Certificato ISE SAML

Sommario

Introduzione

Questo documento descrive i certificati di sistema SAML (Security Assertion Markup Language) in Cisco Identity Services Engine (ISE). Descrive lo scopo dei certificati SAML, come eseguire il rinnovo e infine risponde alle domande frequenti. Copre l'ISE dalla versione 2.4 alla 3.0, ma dovrebbe essere simile o identica ad altre versioni software di ISE 2.x e 3.x, a meno che non sia specificato diversamente.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

1. Cisco ISE
2. La terminologia utilizzata per descrivere i diversi tipi di implementazioni ISE e di autenticazione, autorizzazione e accounting (AAA)
3. Nozioni base sul protocollo RADIUS e sull'AAA
4. protocollo SAML
5. Certificati SSL/TLS e x509
6. Nozioni di base sull'infrastruttura a chiave pubblica (PKI)

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco Identity Services Engine (ISE), release 2.4 - 3.0

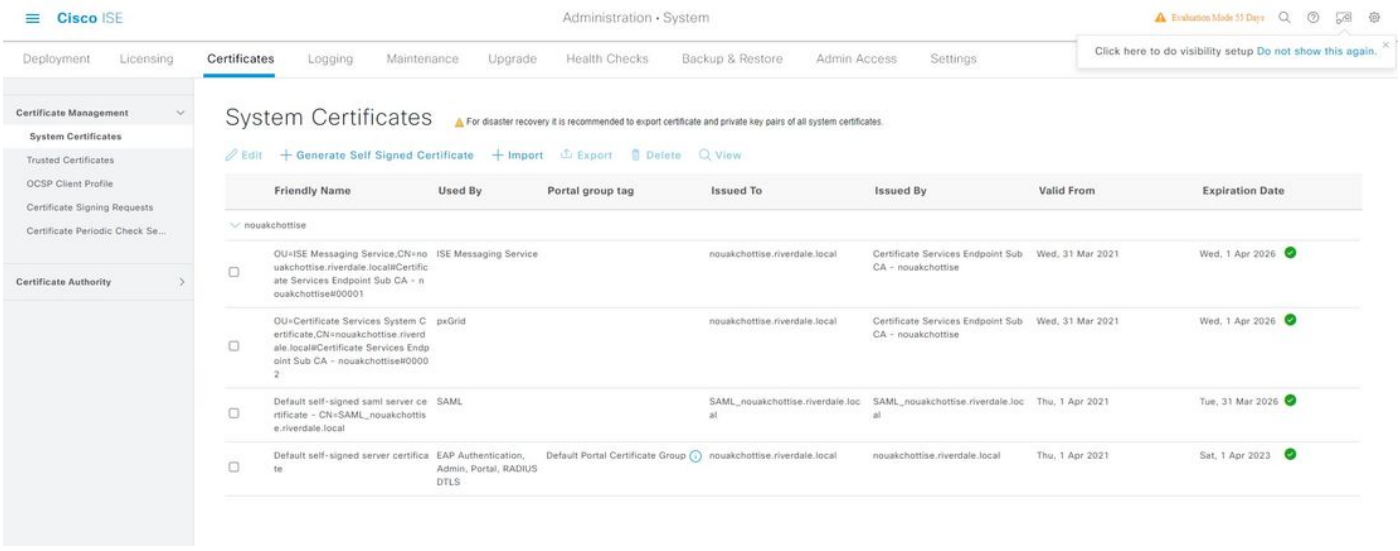
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi o delle configurazioni.

Certificati SSL in ISE

Un certificato SSL (Secure Sockets Layer) è un file digitale che identifica un utente, un server o qualsiasi altra entità digitale e associa tale entità a una chiave pubblica. Un certificato autofirmato è firmato dall'autore. I certificati possono essere autofirmati o firmati digitalmente da un'autorità di certificazione (CA) esterna, in genere un server CA della società o un fornitore CA conosciuto. Un certificato digitale firmato dall'autorità di certificazione è considerato uno standard del settore e più sicuro di un certificato autofirmato.

Cisco ISE si basa sull'infrastruttura a chiave pubblica (PKI) per fornire comunicazioni sicure con endpoint e amministratori, tra ISE e altri server/servizi e tra i nodi Cisco ISE in un'implementazione multinodo. La PKI si basa sui certificati digitali X.509 per trasferire le chiavi pubbliche per la crittografia e la decrittografia dei messaggi e per verificare l'autenticità di altri certificati che rappresentano utenti e dispositivi. Tramite il portale di amministrazione di Cisco ISE, è possibile gestire questi certificati X.509.

Ad ISE, i certificati di sistema sono certificati server che identificano un nodo Cisco ISE per altre applicazioni (come endpoint, altri server, ecc.). Ogni nodo Cisco ISE ha i propri certificati di sistema che vengono archiviati sul nodo insieme alle chiavi private corrispondenti. È possibile mappare ogni certificato di sistema a "Ruoli" che indicano lo scopo del certificato, come illustrato nell'immagine.

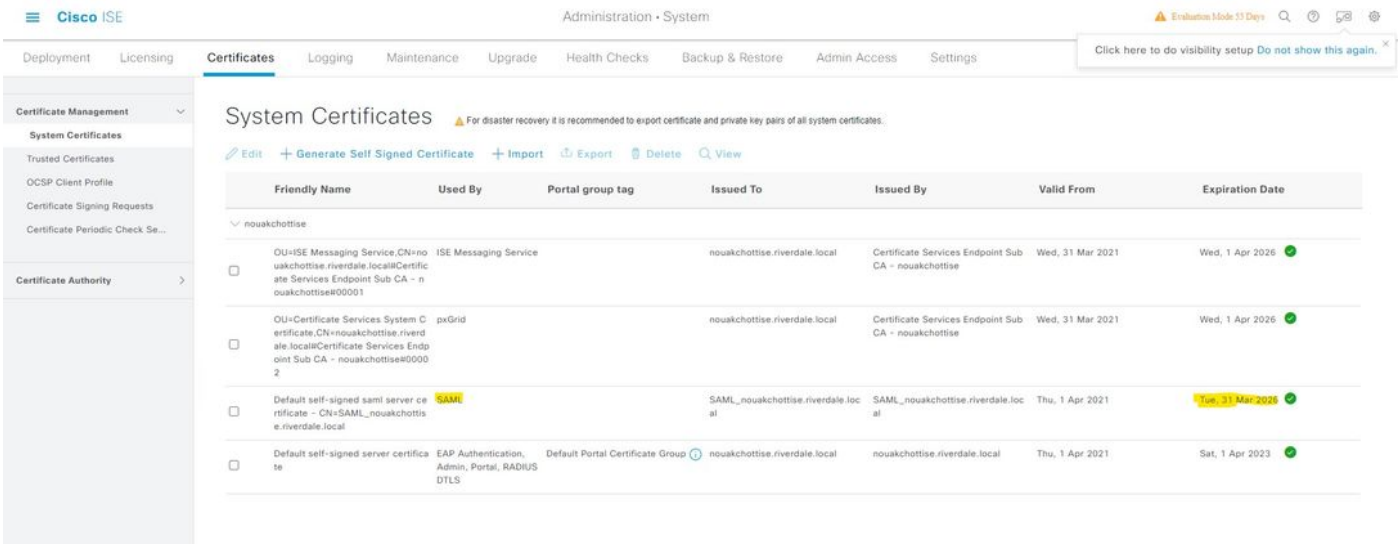


Certificati di sistema ISE 3.0

L'ambito di questo documento è solo per il certificato SAML. Per altri certificati ISE e per ulteriori informazioni sui certificati SSL in generale, fare riferimento a questo documento: TLS/SSL Certificates in ISE - Cisco

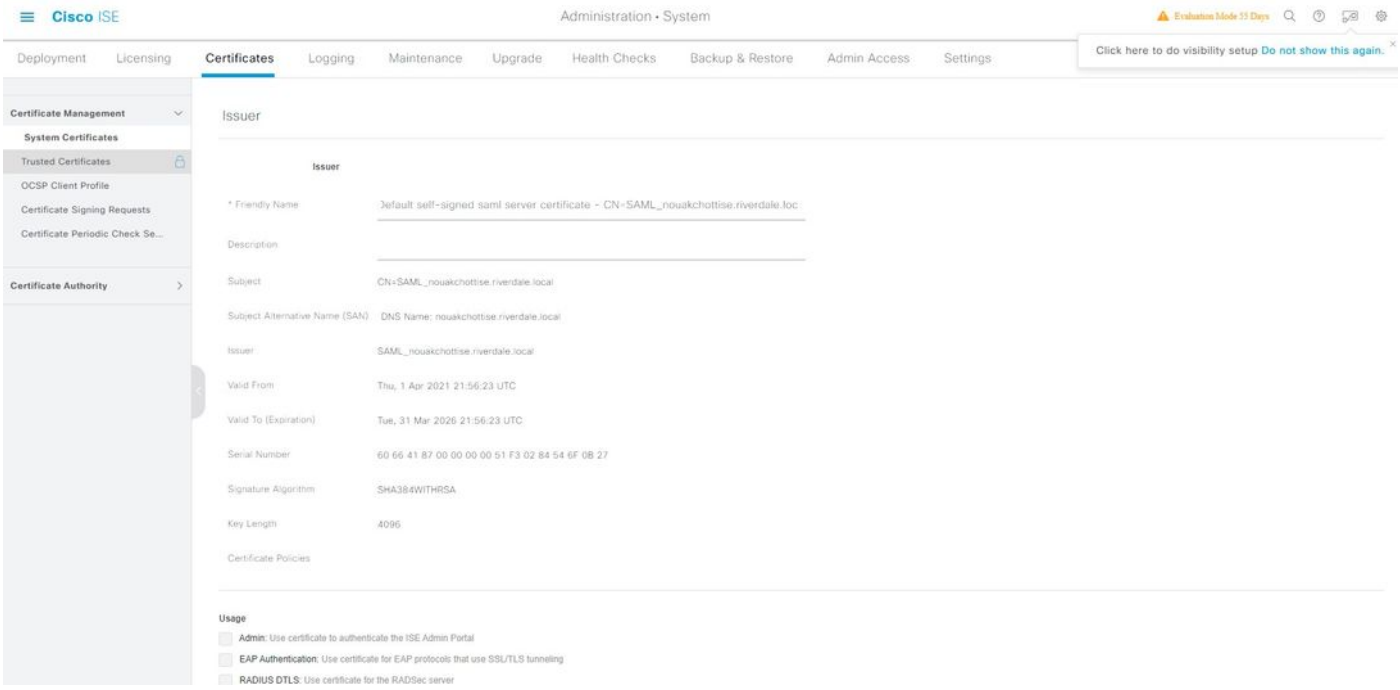
Certificato SAML in ISE

Il certificato SAML in ISE viene determinato cercando i certificati di sistema con la voce SAML nel campo Usi. Questo certificato verrà utilizzato per comunicare con i provider di identità SAML (IdP), ad esempio per verificare che le risposte SAML vengano ricevute dal provider di identità corretto e per proteggere la comunicazione con il provider di identità. Si noti che i certificati designati per l'utilizzo SAML non possono essere utilizzati per altri servizi, ad esempio Amministrazione, Autenticazione EAP e così via.



Per la prima volta in cui ISE viene installato, ISE viene fornito con un certificato server SAML autofirmato dotato delle seguenti proprietà:

Dimensioni chiave: 2048
Validità: un anno
Utilizzo chiave: Firma digitale (firma)
Utilizzo chiave esteso: Autenticazione server Web TLS (1.3.6.1.5.5.7.3.1)



> **Nota:** Si consiglia di non utilizzare un certificato contenente il valore 2.5.29.37.0 per l'identificatore di oggetto Any Purpose nell'attributo Extended Key Usage. Se si utilizza un certificato che contiene il valore 2.5.29.37.0 per l'identificatore di oggetto Any Purpose nell'attributo Utilizzo chiave esteso, il certificato viene considerato non valido e viene visualizzato il seguente messaggio di errore: "source=local ; type=fatal ; message="certificato non supportato".

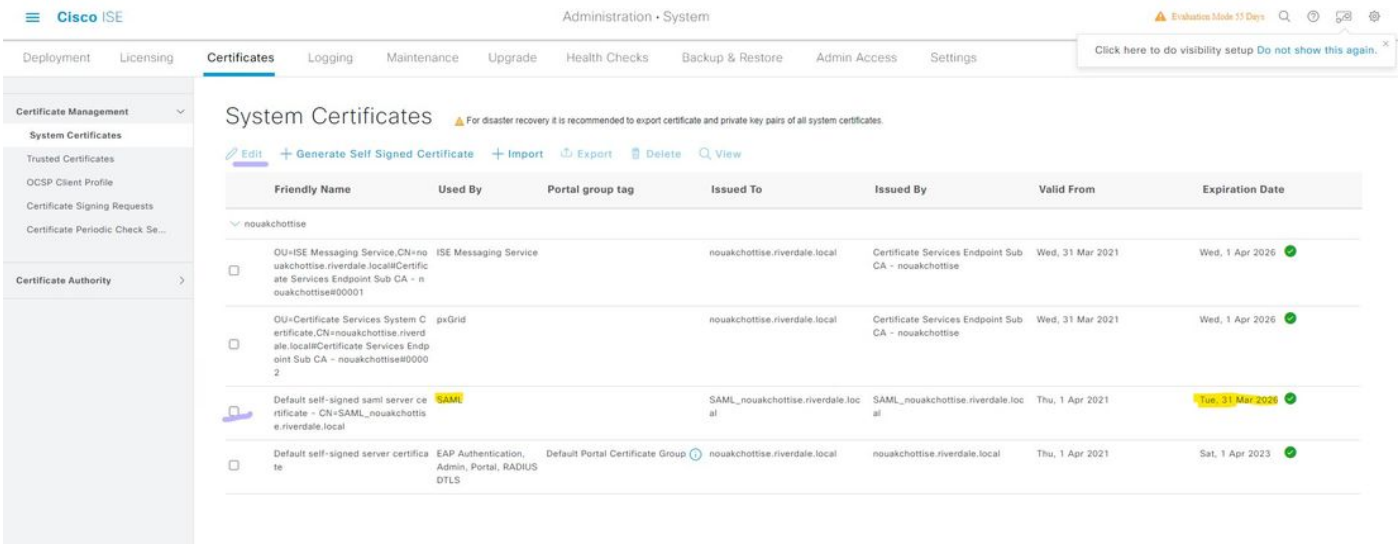
Gli amministratori ISE dovranno rinnovare questo certificato SAML autofirmato prima della scadenza, anche se la funzione SAML non è attivamente utilizzata.

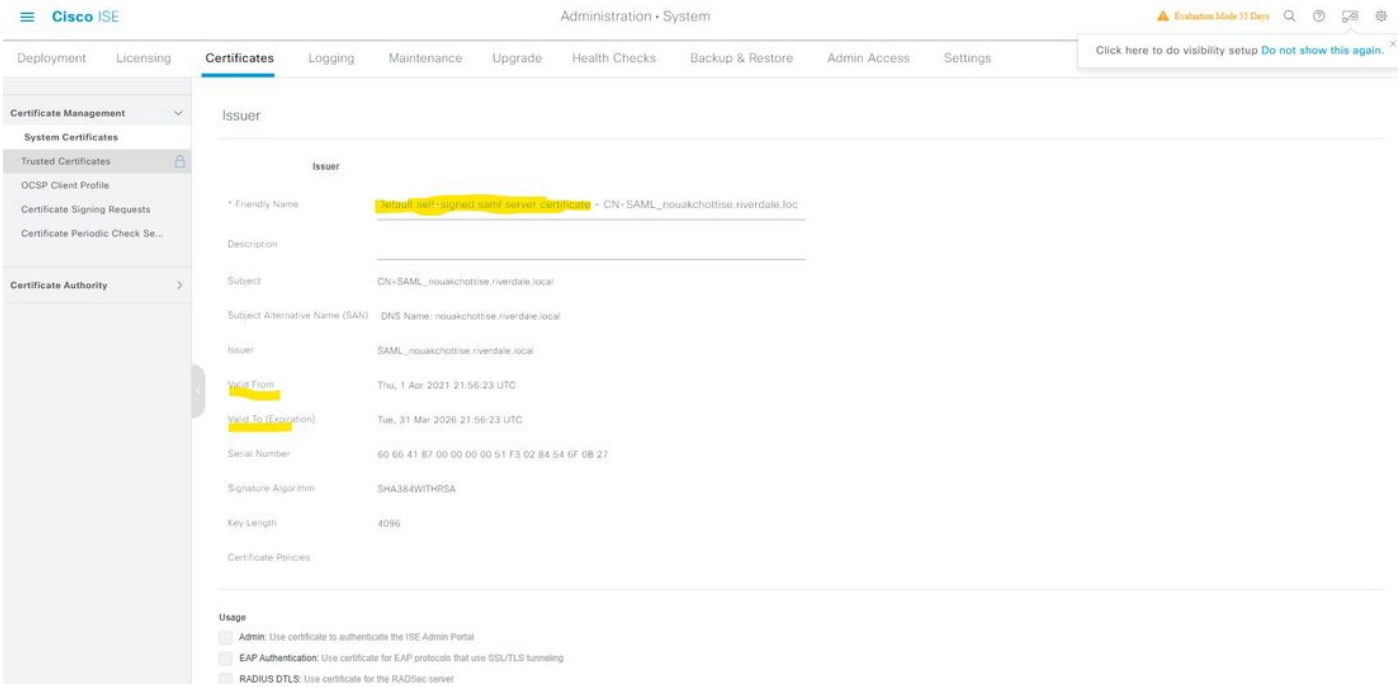
Rinnova un certificato SAML autofirmato in ISE

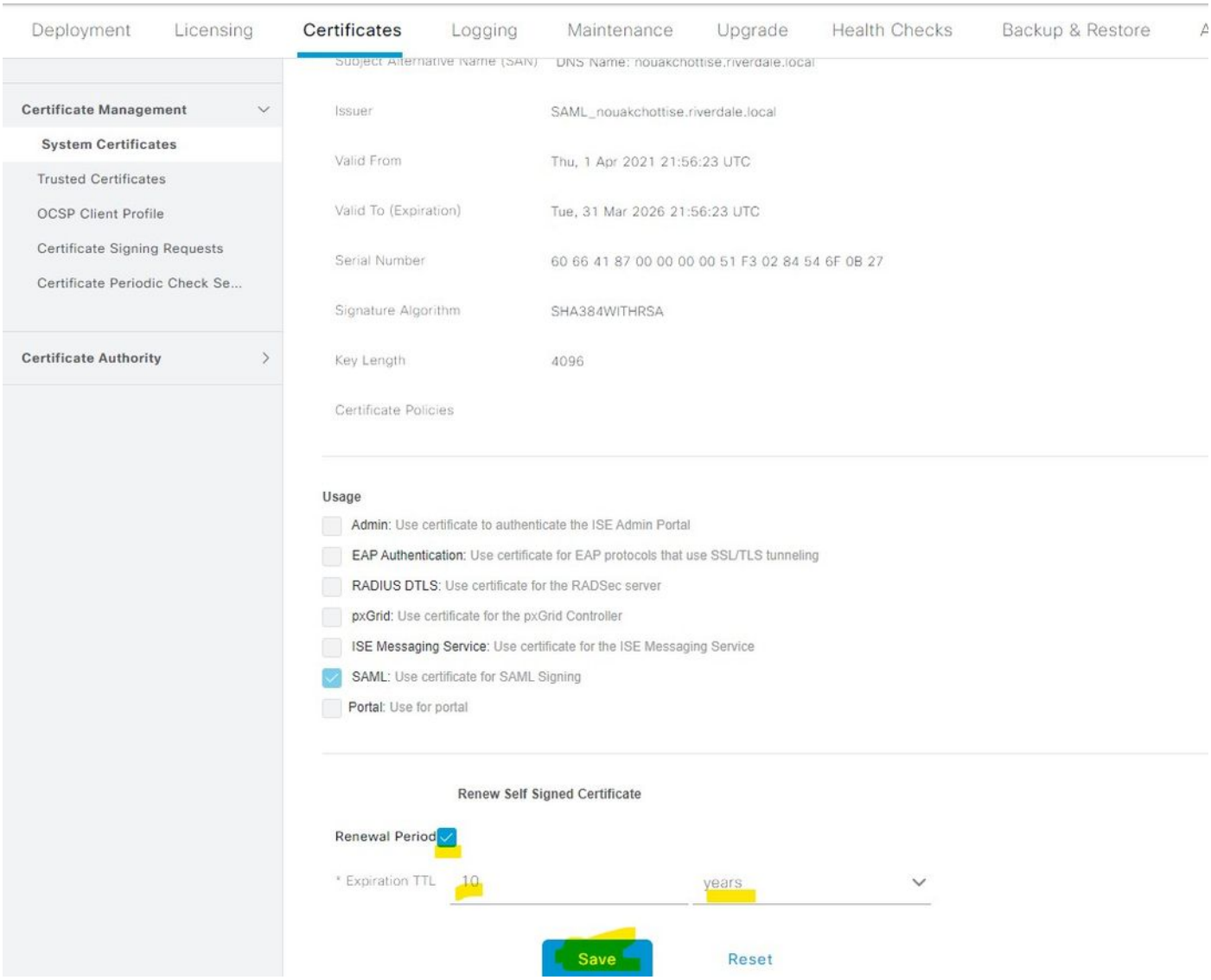
Un problema comune che gli utenti si trovano ad affrontare è che i loro certificati SAML alla fine scadranno, e ISE avvisa gli utenti con questo messaggio:

```
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.
```

Per i certificati server autofirmati, è possibile rinnovare il certificato solo per selezionare la casella periodo di rinnovo e inserire 5-10 anni come mostrato nell'immagine.







Infatti, qualsiasi certificato autofirmato che non sia attivo utilizzato dai nodi di implementazione ISE può essere semplicemente rinnovato per un periodo di 10 anni; in questo modo non si riceveranno avvisi di scadenza per i certificati relativi a servizi non utilizzati. La durata massima consentita per i

certificati autofirmati ISE è di 10 anni, e in genere dovrebbe essere sufficiente. L'aggiornamento di qualsiasi certificato di sistema sull'ISE non attiva il riavvio dei servizi se non è designato per l'utilizzo da parte dell'amministratore.

Conclusioni

Se un certificato di sistema ISE scaduto (autofirmato e firmato dalla CA) non è in uso, è possibile sostituirlo, eliminarlo o rinnovarlo. Si consiglia di non lasciare certificati scaduti (System o Trusted) su ISE prima di eseguire un aggiornamento di ISE.

Informazioni correlate

- ISE 3.0 Manage Certificates: Guida per l'amministratore di Cisco Identity Services Engine, versione 3.0 - Configurazione di base [Cisco Identity Services Engine] - Cisco
- Certificati SSL in ISE: Certificati TLS/SSL in ISE - Cisco
- Documentazione e supporto tecnico – Cisco Systems