ISE SAML 인증서

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine)의 SAML(Security Assertion Markup Language) 시스템 인증서에 대해 설명합니다. SAML 인증서의 용도, 갱신 수행 방법, 그리고 자주 묻는 FAQ에 대한 답변을 제공합니다.버전 2.4에서 3.0으로 ISE를 지원하지만 달리 명시되지 않은 한 다른 ISE 2.x 및 3.x 소프트웨어 릴리스와 유사하거나 동일해야 합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

1. Cisco ISE
2. 다양한 유형의 ISE 및 인증, 권한 부여 및 계정 관리(AAA) 구축을 설명하는 데 사용되는 용어
3. RADIUS 프로토콜 및 AAA 기본 사항
4. SAML 프로토콜
5. SSL/TLS 및 x509 인증서
6. PKI(Public Key Infrastructure) 기본 사항

사용되는 구성 요소

이 문서의 정보는 Cisco ISE(Identity Services Engine), 릴리스 2.4 - 3.0을 기반으로 합니다.

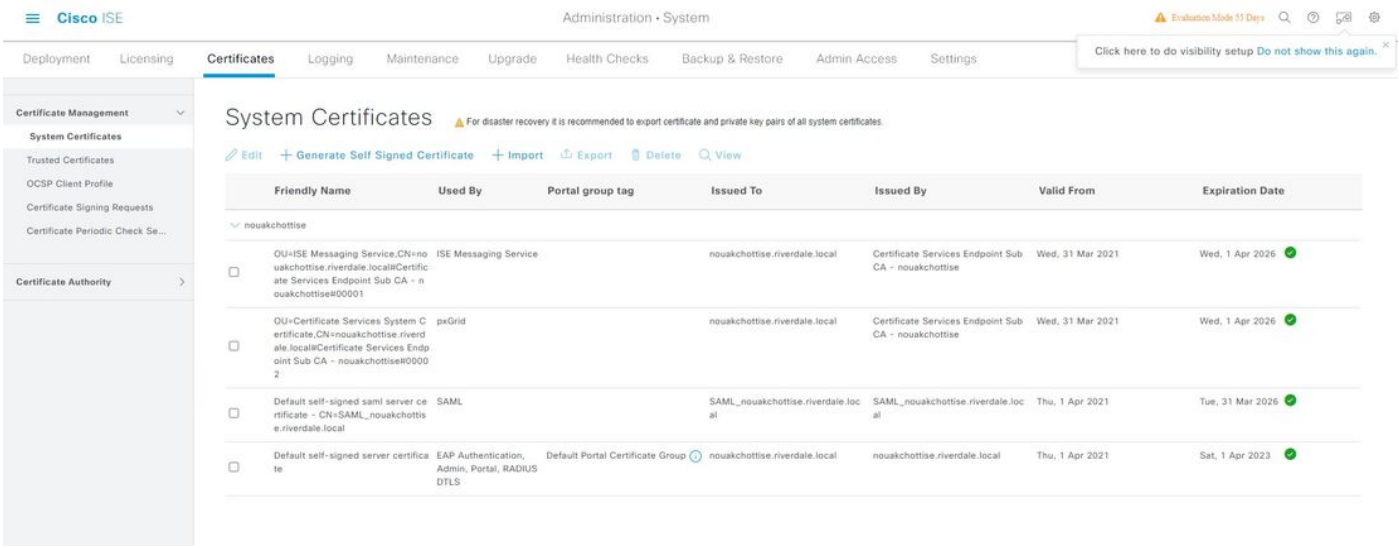
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령 또는 컨피그레이션의 잠재적인 영향을 이해해야 합니다.

ISE의 SSL 인증서

SSL(Secure Sockets Layer) 인증서는 개인, 서버 또는 기타 디지털 엔티티를 식별하고 해당 엔티티를 공개 키와 연결하는 디지털 파일입니다.자체 서명 인증서는 생성자가 서명합니다.인증서는 자체 서명 또는 외부 CA(Certificate Authority)에 의해 디지털 서명(일반적으로 회사의 고유 CA 서버 또는 잘 알려진 CA 공급업체)될 수 있습니다.CA 서명 디지털 인증서는 업계 표준으로 간주되며 자체 서명 인증서보다 더 안전합니다.

Cisco ISE는 PKI에 의존하여 엔드포인트와 관리자, ISE와 기타 서버/서비스 간, 다중 노드 구축의 Cisco ISE 노드 간에 보안 통신을 제공합니다.PKI는 X.509 디지털 인증서를 사용하여 메시지의 암호화 및 암호 해독을 위한 공개 키를 전송하고 사용자 및 디바이스를 나타내는 다른 인증서의 신뢰성을 확인합니다.Cisco ISE 관리 포털을 통해 이러한 X.509 인증서를 관리할 수 있습니다.

ISE에서 시스템 인증서는 다른 애플리케이션(예: 엔드포인트, 기타 서버 등)에 대한 Cisco ISE 노드를 식별하는 서버 인증서입니다. 모든 Cisco ISE 노드는 해당 개인 키와 함께 노드에 저장 된 자체 시스템 인증서를 가지고 있습니다.각 시스템 인증서는 이미지에 표시된 대로 인증서의 용도를 나타내는 '역할'에 매핑될 수 있습니다.

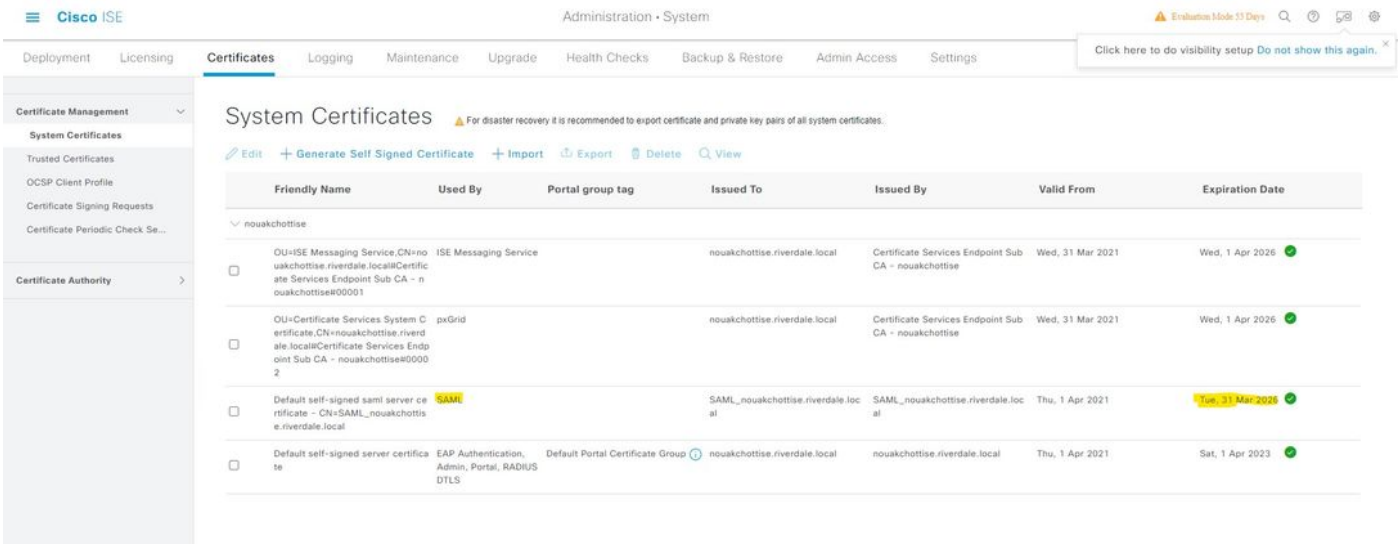


ISE 3.0 시스템 인증서

이 문서의 범위는 SAML 인증서에만 적용됩니다.ISE의 다른 인증서 및 일반적으로 ISE의 SSL 인증서에 대한 자세한 내용은 다음 문서, ISE의 TLS/SSL 인증서 - Cisco를 참조하십시오.

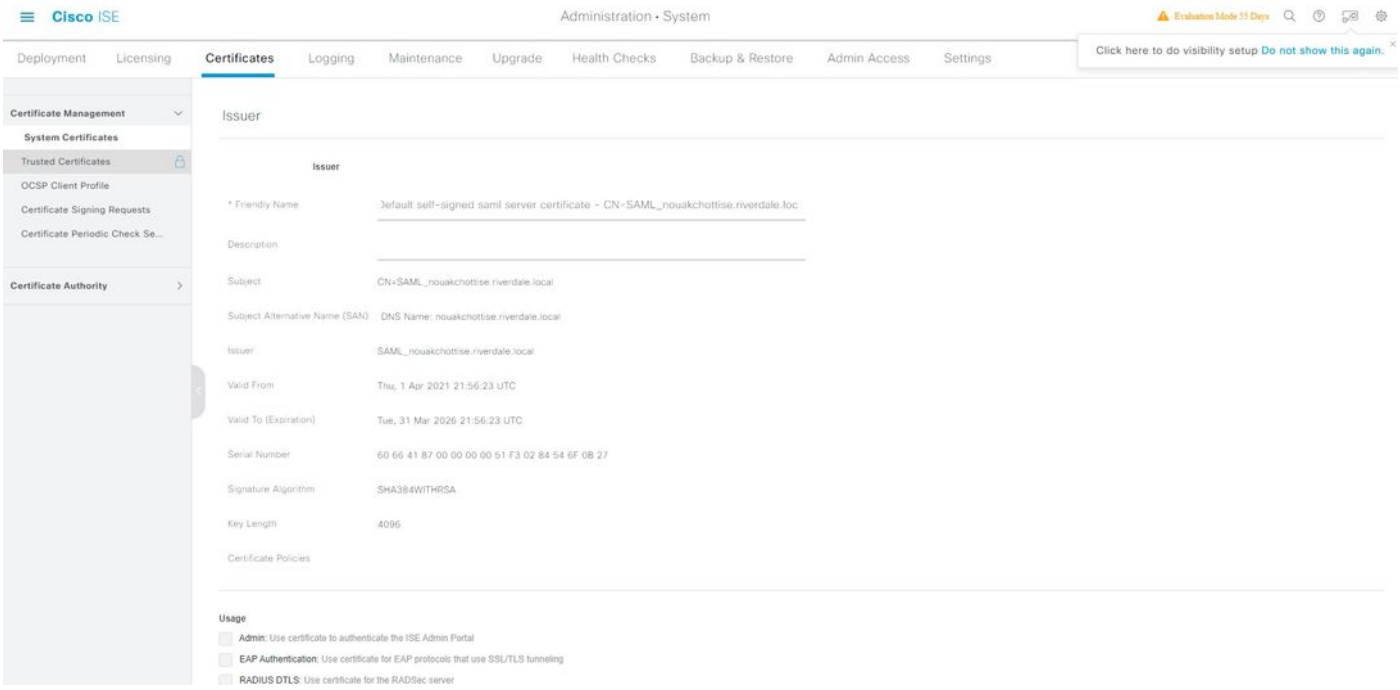
ISE의 SAML 인증서

ISE의 SAML 인증서는 Uses(사용) 필드 아래에 SAML 항목이 있는 시스템 인증서를 찾아 결정됩니다.이 인증서는 SAML 응답이 올바른 IdP에서 수신되는지 확인하고 IdP와의 통신을 보호하기 위해 SAML ID 제공자(IdP)와 통신하는 데 사용됩니다.참고: SAML 사용을 위해 지정된 인증서는 관리, EAP 인증 등과 같은 다른 서비스에 사용할 수 없습니다.



ISE를 처음 설치하는 경우 ISE는 다음과 같은 속성을 가진 자체 서명 SAML 서버 인증서와 함께 제공됩니다.

키 크기:2048
유효성:1년
키 사용:디지털 서명(서명)
확장 키 사용:TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1)



> **참고:**Extended Key Usage 속성에서 Any Purpose 개체 식별자에 대한 2.5.29.37.0 값을 포함하는 인증서를 사용하지 않는 것이 좋습니다.Extended Key Usage 속성에서 Any Purpose 개체 식별자의 값이 2.5.29.37.0인 인증서를 사용하는 경우 인증서가 유효하지 않은 것으로 간주되고 다음 오류 메시지가 표시됩니다."source=local ; type=fatal ; message="unsupported certificate"

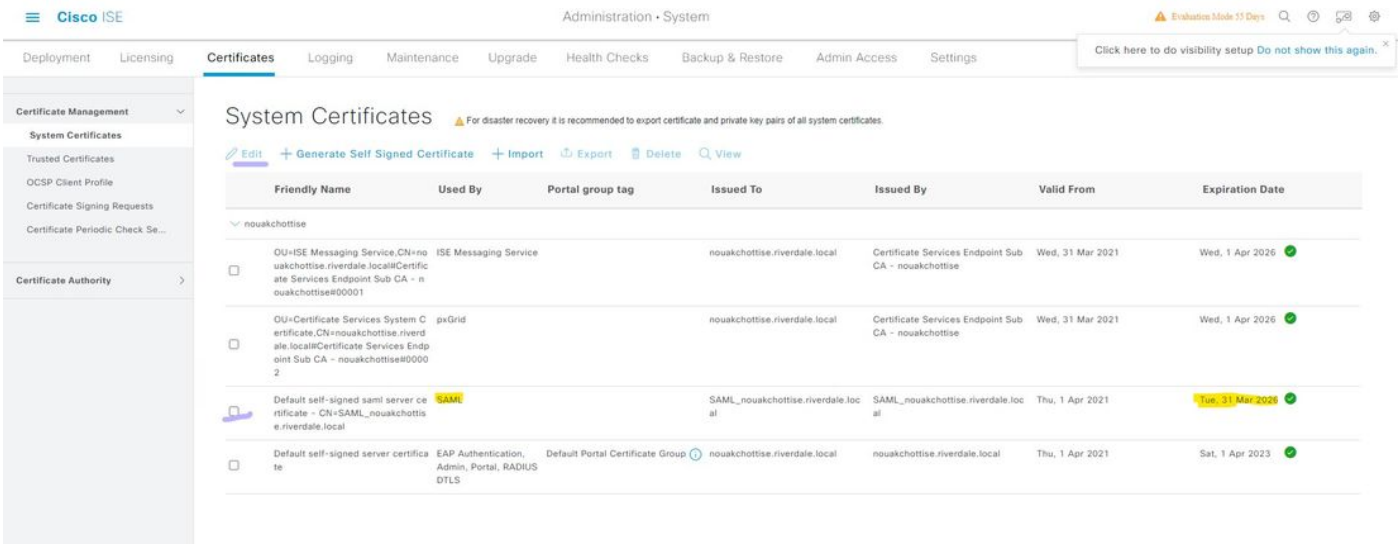
ISE 관리자는 SAML 기능이 적극적으로 사용되지 않더라도 만료 전에 이 자체 서명 SAML 인증서를 갱신해야 합니다.

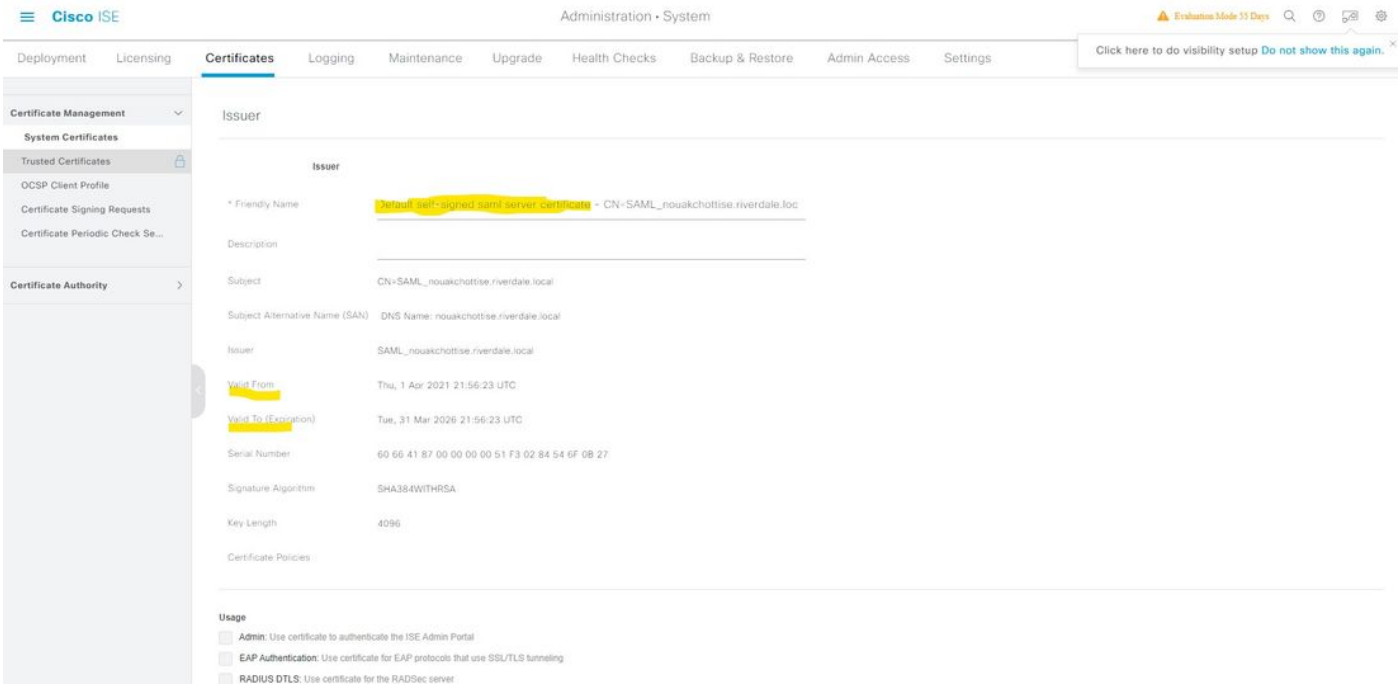
ISE에서 자체 서명 SAML 인증서 갱신

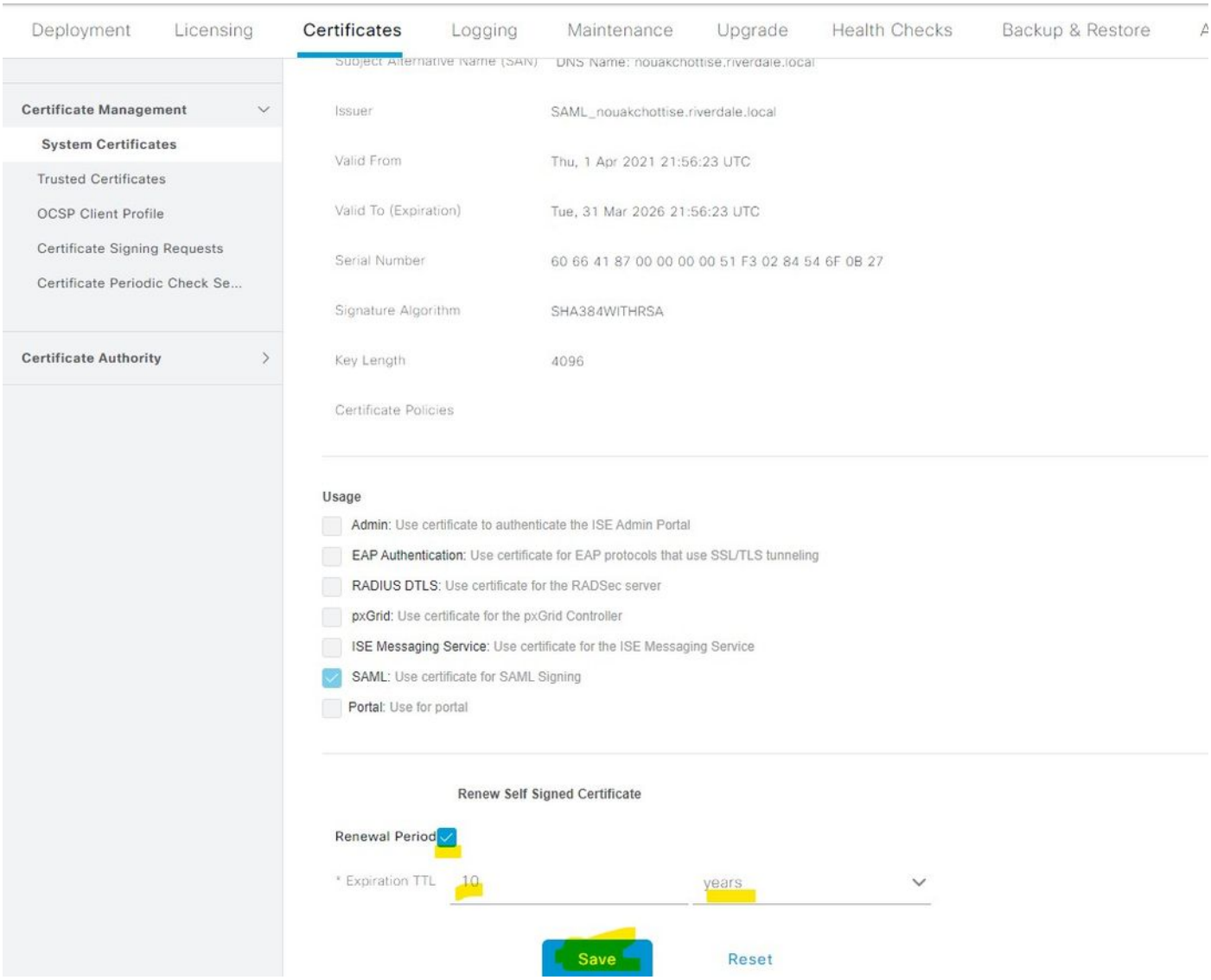
사용자가 겪는 일반적인 문제는 SAML 인증서가 결국 만료되고 ISE가 다음 메시지를 통해 사용자에게 알림을 보내는 것입니다.

```
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.
```

자체 서명 서버 인증서의 경우, 인증서를 갱신하여 박스 갱신 기간을 확인하고 이미지에 표시된 대로 5-10년을 사용할 수 있습니다.







실제로 ISE 구축 노드에서 사용하지 않는 자체 서명 인증서는 10년 동안 갱신하면 됩니다.이렇게 하면 사용하지 않는 서비스의 인증서에 대한 만료 알림이 표시되지 않습니다.10년은 ISE 자체 서명 인증서에 대해 허용되는 최대 기간이며, 일반적으로 충분합니다. ISE에서 시스템 인증서를 업데이

트해도 'Admin' 사용을 위해 지정되지 않은 경우 서비스가 다시 시작되지 않습니다.

결론

사용 중이 아닌 만료된 ISE 시스템 인증서(자체 서명 및 CA 서명)의 경우 교체, 삭제 또는 갱신할 수 있으며, ISE 업그레이드를 수행하기 전에 ISE에 만료된 인증서(System 또는 Trusted)가 남아 있지 않는 것이 좋습니다.

관련 정보

- ISE 3.0 인증서 관리:Cisco Identity Services Engine 관리자 가이드, 릴리스 3.0 - 기본 설정 [Cisco Identity Services Engine] - Cisco
- ISE의 SSL 인증서:ISE의 TLS/SSL 인증서 - Cisco
- 기술 지원 및 문서 – Cisco Systems