth...	Profiled	
Aug 27, 2022 01:35:42.2...	■			rupal.acumensec...	00:50:56:8B:04:E4	VMWare...	Default >>	Default >>	PermitAcc...	10.1.9.162	switch3550	GigabitEth...	Profiled	
Aug 27, 2022 01:34:16.7...	■			rupal.acumensec...	00:50:56:8B:04:E4	VMWare...	Default >>	Default >>	PermitAcc...	10.1.9.162	switch3550	GigabitEth...	Profiled	
Aug 27, 2022 01:33:12.4...	■			rupal.acumensec...	00:50:56:8B:04:E4	VMWare...	Default >>	Default >>	PermitAcc...	10.1.9.162	switch3550	GigabitEth...	Profiled	
Aug 27, 2022 01:31:41.8...	■			rupal.acumensec...	00:50:56:8B:04:E4	VMWare...	Default >>	Default >>	PermitAcc...	10.1.9.162	switch3550	GigabitEth...	Profiled	
Aug 27, 2022 01:29:01.8...	■			rupal.acumensec...	00:50:56:8B:04:E4	VMWare...	Default >>	Default >>	PermitAcc...	10.1.9.162	switch3550	GigabitEth...	Profiled	
Aug 27, 2022 01:22:50.1...	■			rupal.acumensec...	00:50:56:8B:04:E4	VMWare...	Default >>	Default >>	PermitAcc...	10.1.9.162	switch3550	GigabitEth...	Profiled	
Aug 27, 2022 01:22:20.7...	■			rupal.acumensec...	00:50:56:8B:04:E4	VMWare...	Default >>	Default >>	PermitAcc...	10.1.9.162	switch3550	GigabitEth...	Profiled	
Aug 27, 2022 01:15:43.7...	■			rupal.acumensec...	00:50:56:8B:04:E4	VMWare...	Default >>	Default >>	PermitAcc...	10.1.9.162	switch3550	GigabitEth...	Profiled	

Overview

Event 5200 Authentication succeeded

Username rupal.acumensec.local

Endpoint Id 00:50:56:8B:04:E4

Endpoint Profile VMWare-Device

Authentication Policy Default >> EAP-TLS_DOT1X

Authorization Policy Default >> EAP-TLS_DOT1X

Authorization Result PermitAccess

Authentication Details

Source Timestamp 2022-08-27 01:44:01.534

Received Timestamp 2022-08-27 01:44:01.534

Policy Server ISE3615

Event 5200 Authentication succeeded

Username rupal.acumensec.local

Endpoint Id 00:50:56:8B:04:E4

Calling Station Id 00-50-56-8B-04-E4

Endpoint Profile VMWare-Device

IPv4 Address 10.1.9.162

Identity Group Profiled

Audit Session Id 0000000000001R05C27DR6

- Steps
- 11001 Received RADIUS Access-Request
 - 11017 RADIUS created a new session
 - 15049 Evaluating Policy Group
 - 15008 Evaluating Service Selection Policy
 - 11507 Extracted EAP-Response/Identity
 - 12500 Prepared EAP-Request proposing EAP-TLS with challenge
 - 12625 Valid EAP-Key-Name attribute received
 - 11006 Returned RADIUS Access-Challenge
 - 11001 Received RADIUS Access-Request
 - 11018 RADIUS is re-using an existing session
 - 12502 Extracted EAP-Response containing EAP-TLS challenge-response and accepting EAP-TLS as negotiated
 - 12800 Extracted first TLS record; TLS handshake started
 - 12805 Extracted TLS ClientHello message
 - 12806 Prepared TLS ServerHello message
 - 12807 Prepared TLS Certificate message
 - 12809 Prepared TLS CertificateRequest message
 - 12810 Prepared TLS ServerDone message
 - 12505 Prepared EAP-Request with another EAP-TLS challenge
 - 11006 Returned RADIUS Access-Challenge
 - 11001 Received RADIUS Access-Request
 - 11018 RADIUS is re-using an existing session
 - 12504 Extracted EAP-Response containing EAP-TLS challenge-response
 - 12505 Prepared EAP-Request with another EAP-TLS challenge
 - 11006 Returned RADIUS Access-Challenge
 - 11001 Received RADIUS Access-Request
 - 11018 RADIUS is re-using an existing session