

Instalación de un certificado firmado por CA de terceros en ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Paso 1. Generar solicitud de firma de certificado \(CSR\).](#)

[Paso 2. Importar una nueva cadena de certificados.](#)

[Verificación](#)

[Troubleshoot](#)

[El solicitante no confía en el certificado de servidor local de ISE durante una autenticación dot1x](#)

[La cadena de certificados de ISE es correcta, pero el terminal rechaza el certificado de servidor ISE durante la autenticación](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo instalar un certificado firmado por una autoridad de certificación (CA) de terceros en Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos de la infraestructura básica de clave pública.

Componentes Utilizados

La información de este documento se basa en Cisco Identity Services Engine (ISE) versión 3.0. La misma configuración se aplica a las versiones 2.X

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

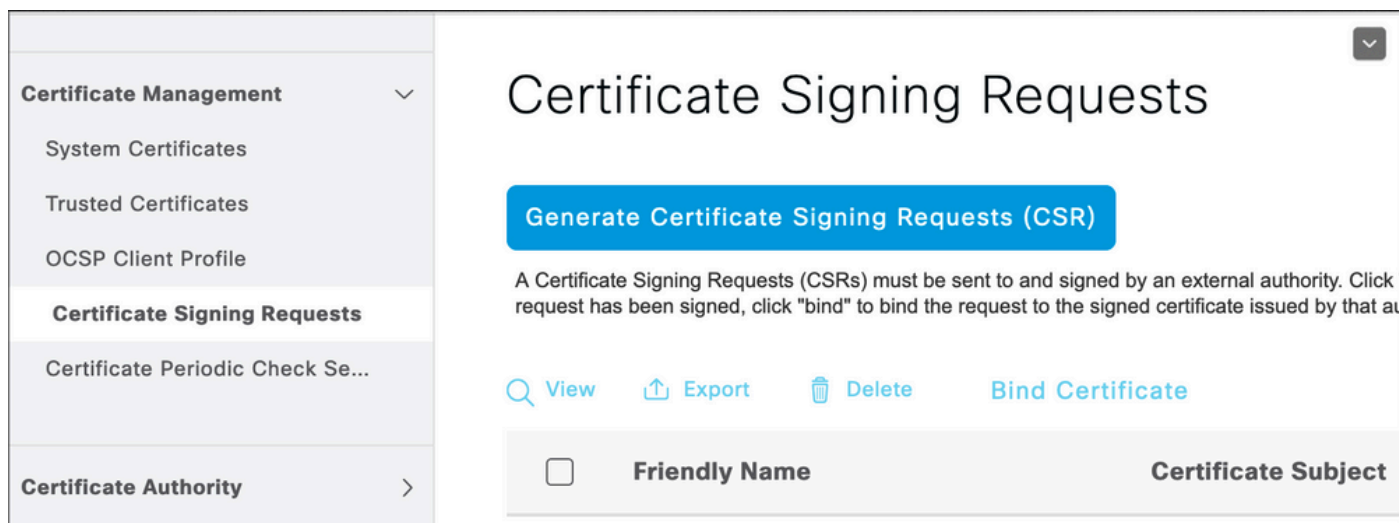
Antecedentes

Este proceso es el mismo independientemente del rol de certificado final (autenticación EAP, portal, administrador y pxGrid).

Configurar


Paso 1. Generar solicitud de firma de certificado (CSR).

Para generar el CSR, navegue hasta Administration > Certificates > Certificate Signing Requests y haga clic en Generate Certificate Signing Requests (CSR).



The screenshot shows the 'Certificate Signing Requests' page. On the left is a navigation menu with categories: Certificate Management, Certificate Authority, Certificate Signing Requests, and Certificate Periodic Check Se... The main content area has a title 'Certificate Signing Requests' and a prominent blue button 'Generate Certificate Signing Requests (CSR)'. Below the button is a note: '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'. There are four action buttons: 'View', 'Export', 'Delete', and 'Bind Certificate'. At the bottom, there is a table header with a checkbox, 'Friendly Name', and 'Certificate Subject'.


1. En la sección Uso, seleccione el rol que se utilizará en el menú desplegable. Si el certificado se utiliza para varias funciones, puede seleccionar Multiuso. Una vez generado el certificado, las funciones se pueden cambiar si es necesario.
2. Seleccione el nodo para el que se puede generar el certificado.
3. Rellene la información según sea necesario (Unidad organizativa, Organización, Ciudad, Estado y País).

 Nota: en el campo Nombre común (CN), ISE rellena automáticamente el nombre de dominio completo (FQDN) del nodo.

Comodines:

- Si el objetivo es generar un certificado comodín, marque la casilla Allow Wildcard Certificates.
- Si el certificado se utiliza para las autenticaciones EAP, el símbolo * no debe estar en el campo Asunto CN, ya que los solicitantes de Windows rechazan el certificado del servidor.
- Incluso cuando se inhabilita Validate Server Identity en el solicitante, el intercambio de señales SSL puede fallar cuando * está en el campo CN.


- En su lugar, se puede utilizar un FQDN genérico en el campo CN y, a continuación, el *.domain.com se puede utilizar en el campo Nombre DNS del nombre alternativo del sujeto (SAN).
-

 Nota: algunas autoridades de certificación (CA) pueden agregar automáticamente el carácter comodín (*) en la NC del certificado, incluso si no está presente en la CSR. En este escenario, se requiere una solicitud especial para evitar esta acción.

Ejemplo de CSR de certificado de servidor individual:

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
<input checked="" type="checkbox"/> 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  

Ejemplo de CSR de comodín:

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



 Nota: Cada dirección IP de nodo de implementación se puede agregar al campo SAN para evitar una advertencia de certificado cuando acceda al servidor a través de la dirección IP.

Una vez creada la CSR, ISE muestra una ventana emergente con la opción de exportarla. Una vez exportado, este archivo debe enviarse a la CA para su firma.



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

OK

Export

Paso 2. Importar una nueva cadena de certificados.

La autoridad de certificación devuelve el certificado de servidor firmado junto con la cadena de certificado completa (raíz/intermedia). Una vez recibidos, realice los pasos siguientes para importar los certificados a su servidor ISE:

1. Para importar cualquier certificado raíz y (o) intermedio proporcionado por la CA, navegue hasta Administration > Certificates > Trusted Certificates.
2. Haga clic en Importar y luego elija el certificado raíz y/o intermedio y elija las casillas de verificación relevantes según se aplican para enviar.
3. Para importar el certificado del servidor, navegue hasta Administration > Certificates > Certificate Signing Requests.
4. Seleccione el CSR creado anteriormente y haga clic en Bind Certificate.
5. Seleccione la nueva ubicación del certificado e ISE lo vincula a la clave privada creada y almacenada en la base de datos.



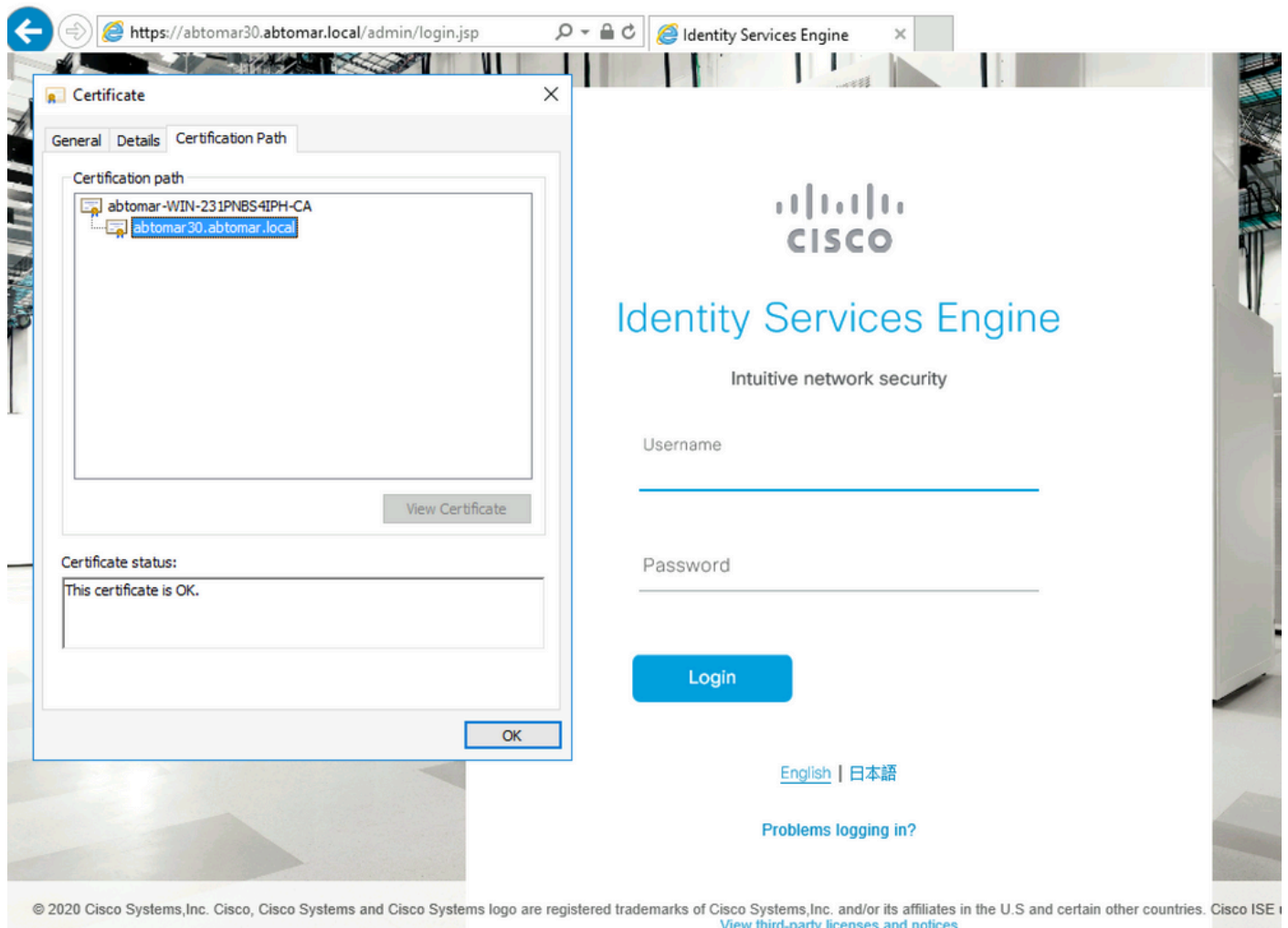
Nota: si se ha seleccionado el rol de administrador para este certificado, se reinician los servicios de servidor ISE específicos.



Precaución: si el certificado importado es para el nodo de administración principal de la implementación y se selecciona el rol de administrador, los servicios de todos los nodos se reinician uno tras otro. Se espera esto y se recomienda un tiempo de inactividad para realizar esta actividad.

Verificación

Si se seleccionó el rol de administrador durante la importación del certificado, puede comprobar que el nuevo certificado está instalado cargando la página de administración en el explorador. El explorador debe confiar en el nuevo certificado de administrador siempre que la cadena se haya creado correctamente y si el explorador confía en la cadena de certificados.



Para una verificación adicional, seleccione el símbolo de bloqueo en el navegador y, bajo la ruta del certificado, verifique que la cadena completa esté presente y que la máquina confíe en ella. Este no es un indicador directo de que el servidor transmitió correctamente la cadena completa, sino un indicador del explorador capaz de confiar en el certificado del servidor basado en su almacén de confianza local.

Troubleshoot

El solicitante no confía en el certificado de servidor local de ISE durante una autenticación dot1x

Verifique que ISE esté pasando la cadena de certificados completa durante el proceso de protocolo de enlace SSL.

Cuando se utilizan métodos EAP que requieren un certificado de servidor (es decir, PEAP) y se selecciona Validar identidad del servidor, el solicitante valida la cadena de certificados utilizando los certificados que tiene en su almacén de confianza local como parte del proceso de autenticación. Como parte del proceso de protocolo de enlace SSL, ISE presenta su certificado y también cualquier certificado raíz o intermedio presente en su cadena. El solicitante no podrá validar la identidad del servidor si la cadena está incompleta. Para comprobar que la cadena de certificados se devuelve al cliente, puede realizar los siguientes pasos:

1. Para tomar una captura de ISE (TCPDump) durante la autenticación, navegue hasta Operaciones > Herramientas de diagnóstico > Herramientas generales > Volcado TCP.
2. Descargue/abra la captura y aplique el filtro ssl.handshake.certificates en Wireshark y encuentre un desafío de acceso.
3. Una vez seleccionada, navegue hasta Expandir protocolo Radius > Pares de valor de atributo > EAP-Mensaje último segmento > Protocolo de autenticación extensible > Capa de sockets seguros > Certificado > Certificados.

Cadena de certificados en la captura.

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

```

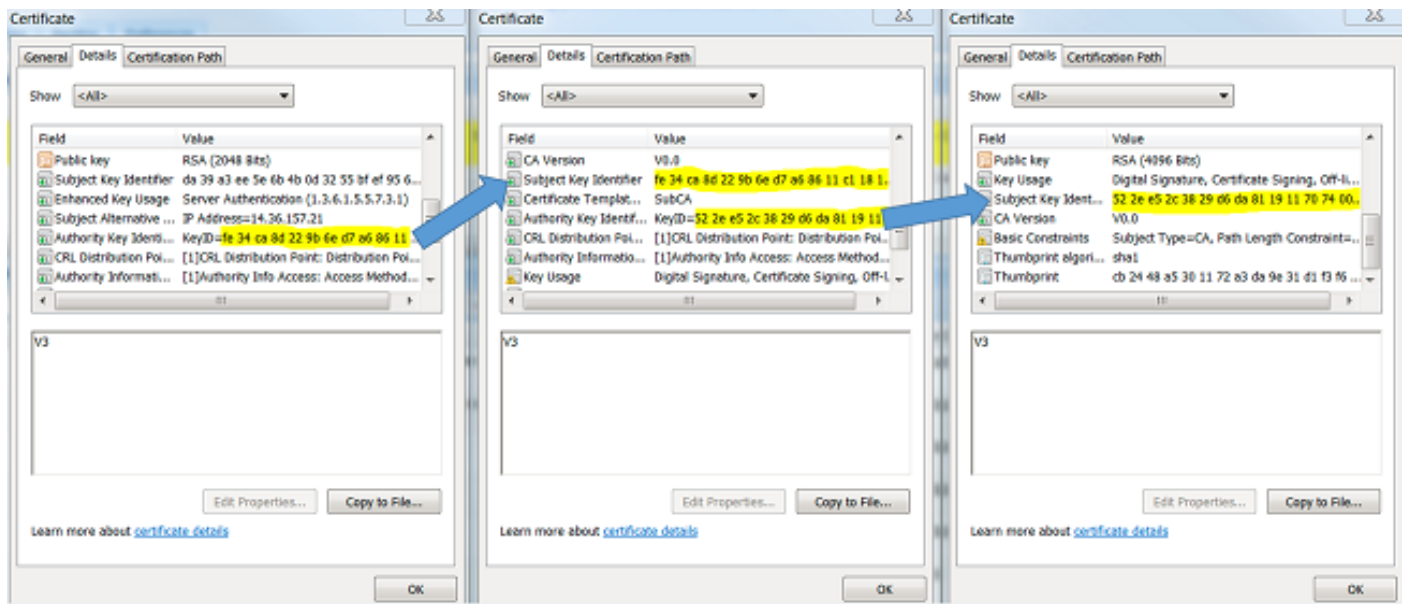
EAP fragment
  Extensible Authentication Protocol
    Code: Request (1)
    Id: 41
    Length: 1012
    Type: Protected EAP (EAP-PEAP) (25)
    EAP-TLS Flags: 0xc0
    EAP-TLS Length: 3141
    [4 EAP-TLS Fragments (3141 bytes): #857(1002), #860(1002), #862(1002), #864(135)]
  Secure Sockets Layer
    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
  
```

Si la cadena está incompleta, navegue hasta ISE Administration > Certificates > Trusted Certificates y verifique que los certificados raíz y (o) intermedios estén presentes. Si la cadena de certificados se pasa correctamente, se debe comprobar que la cadena en sí es válida mediante el método descrito aquí.

Abra cada certificado (servidor, intermedio y raíz) y verifique la cadena de confianza haciendo coincidir el identificador de clave de sujeto (SKI) de cada certificado con el identificador de clave

de autoridad (AKI) del siguiente certificado de la cadena.

Ejemplo de una cadena de certificados.

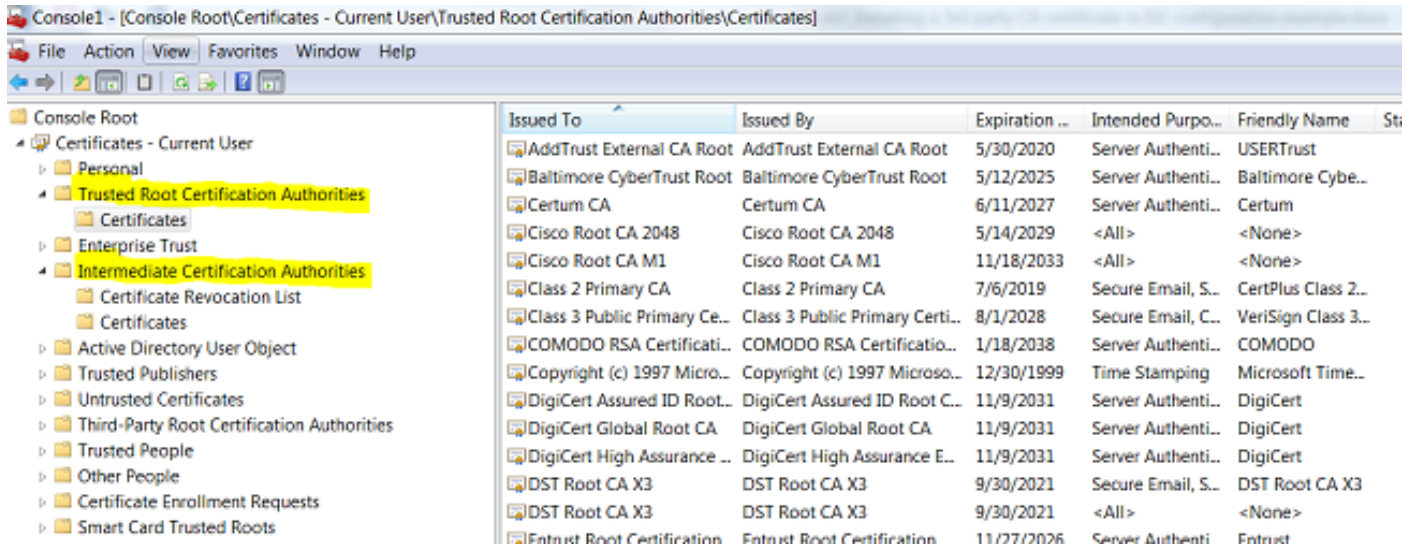


La cadena de certificados de ISE es correcta, pero el terminal rechaza el certificado de servidor de ISE durante la autenticación

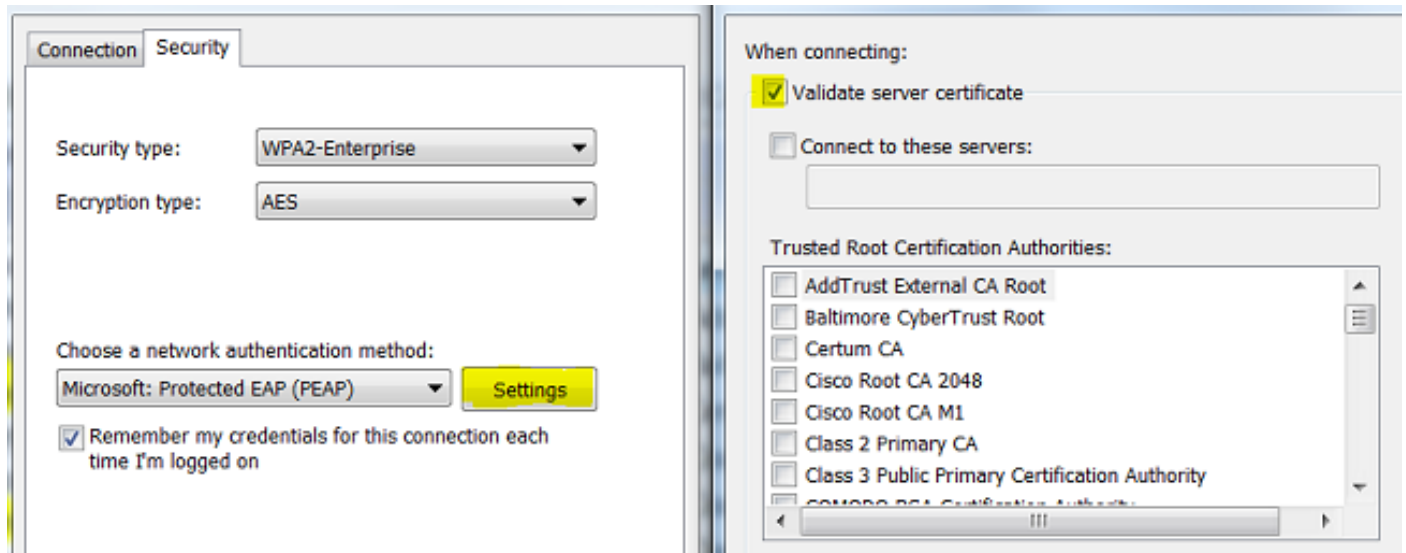
Si ISE presenta su cadena de certificados completa durante el protocolo de enlace SSL y el solicitante sigue rechazando la cadena de certificados; el siguiente paso es verificar que los certificados raíz y/o intermedios se encuentran en el almacén de confianza local del cliente.

Para verificar esto desde un dispositivo Windows, navegue hasta mmc.exe File > Add-Remove Snap-in. En la columna Complementos disponibles, seleccione Certificados y haga clic en Agregar. Seleccione Mi cuenta de usuario o cuenta de computadora dependiendo del tipo de autenticación en uso (Usuario o Equipo) y luego haga clic en Aceptar.

En la vista de consola, seleccione Entidades emisoras de certificados raíz de confianza y Entidades emisoras de certificados intermedias para comprobar la presencia del certificado raíz e intermedio en el almacén de confianza local.



Una manera fácil de verificar que este es un problema de Verificación de identidad del servidor, desmarque Validar certificado de servidor bajo la configuración del perfil del solicitante y pruébelo nuevamente.



Información Relacionada

- [Guía del administrador de Cisco Identity Services Engine, versión 3.0](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).