Certificado SAML ISE

Contenido

Introducción

Este documento describe los certificados del sistema del lenguaje de marcado de aserción de seguridad (SAML) en Cisco Identity Services Engine (ISE). Abarca el propósito de los certificados SAML, cómo realizar la renovación y, por último, responde a las preguntas frecuentes frecuentes. Abarca ISE de la versión 2.4 a la 3.0; sin embargo, debería ser similar o idéntico a otras versiones de software ISE 2.x y 3.x, a menos que se indique lo contrario.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

1. ISE de Cisco
2. La terminología utilizada para describir diferentes tipos de ISE y implementaciones de autenticación, autorización y contabilidad (AAA)
3. Conceptos básicos de AAA y protocolo RADIUS
4. protocolo SAML
5. Certificados SSL/TLS y x509
6. Conceptos básicos de la infraestructura de clave pública (PKI)

Componentes Utilizados

La información de este documento se basa en Cisco Identity Services Engine (ISE), versiones 2.4 - 3.0

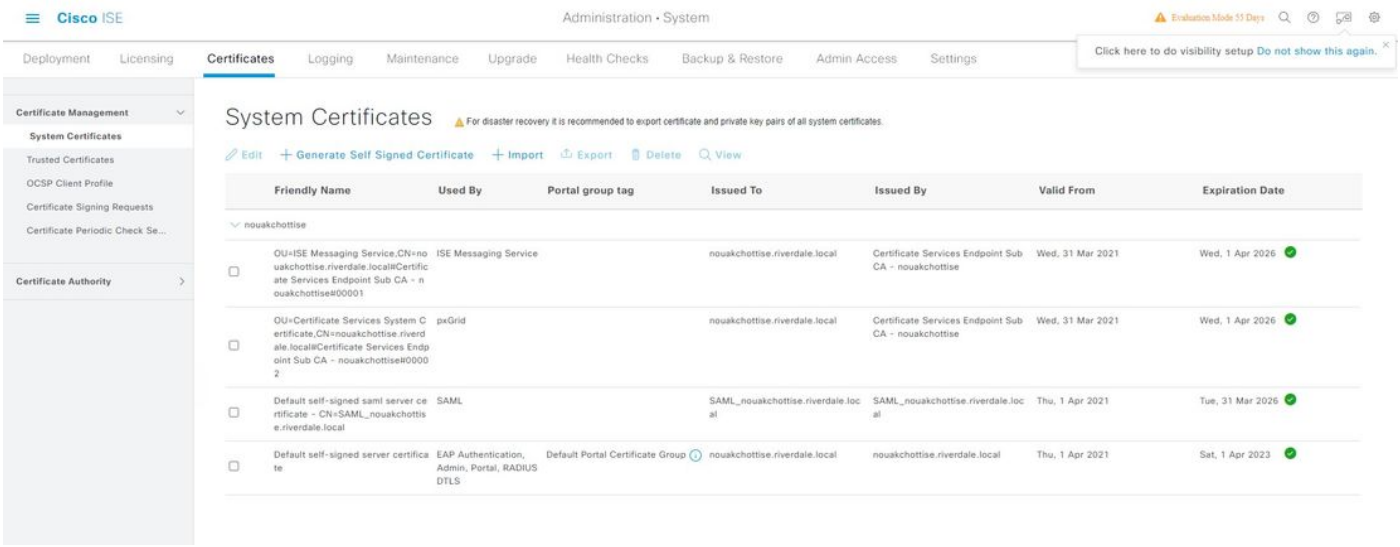
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier comando o configuración.

Certificados SSL en ISE

Un certificado de Secure Sockets Layer (SSL) es un archivo digital que identifica a una persona, un servidor o cualquier otra entidad digital y asocia esa entidad a una clave pública. El creador firma un certificado autofirmado. Los certificados pueden ser firmados automáticamente o firmados digitalmente por una autoridad certificadora externa (CA), normalmente el propio servidor de la CA de una empresa o un proveedor de la CA bien conocido. Un certificado digital firmado por CA se considera un estándar del sector y más seguro que un certificado autofirmado.

Cisco ISE se basa en PKI para proporcionar una comunicación segura con los terminales y los administradores, entre ISE y otros servidores/servicios, y entre los nodos Cisco ISE en una implementación de varios nodos. PKI se basa en certificados digitales X.509 para transferir claves públicas para el cifrado y el descifrado de mensajes y para verificar la autenticidad de otros certificados que representan a usuarios y dispositivos. A través del portal de administración de Cisco ISE, puede administrar estos certificados X.509.

En ISE, los certificados del sistema son certificados de servidor que identifican un nodo de Cisco ISE a otras aplicaciones (como terminales, otros servidores, etc.). Cada nodo de Cisco ISE tiene sus propios certificados de sistema almacenados en el nodo junto con las claves privadas correspondientes. Cada certificado del sistema se puede asignar a 'Roles' que indican el propósito del certificado como se muestra en la imagen.

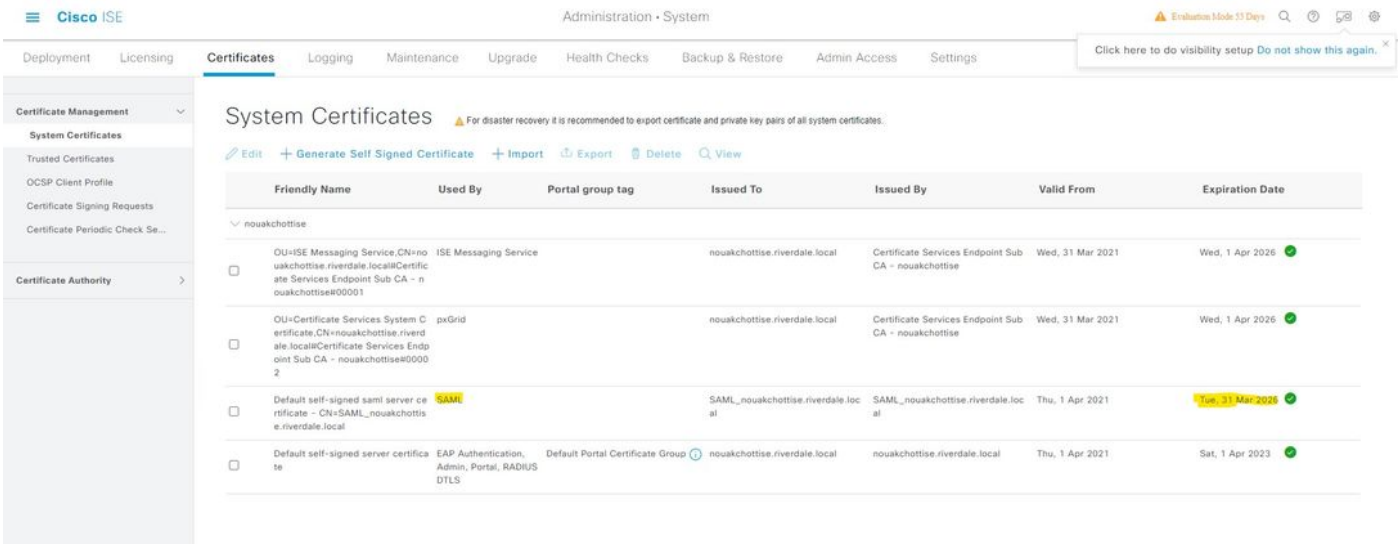


Certificados del sistema ISE 3.0

El alcance de este documento es sólo para el certificado SAML. Para ver otros certificados en ISE, y más sobre los certificados SSL en ISE en general, consulte este documento: Certificados TLS/SSL en ISE - Cisco

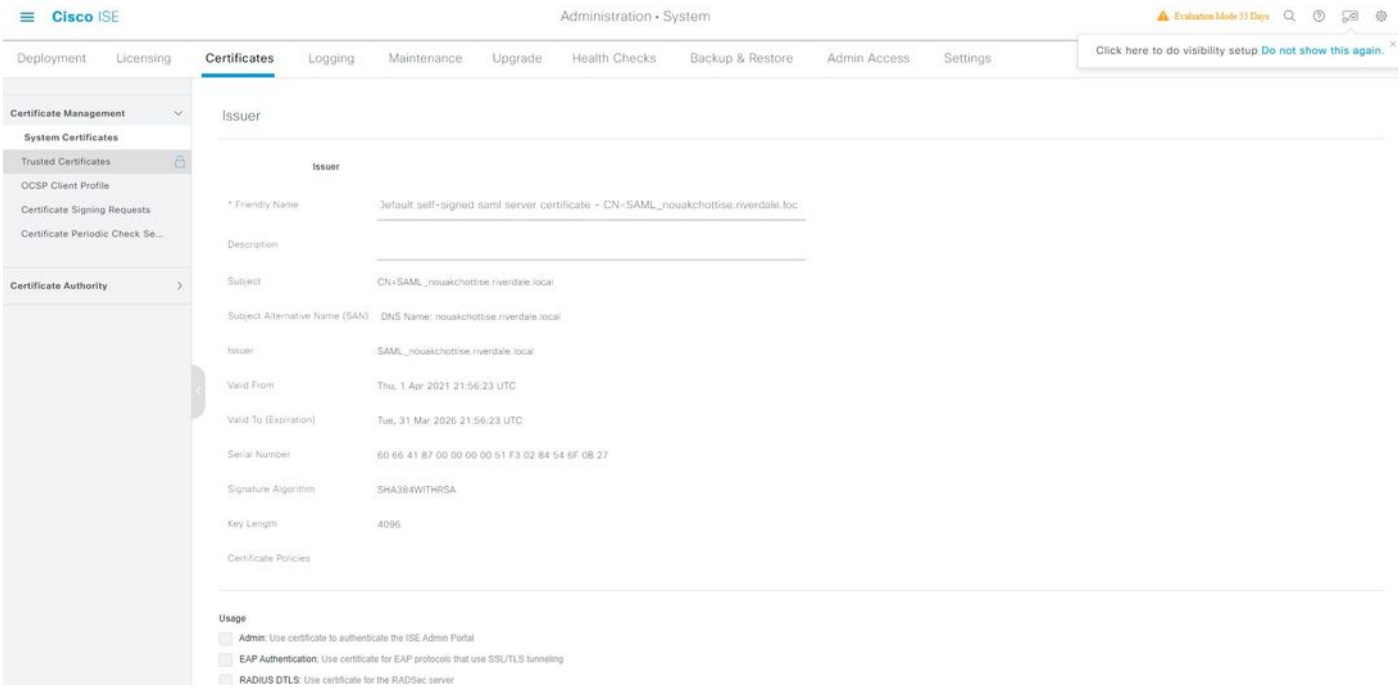
Certificado SAML en ISE

El certificado SAML en ISE se determina buscando certificados del sistema que tengan la entrada SAML en el campo Usos. Este certificado se utilizará para comunicarse con los proveedores de identidad (IdP) de SAML, como para verificar que las respuestas de SAML se reciban del IdP correcto y para asegurar la comunicación con el IdP. Tenga en cuenta que los certificados designados para el uso de SAML no se pueden utilizar para ningún otro servicio como Admin, EAP authentication, etc.



Por primera vez en las instalaciones de ISE, ISE viene con un certificado de servidor SAML autofirmado que tiene estas propiedades:

Tamaño de clave: 2048
Validez: un año
Uso clave: Firma digital (firma)
Uso de clave extendido: Autenticación de servidor Web TLS (1.3.6.1.5.5.7.3.1)



> **Nota:** Se recomienda no utilizar un certificado que contenga el valor 2.5.29.37.0 para el identificador de objeto Any Purpose en el atributo Extended Key Usage. Si utiliza un certificado que contiene el valor 2.5.29.37.0 para el identificador de objeto Any Purpose en el atributo Extended Key Usage, el certificado se considera no válido y se muestra el siguiente mensaje de error: "source=; local type=mensaje ; fatal="certificado no admitido".

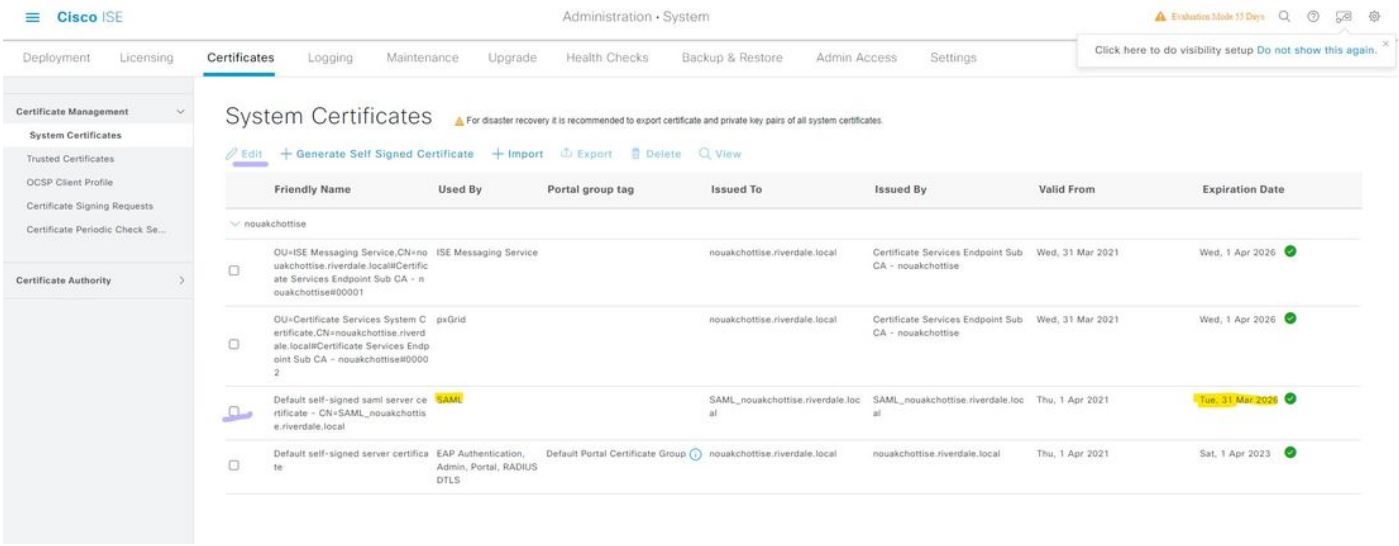
Los administradores de ISE tendrán que renovar este certificado SAML firmado automáticamente antes de la expiración, incluso si la función SAML no se utiliza activamente.

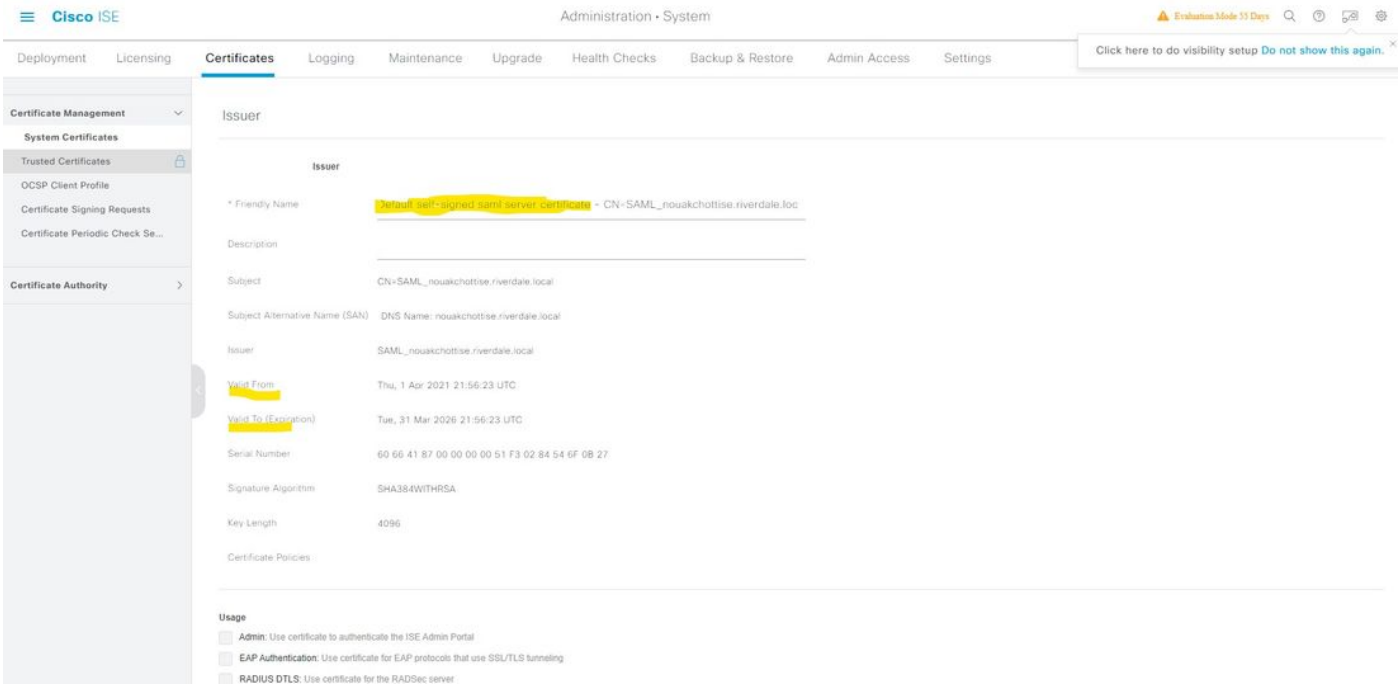
Renovación de un certificado SAML firmado automáticamente en ISE

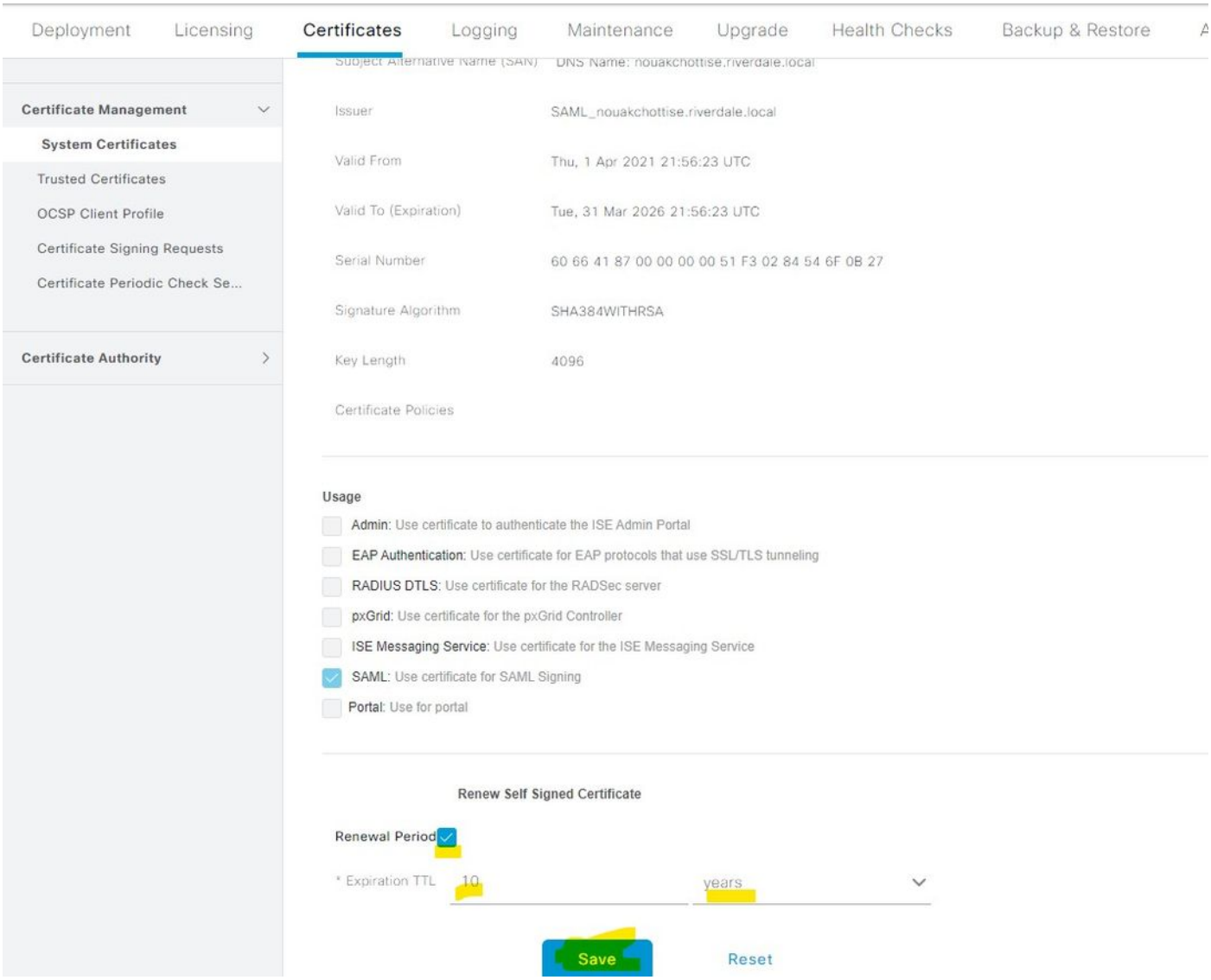
Un problema común al que se enfrentan los usuarios es que sus certificados SAML caducarán finalmente e ISE les alerta con este mensaje:

```
Alarm Name :
Certificate Expiration

Details :
Trust certificate 'Default self-signed server certificate' will expire in 60 days :
Server=Kolkata-ISE-001

Description :
This certificate will expire soon. When it expires, ISE may fail when attempting to establish
secure communications with clients. Inter-node communication may also be affected

Severity :
Warning

Suggested Actions :
Replace the certificate. For a trust certificate, contact the issuing Certificate Authority
(CA). For a CA-signed local certificate, generate a CSR and have the CA create a new
certificate. For a self-signed local certificate, use ISE to extend the expiration date. You can
just delete the certificate if it is no longer used.
```

Para los certificados de servidor autofirmados, es posible renovar el certificado sólo para marcar el período de renovación de la casilla y poner entre 5 y 10 años como se muestra en la imagen.







De hecho, cualquier certificado autofirmado que no esté activo utilizado por sus nodos de implementación de ISE puede renovarse simplemente por un período de 10 años; esto le asegura que no reciba ningún aviso de vencimiento para los certificados de los servicios que no esté

utilizando. 10 años es la duración máxima permitida para los certificados autofirmados de ISE, y normalmente debería ser suficiente. La actualización de cualquier certificado del sistema en el ISE no activa un reinicio de servicios siempre que no esté designado para el uso 'Admin'.

Conclusión

Para cualquier certificado de sistema ISE caducado (firmado automáticamente y firmado por CA) que no se esté utilizando, está bien sustituirlo, eliminarlo o renovarlo, y se recomienda no dejar ningún certificado caducado (sistema o de confianza) en ISE antes de realizar una actualización de ISE.

Información Relacionada

- ISE 3.0 Gestión de certificados: Guía del administrador de Cisco Identity Services Engine, versión 3.0 - Configuración básica [Cisco Identity Services Engine] - Cisco
- Certificados SSL en ISE: Certificados TLS/SSL en ISE - Cisco
- Soporte Técnico y Documentación - Cisco Systems