Contents

Introduction

This document describes installing a 3rd party CA signed certificate in Cisco Identity Services Engine.

The process is the same regardless of the final certificate role (EAP authentication, Portal, Admin and pxGrid).

Requirements

Basic Public Key Infrastructure knowledge.

Components Used

The information in this document is based on the following hardware and software versions:

- Cisco Identity Services engine (ISE) Release 2.0. The same configuration applies to releases 1.3 and 1.4.

Configure

Generating Certificate Signing Request (CSR):

To generate the CSR go to Administration > Certificates > Certificate Signing Requests and select Generate Certificate Signing Requests (CSR).

- Under the Usage section select the role to be used from the drop down menu. If the certificate will be used for multiple roles you can select Multi-Use. Once the certificate is generated the roles can be changed if necessary.
- Select the node for which the certificate will be generated.
- Fill out the information as needed (Organizational Unit, Organization, City, State and Country).

Note: Under Common Name (CN) field ISE will auto populate 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 will be used for EAP authentications the "*" symbol should not be in the Subject CN field as Windows supplicants will 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 will need to me made to prevent this action.

Individual server certificate CSR example:

Wildcard CSR example:

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 has been created, ISE will display a pop up window with the option to export it. Once exported, this file should be sent to the CA for signing.

Importing new Certificate chain:

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

1. Import any Root and (or) Intermediate certificates provided by the CA by going to Administration > Certificates > Trusted Certificates.
2. Import the Server certificate by going to Administration >> Certificates >> Certificate Signing Requests.
3. Select the CSR previously created and click on Bind Certificate.
4. Select the new certificate location and ISE will bind the certificate to the private key created and stored in the database.

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

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.

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

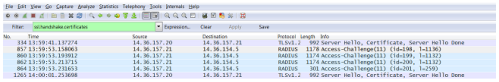
The supplicant does not trust the ISE local server certificate during a dot1x authentication.

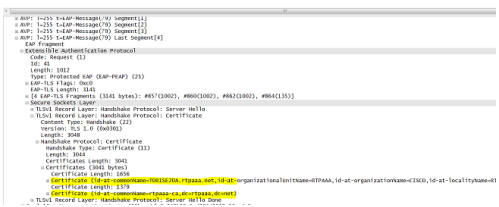
Verify ISE is passing the full certificate chain during the SSL handshake process.

When using EAP methods that require a server certificate (i.e. PEAP) and “Validate Server Identity” is selected, the supplicant will validate 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 will present 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. Take a capture from ISE (TCPDump) during the authentication. Found under 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, Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates

Certificate chain in the capture.



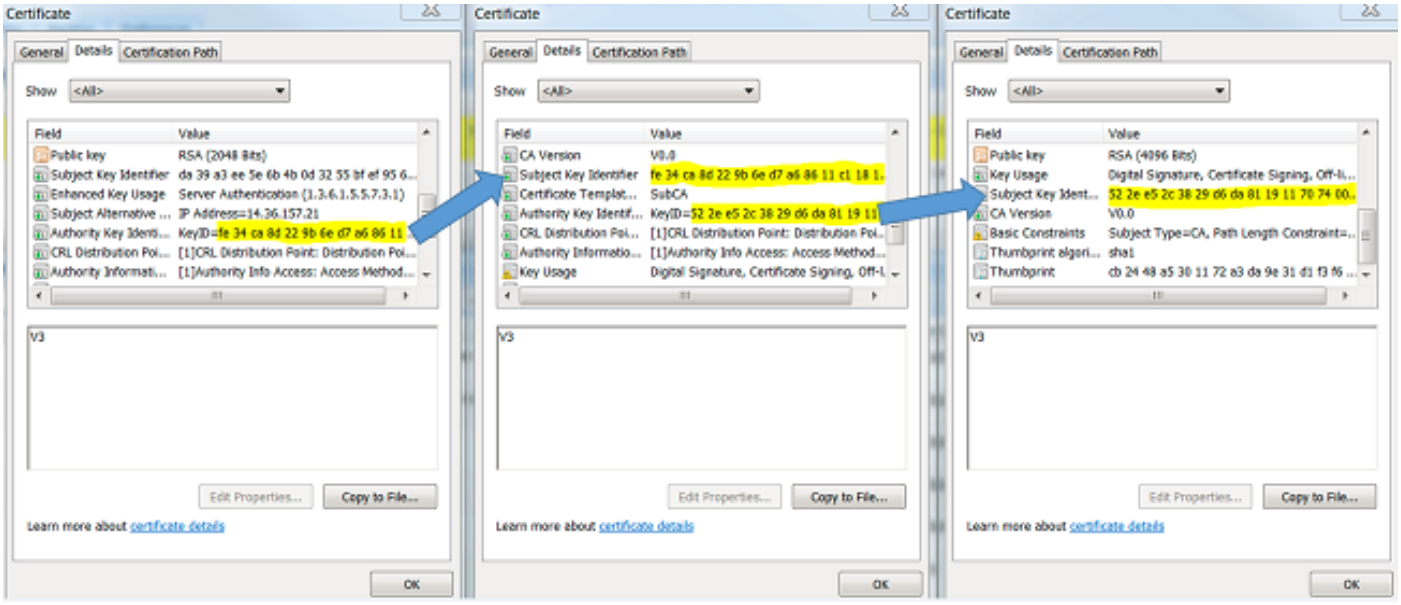


If the chain is not complete you should go to ISE Administration > Certificates > Trusted Certificates and verify that the Root and (or) Intermediate certificates

are present. If the certificate chain is passed successfully, the chain itself should be verified as valid by using the method outlined below.

Open each certificate (server, intermediate and root) and verify 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 certificate chain.

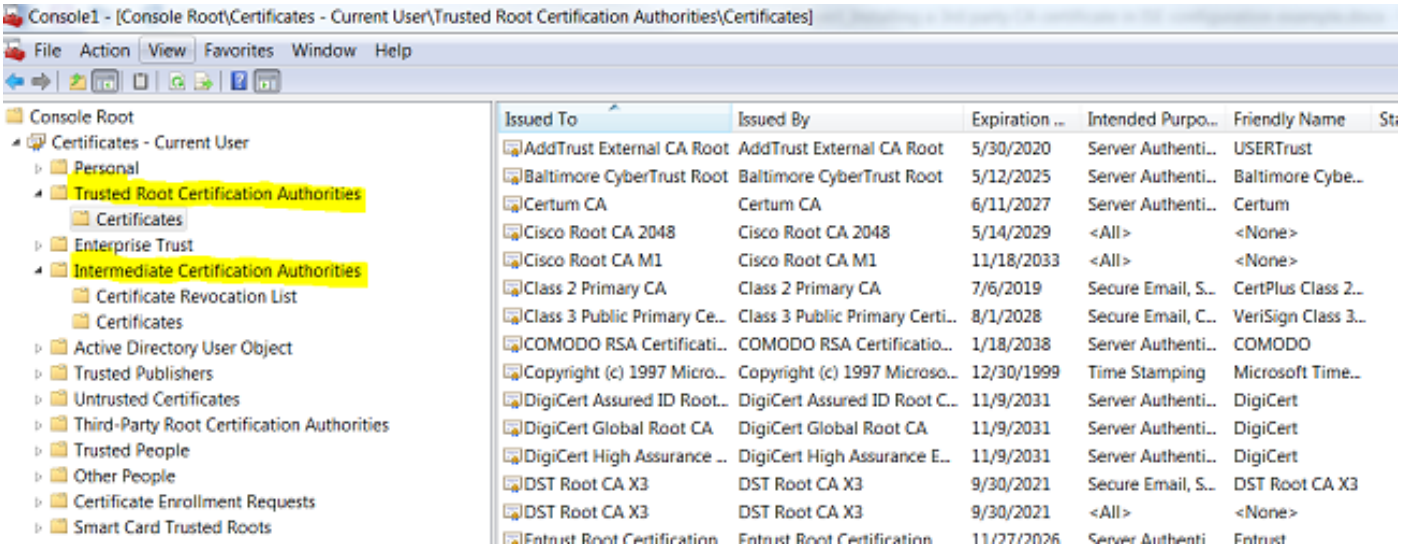


ISE certificate chain is correct but Endpoint rejects ISE's Server Certificate during authentication.

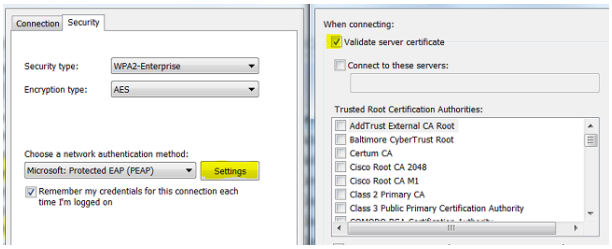
If ISE is presenting its full certificate chain during the SSL handshake and the supplicant is still rejecting the certificate chain; the next step is to verify that the Root and(or) Intermediate certificates are in the client Local Trust Store.

To verify this from a Windows device open mmc.exe File > Add-Remove Snap-in > From Available snap-ins column select certificates > Add > select either "My user account" or "computer account" depending on the authentication type in use (User or Machine). > OK

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



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.



Note: ISE currently does not support processing certificates using RSASSA-PSS as signature algorithm. This includes server certificate, Root, Intermediate

or client certificate (i.e. EAP-TLS, PEAP (TLS), etc.). Refer to bug CSCug22137.

References

- Cisco Identity Services Engine Administrator Guide, Release 2.0