Crea e utilizza certificato di terze parti su UCSM

Sommario

Introduzione

Questo documento descrive la procedura per creare e utilizzare certificati di terze parti su Unified Computing System (UCS) per comunicazioni protette.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso all'autorità CA
- UCS SM 3.1

Componenti usati

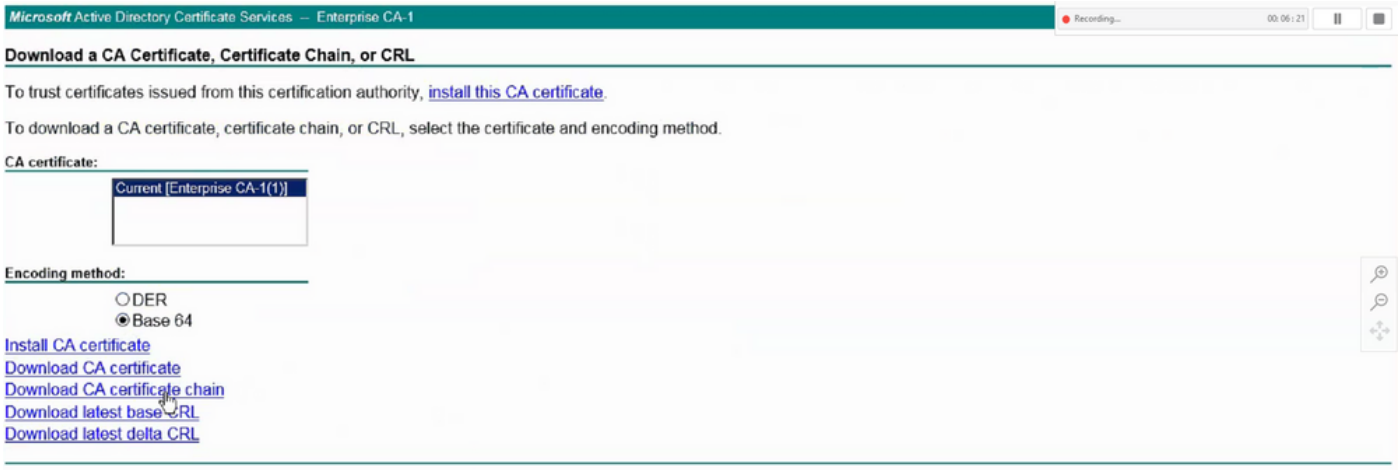
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Passi da configurare

Configura trust point

Passaggio 1

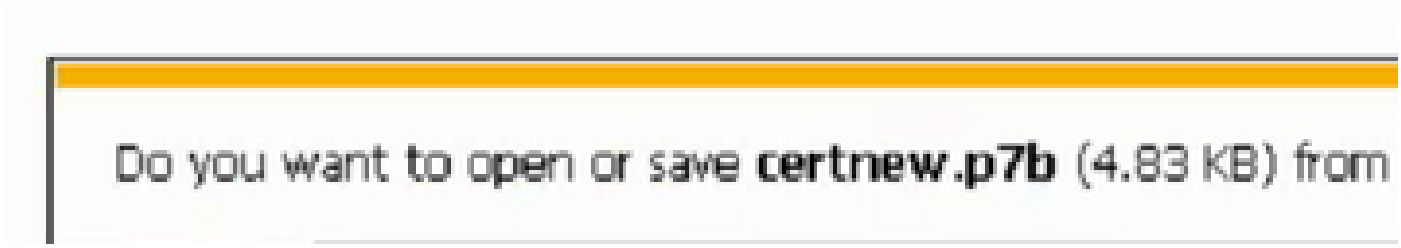
- Scaricare la catena di certificati dall'autorità CA per creare il trust point. Fare riferimento a http://localhost/certsrv/Default.asp all'interno di Cert Server.
- Assicurarsi che la codifica sia impostata su Base 64.



Scarica catena di certificati dall'autorità CA

Passaggio 2

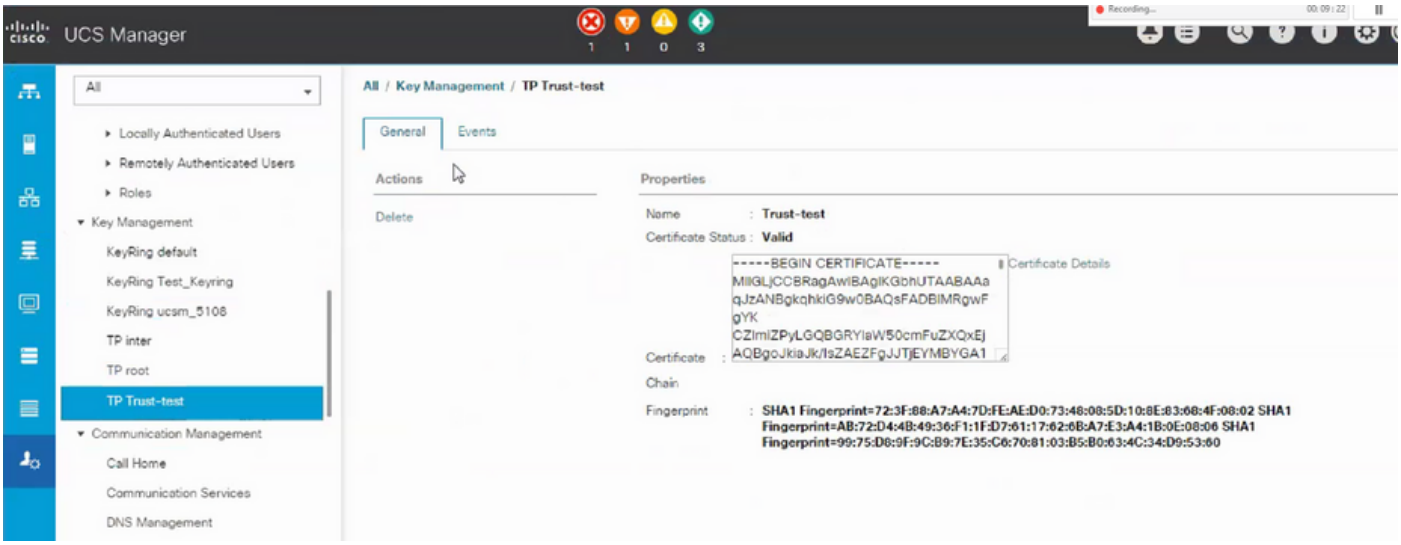
- La catena di certificati scaricata è in formato PB7.



- Convertire il file .pb7 in formato PEM con lo strumento OpenSSL.
- Ad esempio, in Linux, è possibile eseguire questo comando in terminal per eseguire la conversione - openssl pkcs7 -print_certs -in <nome_cert>.p7b -out <nome_cert>.pem.

Passaggio 3

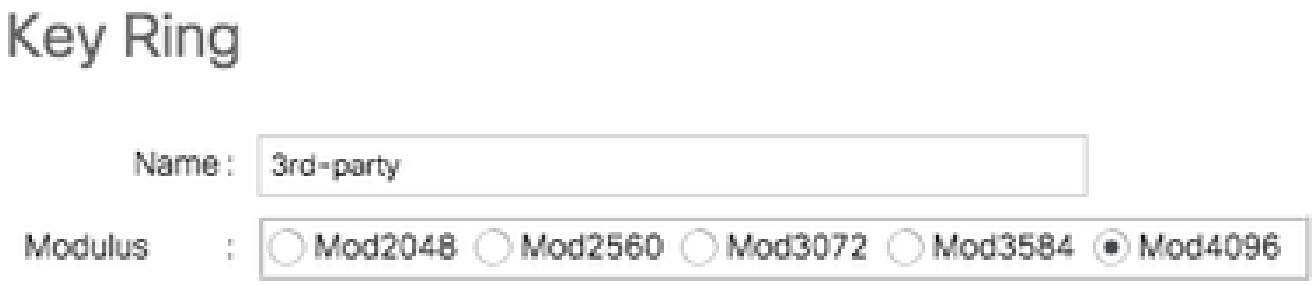
- Creare un trust point su UCSM.
- Passare ad Amministrazione > Gestione chiavi > Trustpoint.
- Quando si crea il trust point, incollare il contenuto completo del file PEM creato nel passaggio 2 di questa sezione nello spazio dei dettagli del certificato.



Creazione di portachiavi e CSR

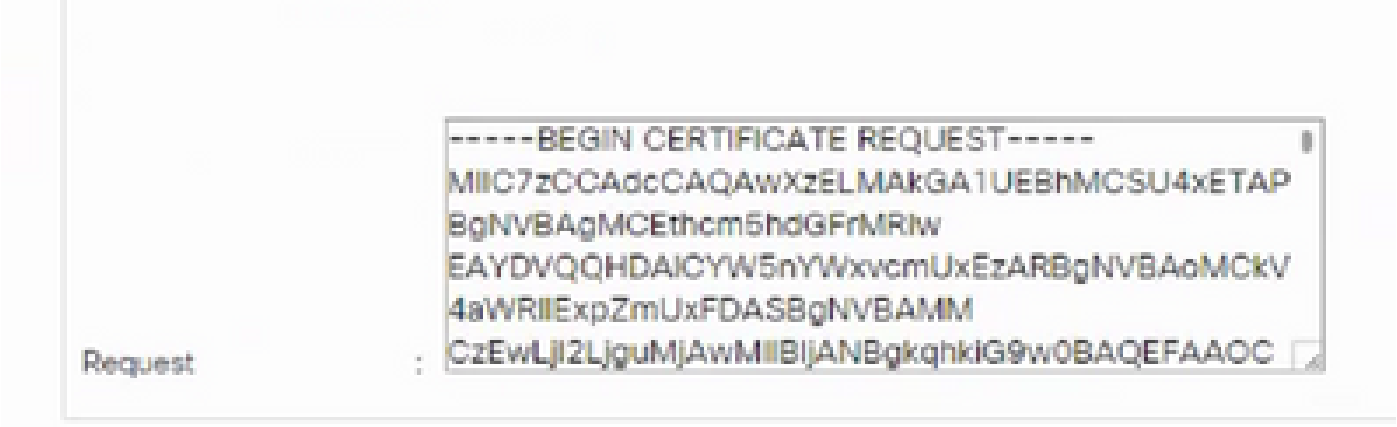
Passaggio 1

- Passare a UCSM > Admin > Gestione tasti > Gruppo di chiavi.
- Scegliere il modulo necessario per il certificato di terze parti.



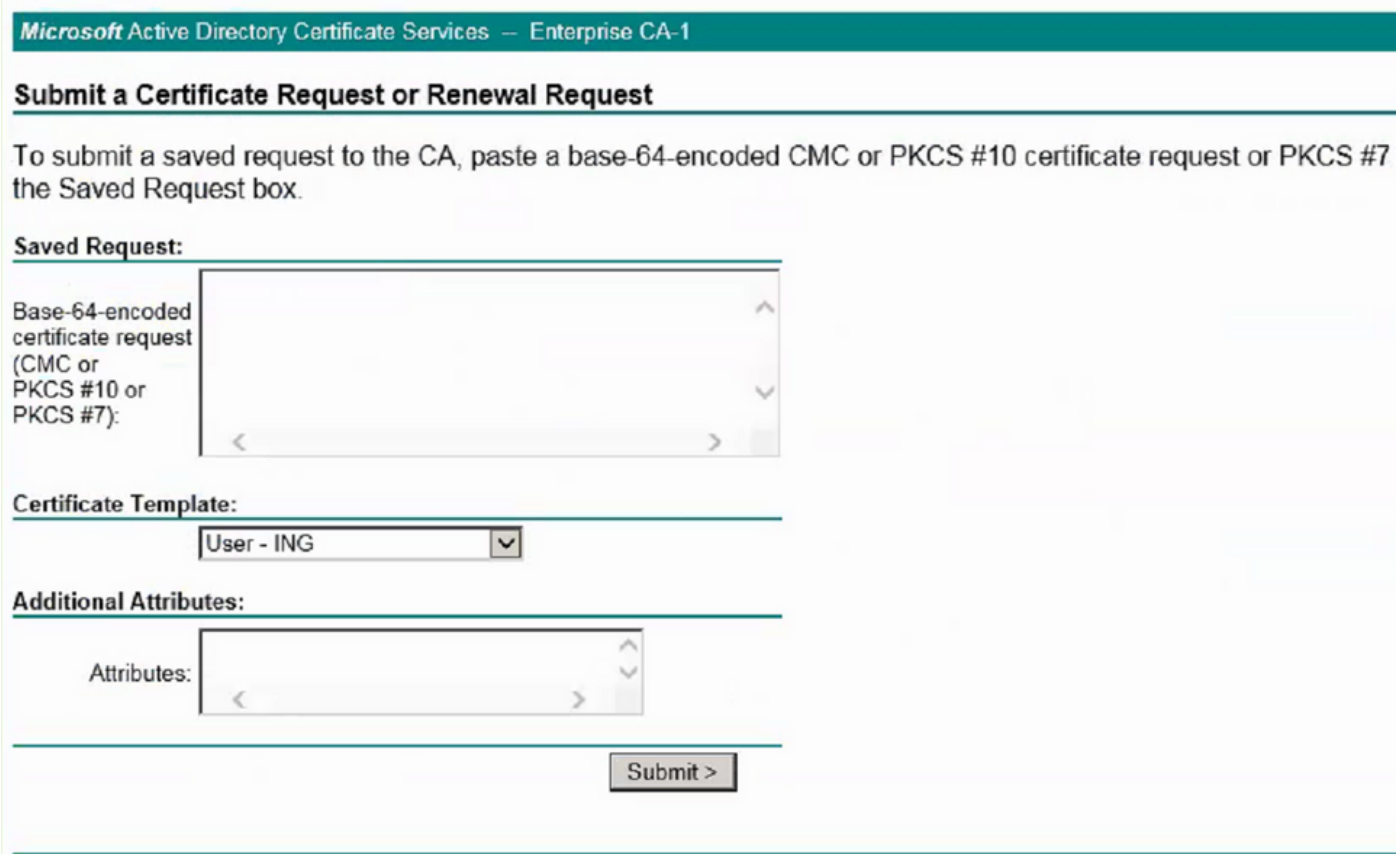
Passaggio 2

- Fare clic su Crea richiesta certificato e specificare i dettagli richiesti.
- Copiare il contenuto del campo della richiesta.



Passaggio 3

Per generare il certificato, incollare la richiesta copiata dal passaggio 2 nello spazio indicato di seguito:



Passaggio 4

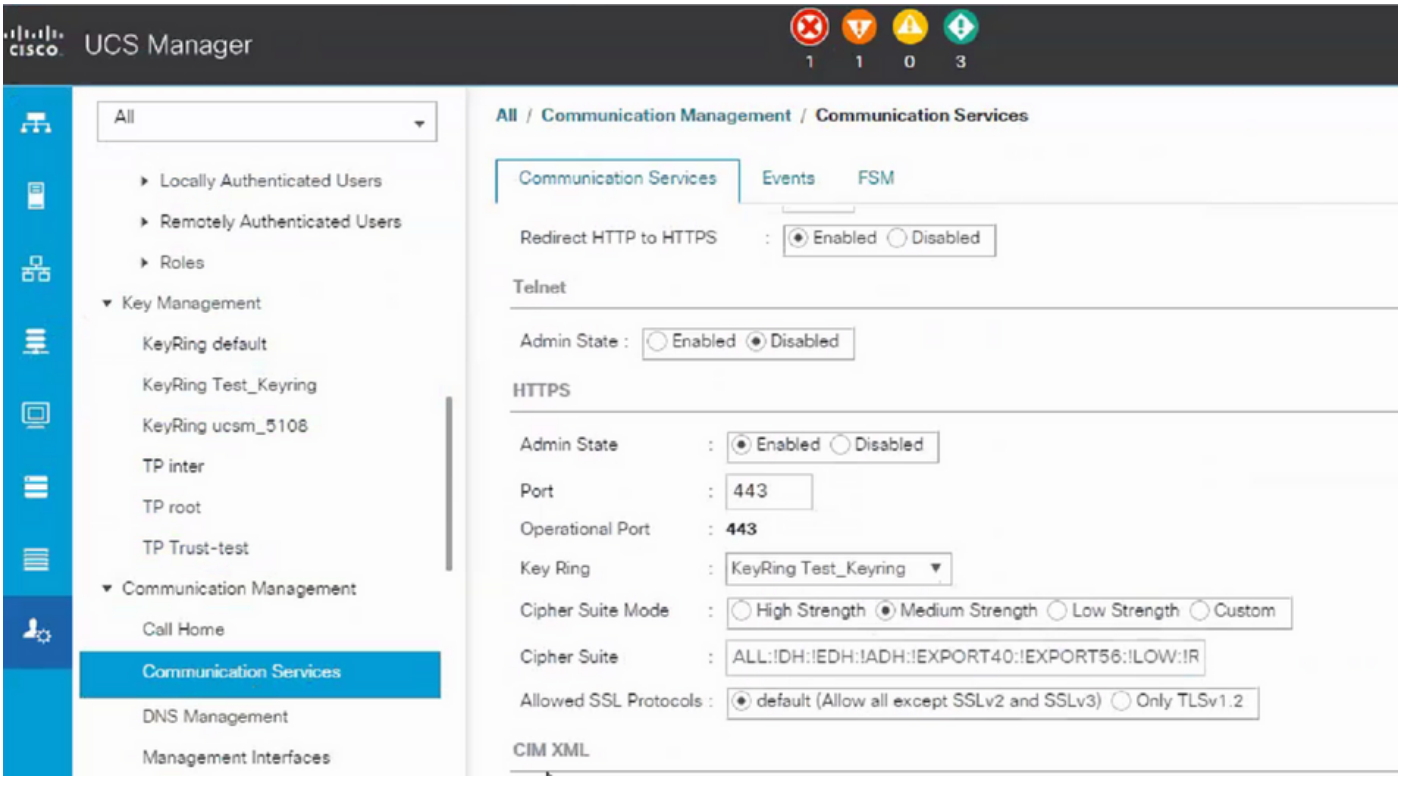
- Una volta inviato, viene generato un nuovo certificato. Aprire il file e copiare tutto il contenuto del certificato appena generato nel campo del certificato sul keyring creato al passaggio 1 di questa sezione.

- Scegliere il trust-point dall'elenco a discesa creato nel passaggio 3 di Crea keyring e CSR.

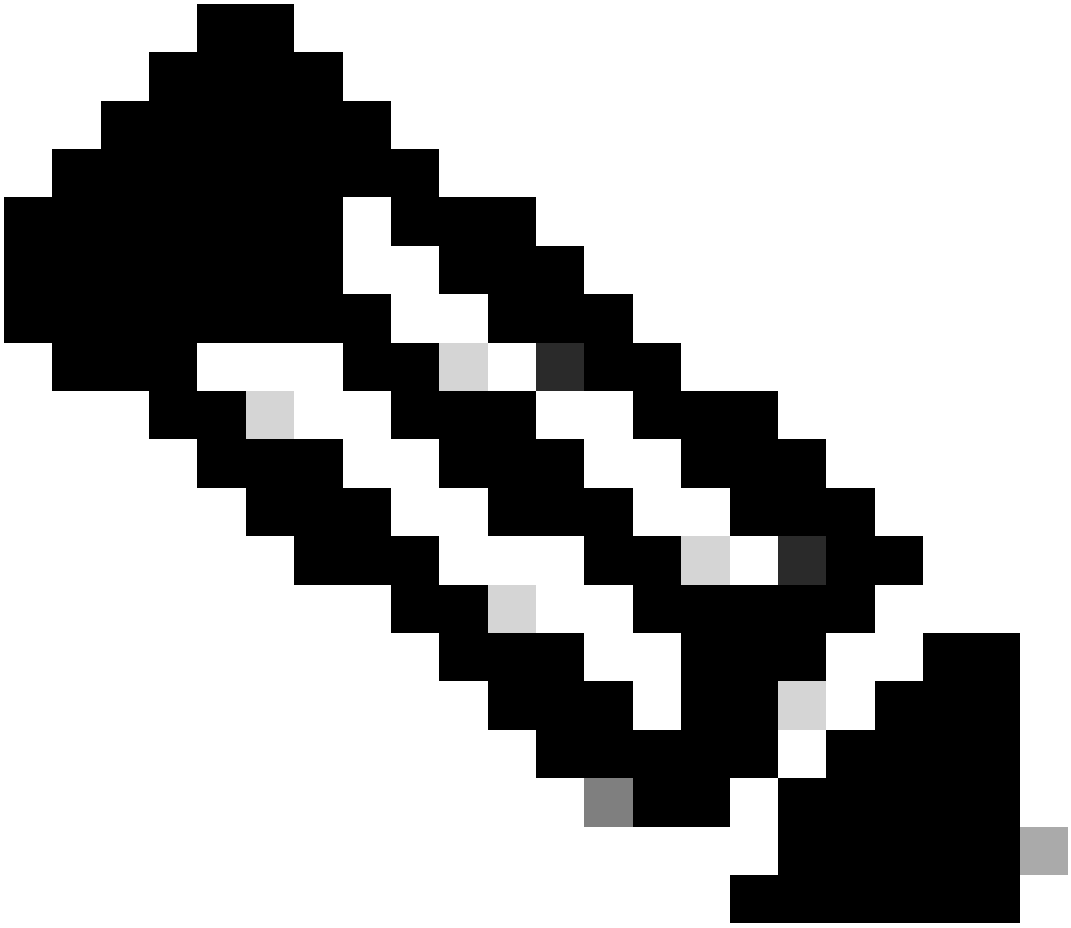
Applicazione della sequenza di tasti

Passaggio 1

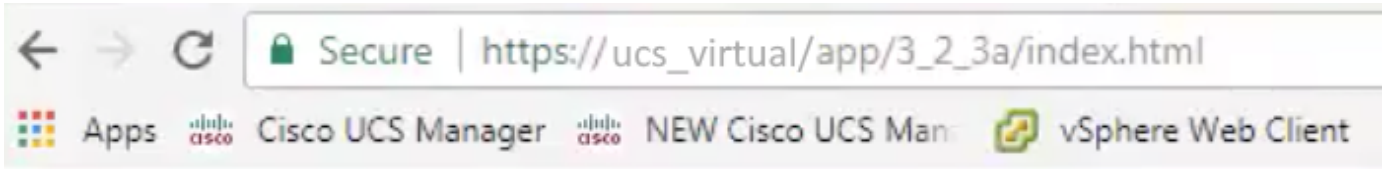
Scegliere la sequenza di tasti creata nei servizi di comunicazione come illustrato di seguito:



Dopo la modifica della sequenza di tasti, la connessione HTTPS al modulo UCSM risulta protetta nel browser Web.



Nota: è necessario che anche il desktop locale utilizzi il certificato della stessa autorità CA del modulo UCSM.



Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).