

ISE SAML证书

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[ISE中的SSL证书](#)

[ISE中的SAML证书](#)

[在ISE中更新自签名SAML证书](#)

[结论](#)

[相关信息](#)

简介

本文档介绍思科身份服务引擎(ISE)中的安全断言标记语言(SAML)系统证书。它涵盖SAML证书的用途、如何执行续约，最后回答常见问题。它涵盖2.4版到3.0版的ISE，但是，除非另有说明，否则它应与其他ISE 2.x和3.x软件版本类似或相同。

先决条件

要求

Cisco 建议您了解以下主题：

1. 思科ISE
2. 用于描述不同类型的ISE和身份验证、授权和记帐(AAA)部署的术语
3. RADIUS协议和AAA基础
4. SAML协议
5. SSL/TLS和x509证书
6. 公钥基础设施(PKI)基础

使用的组件

本文档中的信息基于思科身份服务引擎(ISE)版本2.4 - 3.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解任何命令或配置的潜在影响。

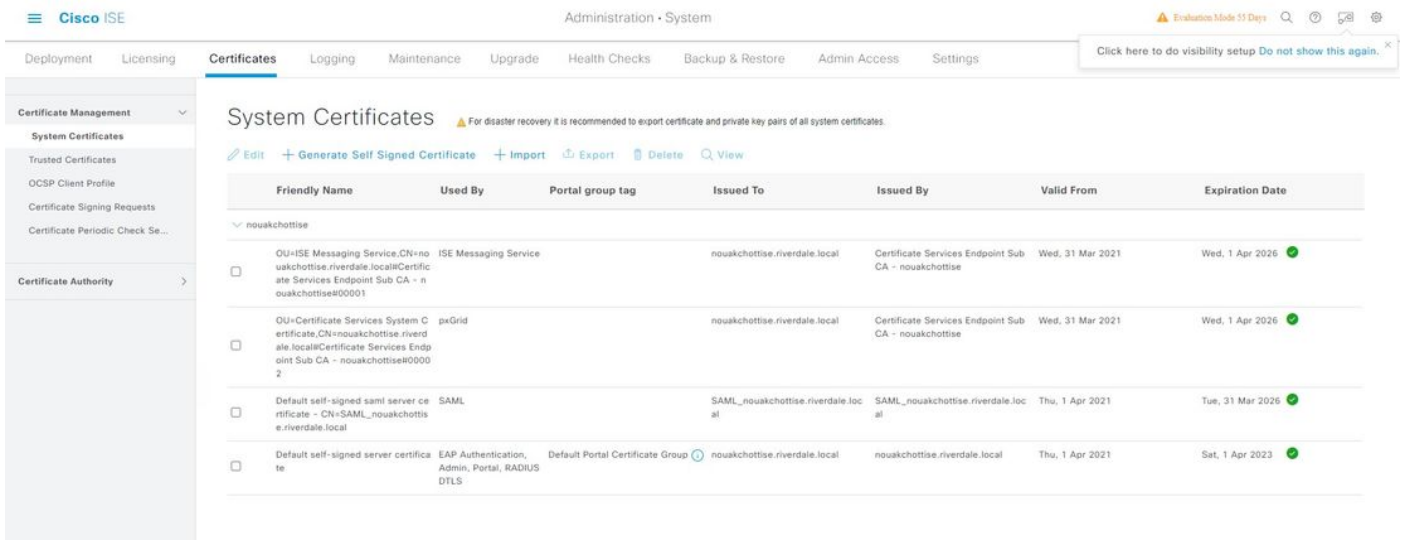
ISE中的SSL证书

安全套接字层(SSL)证书是标识个人、服务器或任何其他数字实体并将该实体与公钥关联的数字文件

。自签名证书由其创建者签名。证书可以由外部证书颁发机构(CA)自签名或数字签名 — 通常是公司自己的CA服务器或公认CA供应商。CA签名的数字证书被视为行业标准，比自签名证书更安全。

思科ISE依赖PKI以在多节点部署中提供与终端和管理员、ISE和其他服务器/服务之间以及思科ISE节点之间的安全通信。PKI依靠X.509数字证书来传输用于消息加密和解密的公钥，并验证代表用户和设备的其他证书的真实性。通过思科ISE管理门户，您可以管理这些X.509证书。

在ISE中，系统证书是服务器证书，用于标识思科ISE节点到其他应用（如终端、其他服务器等）。每个思科ISE节点都有自己的系统证书和相应的私钥一起存储在节点上。每个系统证书都可映射到“角色”，指示证书的用途，如图所示。

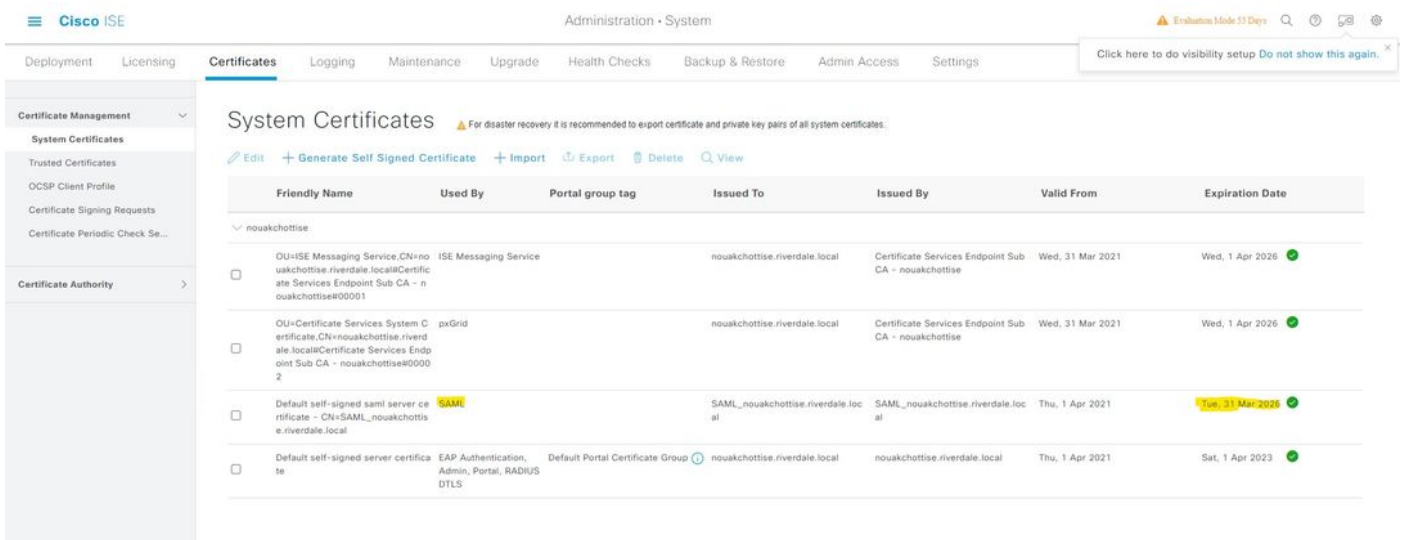


ISE 3.0系统证书

本文档的范围仅用于SAML证书。有关ISE中的其他证书，以及有关ISE中SSL证书的更多信息，请参阅本文档：[ISE中的TLS/SSL证书 — 思科](#)

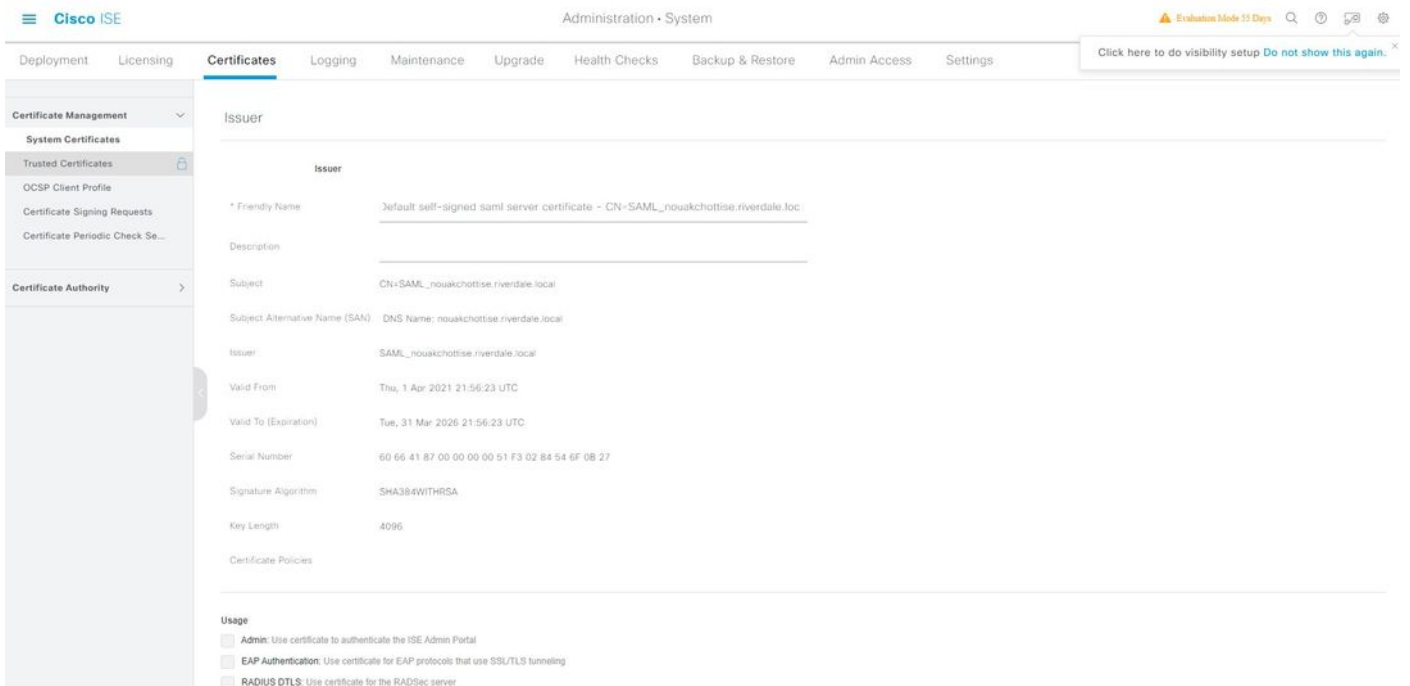
ISE中的SAML证书

在ISE中的SAML证书通过在Usages字段下查找具有SAML条目的系统证书来确定。此证书将用于与SAML身份提供程序(IdP)通信，例如验证是否从正确的IdP接收SAML响应，以及与IdP的安全通信。注意，为SAML使用指定的证书不能用于任何其他服务，如Admin、EAP身份验证等。



ISE首次安装时，ISE附带自签名SAML服务器证书，该证书具有以下属性：

密钥大小:2048
有效性：一年
密钥用法：数字签名（签名）
扩展密钥使用：TLS Web服务器身份验证(1.3.6.1.5.5.7.3.1)



注意：建议您不要将包含值2.5.29.37.0的证书用于“扩展密钥使用”属性中的“任何用途”对象标识符。如果将包含值2.5.29.37.0的证书用于“扩展密钥使用”属性中的“任何用途”对象标识符，则证书被视为无效，并显示以下错误消息：“source=local type=;fatal message=;unsupported certificate”。

即使SAML功能未被主动使用，ISE管理员也需要在到期前续订此自签名SAML证书。

在ISE中更新自签名SAML证书

用户面临的一个常见问题是其SAML证书最终将过期，ISE会用以下消息提醒他们：

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.

对于自签名服务器证书，只要选中复选框续约期，即可续约证书，并按照图中所示延长5-10年。

The screenshot shows the 'System Certificates' page in Cisco ISE. The table lists certificates with columns for Friendly Name, Used By, Portal group tag, Issued To, Issued By, Valid From, and Expiration Date. One certificate is highlighted with a yellow background, indicating its expiration date is being extended.

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
DU-ISE Messaging Service.CN=nouakchottise.riverdale.local@Certificate Services Endpoint Sub CA - nouakchottise#00001	ISE Messaging Service		nouakchottise.riverdale.local	Certificate Services Endpoint Sub CA - nouakchottise	Wed, 31 Mar 2021	Wed, 1 Apr 2026
DU-Certificate Services System Certificate.CN=nouakchottise.riverdale.local@Certificate Services Endpoint Sub CA - nouakchottise#00002	pxGrid		nouakchottise.riverdale.local	Certificate Services Endpoint Sub CA - nouakchottise	Wed, 31 Mar 2021	Wed, 1 Apr 2026
Default self-signed saml server certificate - CN=SAML_nouakchottise.riverdale.local	SAML		SAML_nouakchottise.riverdale.local	SAML_nouakchottise.riverdale.local	Thu, 1 Apr 2021	Tue, 31 Mar 2026
Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group	nouakchottise.riverdale.local	nouakchottise.riverdale.local	Thu, 1 Apr 2021	Sat, 1 Apr 2023

The screenshot shows the details of a selected certificate in the 'Issuer' section. The 'Friendly Name' is highlighted in yellow. The 'Valid From' and 'Valid To (Expiration)' dates are also highlighted in yellow.

Issuer

* Friendly Name: Default self-signed saml server certificate - CN=SAML_nouakchottise.riverdale.local

Description:

Subject: CN=SAML_nouakchottise.riverdale.local

Subject Alternative Name (SAN): DNS Name: nouakchottise.riverdale.local

Issuer: SAML_nouakchottise.riverdale.local

Valid From: Thu, 1 Apr 2021 21:56:23 UTC

Valid To (Expiration): Tue, 31 Mar 2026 21:56:23 UTC

Serial Number: 60 66 41 87 00 00 00 00 51 F3 02 84 54 6F 0B 27

Signature Algorithm: SHA384WITHRSA

Key Length: 4096

Certificate Policies:

Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore A

Subject Alternative Name (SAN) DNS Name: nouakchottise.riverdale.local

Issuer	SAML_nouakchottise.riverdale.local
Valid From	Thu, 1 Apr 2021 21:56:23 UTC
Valid To (Expiration)	Tue, 31 Mar 2026 21:56:23 UTC
Serial Number	60 66 41 87 00 00 00 00 51 F3 02 84 54 6F 0B 27
Signature Algorithm	SHA384WITHRSA
Key Length	4096
Certificate Policies	

Certificate Management ▾

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Se...

Certificate Authority >

Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- ISE Messaging Service: Use certificate for the ISE Messaging Service
- SAML: Use certificate for SAML Signing
- Portal: Use for portal

Renew Self Signed Certificate

Renewal Period

* Expiration TTL 10 years

Save Reset

事实上，ISE部署节点未使用的任何自签名证书都可以续约10年；这可确保您不会收到任何有关您未使用的服务的证书的过期通知。10年是ISE自签名证书允许的最长寿命，通常应足够。只要ISE上的任何系统证书未指定为“管理员”使用，更新ISE上的任何系统证书不会触发服务重新启动。

结论

对于未使用的任何过期ISE系统证书（自签名和CA签名），可以更换、删除或续订它，并且建议在执行ISE升级之前，不要在ISE上保留任何过期证书（系统或受信任）。

相关信息

- ISE 3.0管理证书：[思科身份服务引擎管理员指南，版本3.0 — 基本设置\[思科身份服务引擎\] — 思科](#)
- ISE中的SSL证书：[ISE中的TLS/SSL证书 — 思科](#)
- [技术支持和文档 - Cisco Systems](#)