Instale un certificado de CA de las de otras compañías en ISE 2.0

Contenido

Introducción

Este documento describe el instalar de un certificado firmado de CA de las de otras compañías en Cisco Identity Services Engine.

El proceso es lo mismo sin importar el papel final del certificado (autenticación EAP, portal, Admin y pxGrid).

Requisitos

Conocimiento básico del Public Key Infrastructure.

Componentes Utilizados

La información en este documento se basa en las versiones de software y hardware siguientes:

- Versión 2.0 del Cisco Identity Services Engine (ISE). La misma configuración se aplica a las versiones 1.3 y 1.4.

Configurar

Generación del pedido de firma de certificado (CSR):

Para generar el CSR vaya a la administración > a los Certificados > a los pedidos de firma de certificado y selecto genere los pedidos de firma de certificado (CSR).

- Bajo sección del uso seleccione el papel para ser utilizado del menú desplegable. Si el certificado es utilizado para los papeles múltiples usted puede seleccionar el Multi-uso. Una vez que se genera el certificado los papeles se pueden cambiar en caso necesario.
- Seleccione el nodo para el cual el certificado será generado.
- Complete la información según las necesidades (unidad organizativa, organización, ciudad, estado y país).

Note: Bajo campo del Common Name (CN) el ISE auto poblará el nombre de dominio completo (FQDN) del nodo.

Comodines:

- Si la meta es generar un control del certificado del comodín “permita el cuadro de los Certificados del comodín”.
- Si el certificado es utilizado para las autenticaciones EAP “*” el símbolo no debe estar en el campo del tema CN pues los suplicantes de Windows rechazarán el certificado de servidor.
- Incluso cuando “valide la identidad del servidor” se inhabilita en el supplicant, el contacto SSL puede fallar cuando “*” está en el campo CN.
- En lugar, un FQDN genérico se puede utilizar en el campo CN, y entonces el “*.domain.com” se puede utilizar en el campo de nombre DNS alternativo sujeto del nombre (SAN).

Note: Algunas autoridades de certificación pueden agregar al comodín (*) en el CN del certificado automáticamente incluso si él no presente en el CSR. En este escenario, una petición especial me necesitará hizo para prevenir esta acción.

Ejemplo del certificado de servidor individual CSR:

Ejemplo del comodín CSR:

Note: La dirección IP de cada nodo del despliegue se puede agregar al campo SAN para evitar una advertencia del certificado cuando usted accede el servidor vía la dirección IP.

Una vez que se ha creado el CSR, el ISE visualizará un estallido encima de la ventana con la opción para exportarla. Una vez que está exportado, este archivo se debe enviar a CA para firmar.

Importación de la nueva Cadena de certificados:

El Certificate Authority devolverá el certificado de servidor firmado junto con el encadenamiento de firma lleno (raíz/intermedio). Una vez que está recibido, siga los pasos abajo para importar los Certificados en su servidor ISE.

1. Importe cualquier raíz y (o) Certificados intermedio proporcionados por CA yendo a la administración > a los Certificados > a los certificados confiables.
2. Importe el certificado de servidor yendo a la administración >> a los Certificados >> a los pedidos de firma de certificado.
3. Seleccione el CSR creado previamente y haga clic en el certificado del lazo.
4. Seleccione la nueva ubicación del certificado y el ISE atará el certificado a la clave privada creada y salvada en la base de datos.

Note: Si el papel Admin se ha seleccionado para este certificado, el ISE recomenzará los servicios.

Verificación

Si el papel admin fue seleccionado durante la importación del certificado usted puede verificar el nuevo certificado existe cargando la página de administración en el navegador. El navegador debe confiar en el nuevo certificado admin mientras el encadenamiento fuera construido correctamente y si la Cadena de certificados es confiada en por el navegador.

Para la verificación adicional seleccione el símbolo del bloqueo en el navegador y bajo la trayectoria del certificado verifique el encadenamiento lleno es presente y confiado en por la máquina. Esto no es un indicador directo que el encadenamiento lleno fue pasado abajo correctamente por el servidor pero un indicador del navegador capaz de confiar en el certificado de servidor basado en su almacén local de la confianza.

Troubleshooting

El supplicant no confía en el certificado de servidor local ISE durante una autenticación del dot1x.

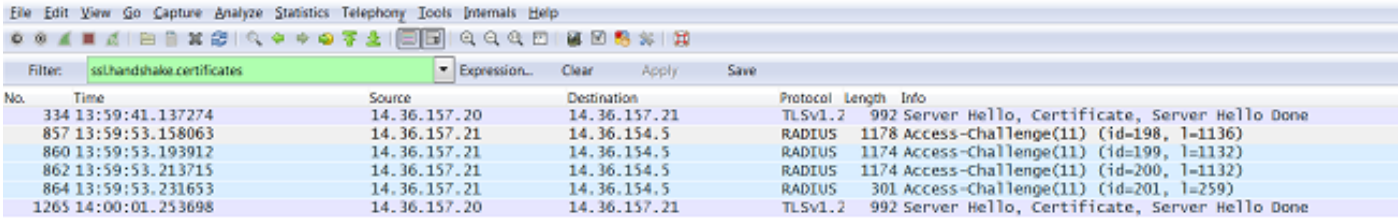
Verifique el ISE está pasando la Cadena de certificados llena durante el proceso del contacto SSL.

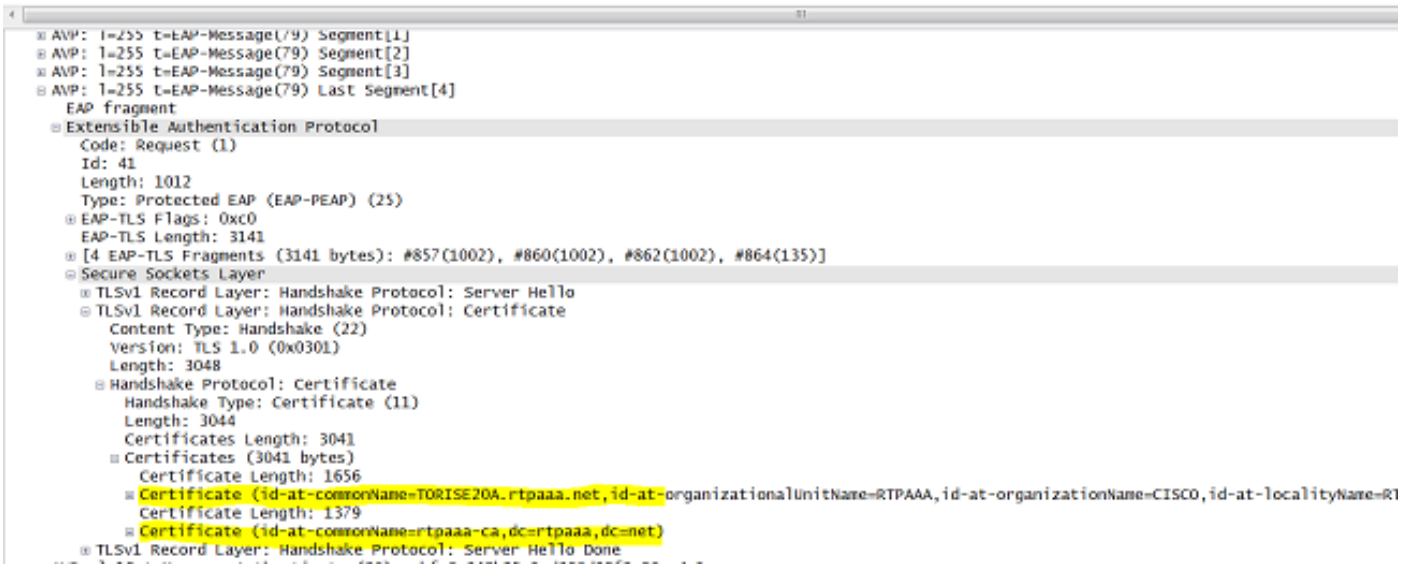
Al usar los métodos EAP que requieren un certificado de servidor (es decir PEAP) y “valide la identidad del servidor” se selecciona, el supplicant validará la Cadena de certificados usando los Certificados que tiene en su almacén local de la confianza como parte del proceso de autenticación. Como parte del proceso del contacto SSL el ISE presentará su certificado y también cualquier raíz y (o) Certificados intermedio presentes en su encadenamiento. El supplicant no podrá validar la identidad del servidor si el encadenamiento es incompleto. Para verificar la Cadena de certificados se devuelve a su cliente, usted puede realizar los pasos siguientes:

1. Tome una captura de ISE (tcpdump) durante la autenticación. Encontró bajo las operaciones > Diagostic equipa > las herramientas generales > volcado TCP
2. Descargue/abra la captura y aplique el filtro “ssl.handshake.certificates” en Wireshark y encuentre un acceso-desafío.
3. Una vez que está seleccionado, amplíe el protocolo RADIUS > los pares de valores de atributos > el segmento > el protocolo extensible

authentication > Secure Sockets Layer > el certificado > los Certificados más recientes del mensaje EAP

Cadena de certificados en la captura.

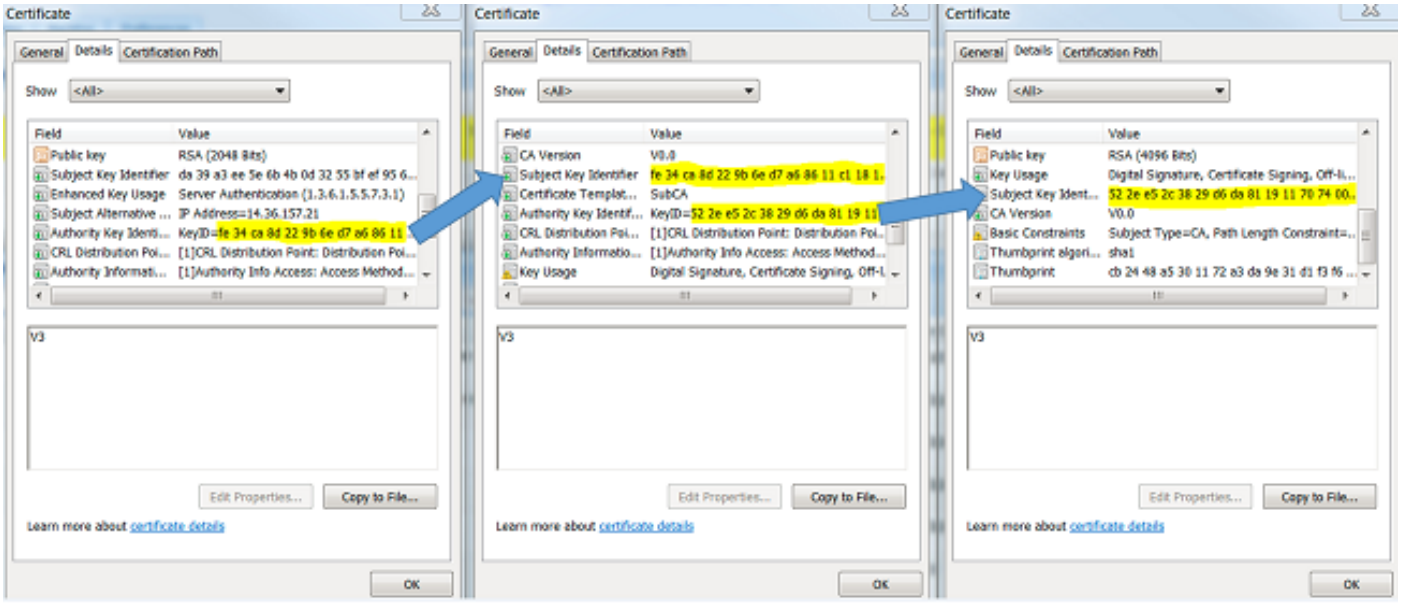




Si el encadenamiento no es completo usted debe ir a la administración > a los Certificados > a los certificados confiables ISE y verificar que la raíz y (o) los Certificados intermedios están presentes. Si la Cadena de certificados se pasa con éxito, el encadenamiento sí mismo se debe verificar como válido usando el método delineado abajo.

Abra cada certificado (servidor, intermedio y raíz) y verifique el encadenamiento de la confianza correspondiendo con el identificador dominante sujeto (ESQUÍ) de cada certificado al identificador de la clave de la autoridad (AKI) del certificado siguiente en el encadenamiento.

Ejemplo de la Cadena de certificados.



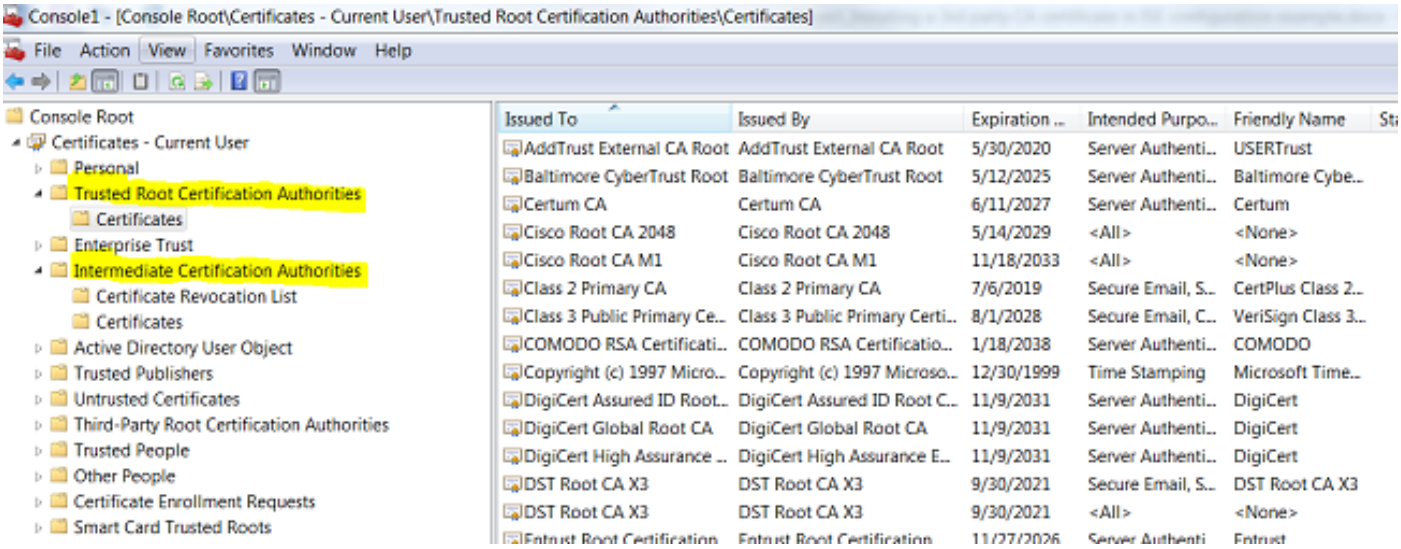
La Cadena de certificados ISE es certificado de servidor correcto pero del punto final de los rechazos ISE durante la autenticación.

Si el ISE está presentando su Cadena de certificados llena durante el contacto SSL y el supplicant todavía está rechazando la Cadena de certificados; el siguiente paso es verificar que los Certificados intermedios del and(or) de la raíz están en el almacén local de la confianza del cliente.

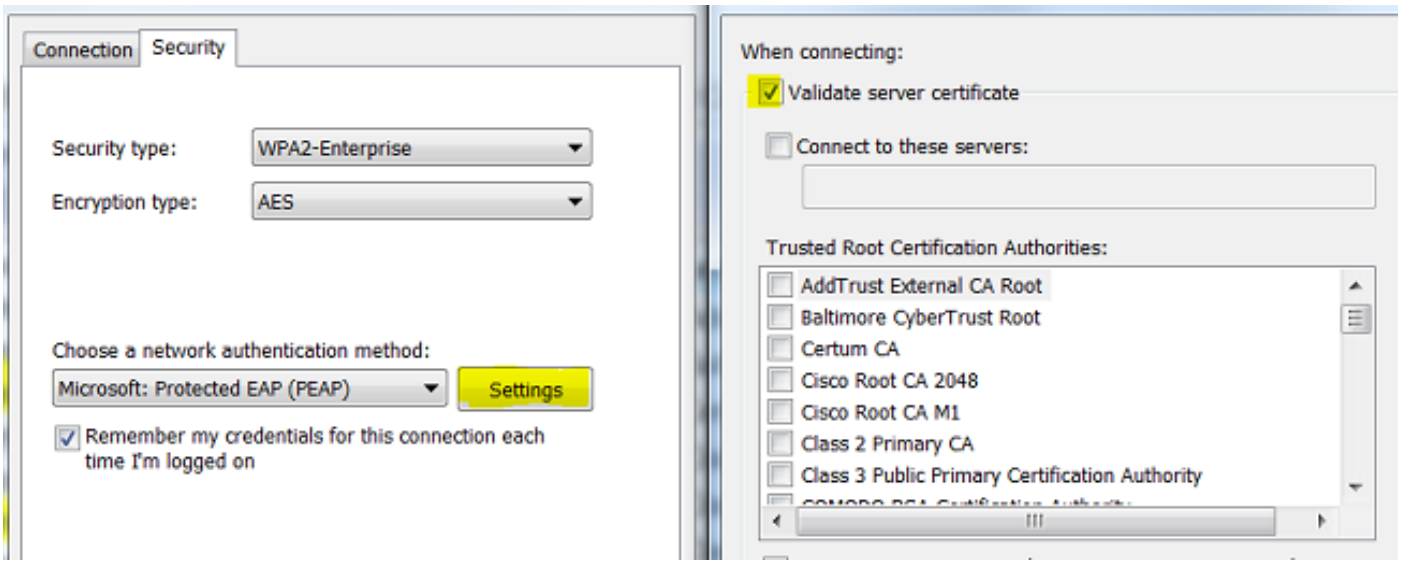
Para verificar esto de un archivo abierto del dispositivo mmc.exe de Windows > Agregar-quite Broche-en > de los Certificados selectos de la columna

disponible broche-INS > Add > seleccionan “mi cuenta de usuario” o la “cuenta del ordenador” dependiendo del tipo de autenticación funcionando (usuario o máquina). > ACEPTABLE

Bajo Trusted Root Certification Authority selectos” de la opinión de la consola los “y “autoridades de certificación intermedias” para verificar la presencia de certificado de la raíz y del intermedio en el almacén local de la confianza.



Una forma sencilla de verificar que esto sea un problema del control de la identidad del servidor, desmarca “valida el certificado de servidor” bajo configuración del perfil del supplicant y lo prueba otra vez.



Note: El ISE no soporta actualmente el proceso de los Certificados usando RSASSA-PSS como algoritmo de la firma. Esto incluye el certificado de servidor, la raíz, el intermedio o el certificado del cliente (es decir EAP-TLS, PEAP (TLS), etc.). Refiera al bug CSCug22137.

Referencias

- Guía del administrador del Cisco Identity Services Engine, versión 2.0