ISE SAML証明書

内容

概要

このドキュメントでは、Cisco Identity Services Engine(ISE)のSecurity Assertion Markup Language(SAML)システム証明書について説明します。 SAML証明書の目的、更新の実行方法、および頻繁に発生するFAQへの回答が記載されています。バージョン2.4から3.0までのISEを対象としていますが、特に明記されていない限り、他のISE 2.xおよび3.xソフトウェアリリースと同様または同一である必要があります。

前提条件

要件

次の項目に関する知識があることが推奨されます。

1. Cisco ISE
2. さまざまなタイプのISEおよびAuthentication, Authorization and Accounting(AAA)導入を説明するために使用される用語
3. RADIUSプロトコルとAAAの基本
4. SAMLプロトコル
5. SSL/TLSおよびx509証明書
6. 公開キーインフラストラクチャ(PKI)の基本

使用するコンポーネント

このドキュメントの情報は、Cisco Identity Services Engine(ISE)リリース2.4 ~ 3.0に基づくものです

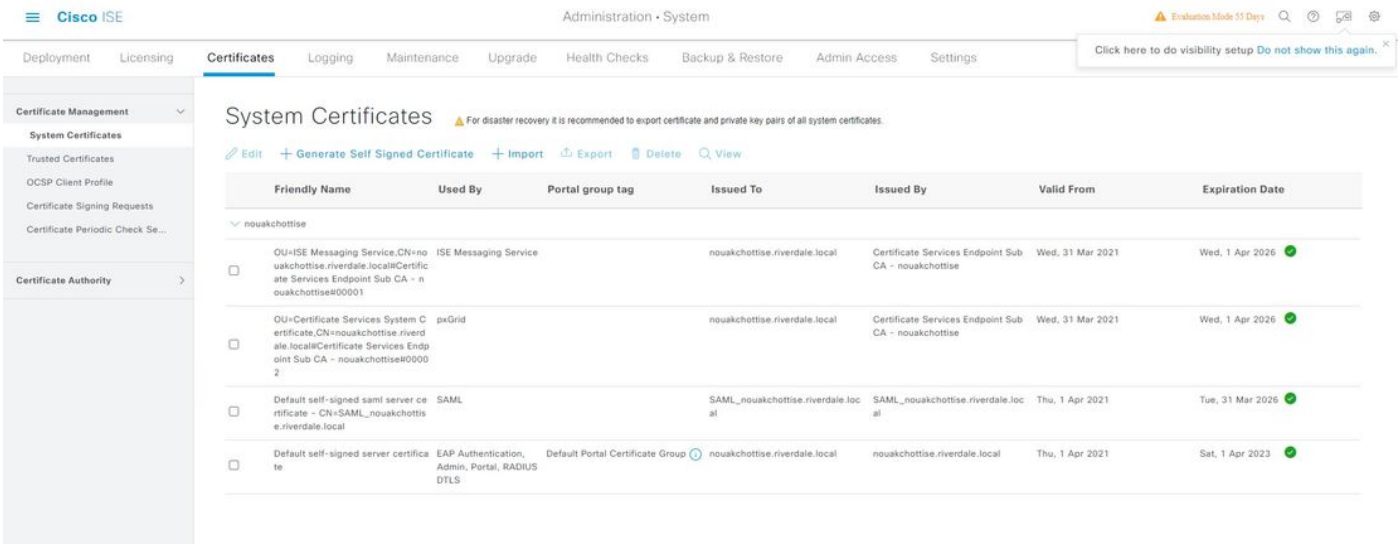
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。ネットワークが稼働中の場合は、コマンドや設定による潜在的な影響について確実に理解しておく必要があります。

ISEのSSL証明書

セキュアソケットレイヤ(SSL)証明書は、個人、サーバ、またはその他のデジタルエンティティを識別し、そのエンティティを公開キーに関連付けるデジタルファイルです。自己署名証明書は、作成者によって署名されます。証明書は、外部認証局(CA)（通常は企業独自のCAサーバ、または既知のCAベンダー）によって自己署名またはデジタル署名できます。CA署名付きデジタル証明書は、自己署名証明書よりも業界標準で安全性が高いと見なされます。

Cisco ISEは、エンドポイントと管理者、ISEと他のサーバ/サービス間、およびマルチノード展開のCisco ISEノード間のセキュアな通信を提供するために、PKIに依存します。PKIはX.509デジタル証明書を使用して、メッセージの暗号化と復号化のための公開キーを転送し、ユーザとデバイスを表す他の証明書の信頼性を確認します。Cisco ISE管理ポータルを使用して、これらのX.509証明書を管理できます。

ISEでは、システム証明書は、Cisco ISEノードを他のアプリケーション（エンドポイント、他のサーバなど）に識別するサーバ証明書です。 すべてのCisco ISEノードには、対応する秘密キーとともにノードに保存される独自のシステム証明書があります。各システム証明書は、図に示すように、証明書の目的を示す「ロール」にマッピングできます。

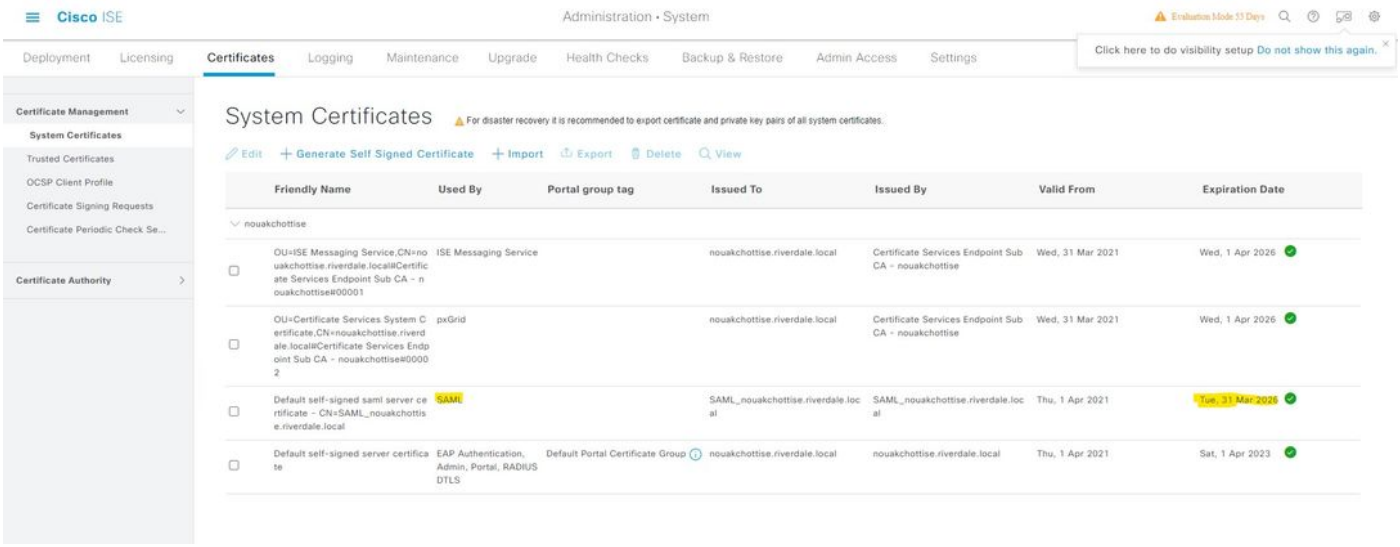


ISE 3.0システム証明書

このドキュメントの対象範囲は、SAML証明書のみです。ISEの他の証明書、およびISEのSSL証明書の一般的な詳細については、次のドキュメントを参照してください：[ISEのTLS/SSL証明書 – シスコ]

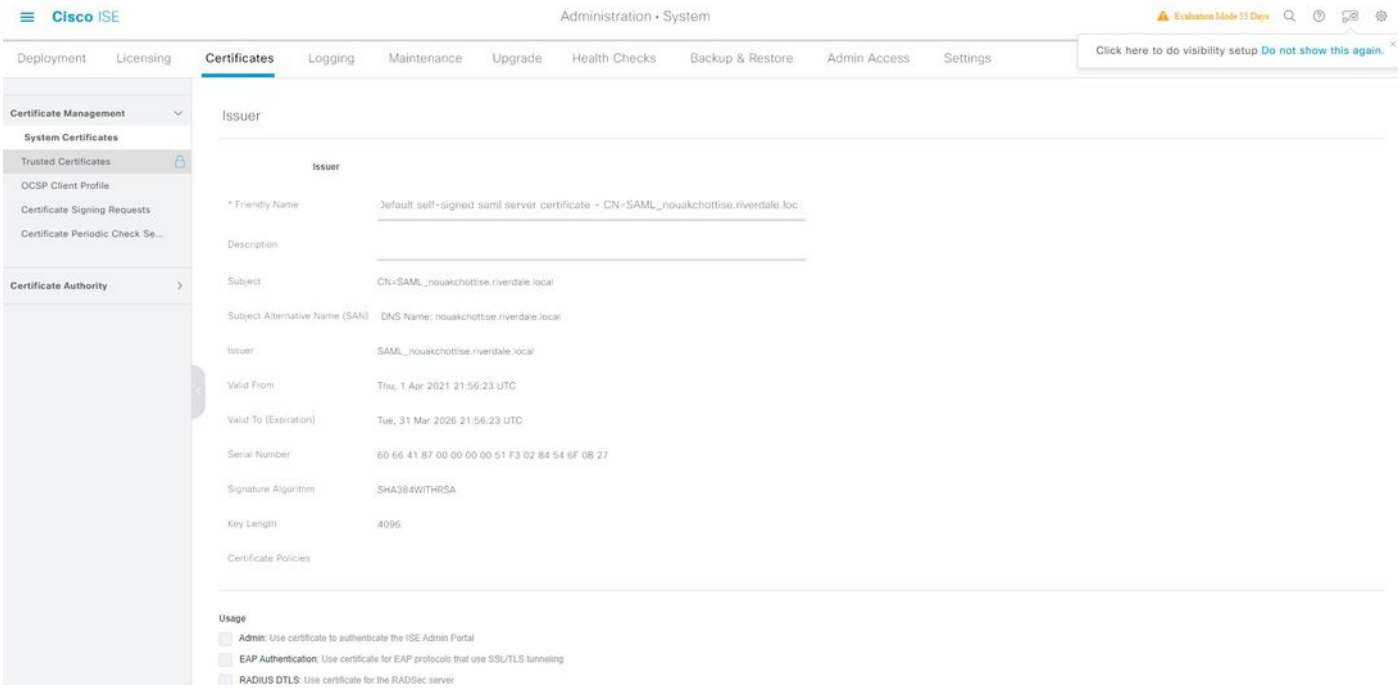
ISEのSAML証明書

ISEのSAML証明書は、[Usage]フィールドの下にSAMLエントリを持つシステム証明書を検索することによって決定されます。この証明書は、正しいIdPからSAML応答を受信していることを確認したり、IdPとの通信を保護したりするなど、SAML IDプロバイダー(IdP)と通信するために使用されます。SAMLの使用に指定された証明書は、管理者、EAP認証などの他のサービスには使用できません。



ISEを初めてインストールする場合、ISEには次のプロパティを持つ自己署名SAMLサーバ証明書が付属します。

[Key Size]：2048
有効性：1年
Key Usage:デジタル署名（署名）
拡張キーの使用法：TLS Webサーバ認証(1.3.6.1.5.5.7.3.1)



> **注**：[拡張キー使用法(Extended Key Usage)]属性の[任意の目的(Any Purpose)]オブジェクト識別子に2.5.29.37.0の値を含む証明書は使用しないことをお勧めします。[拡張キー使用法]属性の[Any Purpose]オブジェクト識別子に2.5.29.37.0の値を含む証明書を使用すると、証明書は無効と見なされ、次のエラーメッセージが表示されます。"source=local ; type=fatal message=";unsupported certificate"。

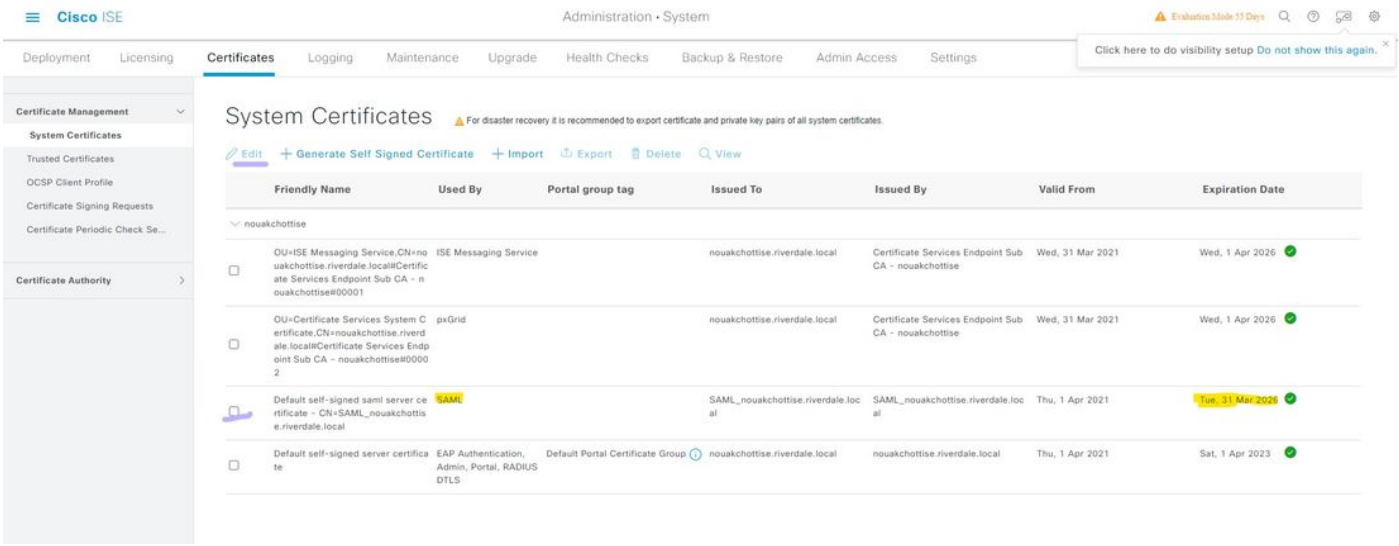
ISE管理者は、SAML機能がアクティブに使用されていない場合でも、有効期限が切れる前にこの自己署名SAML証明書を更新する必要があります。

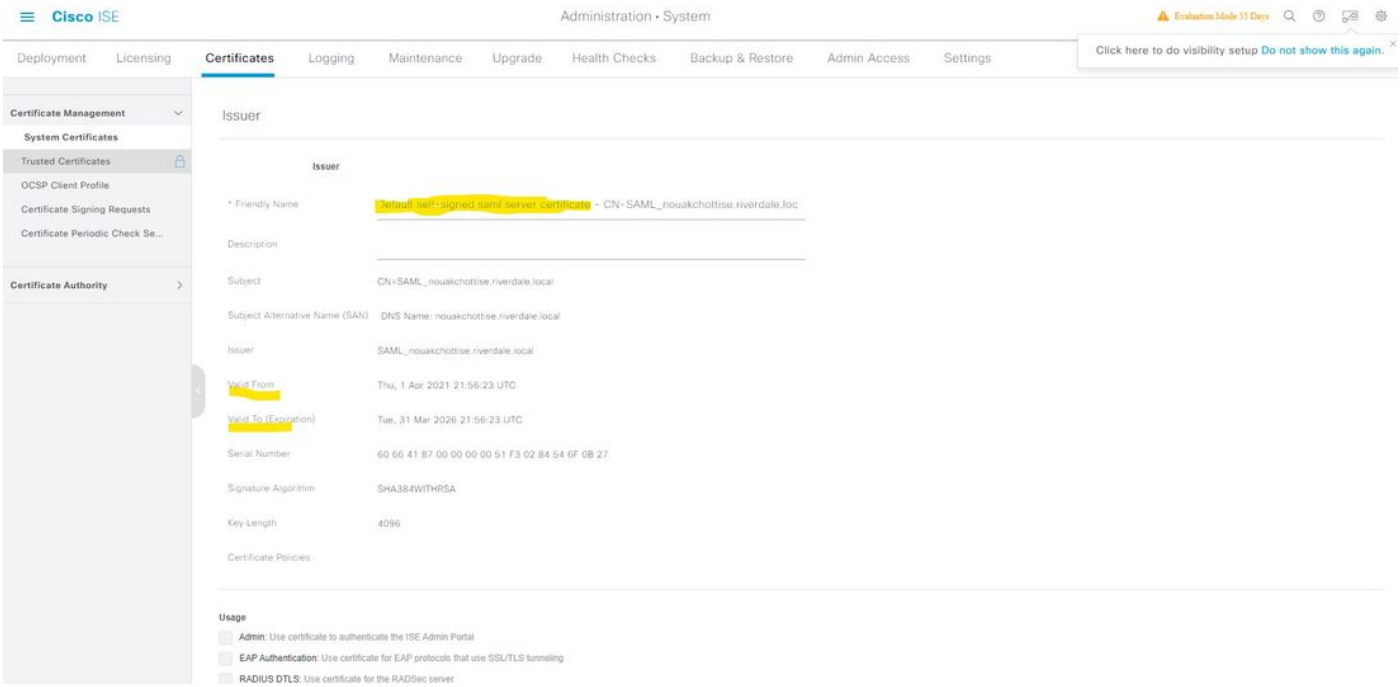
ISEでの自己署名SAML証明書の更新

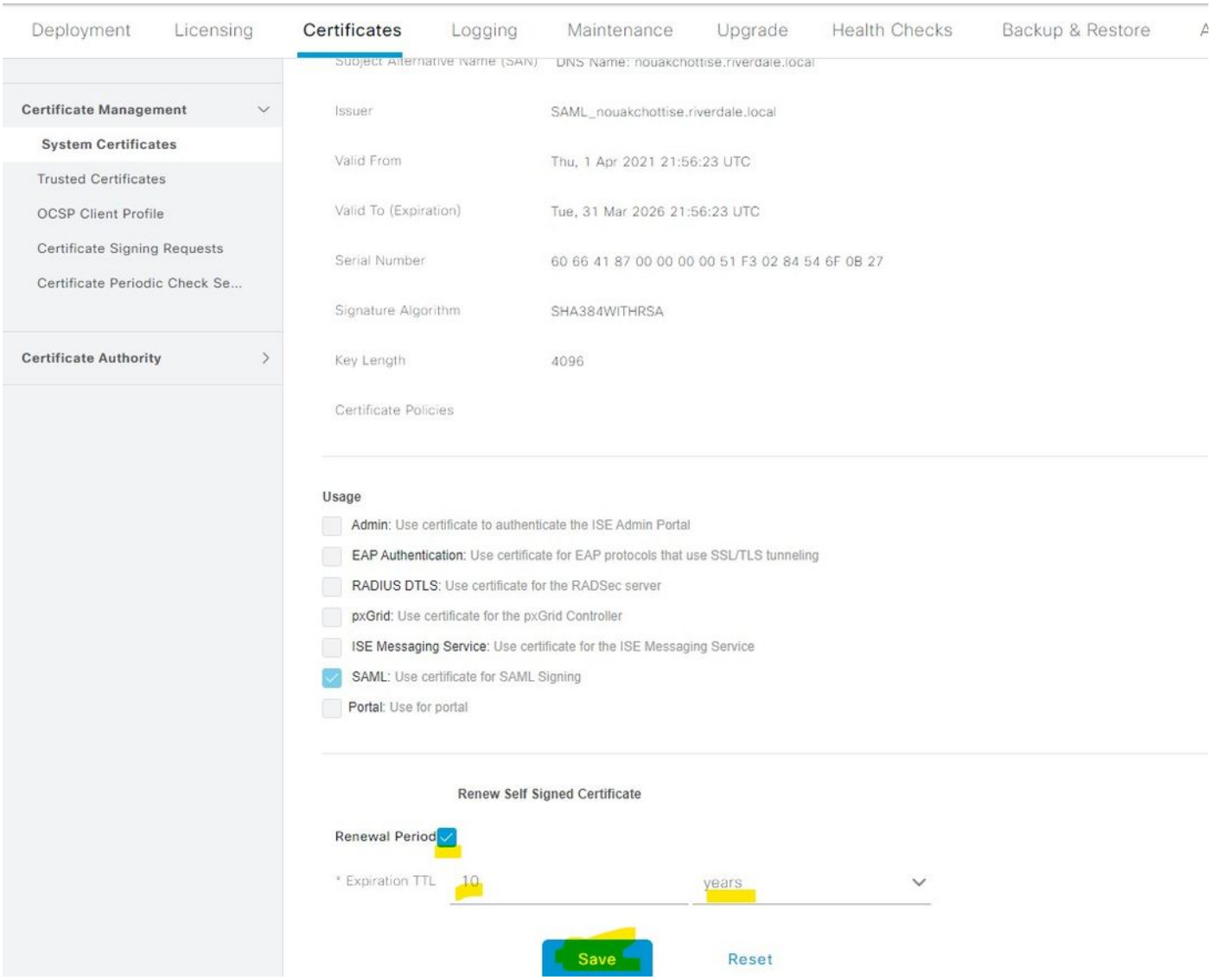
ユーザが直面する一般的な問題は、SAML証明書が最終的に期限切れになり、ISEが次のメッセージでユーザに警告することです。

```
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.
```

自己署名サーバ証明書の場合は、証明書を更新するだけで、ボックス更新期間を確認し、図に示すように5 ~ 10年を経過させることができます。







実際、ISE導入ノードでアクティブに使用されていない自己署名証明書は、10年間更新するだけで済みます。これにより、使用していないサービスの証明書の有効期限が通知されなくなります。ISE自己署名証明書の有効期間は10年で、通常は十分である必要があります。ISE上のシステム

証明書を更新しても、'Admin'の使用に指定されていない限り、サービスの再起動はトリガーされません。

結論

期限切れのISEシステム証明書（自己署名およびCA署名）が使用されていない場合は、それを交換、削除、または更新して、ISEアップグレードを実行する前に期限切れの証明書（システムまたは信頼）をISEに残さないことをお勧めします。

関連情報

- **ISE 3.0証明書の管理**：Cisco Identity Services Engine Administrator Guide, Release 3.0 - Basic Setup [Cisco Identity Services Engine] - Cisco
- **ISEのSSL証明書**：ISEのTLS/SSL証明書：シスコ
- テクニカル サポートとドキュメント – Cisco Systems