Install a 3rd party CA Certificate in ISE

Contents

Introduction

This document describes the installation of a 3rd party CA Signed Certificate in Cisco Identity Services Engine (ISE). The process is the same regardless of the final certificate role (EAP authentication, Portal, Admin, and pxGrid).

Prerequisites

Requirements

Cisco recommends that you have knowledge of Basic Public Key Infrastructure.

Components Used

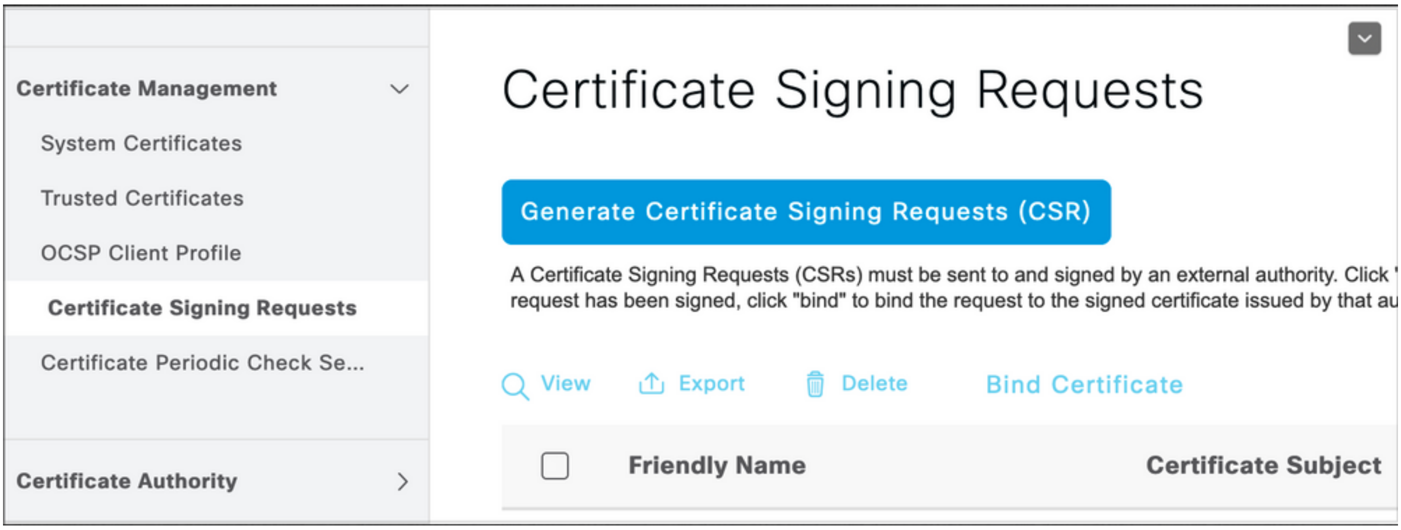
The information in this document is based on Cisco Identity Services Engine (ISE) Release 3.0. The same configuration applies to releases 2.X

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Step 1. Generate Certificate Signing Request (CSR).

In order to generate the CSR, navigate to **Administration > Certificates > Certificate Signing Requests** and click on **Generate Certificate Signing Requests** (CSR).



A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click '
request has been signed, click "bind" to bind the request to the signed certificate issued by that au

1. Under the Usage section, select the role to be used from the drop-down menu. If the certificate is used for multiple roles you can select Multi-Use. Once the certificate is generated the roles can be changed if necessary.

2. Select the node for which the certificate will be generated.

3. Fill out the information as needed (Organizational Unit, Organization, City, State and Country).

   Note: Under Common Name (CN) field ISE auto-populates the node's Fully Qualified Domain Name (FQDN).

Wildcards:

- If the goal is to generate a wildcard certificate check the **Allow Wildcard Certificates** box.

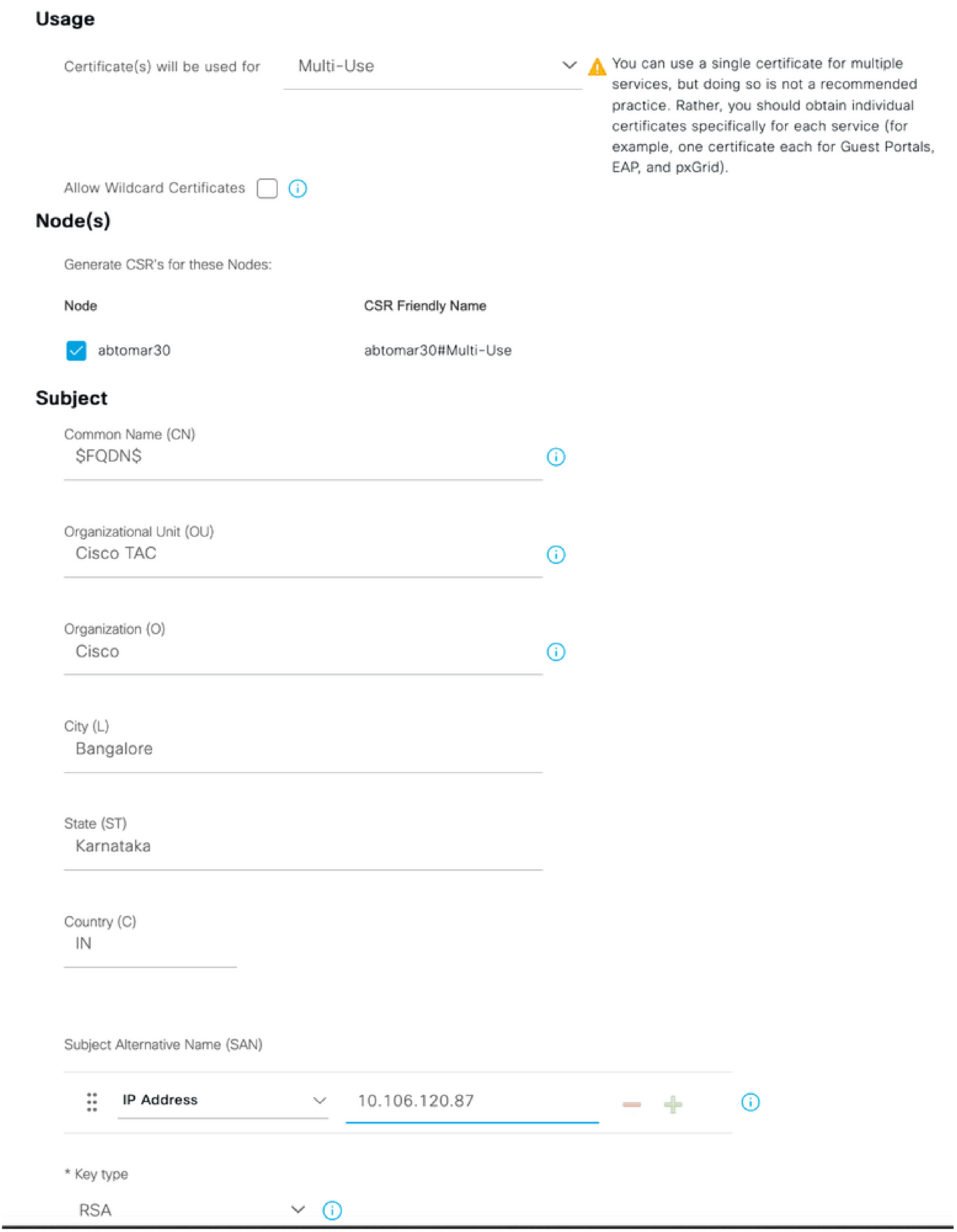
- If the certificate is used for EAP authentications the ***** symbol should not be in the Subject CN field as Windows supplicants reject the server certificate.

- Even when **Validate Server Identity** is disabled on the supplicant, the SSL handshake may fail when the ***** is in the CN field.

- Instead, a generic FQDN can be used in the CN field, and then the ***.domain.com** can be used on the Subject Alternative Name (SAN) DNS Name field.

  Note: Some Certificate Authorities (CA) may add the wildcard (*) in the CN of the certificate automatically even if it not present in the CSR. In this scenario, a special request is required to be raised to prevent this action.

Individual server certificate CSR example:



Usage

Certificate(s) will be used for Multi-Use

You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).

Allow Wildcard Certificates □

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ abtomar30	abtomar30#Multi-Use

Subject

Common Name (CN) $FQDN$

Organizational Unit (OU) Cisco TAC

Organization (O) Cisco

City (L) Bangalore

State (ST) Karnataka

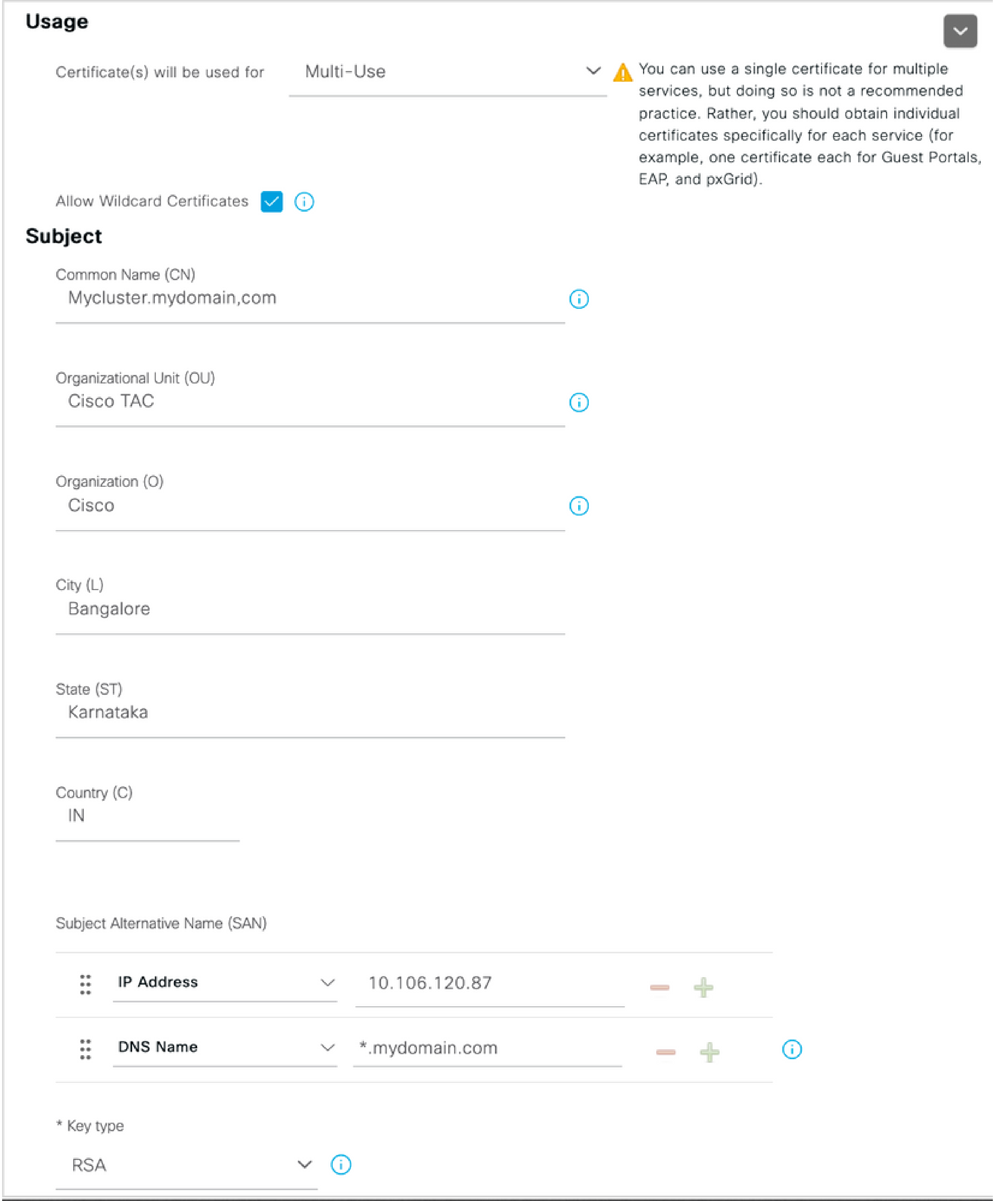
Country (C) IN

Subject Alternative Name (SAN)

IP Address 10.106.120.87

* Key type RSA

Wildcard CSR example:



Usage

Certificate(s) will be used for: Multi-Use

⚠ You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).

Allow Wildcard Certificates ☑

Subject

Common Name (CN): Mycluster.mydomain,com

Organizational Unit (OU): Cisco TAC

Organization (O): Cisco

City (L): Bangalore

State (ST): Karnataka

Country (C): IN

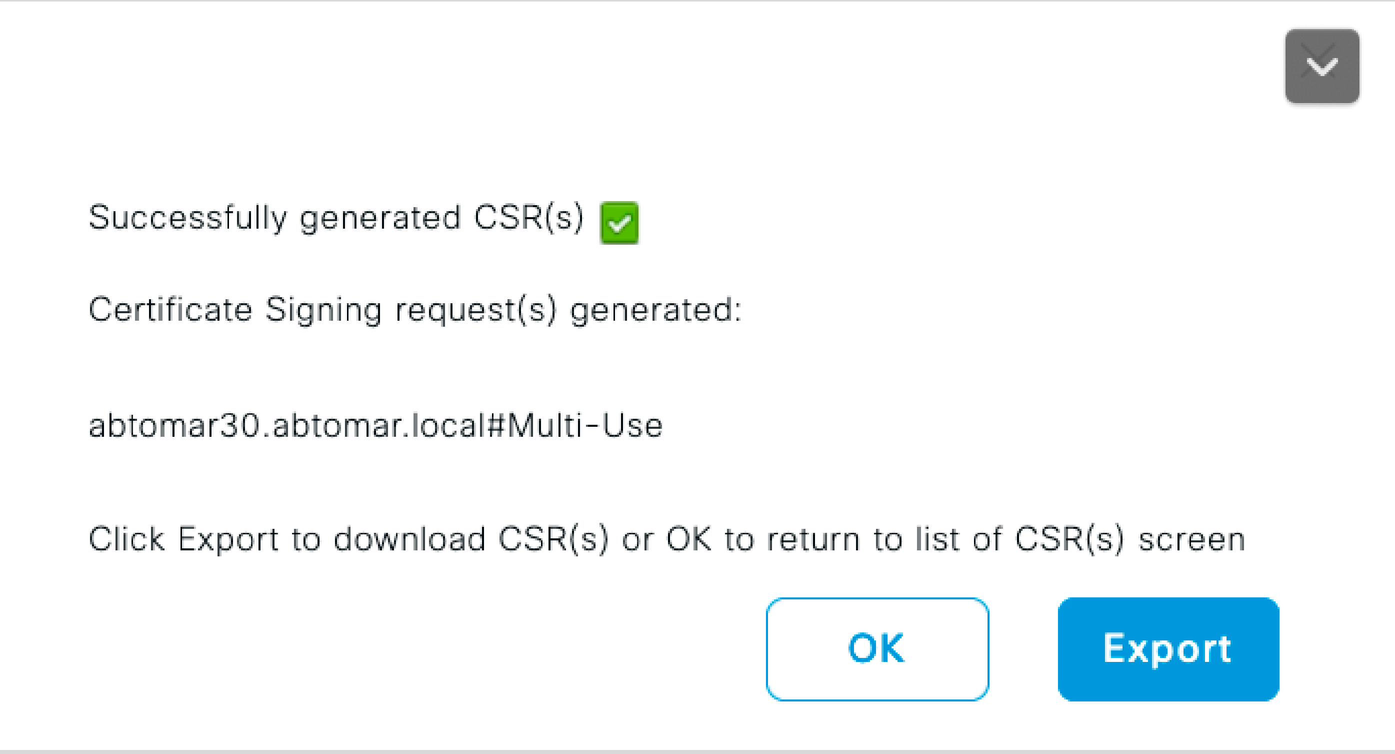
Subject Alternative Name (SAN)

IP Address	10.106.120.87
DNS Name	*.mydomain.com

* Key type: RSA

Note: Each deployment node(s)'s IP address can be added to the SAN field to avoid a certificate warning when you access the server via the IP address.

Once the CSR is created, ISE displays a pop-up window with the option to export it. Once exported, this file should be sent to the CA for signing.


Successfully generated CSR(s) ✓

Certificate Signing request(s) generated:

abtomar30.abtomar.local#Multi-Use

Click Export to download CSR(s) or OK to return to list of CSR(s) screen

Step 2. Import a New Certificate Chain.

The Certificate Authority returns the signed server certificate along with the full certificate chain (Root/Intermediate). Once received, follow the steps here to import the certificates into your ISE server:

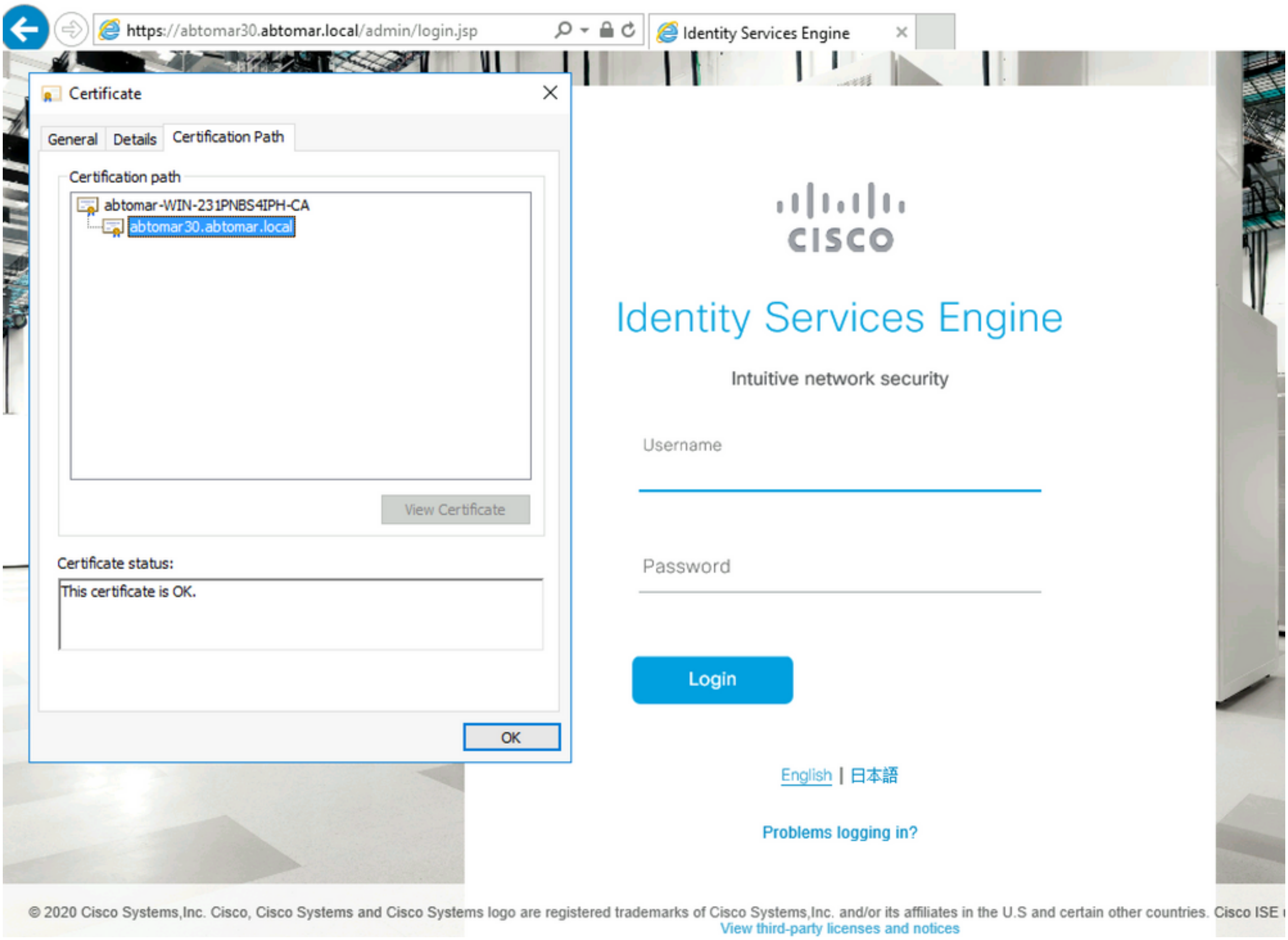
1. In order to import any Root and (or) Intermediate certificates provided by the CA, navigate to **Administration > Certificates > Trusted Certificates**.
2. Click **Import** and then choose the Root and/or Intermediate certificate and choose the relevant check boxes as they apllied to submit.
3. In order to import the Server certificate, navigate to **Administration > Certificates > Certificate Signing Requests**.
4. Select the CSR previously created and click on **Bind Certificate**.
5. Select the new certificate location and ISE binds the certificate to the private key created and stored in the database.

   Note: If the Admin Role has been selected for this certificate, the specific ISE server services restart.

   Caution: If the certificate imported is for the Primary Administratino Node of the deployment and if the Admin role is selected, then the services on all nodes restart one after the other. This is expected and a downtime is recommended to perform this activity.

Verify

If the admin role was selected during the certificate import you can verify the new certificate is in place by loading the admin page in the browser. The browser should trust the new admin certificate as long as the chain was built correctly and if the certificate chain is trusted by the browser.



https://abtomar30.abtomar.local/admin/login.jsp

Certification path:

abtomar-WIN-231PNBS4IPH-CA
- abtomar30.abtomar.local

Certificate status:

This certificate is OK.

© 2020 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc. and/or its affiliates in the U.S and certain other countries. Cisco ISE

For additional verification select the lock symbol in the browser and under the certificate path verify the full chain is present and trusted by the machine. This is not a direct indicator that the full chain was passed down correctly by the server but an indicator of the browser able to trust the server certificate based on its local trust store.

Troubleshoot

Supplicant Doesn't Trust the ISE Local Server Certificate during a dot1x Authentication

Verify ISE is passing the full certificate chain during the SSL handshake process.

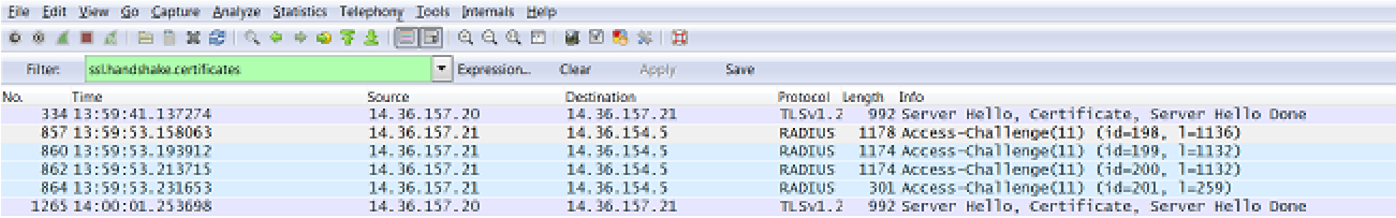
When using EAP methods that require a server certificate (i.e. PEAP) and **Validate Server Identity** is selected, the supplicant validates the certificate chain using the certificates it has in its local trust store as part of the authentication process. As part of the SSL handshake process, ISE presents its certificate and also any Root and (or) intermediate certificates present in its chain. The supplicant won’t be able to validate the server identity if the chain is incomplete. To verify the certificate chain is passed back to your client, you can perform the following steps:

1. In order to take a capture from ISE (TCPDump) during the authentication, navigate to **Operations > Diagostic Tools > General Tools > TCP Dump**.

2. Download/Open the capture and apply the filter **ssl.handshake.certificates** in Wireshark and find an access-challenge.

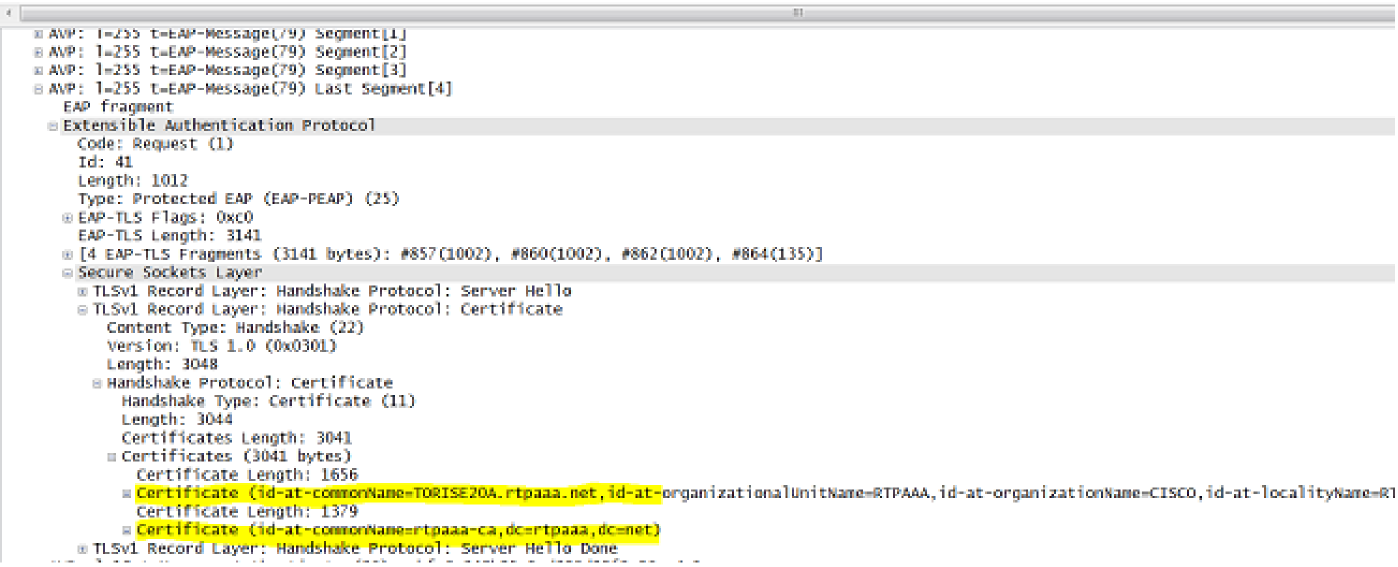
3. Once Selected, navigate to **Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates**.

Certificate chain in the capture.



Filter: ssl.handshake.certificates

```
No.   Time               Source          Destination     Protocol Length Info
  334 13:59:41.137274    14.36.157.20    14.36.157.21    TLSv1.2    992 Server Hello, Certificate, Server Hello Done
  857 13:59:53.158063    14.36.157.21    14.36.154.5     RADIUS    1178 Access-Challenge(11) (id=198, l=1136)
  860 13:59:53.193912    14.36.157.21    14.36.154.5     RADIUS    1174 Access-Challenge(11) (id=199, l=1132)
  862 13:59:53.213715    14.36.157.21    14.36.154.5     RADIUS    1174 Access-Challenge(11) (id=200, l=1132)
  864 13:59:53.231653    14.36.157.21    14.36.154.5     RADIUS     301 Access-Challenge(11) (id=201, l=259)
 1265 14:00:01.253698    14.36.157.20    14.36.157.21    TLSv1.2    992 Server Hello, Certificate, Server Hello Done
```

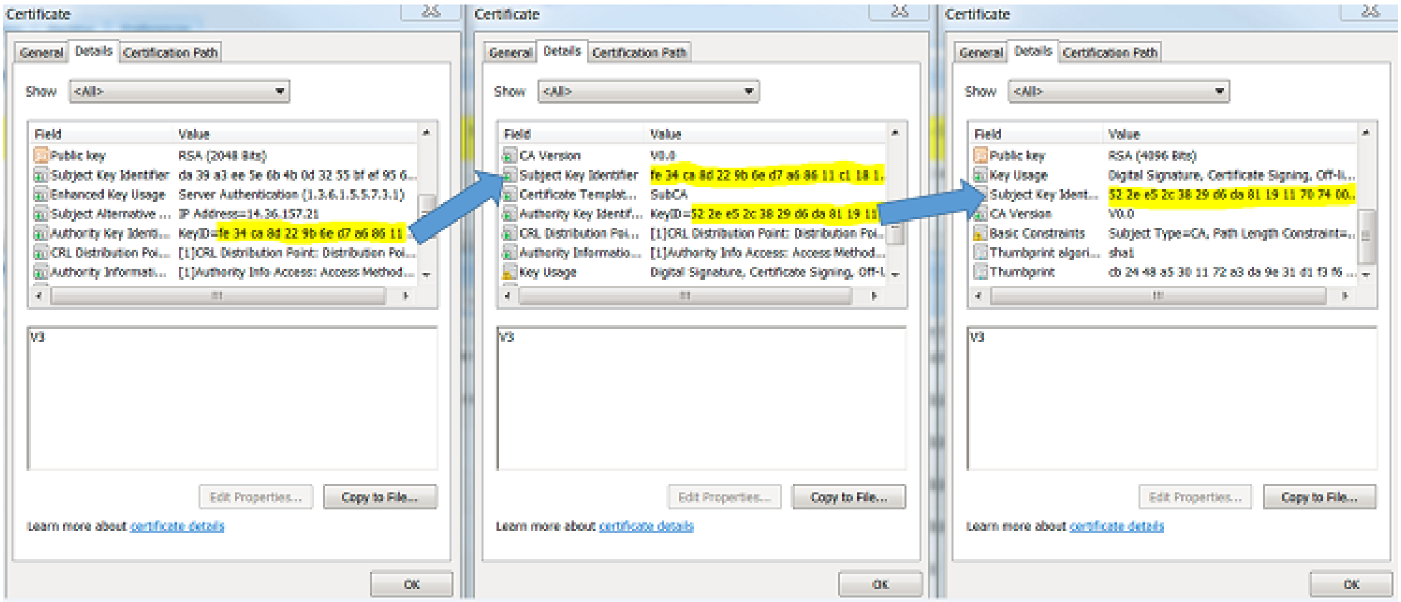


```
⊞ AVP: l=255 t=EAP-Message(79) Segment[1]
⊞ AVP: l=255 t=EAP-Message(79) Segment[2]
⊞ AVP: l=255 t=EAP-Message(79) Segment[3]
⊟ AVP: l=255 t=EAP-Message(79) Last Segment[4]
    EAP fragment
  ⊟ Extensible Authentication Protocol
      Code: Request (1)
      Id: 41
      Length: 1012
      Type: Protected EAP (EAP-PEAP) (25)
    ⊞ EAP-TLS Flags: 0xc0
      EAP-TLS Length: 3141
    ⊞ [4 EAP-TLS Fragments (3141 bytes): #857(1002), #860(1002), #862(1002), #864(135)]
    ⊟ Secure Sockets Layer
      ⊞ TLSv1 Record Layer: Handshake Protocol: Server Hello
      ⊟ TLSv1 Record Layer: Handshake Protocol: Certificate
          Content Type: Handshake (22)
          Version: TLS 1.0 (0x0301)
          Length: 3048
        ⊟ Handshake Protocol: Certificate
            Handshake Type: Certificate (11)
            Length: 3044
            Certificates Length: 3041
          ⊟ Certificates (3041 bytes)
              Certificate Length: 1656
            ⊞ Certificate (id-at-commonName=TORISE20A.rtpaaa.net,id-at-organizationalUnitName=RTPAAA,id-at-organizationName=CISCO,id-at-localityName=R1
              Certificate Length: 1379
            ⊞ Certificate (id-at-commonName=rtpaaa-ca,dc=rtpaaa,dc=net)
      ⊞ TLSv1 Record Layer: Handshake Protocol: Server Hello Done
```

If the chain is incomplete, navigate to **ISE Administration > Certificates > Trusted Certificates** and verify that the Root and (or) Intermediate certificates are present. If the certificate chain is passed successfully, the chain itself should be verified as valid by using the method outlined here.

Open each certificate (server, intermediate and root) and verify the chain of trust by matching the Subject Key Identifier (SKI) of each certificate to the Authority Key Identifier (AKI) of the next certificate in the chain.

Example of a certificate chain.



Field	Value
Public key	RSA (2048 Bits)
Subject Key Identifier	da 39 a3 ee 5e 6b 4b 0d 32 55 bf ef 95 6...
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)
Subject Alternative ...	IP Address=14.36.157.21
Authority Key Identi...	KeyID=fe 34 ca 8d 22 9b 6e d7 a6 86 11
CRL Distribution Poi...	[1]CRL Distribution Point: Distribution Poi...
Authority Informati...	[1]Authority Info Access: Access Method...

V3

Field	Value
CA Version	V0.0
Subject Key Identifier	fe 34 ca 8d 22 9b 6e d7 a6 86 11 c1 18 1...
Certificate Templat...	SubCA
Authority Key Identif...	KeyID=52 2e e5 2c 38 29 d6 da 81 19 11
CRL Distribution Poi...	[1]CRL Distribution Point: Distribution Poi...
Authority Informatio...	[1]Authority Info Access: Access Method...
Key Usage	Digital Signature, Certificate Signing, Off-l...

V3

Field	Value
Public key	RSA (4096 Bits)
Key Usage	Digital Signature, Certificate Signing, Off-li...
Subject Key Ident...	52 2e e5 2c 38 29 d6 da 81 19 11 70 74 00...
CA Version	V0.0
Basic Constraints	Subject Type=CA, Path Length Constraint=...
Thumbprint algori...	sha1
Thumbprint	cb 24 48 a5 30 11 72 a3 da 9e 31 d1 f3 f6 ...

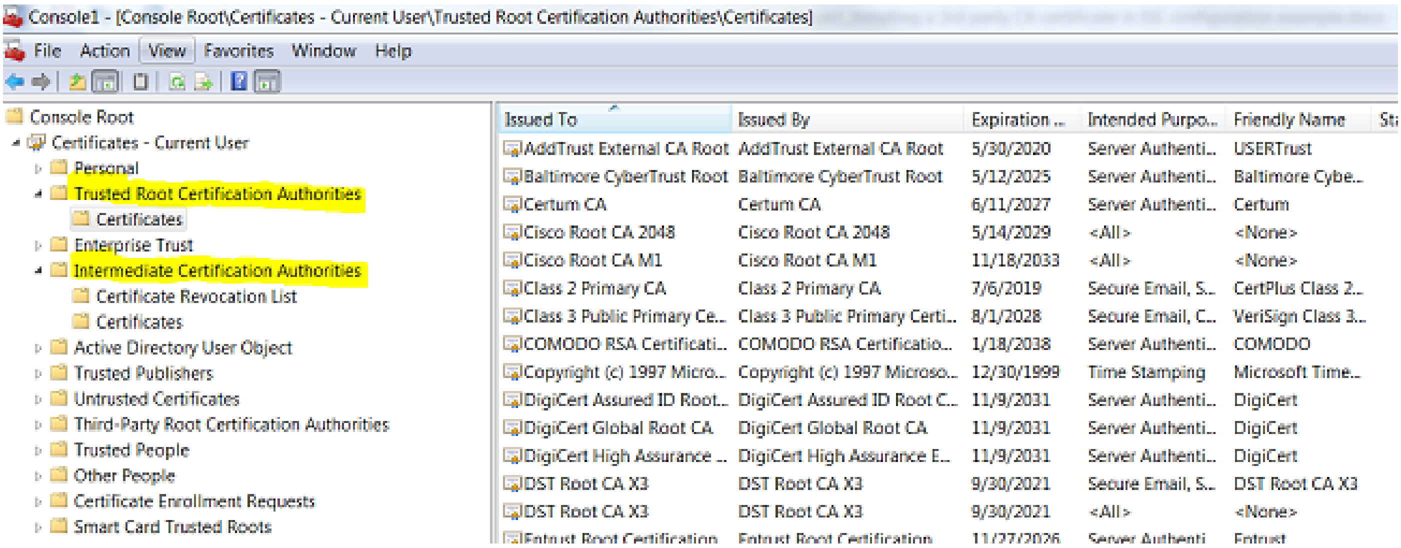
V3

ISE Certificate Chain is Correct but Endpoint Rejects ISE's Server Certificate during Authentication

If ISE is presenting its full certificate chain during the SSL handshake and the supplicant is still rejecting the certificate chain; the next step is to verify that the Root and(or) Intermediate certificates are in the client Local Trust Store.

In order to verify this from a Windows device, navigate to **mmc.exe File > Add-Remove Snap-in**. From Available snap-ins column select **Certificates** and click on **Add**. Select either **My user account** or **computer account** depending upon the authentication type in use (User or Machine) and then click on **OK**.

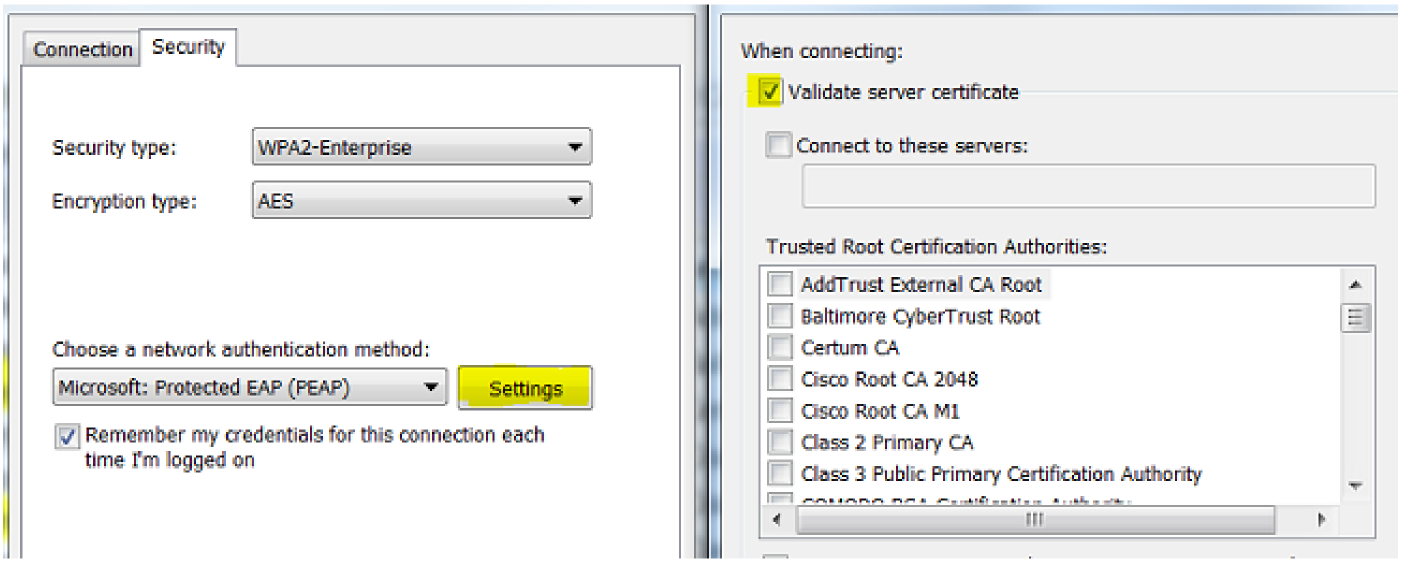
Under the console view, select **Trusted Root Certification Authorities** and **Intermediate Certification Authorities** to verify the presence of Root and Intermediate certificate in the local trust store.


Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help

Console Root
- Certificates - Current User
  - Personal
  - Trusted Root Certification Authorities
    - Certificates
  - Enterprise Trust
  - Intermediate Certification Authorities
    - Certificate Revocation List
    - Certificates
  - Active Directory User Object
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Authorities
  - Trusted People
  - Other People
  - Certificate Enrollment Requests
  - Smart Card Trusted Roots

Issued To	Issued By	Expiration ...	Intended Purpo...	Friendly Name	St
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenti...	USERTrust	
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenti...	Baltimore Cybe...	
Certum CA	Certum CA	6/11/2027	Server Authenti...	Certum	
Cisco Root CA 2048	Cisco Root CA 2048	5/14/2029	<All>	<None>	
Cisco Root CA M1	Cisco Root CA M1	11/18/2033	<All>	<None>	
Class 2 Primary CA	Class 2 Primary CA	7/6/2019	Secure Email, S...	CertPlus Class 2...	
Class 3 Public Primary Ce...	Class 3 Public Primary Certi...	8/1/2028	Secure Email, C...	VeriSign Class 3...	
COMODO RSA Certificati...	COMODO RSA Certificatio...	1/18/2038	Server Authenti...	COMODO	
Copyright (c) 1997 Micro...	Copyright (c) 1997 Microso...	12/30/1999	Time Stamping	Microsoft Time...	
DigiCert Assured ID Root...	DigiCert Assured ID Root C...	11/9/2031	Server Authenti...	DigiCert	
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenti...	DigiCert	
DigiCert High Assurance ...	DigiCert High Assurance E...	11/9/2031	Server Authenti...	DigiCert	
DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, S...	DST Root CA X3	
DST Root CA X3	DST Root CA X3	9/30/2021	<All>	<None>	
Entrust Root Certification	Entrust Root Certification	11/27/2026	Server Authenti	Entrust	

An easy way to verify that this is a Server Identity Check issue, uncheck **Validate Server Certificate** under the supplicant profile configuration and test it again.



Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

When connecting:

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

- □ AddTrust External CA Root
- □ Baltimore CyberTrust Root
- □ Certum CA
- □ Cisco Root CA 2048
- □ Cisco Root CA M1
- □ Class 2 Primary CA
- □ Class 3 Public Primary Certification Authority

Related Information

- [Cisco Identity Services Engine Administrator Guide, Release 3.0]()
- [Technical Support & Documentation - Cisco Systems]()