Certificado SAML do ISE

Contents

Introduction

Este documento descreve os certificados do sistema SAML (Security Assertion Markup Language) no Cisco Identity Services Engine (ISE). Ele abrange a finalidade dos certificados SAML, como executar a renovação e, finalmente, responde às perguntas frequentes. Ele abrange o ISE da versão 2.4 para a 3.0, no entanto, ele deve ser semelhante ou idêntico a outras versões de software do ISE 2.x e 3.x, a menos que declarado de outra forma.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

1. Cisco ISE
2. A terminologia usada para descrever diferentes tipos de implantações de ISE e de AAA (Authentication, Authorization and Accounting, Autenticação, Autorização e Contabilidade)
3. Protocolo RADIUS e conceitos básicos de AAA
4. protocolo SAML
5. Certificados SSL/TLS e x509
6. Princípios básicos da infraestrutura de chave pública (PKI)

Componentes Utilizados

As informações neste documento são baseadas no Cisco Identity Services Engine (ISE), versões 2.4 - 3.0

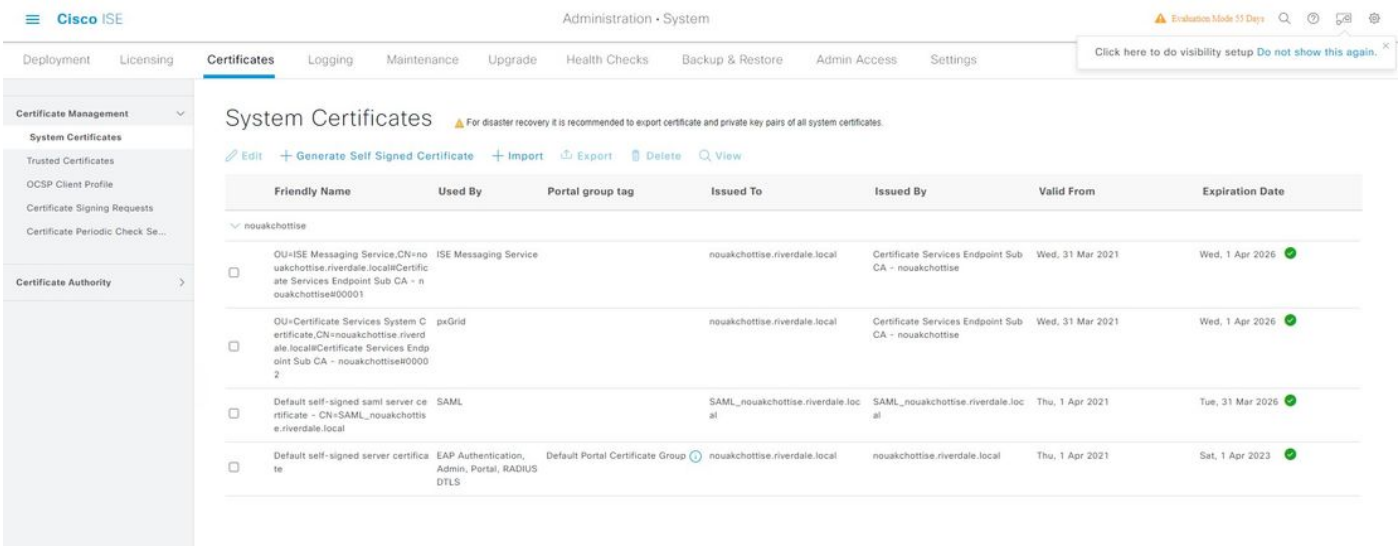
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a sua rede estiver ativa, certifique-se de que você entende o impacto potencial de qualquer comando ou configuração.

Certificados SSL no ISE

Um certificado SSL (Secure Sockets Layer) é um arquivo digital que identifica um indivíduo, um servidor ou qualquer outra entidade digital e associa essa entidade a uma chave pública. Um certificado autoassinado é assinado por seu criador. Os certificados podem ser autoassinados ou assinados digitalmente por uma autoridade de certificação externa (AC) - geralmente um servidor de CA da própria empresa ou um fornecedor de CA bem conhecido. Um certificado digital assinado por CA é considerado um padrão do setor e mais seguro do que um certificado autoassinado.

O Cisco ISE depende do PKI para fornecer comunicação segura com endpoints e administradores, entre o ISE e outros servidores/serviços e entre nós do Cisco ISE em uma implantação de vários nós. O PKI conta com certificados digitais X.509 para transferir chaves públicas para criptografia e descriptografia de mensagens e verificar a autenticidade de outros certificados que representam usuários e dispositivos. Por meio do portal de administração do Cisco ISE, você pode gerenciar esses certificados X.509.

No ISE, os certificados do sistema são certificados de servidor que identificam um nó do Cisco ISE para outros aplicativos (como endpoints, outros servidores, etc.). Cada nó do Cisco ISE tem seus próprios certificados de sistema armazenados no nó juntamente com as chaves privadas correspondentes. Cada certificado do sistema pode ser mapeado para 'Funções' que indicam a finalidade do certificado como mostrado na imagem.



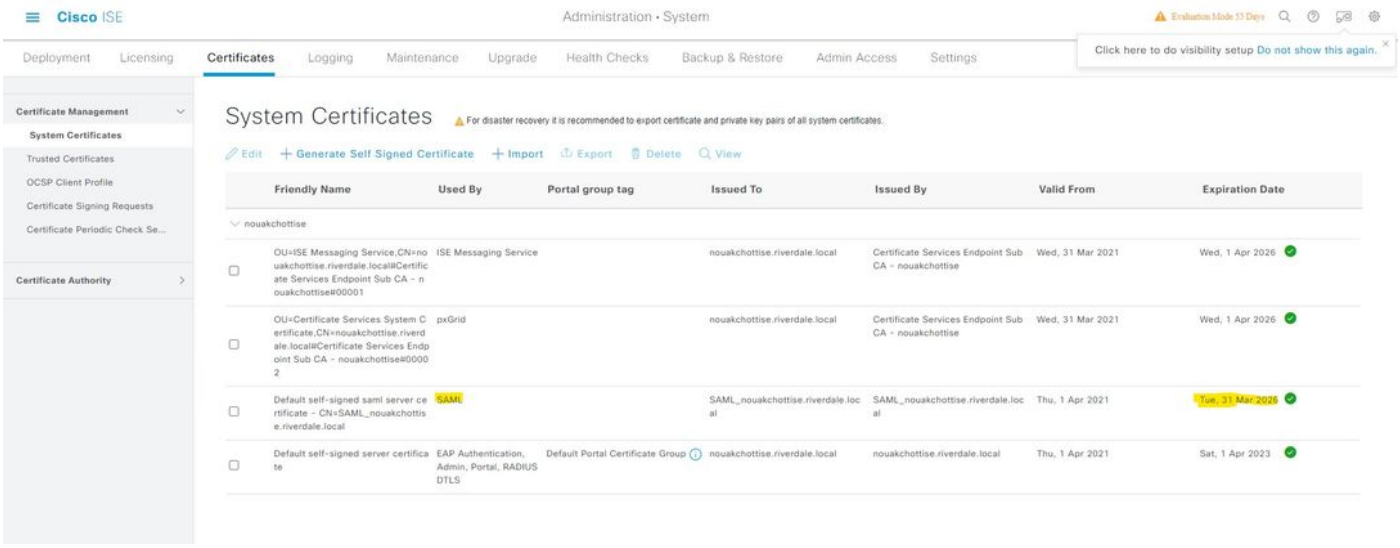
Certificados do sistema ISE 3.0

O escopo deste documento é apenas para o certificado SAML. Para outros certificados no ISE, e mais sobre certificados SSL no ISE em geral, consulte este documento: Certificados TLS/SSL no ISE - Cisco

Certificado SAML no ISE

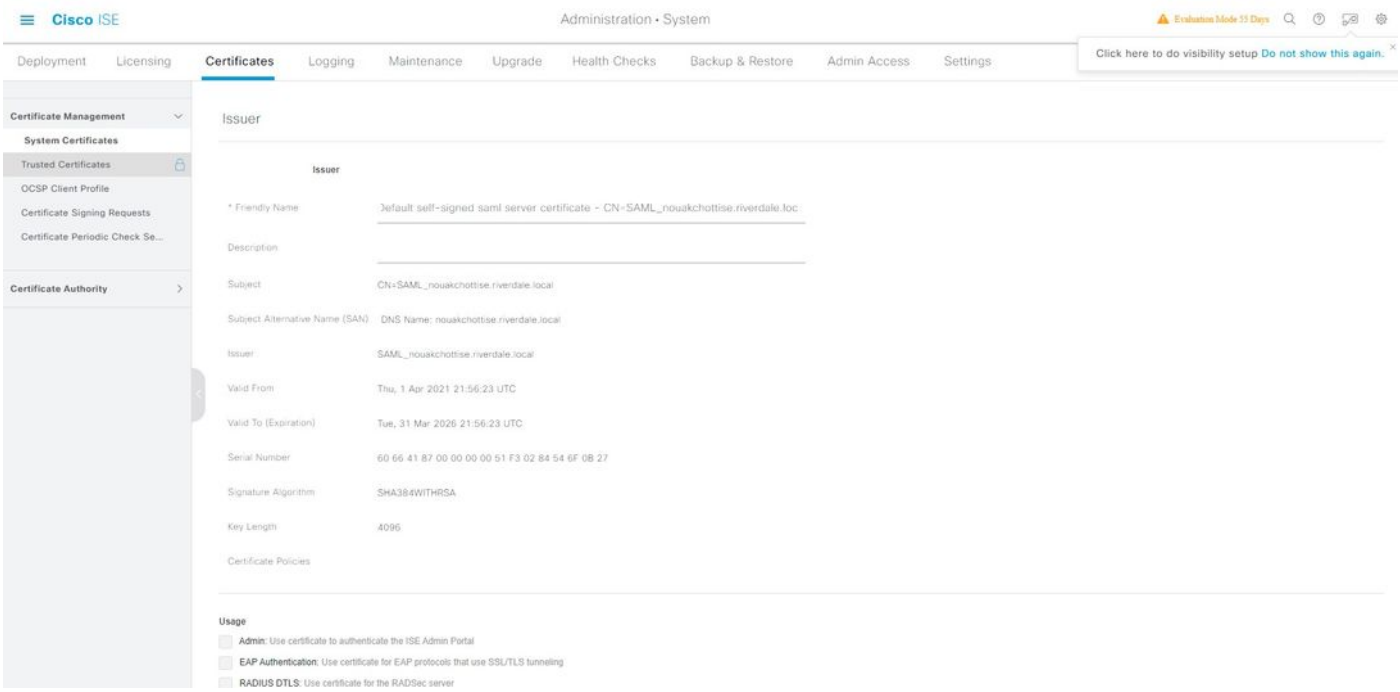
O certificado SAML no ISE é determinado procurando certificados do sistema com a entrada SAML no campo Usages. Este certificado será usado para se comunicar com provedores de identidade SAML (IdP), como verificar se as respostas SAML estão sendo recebidas do IdP correto e para garantir a comunicação com o IdP. Observe que os certificados designados para o uso de SAML não podem ser usados para nenhum outro serviço, como Admin, autenticação EAP

e assim por diante.



Pela primeira vez em instalações do ISE, o ISE vem com um certificado de servidor SAML autoassinado que tem estas propriedades:

Tamanho da chave: 2048
Validade: um ano
Uso principal: Assinatura digital (assinatura)
Uso de chave estendida: Autenticação do servidor Web TLS (1.3.6.1.5.5.7.3.1)



Note: Recomenda-se que você não use um certificado que contenha o valor 2.5.29.37.0 para o identificador de objeto Qualquer Finalidade no atributo Uso de Chave Estendida. Se você usar um certificado que contenha o valor 2.5.29.37.0 para o identificador de objeto Qualquer Finalidade no atributo Uso da Chave Estendida, o certificado será considerado inválido e a seguinte mensagem de erro será exibida: "source=local ; type=fatal ; message="unsupported certificate".

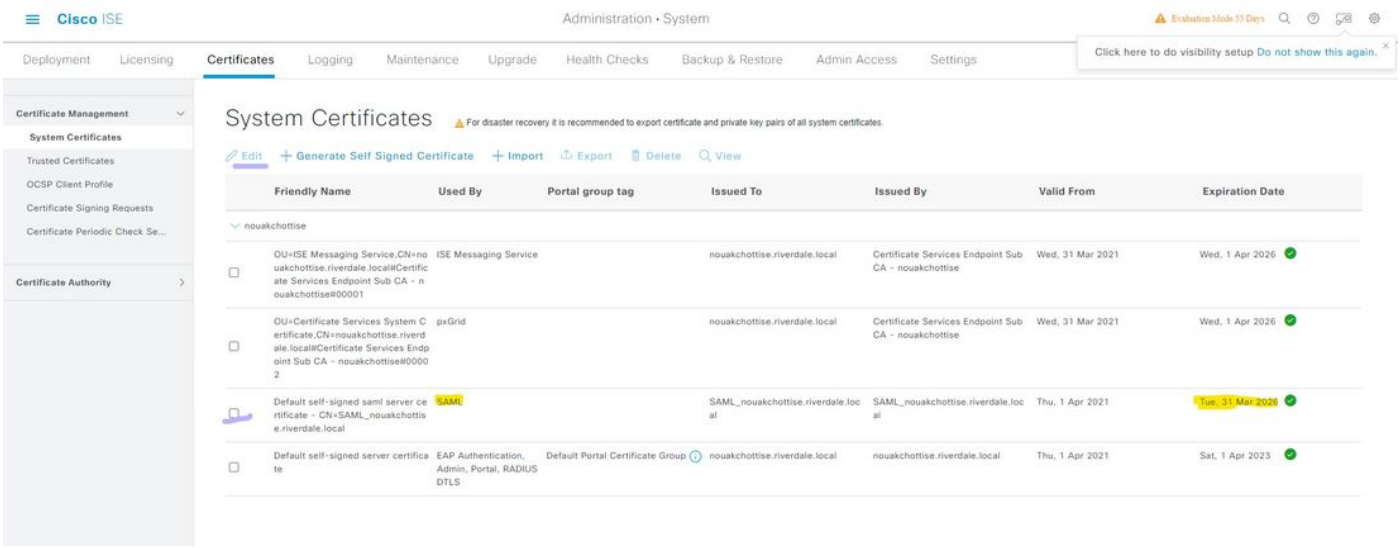
Os administradores do ISE precisarão renovar este certificado SAML autoassinado antes de expirar, mesmo que o recurso SAML não seja usado ativamente.

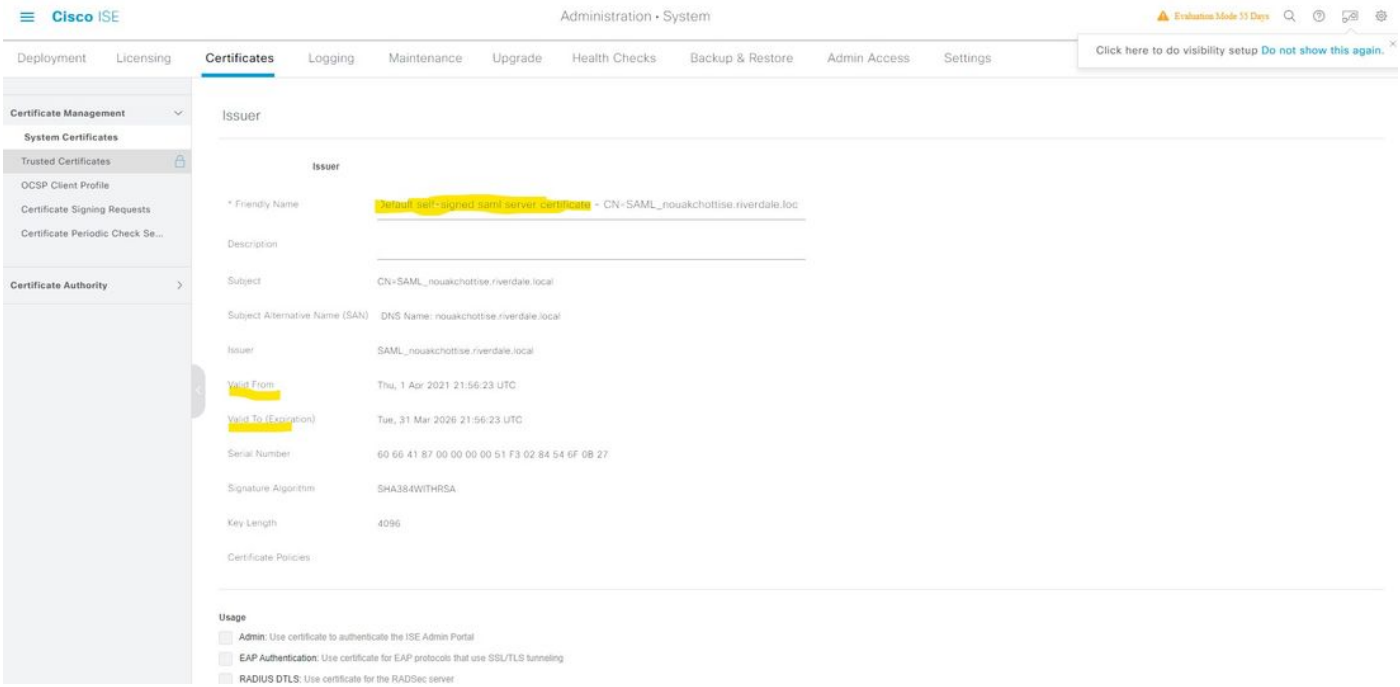
Renove um certificado SAML autoassinado no ISE

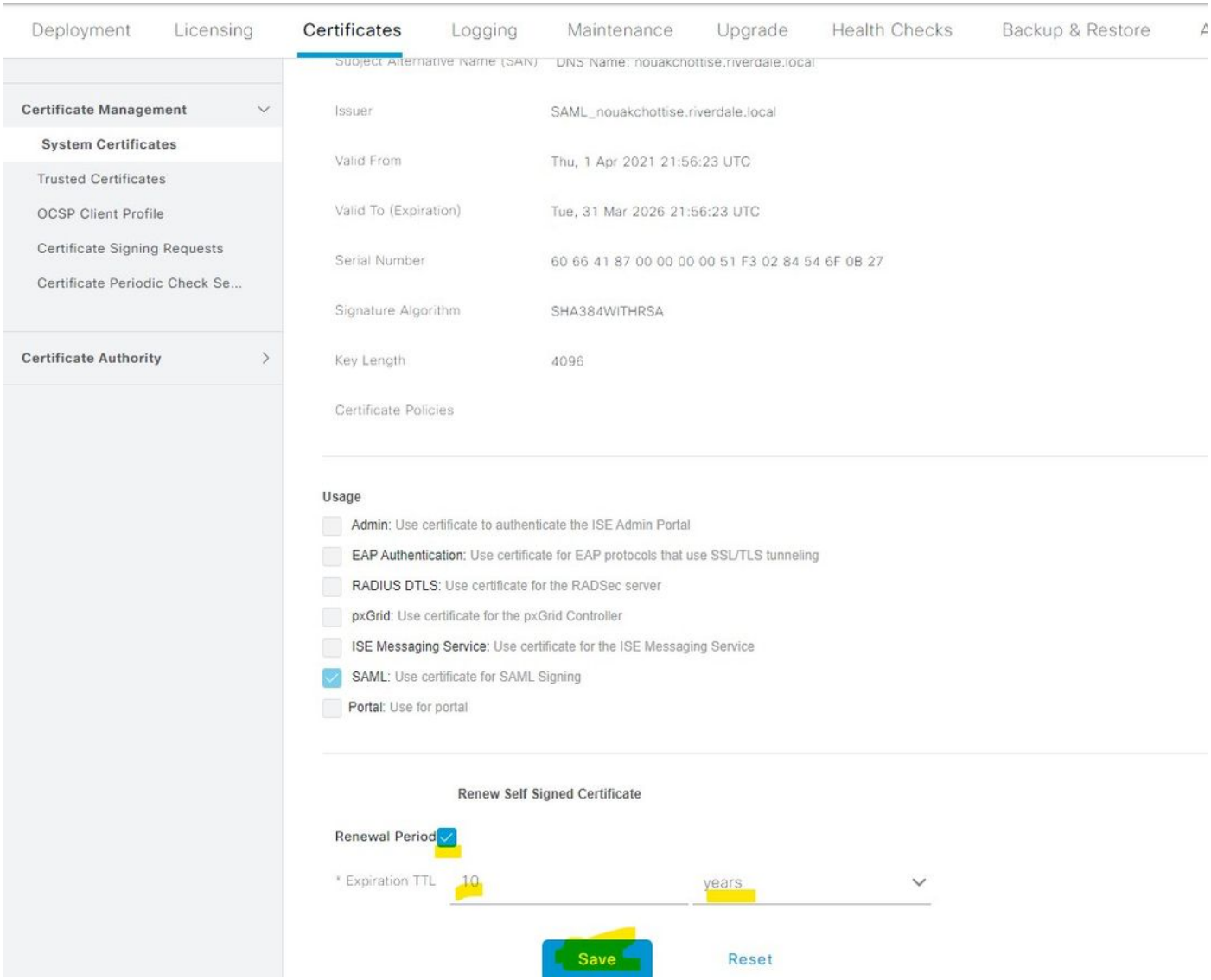
Um problema comum que os usuários enfrentam é que seus certificados SAML serão expirados, e o ISE os alerta com esta mensagem:

```
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 certificados de servidor autoassinados, é possível renovar o certificado apenas para marcar o período de renovação da caixa e colocar de 5 a 10 anos como mostrado na imagem.







Na verdade, qualquer certificado autoassinado que não esteja ativo usado pelos nós de implantação do ISE pode ser simplesmente renovado por um período de 10 anos; isso garante que você não obtenha nenhum aviso de expiração para certificados para serviços que você não

está usando. 10 anos é a vida útil máxima permitida para certificados autoassinados do ISE, e geralmente deve ser suficiente. A atualização de quaisquer certificados de sistema no ISE não aciona uma reinicialização dos serviços, desde que não seja designado para o uso de 'Admin'.

Conclusão

Para qualquer certificado de sistema ISE expirado (autoassinado e com assinatura CA) não em uso, é aceitável substituí-lo, excluí-lo ou renová-lo e é recomendável não ter certificados expirados (Sistema ou Confiável) deixados no ISE antes de executar uma atualização do ISE.

Informações Relacionadas

- O ISE 3.0 gerencia certificados: Guia do administrador do Cisco Identity Services Engine, versão 3.0 - Configuração básica [Cisco Identity Services Engine] - Cisco
- Certificados SSL no ISE: Certificados TLS/SSL no ISE - Cisco
- Suporte Técnico e Documentação - Cisco Systems