ISE SAML Certificate

Contents

Introduction

This document describes Security Assertion Markup Language (SAML) System Certificates in Cisco Identity Services Engine (ISE). It covers the purpose of the SAML certificates, how to perform renewal, and finally answers frequent FAQs. It covers ISE from version 2.4 to 3.0, however, it should be similar or identical to other ISE 2.x and 3.x Software Releases unless stated otherwise.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

1. Cisco ISE
2. The terminology used to describe different types of ISE and Authentication, Authorization and Accounting (AAA) deployments
3. RADIUS protocol and AAA basics
4. SAML protocol
5. SSL/TLS and x509 certificates
6. Public Key Infrastructure (PKI) basics

Components Used

The information in this document is based on Cisco Identity Services Engine (ISE), Releases 2.4 - 3.0

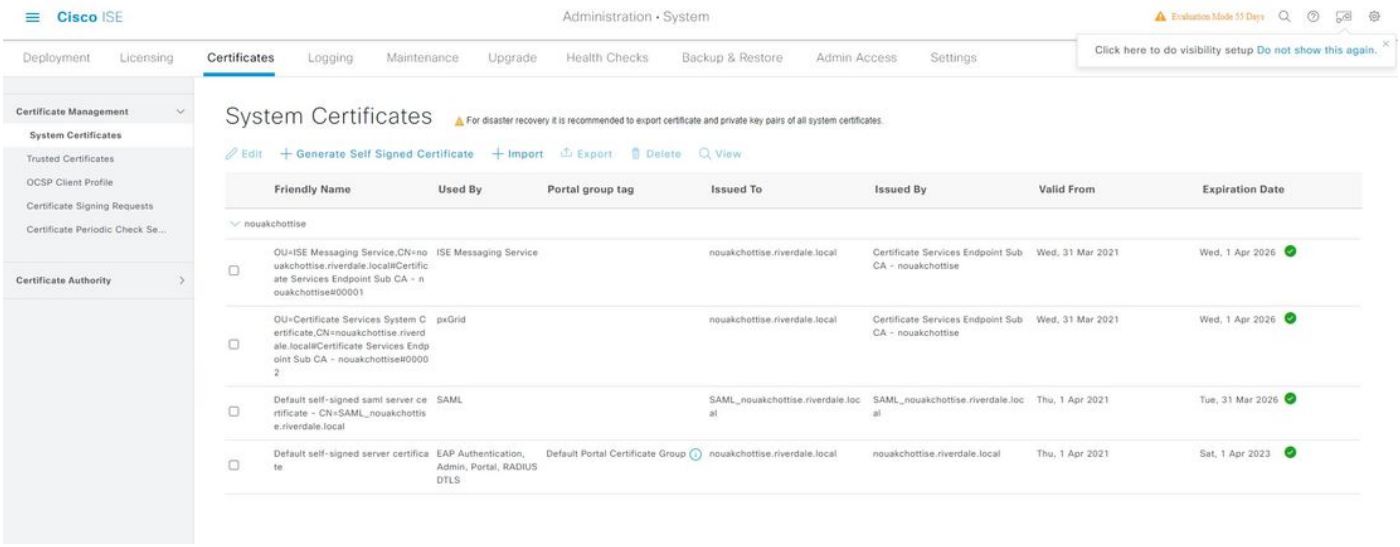
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command or configuration.

SSL Certificates in ISE

A Secure Sockets Layer (SSL) certificate is a digital file that identifies an individual, a server, or any other digital entity, and associates that entity with a Public Key. A self-signed certificate is signed by its creator. Certificates can be self-signed or digitally signed by an external Certificate Authority (CA) - typically a company's own CA server, or a well known CA vendor. A CA-signed digital certificate is considered an industry standard and more secure than a self-signed certificate.

Cisco ISE relies on PKI in order to provide secure communication with both endpoints and administrators, between ISE and other servers/services, and between Cisco ISE nodes in a multinode deployment. PKI relies on X.509 digital certificates to transfer public keys for encryption and decryption of messages and to verify the authenticity of other certificates representing users and devices. Through the Cisco ISE administration portal, you can manage these X.509 certificates.

In ISE, System Certificates are server certificates that identify a Cisco ISE node to other applications (like endpoints, other servers, etc.). Every Cisco ISE node has its own system certificates that are stored on the node along with the corresponding private keys. Each System Certificate can be mapped to 'Roles' that indicate the purpose of the certificate as shown in the image.

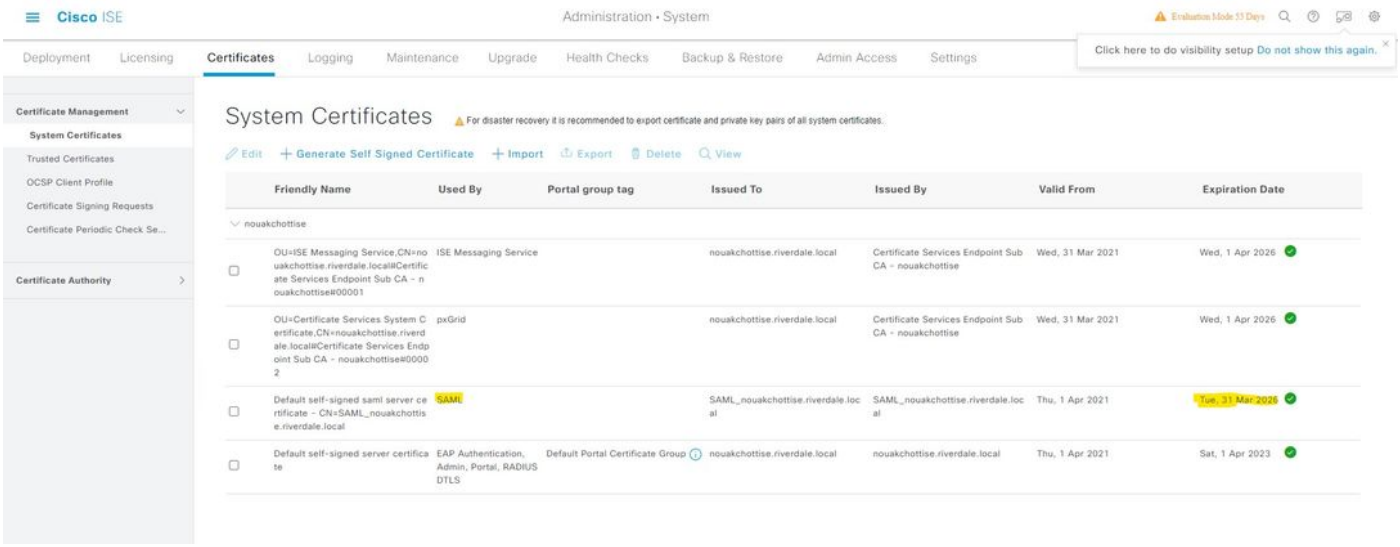


ISE 3.0 System Certificates

The scope of this document is only for the SAML Certificate. For other certificates in ISE, and more about SSL certificates in ISE in general, please refer to this document: TLS/SSL Certificates in ISE - Cisco

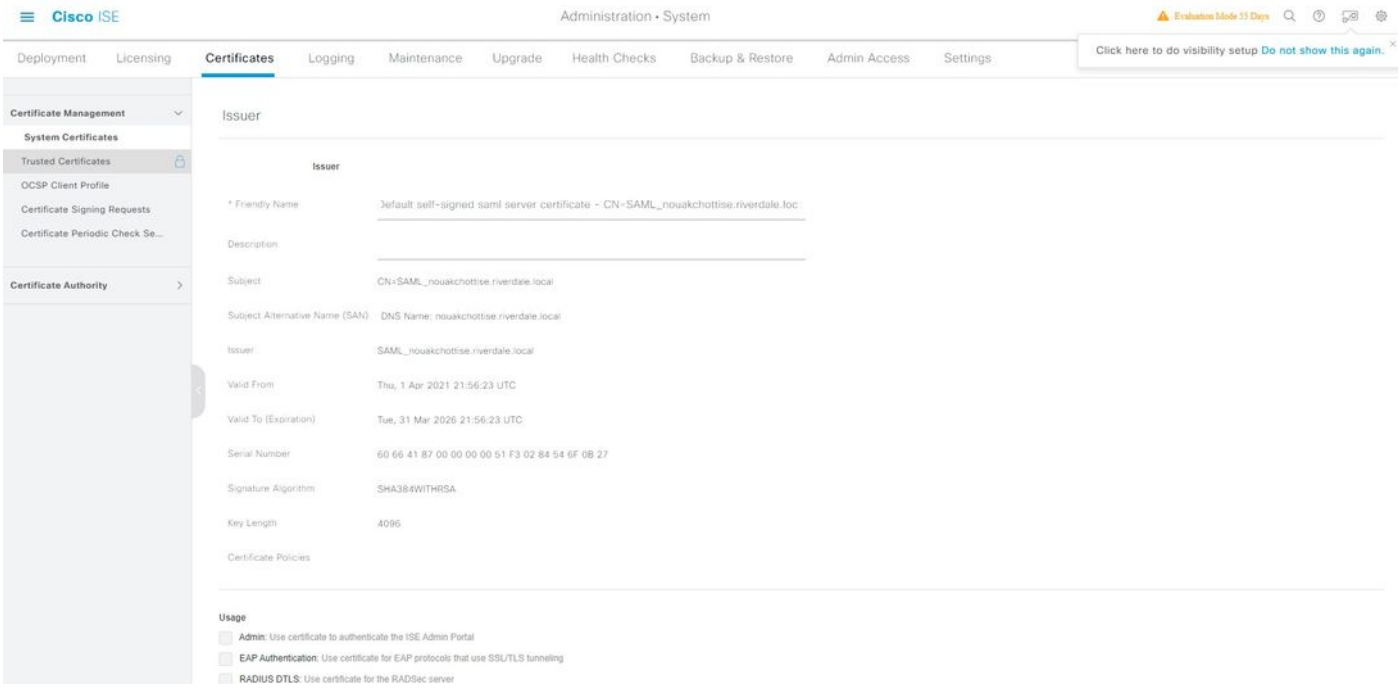
SAML Certificate in ISE

The SAML certificate in ISE is determined by looking for System Certificates having the SAML entry under the Usages field. This certificate will be used to communicate with SAML identity providers (IdP) like verifying that the SAML responses are being received from the correct IdP and to secure communication with the IdP. Note, certificates designated for SAML usage cannot be used for any other service such as Admin, EAP authentication, and so on.



For the first time ISE installations, ISE comes with a self-signed SAML server certificate which has these properties:

Key Size: 2048
Validity: one year
Key Usage: Digital Signature (Signing)
Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)



> **Note**: It is recommended that you do not use a certificate that contains the value of 2.5.29.37.0 for the Any Purpose object identifier in the Extended Key Usage attribute. If you use a certificate that contains the value of 2.5.29.37.0 for the Any Purpose object identifier in the Extended Key Usage attribute, the certificate is considered invalid and the following error message is displayed: "source=local type=fatal message="unsupported certificate".

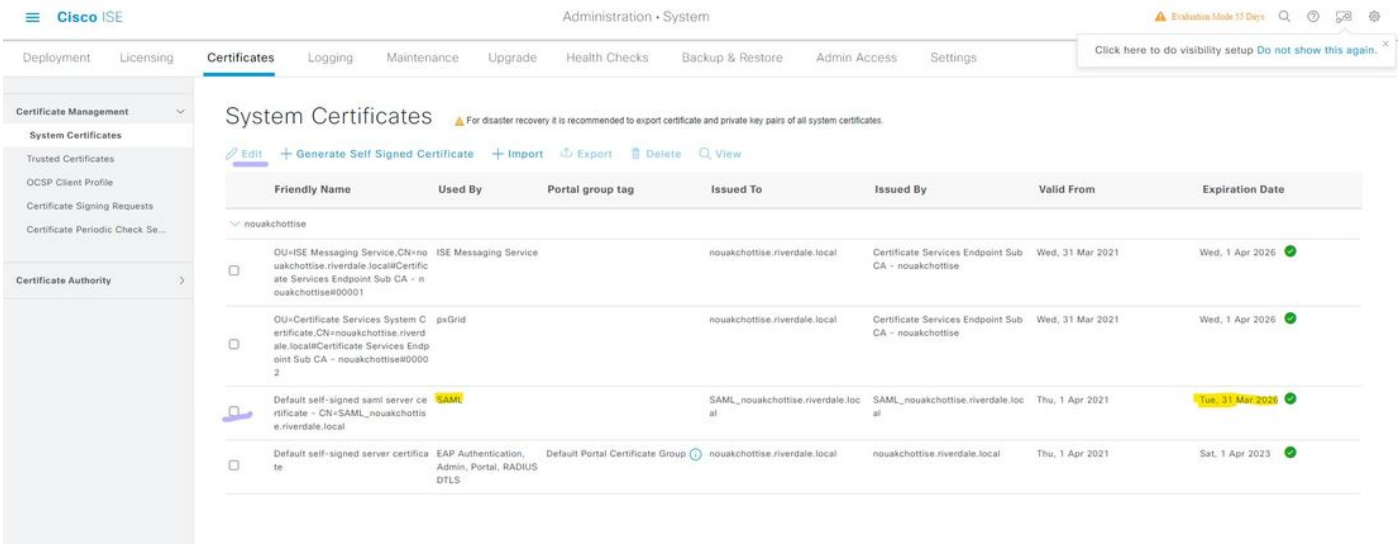
ISE administrators will need to renew this self-signed SAML certificate before expiry, even if the SAML feature is not actively used.

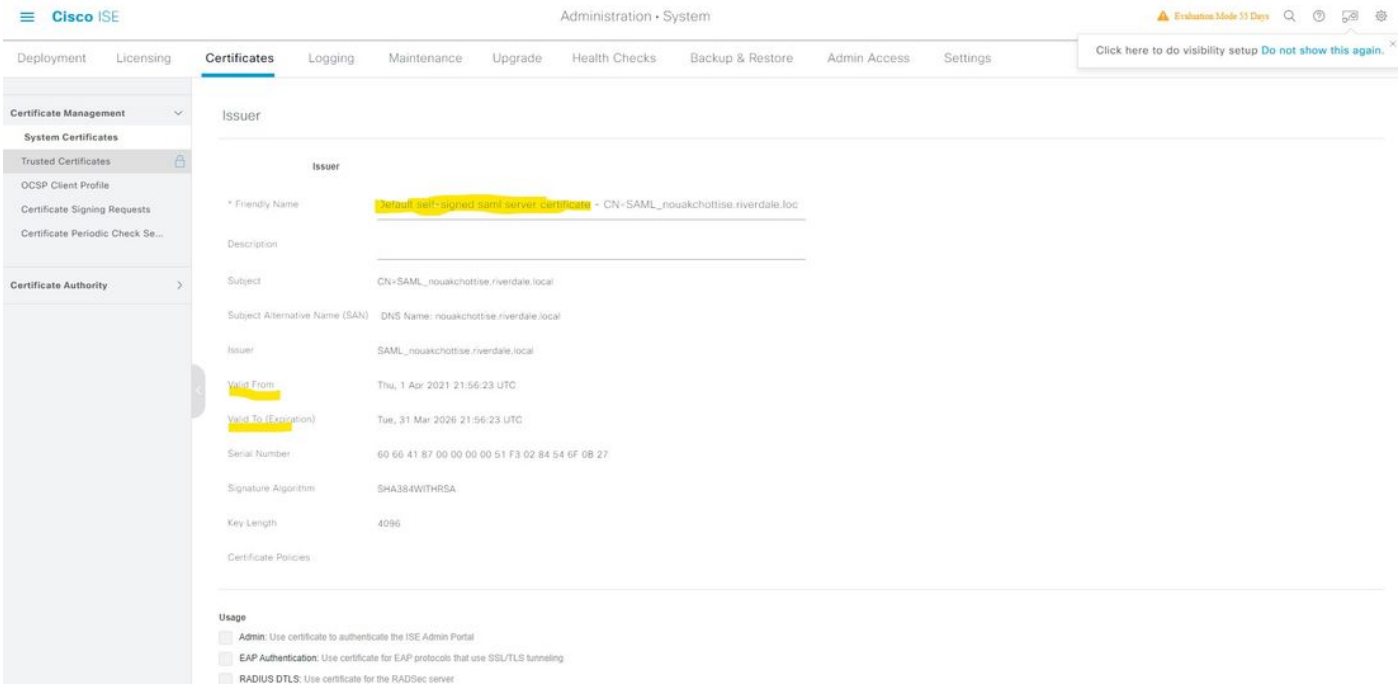
Renew a Self-Signed SAML Certificate in ISE

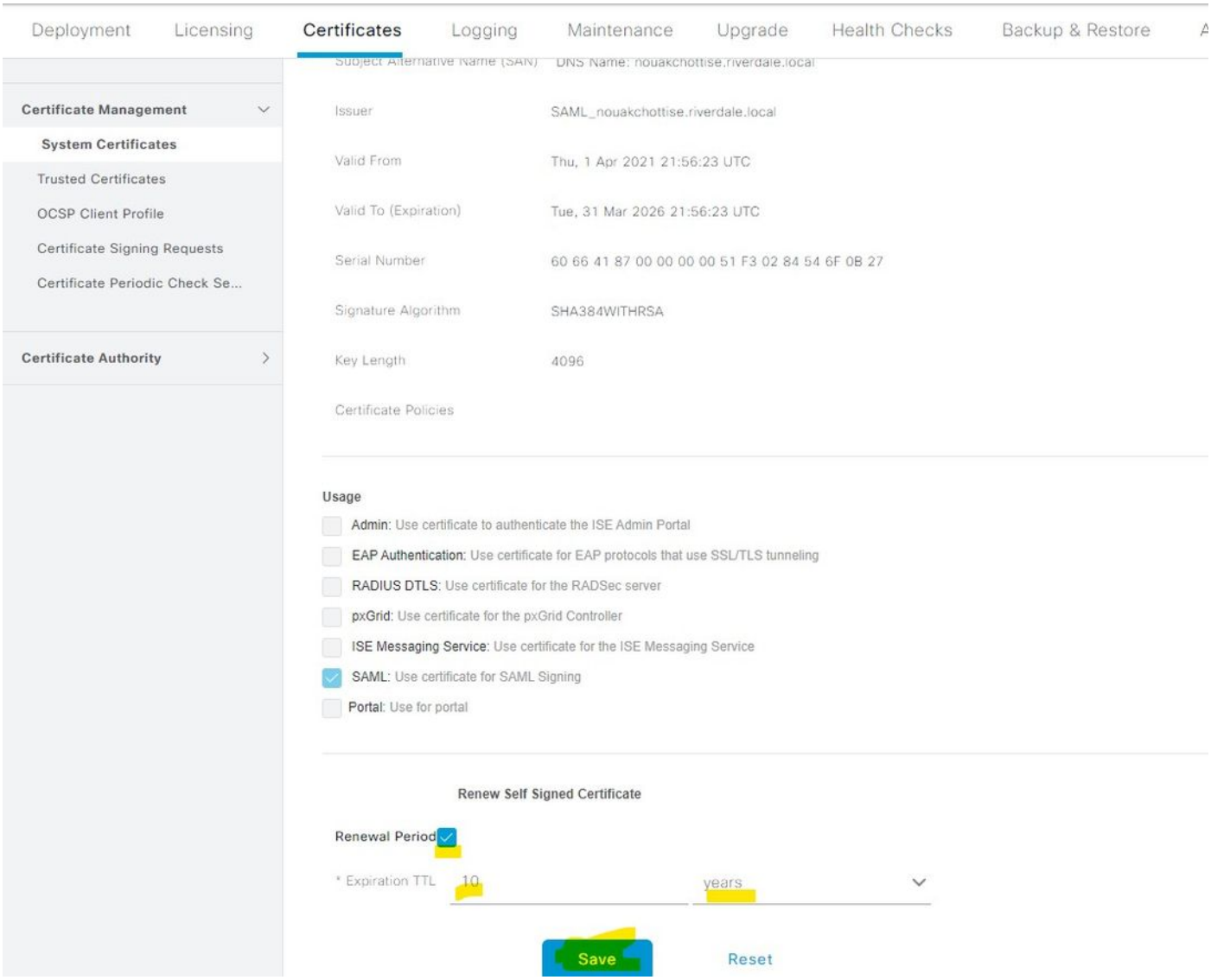
A common problem that users face is that their SAML certificates will be eventually get expired, and ISE alerts them with this message:

```
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.
```

For self-signed server certificates, it is possible to renew the certificate just to check the box renewal period and put 5-10 years as shown in the image.







In fact, any self-signed certificate that is not active used by your ISE deployment nodes can simply be renewed for a 10 year period; this ensures that you don't get any expiration notices for certificates for services you are not using. 10 years is the maximum allowed life for ISE self-signed

certificates, and usually should be enough. Updating any system certificates on the ISE does not trigger a restart of services so long as it is not designated for 'Admin' usage.

Conclusion

For any expired ISE System Certificate (self-signed and CA-signed) not in use, it is fine to replace it, delete it or renew it, and it is recommended to not have any expired certificates (System or Trusted) left on ISE before you perform an ISE upgrade.

Related Information

- **ISE 3.0 Manage Certificates:** **Cisco Identity Services Engine Administrator Guide, Release 3.0 - Basic Setup [Cisco Identity Services Engine] - Cisco**
- **SSL Certificates in ISE:** **TLS/SSL Certificates in ISE - Cisco**
- **Technical Support & Documentation - Cisco Systems**