Configurazione di CSSM su prem e registrazione delle licenze con ISE

Sommario

Introduzione

Questo documento descrive l'integrazione di CSM On-Prem con Cisco Identity Service Engine (ISE) e Cisco Smart Account, garantendo una configurazione ottimale.

Prerequisiti

Requisiti

ISE 3.X

Cisco Smart Software Manager (CSM) versione 8 release 202304 +

Componenti usati

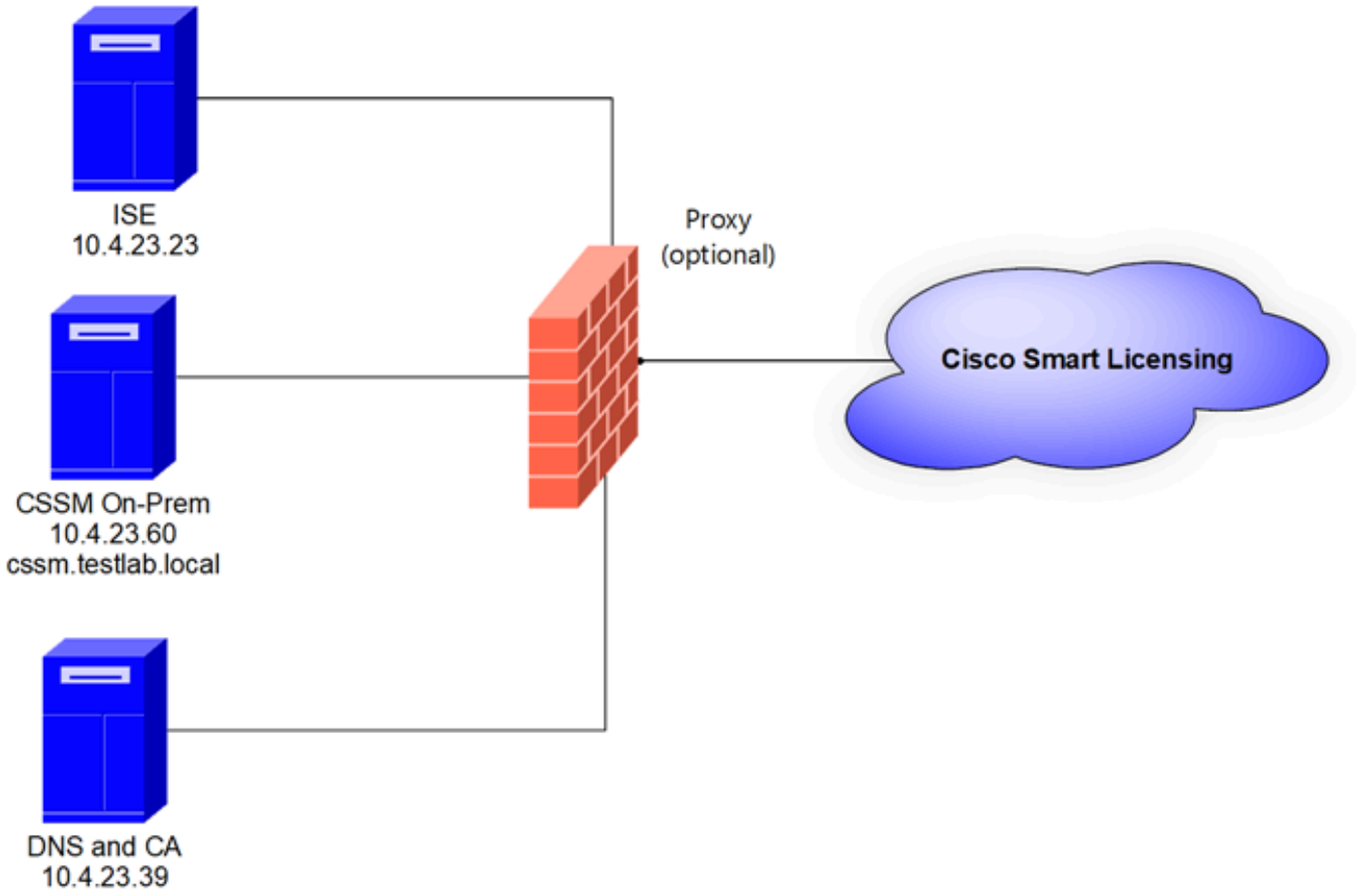
- Patch 2 di Identity Service Engine 3.2
- SSM On Prem 8.20234

- Windows Active Directory 2016 (servizi DNS e Autorità di certificazione)
- VMWare ESXi versione 7

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.

Configurazione

Esempio di rete



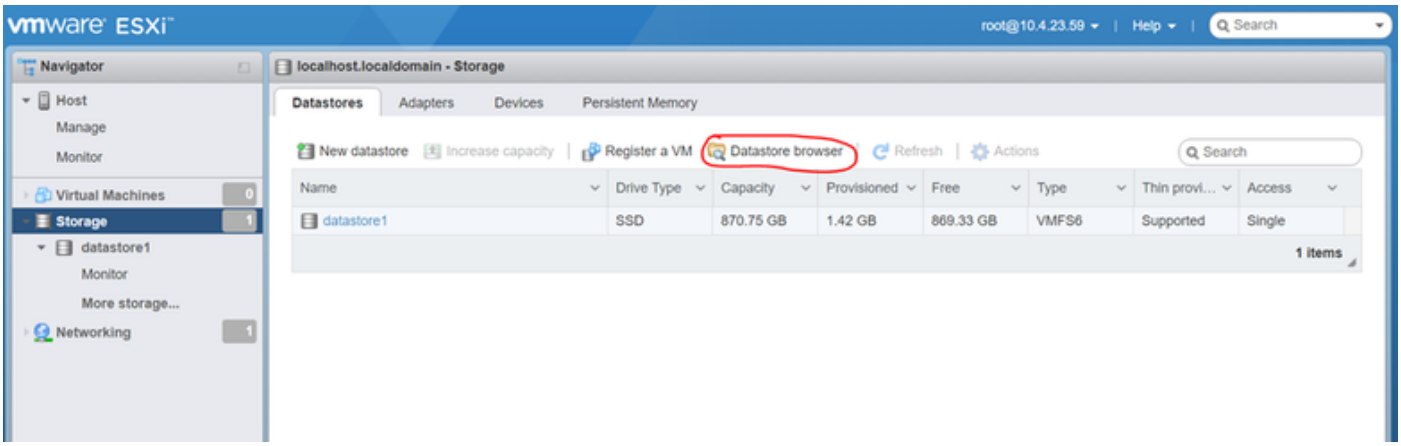
Topologia generale

Installare CSM on-Prem su VMWARE ESXi.

1. Scaricare Cisco IOS®. È possibile utilizzare il collegamento successivo: https://software.cisco.com/download/home/286285506/type/286326948/release/8-202304

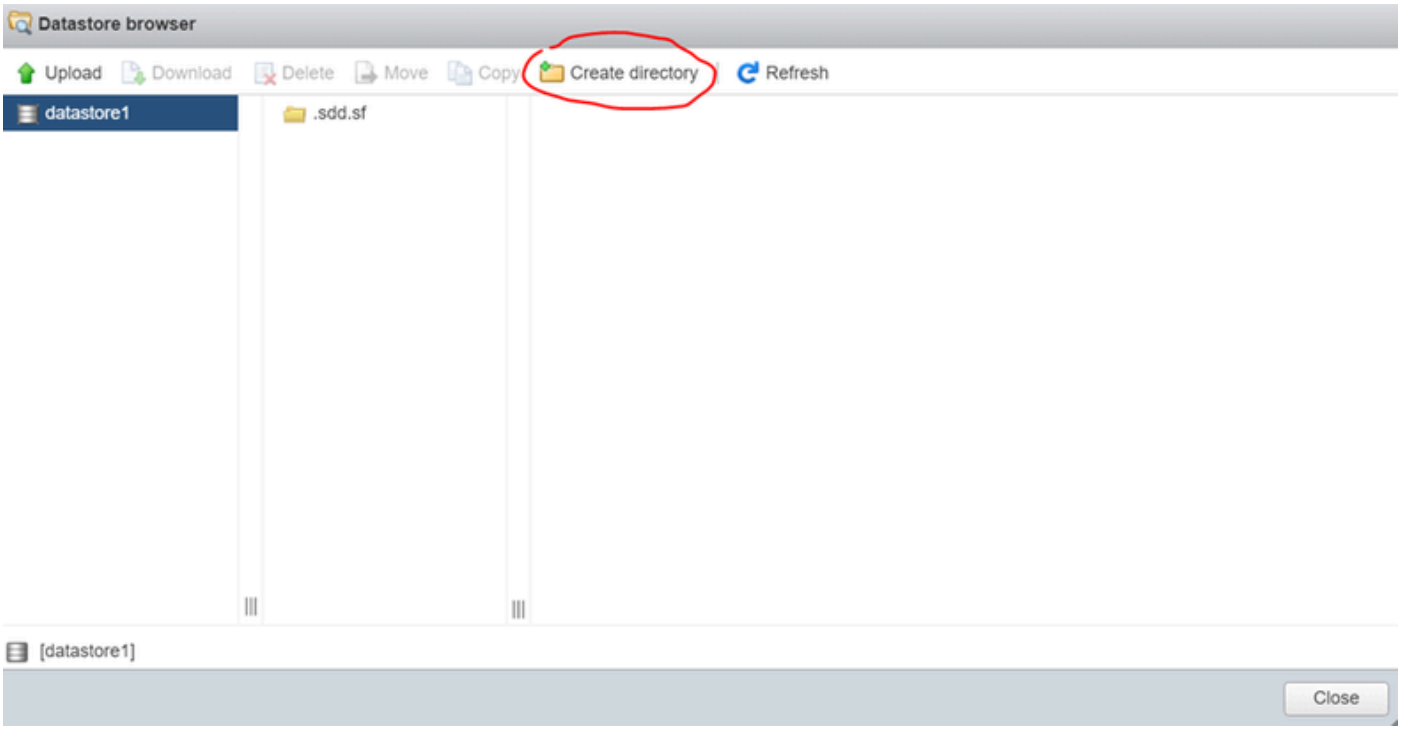
2. Caricare l'ISO in VMWARE ESXi.

Passare a Memoria > Browser archivio dati.



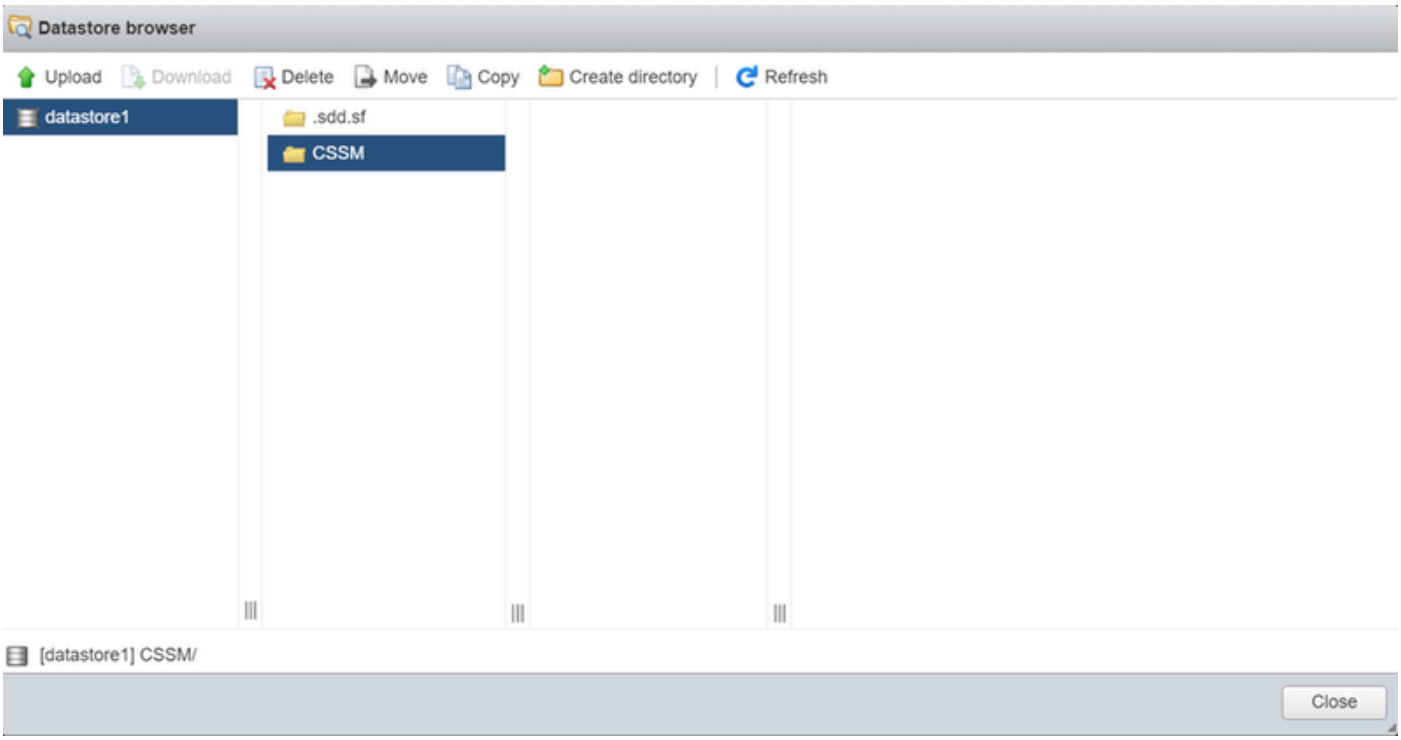
Sezione Data browser

3. Fare clic su Crea directory per creare una nuova cartella (facoltativo).



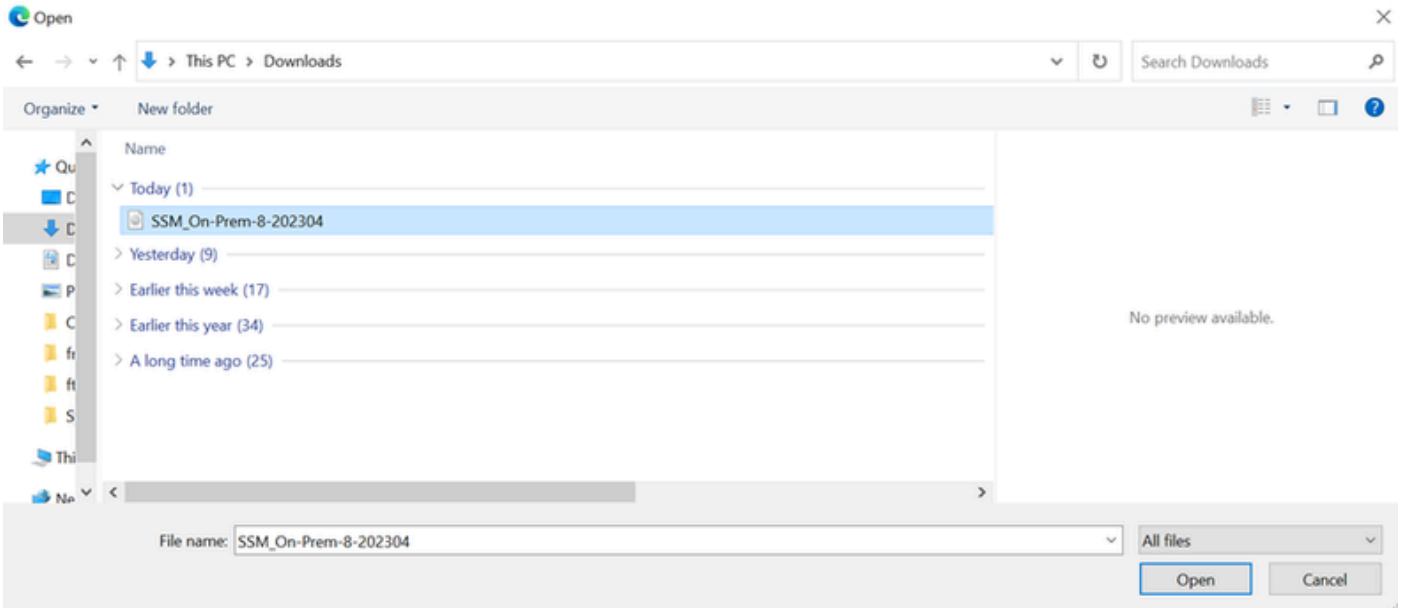
Creazione della directory

Nell'esempio seguente è stata creata la cartella CSSM:



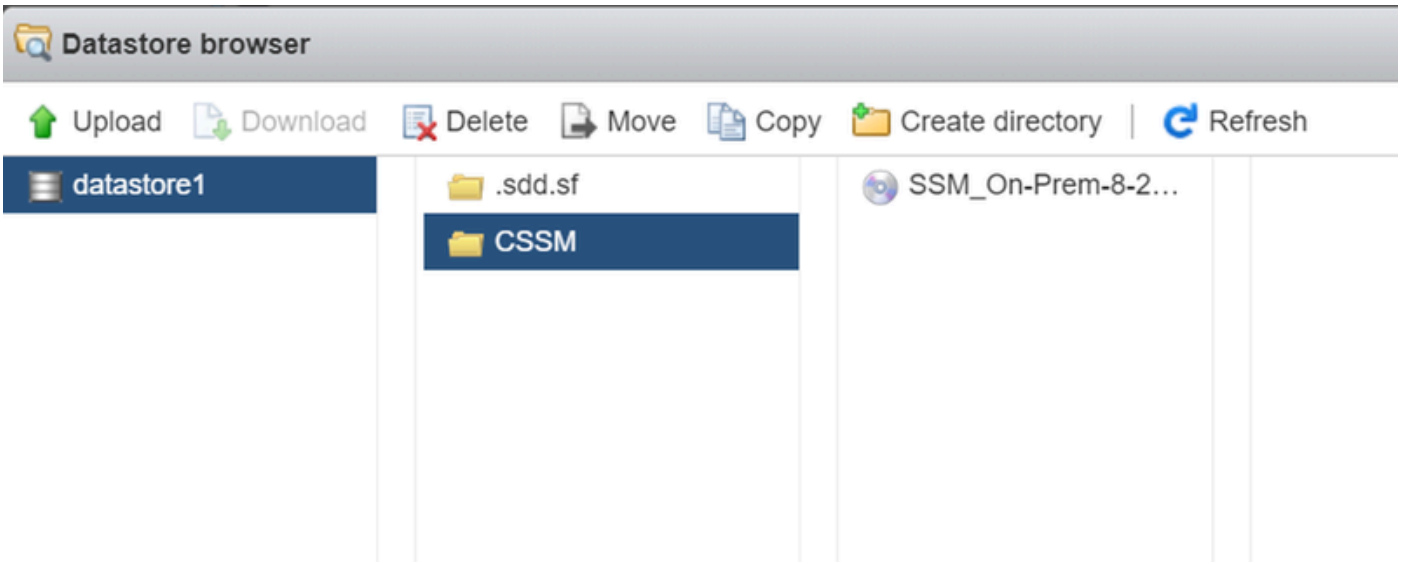
Creazione di cartelle

4. Fare clic su Upload, quindi scegliere il file ISO.



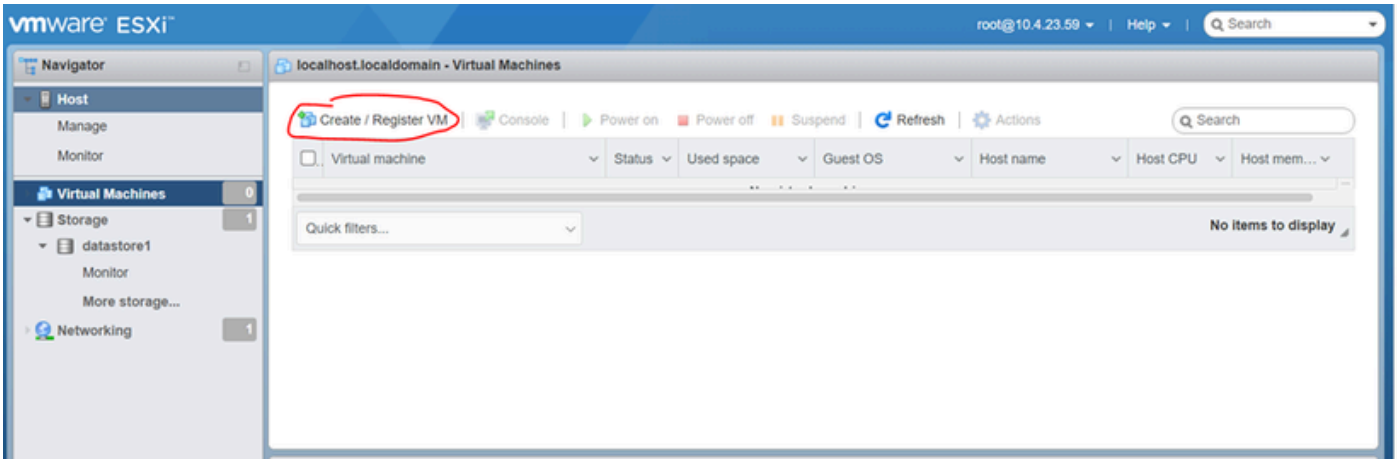
Caricamento ISO

Il file ISO si trova nella cartella CSSM:



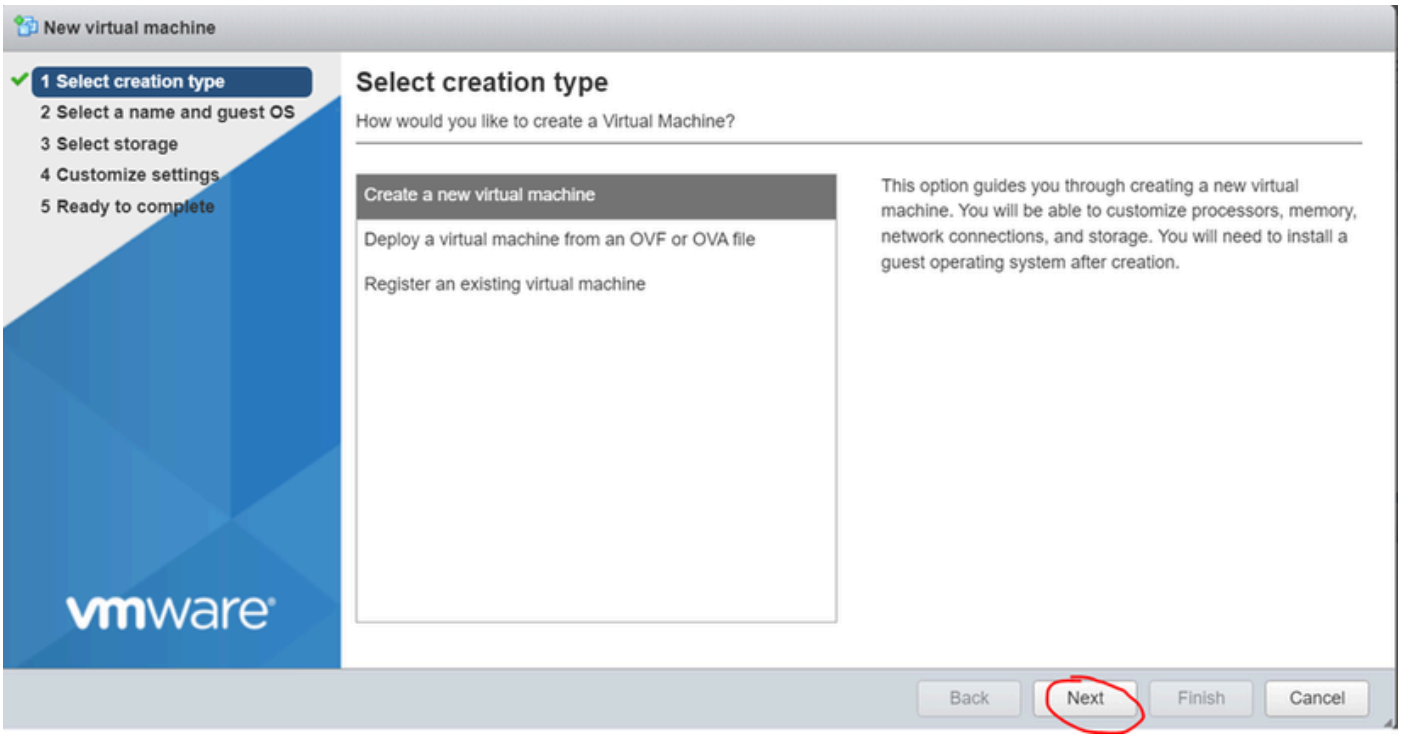
Caricamento ISO completato

5. Creare la macchina virtuale. passare a Macchina virtuale > Crea/registra macchina virtuale.



Creazione di una nuova VM fase 01

6. Scegliere Crea una nuova macchina virtuale e fare clic su Avanti.

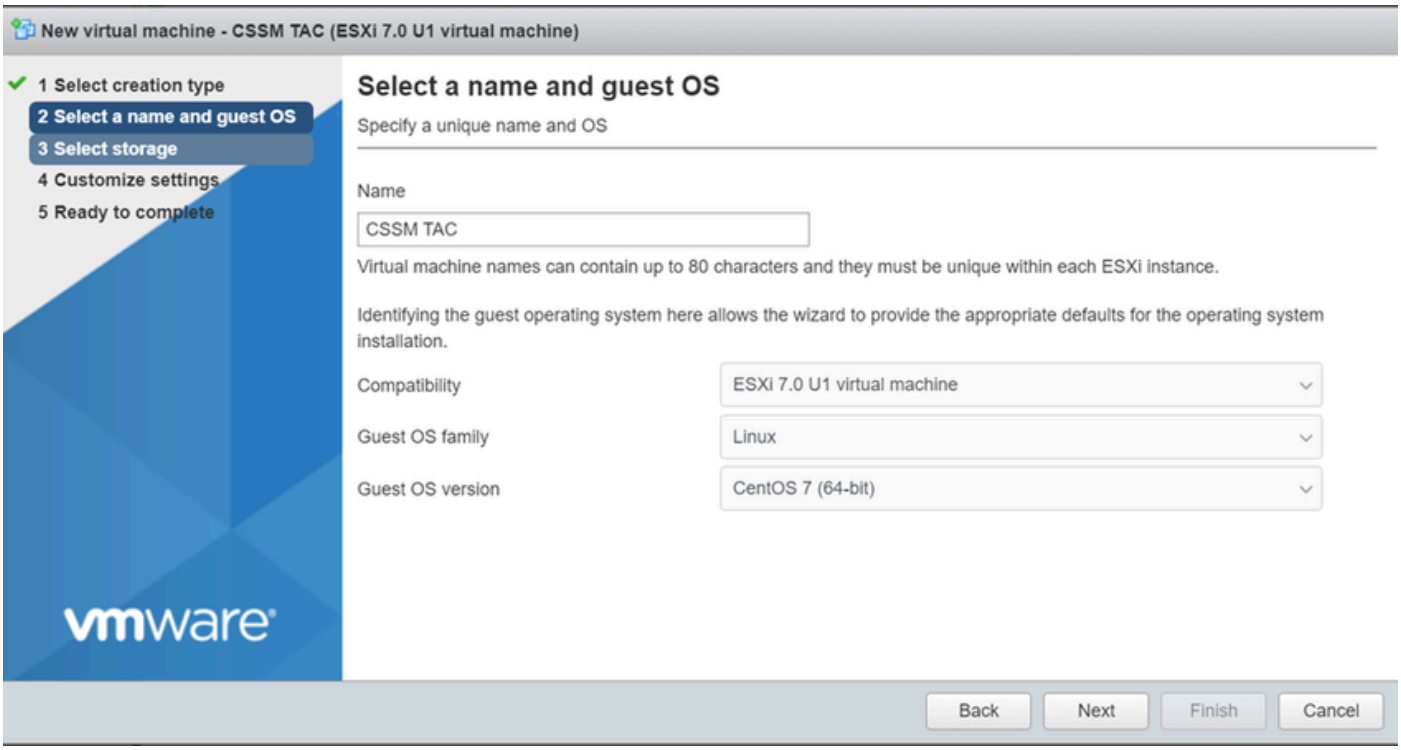


Creazione di una nuova VM fase 02

7. Quindi configurare i parametri successivi:

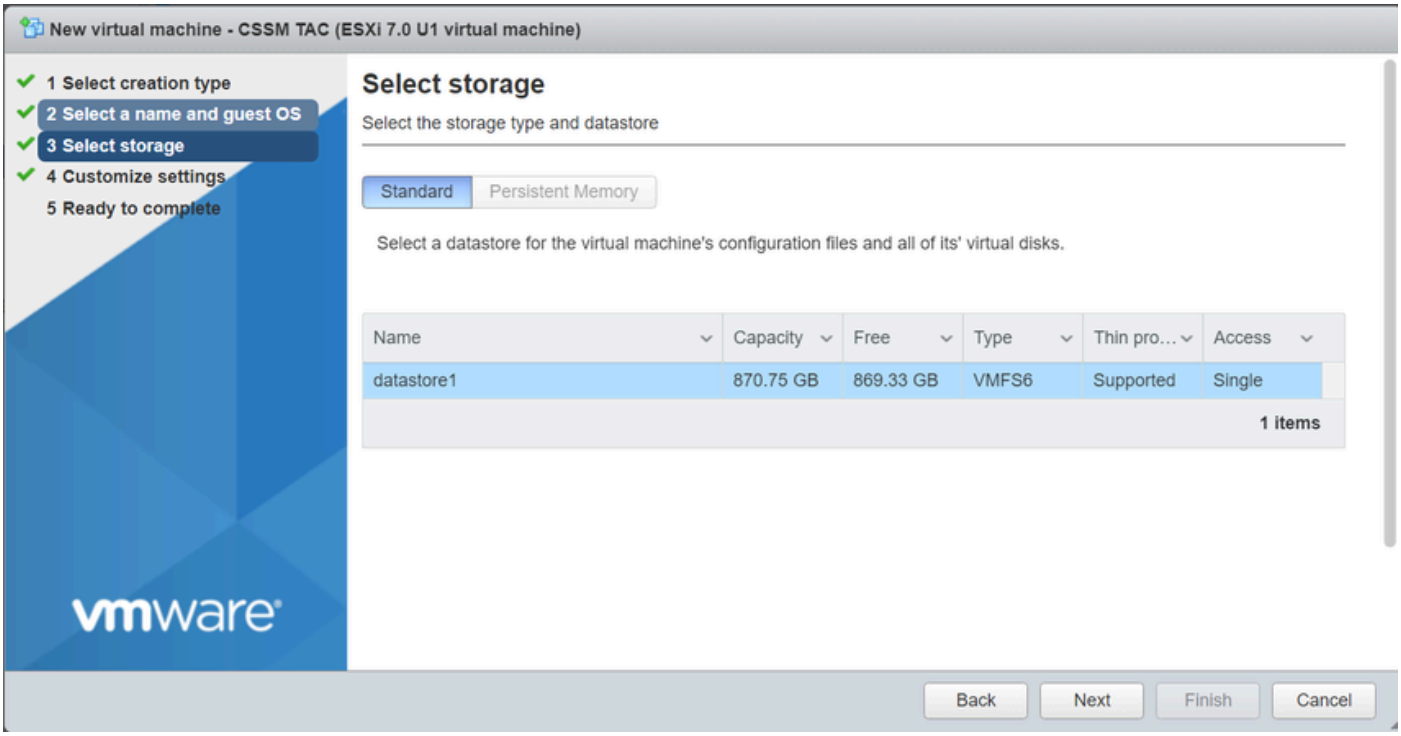
- Nome: immettere il nome della macchina virtuale.
- Compatibilità: selezionare ESXi 6.0 o versione successiva oppure ESXi 6.5 o versione successiva.
- Famiglia di sistemi operativi guest: Linux.
- Versione sistema operativo guest: scegliere CentOS 7 (64 bit) o Altro Linux 2.6x (64 bit)

Fare clic su Next (Avanti).



Nome VM e IOS

8. Selezionare la memoria e fare clic su avanti.



Elenco di archiviazione

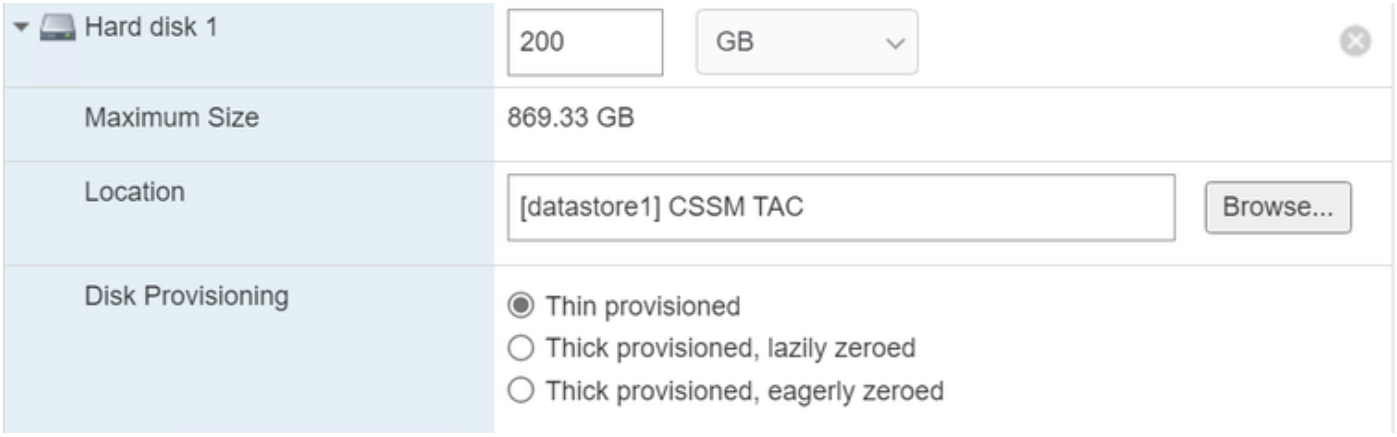
9. Configurare i parametri successivi:

- CPU: almeno 4. L'impostazione effettiva di vCPU dipende dai requisiti di scalabilità

Nota: la quantità di core per socket deve essere impostata su 1 indipendentemente dal numero di socket virtuali selezionati. Ad esempio, una configurazione a 4 vCPU deve essere configurata come 4 socket e 1 core per socket.

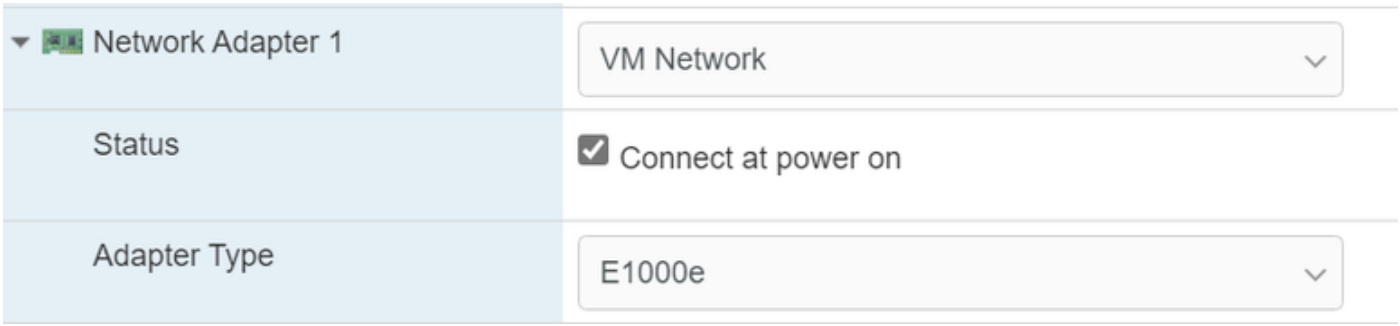
Configurazione dei core

- Memoria: 8 GB
- Disco rigido: 200 GB e la funzione di provisioning di verifica è impostata su Thin Provision.



Configurazione del disco

- Scheda di rete: selezionare il tipo di scheda E1000 e selezionare Connetti all'accensione.



Configurazione delle impostazioni di rete

- Unità CD/DVD: scegliere "File ISO dei dati" e selezionare il file ISO.

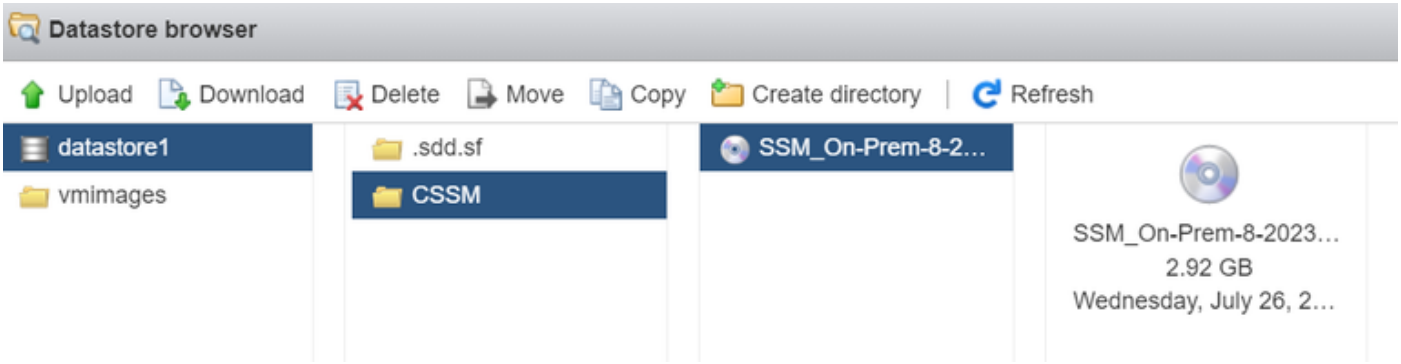
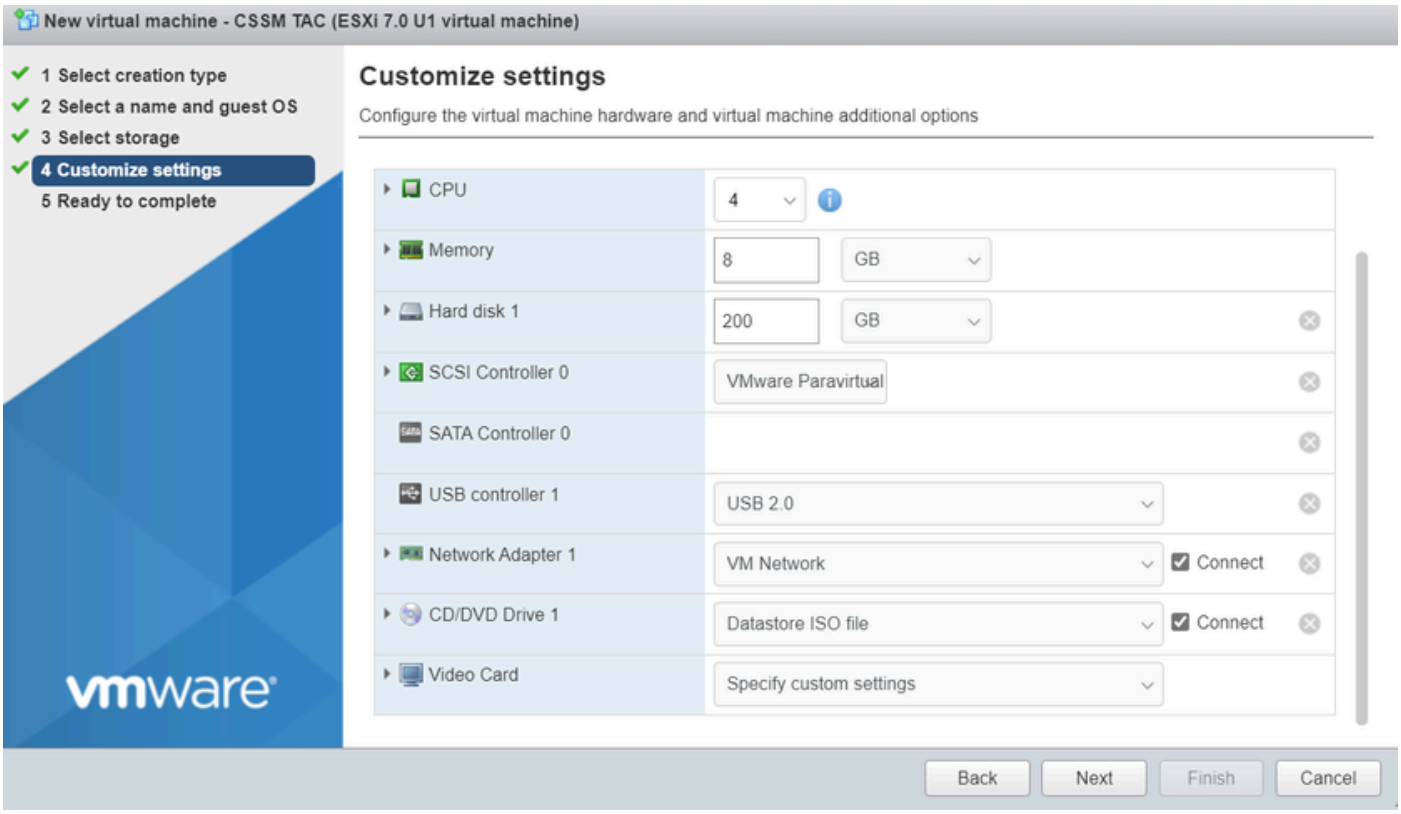


immagine ISO

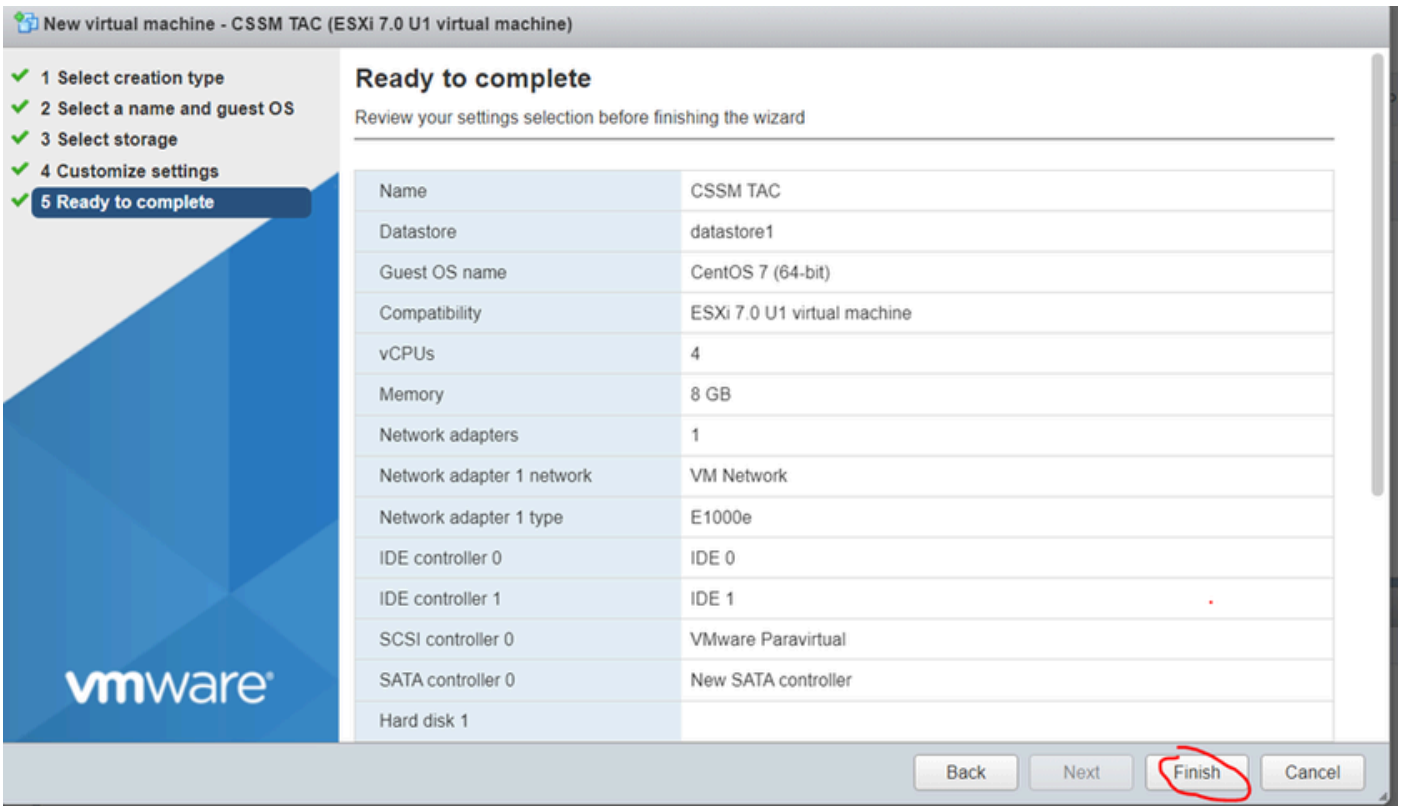
È possibile verificare il riepilogo delle impostazioni dopo aver completato i passaggi precedenti.



Riepilogo configurazione VM 01

Fare clic su Next (Avanti).

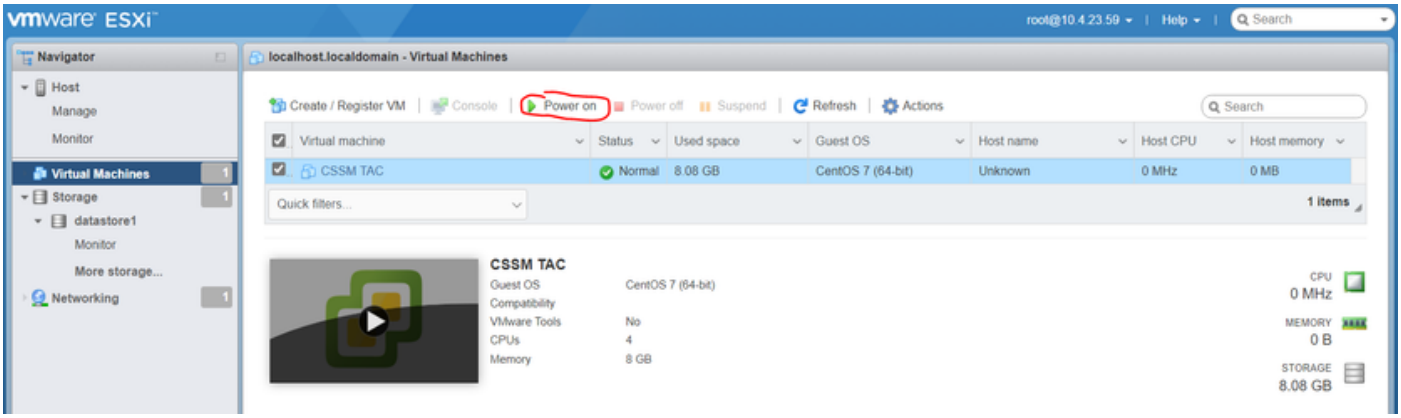
10. Fare clic su Fine.



Riepilogo configurazione VM 02

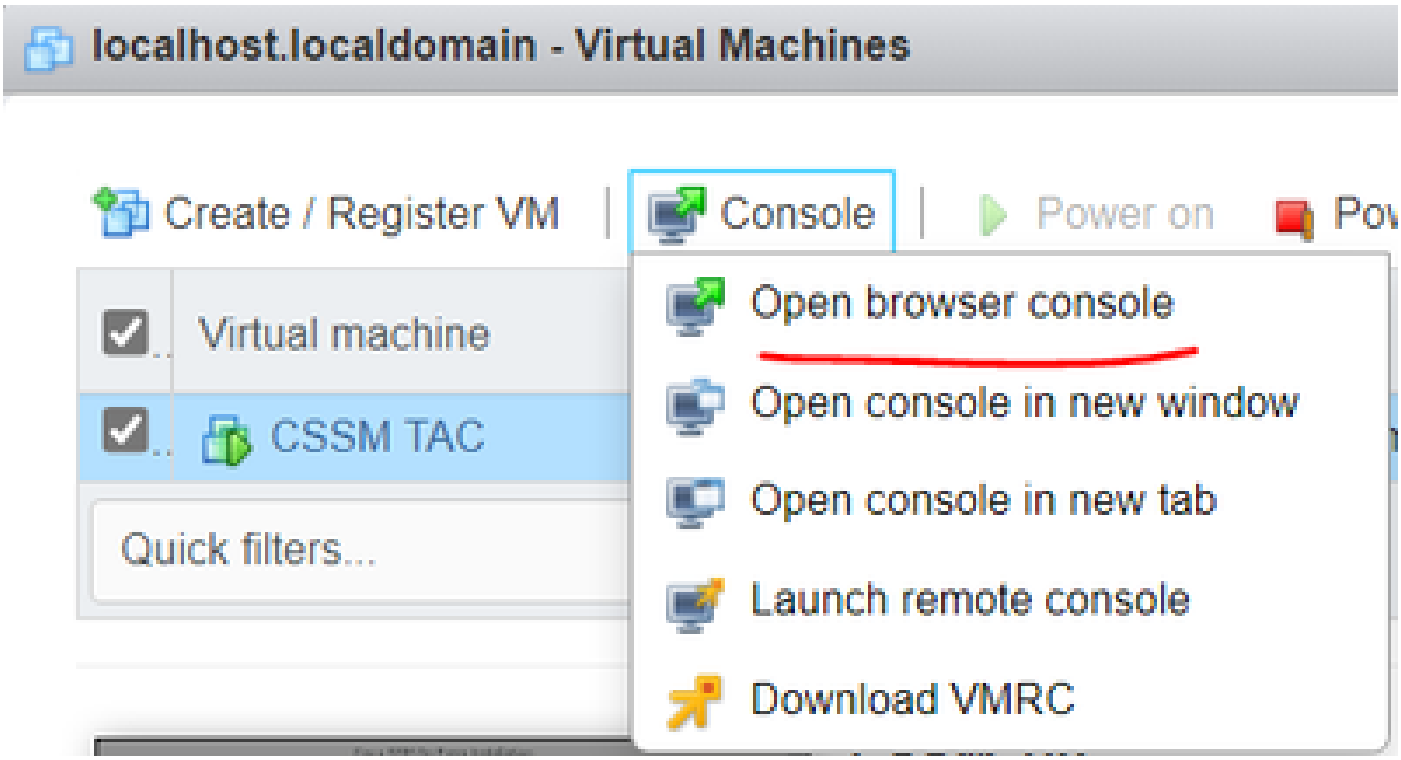
Configurazione iniziale di CSSM locale.

1. In VMWARE ESXi, passare a Virtual Machines (Macchine virtuali) e selezionare la macchina virtuale, quindi fare clic su Power On (Accendi).



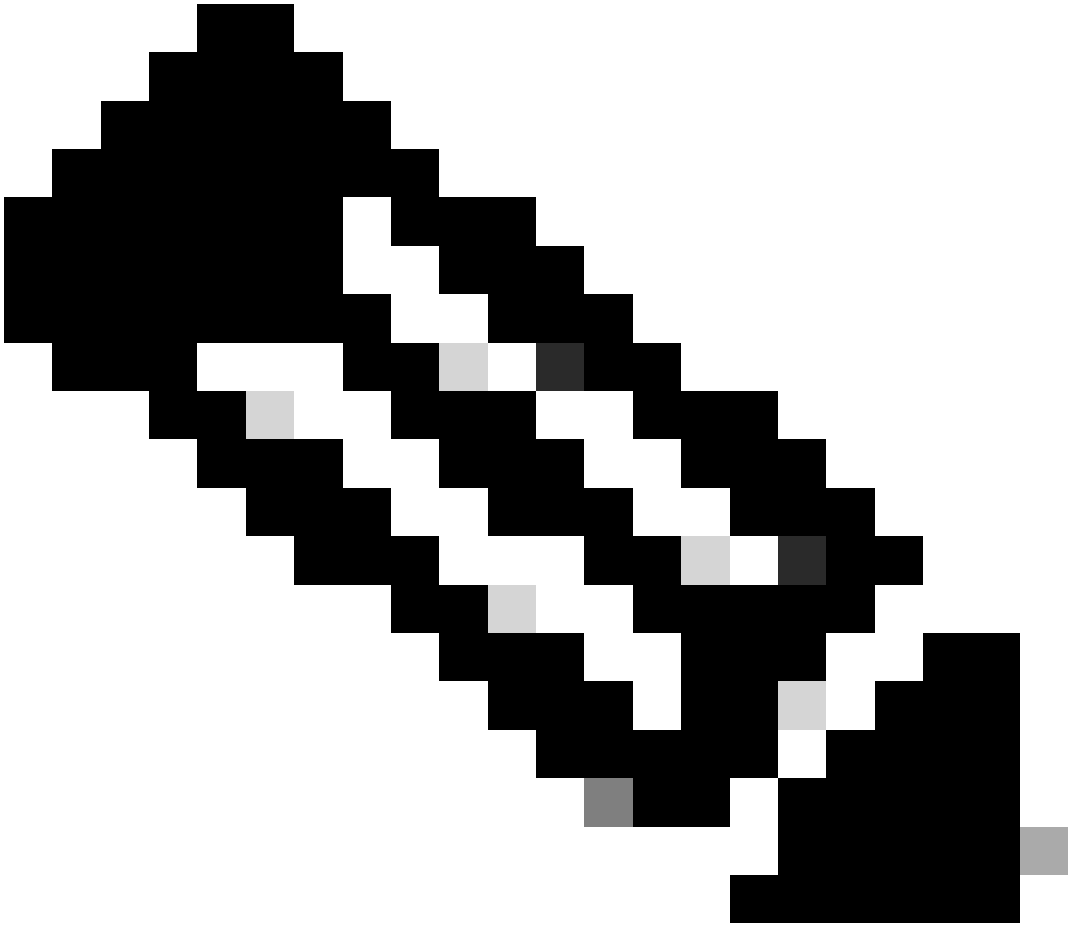
Opzione di accensione

2. Sono disponibili diverse opzioni per gestire la console VM. Selezionare Console > Apri console browser.

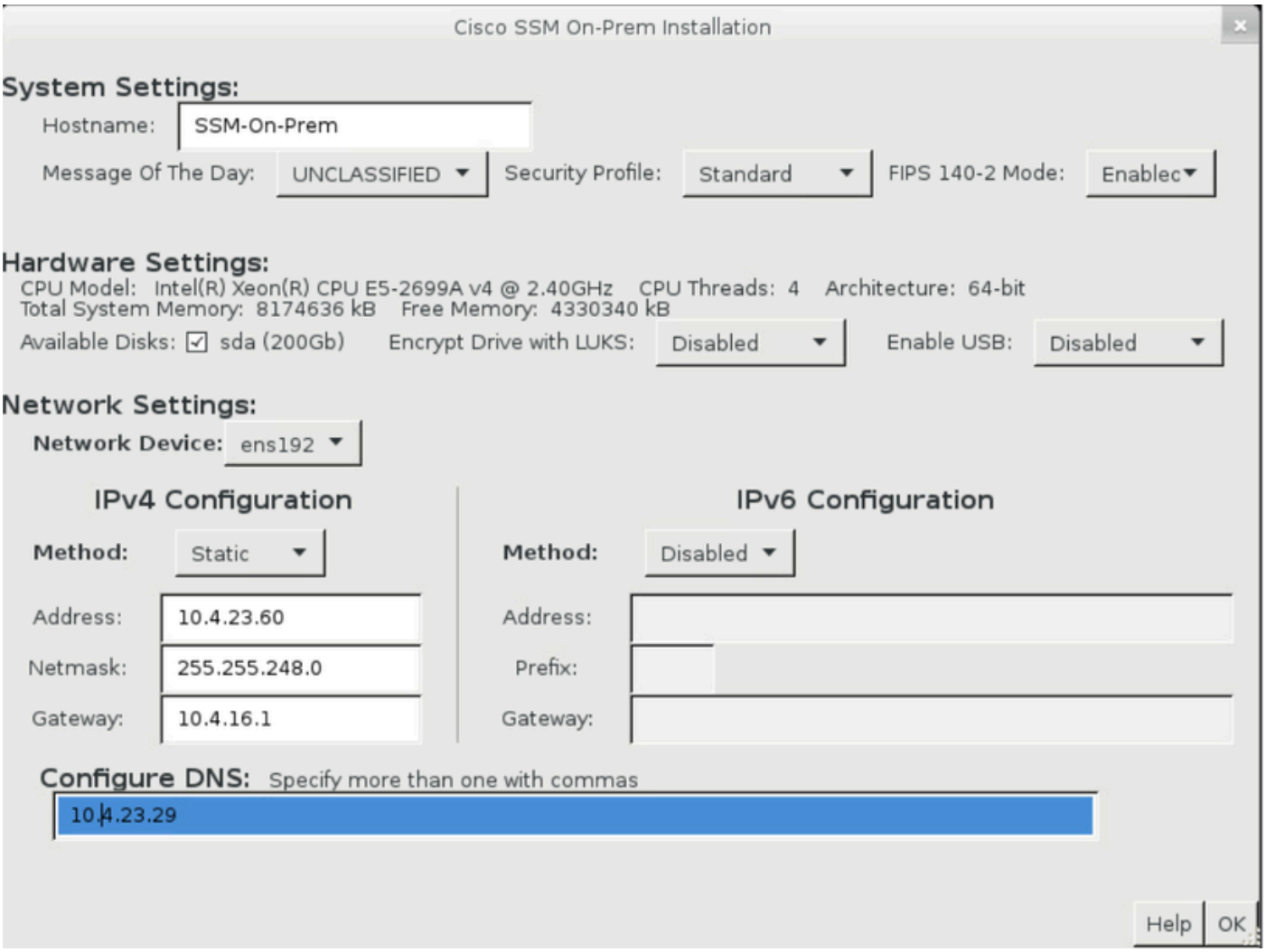


Opzioni per la gestione della VM

3. Configurare le impostazioni di rete.



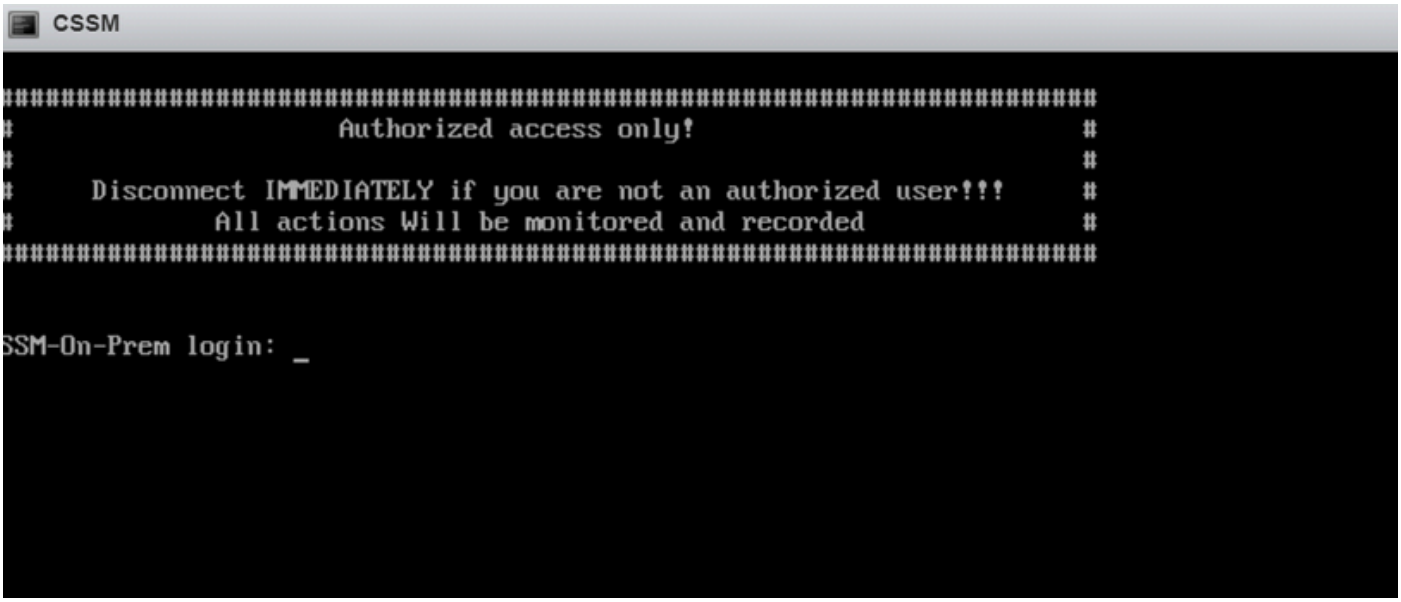
Nota: è importante configurare l'indirizzo IP del server DNS che risolve l'FQDN del modulo CSM.



Configurazione delle impostazioni di rete CSM

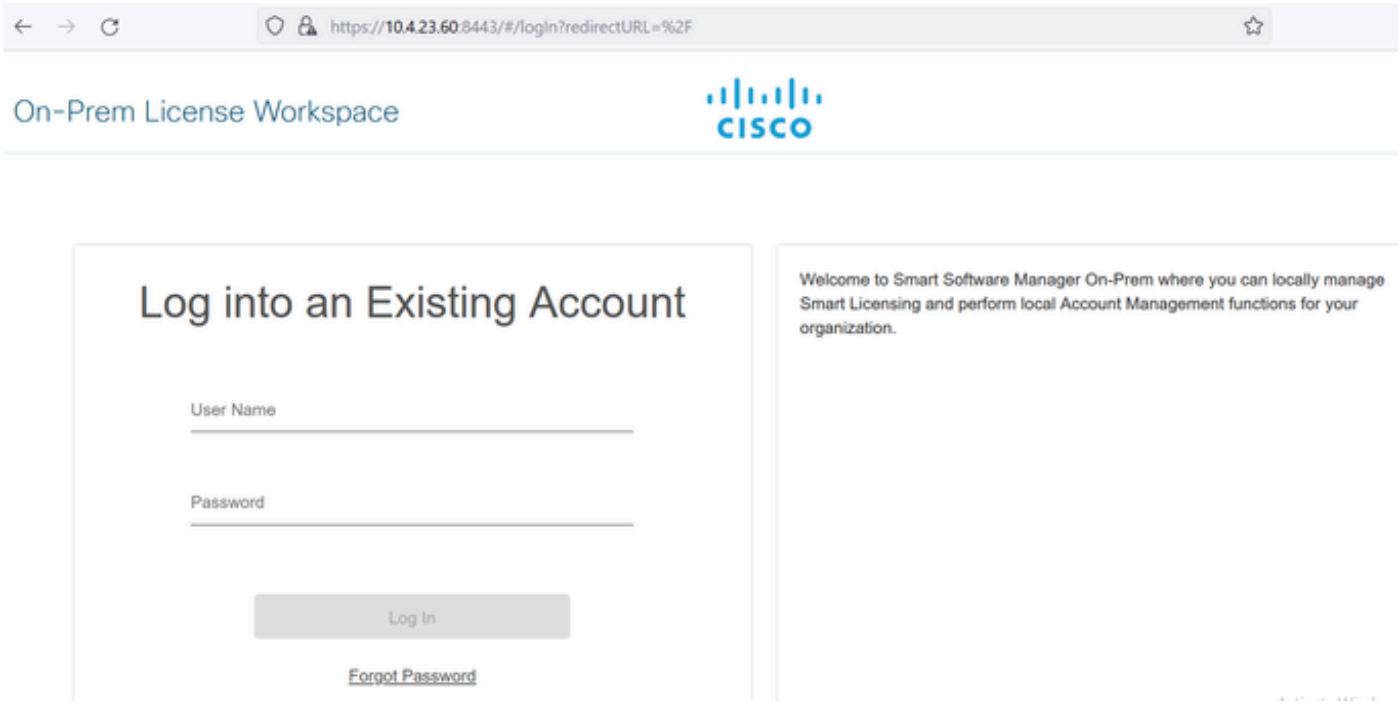
Fare clic su Ok per configurare la nuova password CLI.

4. Il processo di installazione viene quindi avviato e completato fino a quando non viene visualizzato il prompt di accesso.



Configurazione iniziale CSM completata

5. Aprire un browser e immettere https://<ip_address_CSSM>.



Pagina di accesso a CSM

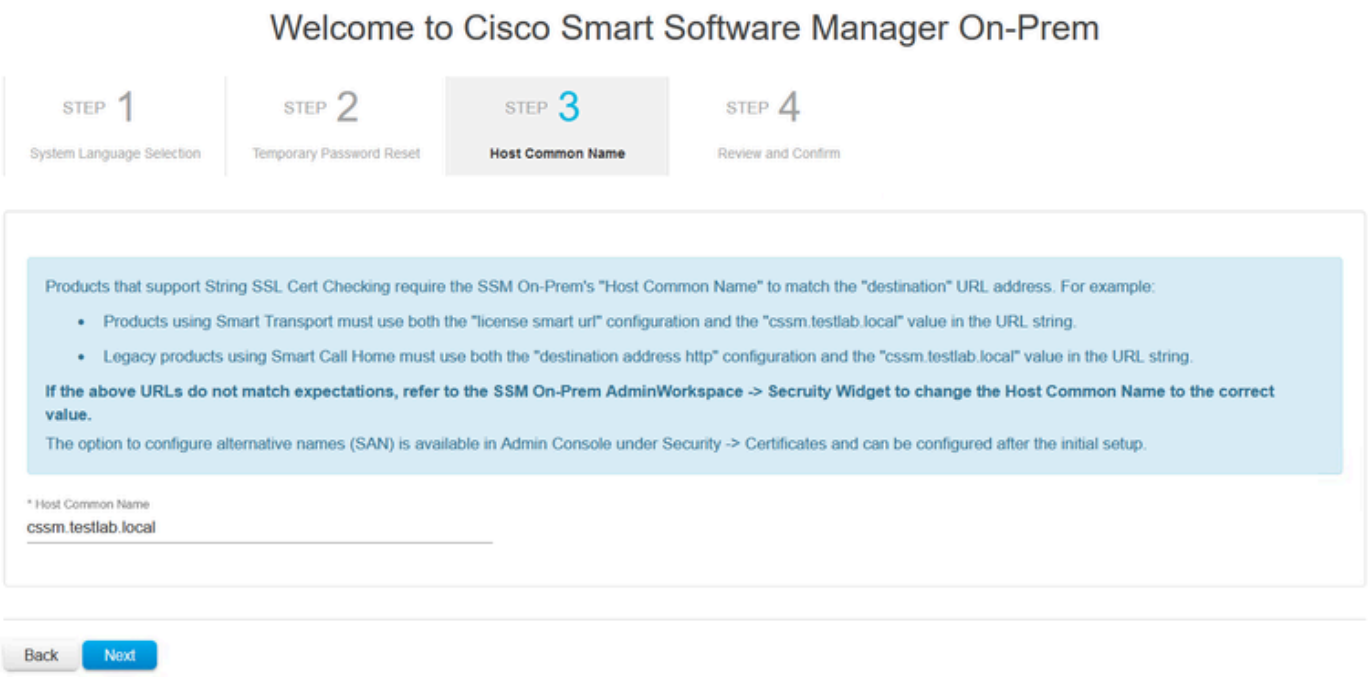
Usa le credenziali predefinite:

Nome utente: admin

Password: CiscoAdmin!2345

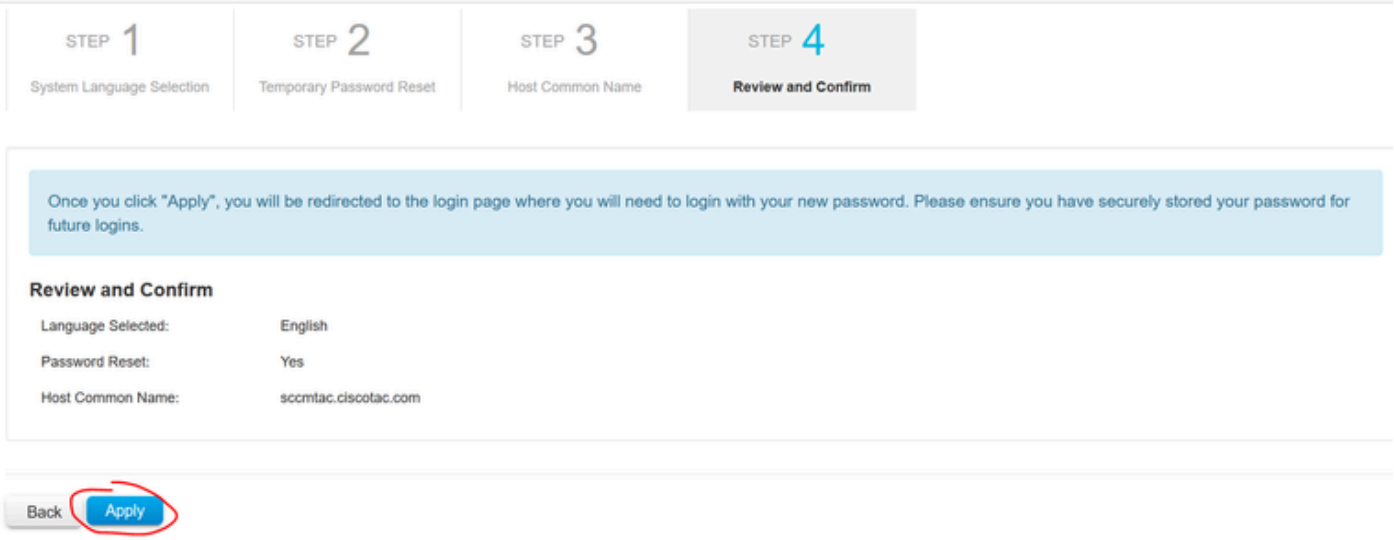
6. Seleziona la lingua.
7. Creare una nuova password GUI.
8. Configurare il nome comune dell'host. (esempio: nomehost.dominio).

In questo caso, cssm.testlab.local è stato configurato come Host Common Name.



Configurazione nome comune host

9. Convalidare la configurazione e fare clic su Applica.



Impostazioni iniziali CSM completate.

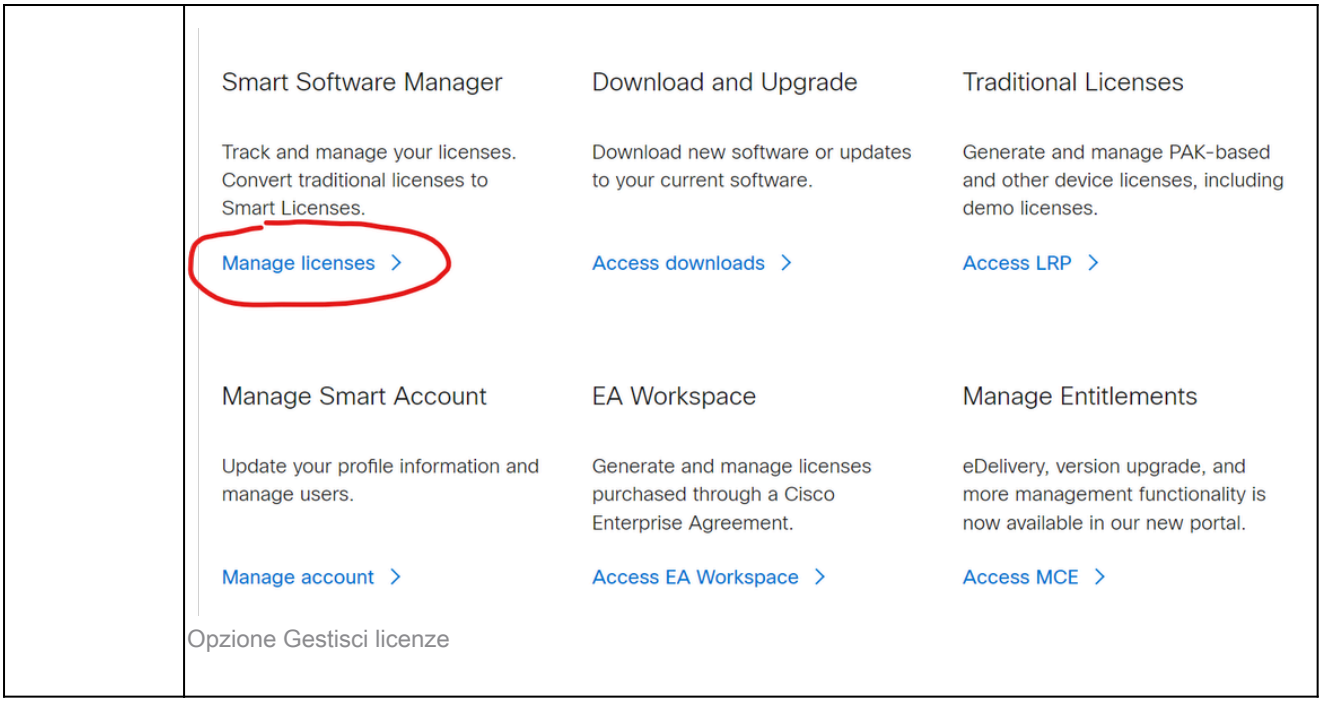
Integrazione di CSM on-prem con Smart Account

È necessario associare lo Smart Account al CSM sul server principale.

1. Aprire lo Smart Account Cisco utilizzando il collegamento successivo:

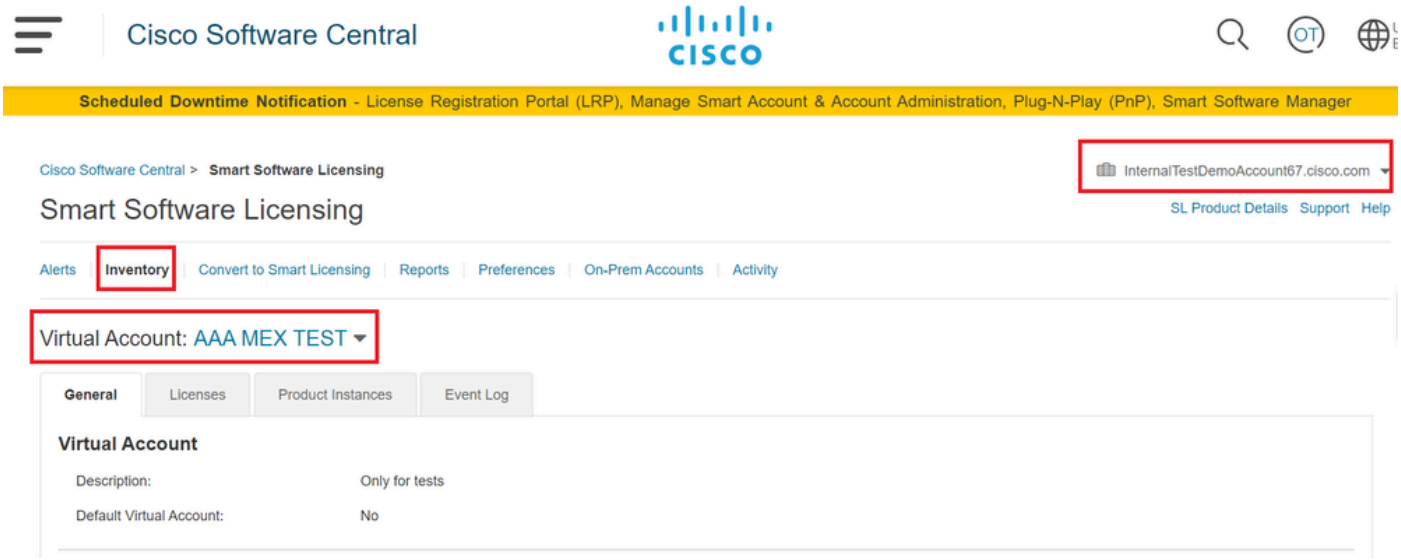
https://software.cisco.com/

2. Quindi, scegliere Gestisci licenze nella sezione Smart Software Manager.



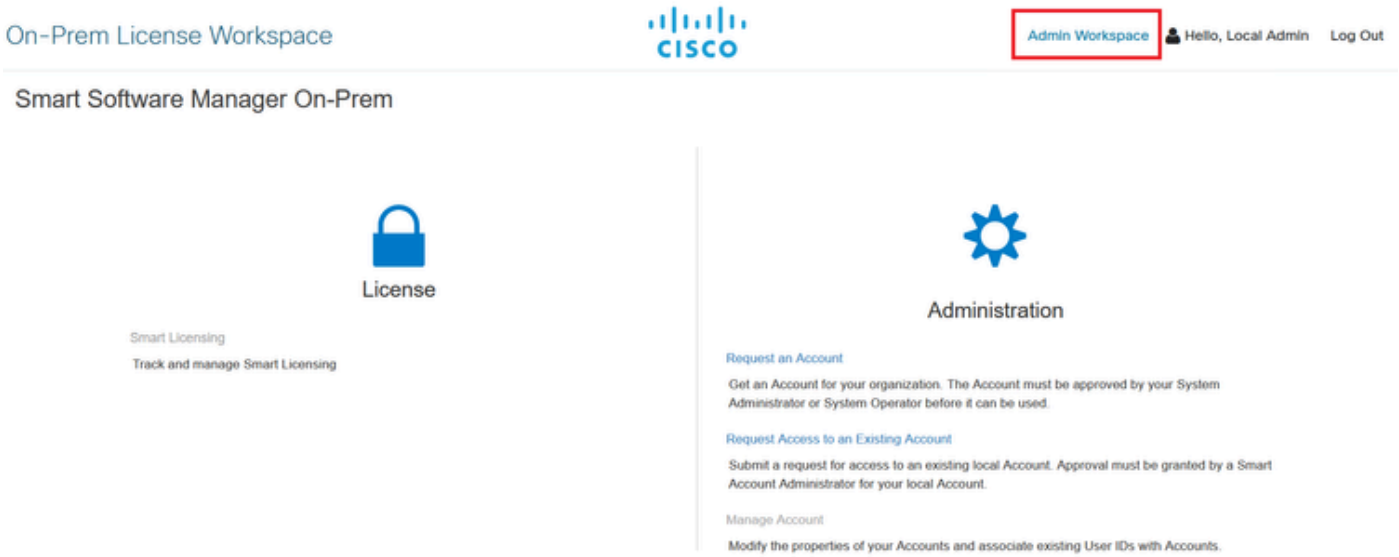
Opzione Gestisci licenze

3. Passare a Inventario e copiare il nome dello Smart Account e dell'account virtuale. In questa guida, si tratta di InternalTestDemoAccount67 e AAA MEX TEST.



Pagina Software Cisco

4. Aprire l'interfaccia utente di CSM e selezionare l'opzione Admin Workspace.

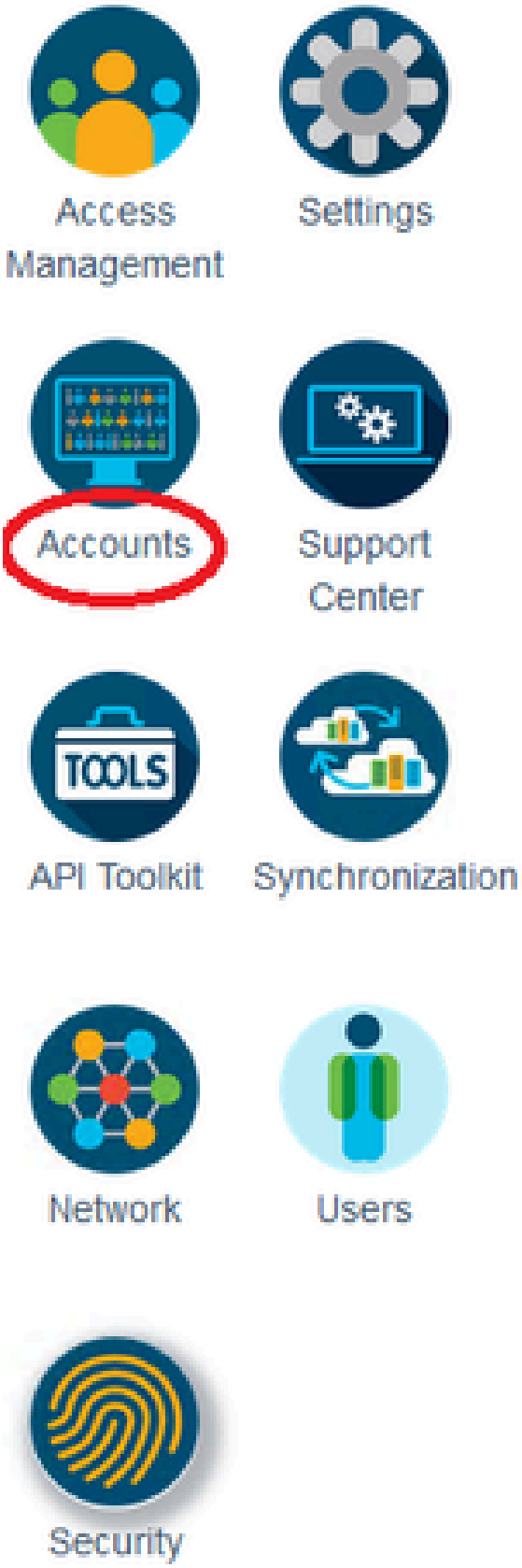


Menu principale CSSM.

5. Quindi selezionare Conti.

On-Prem Admin Workspace

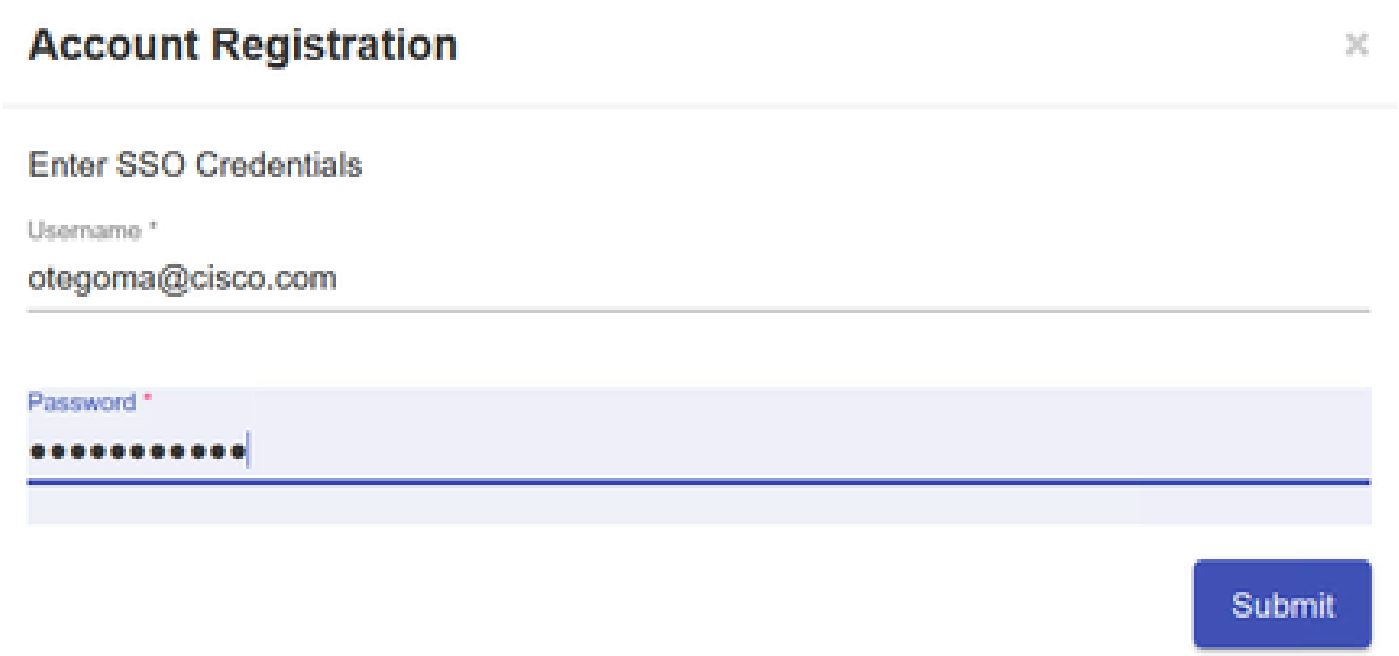
Smart Software Manager On-Prem



utilizzare questa opzione per registrare il modulo CSM locale con lo Smart Account tramite Internet.
- Rifiuta: elimina la richiesta.
- Registrazione manuale: utilizzare questa opzione per registrare il modulo CSM on-Prem con lo Smart Account senza Internet.

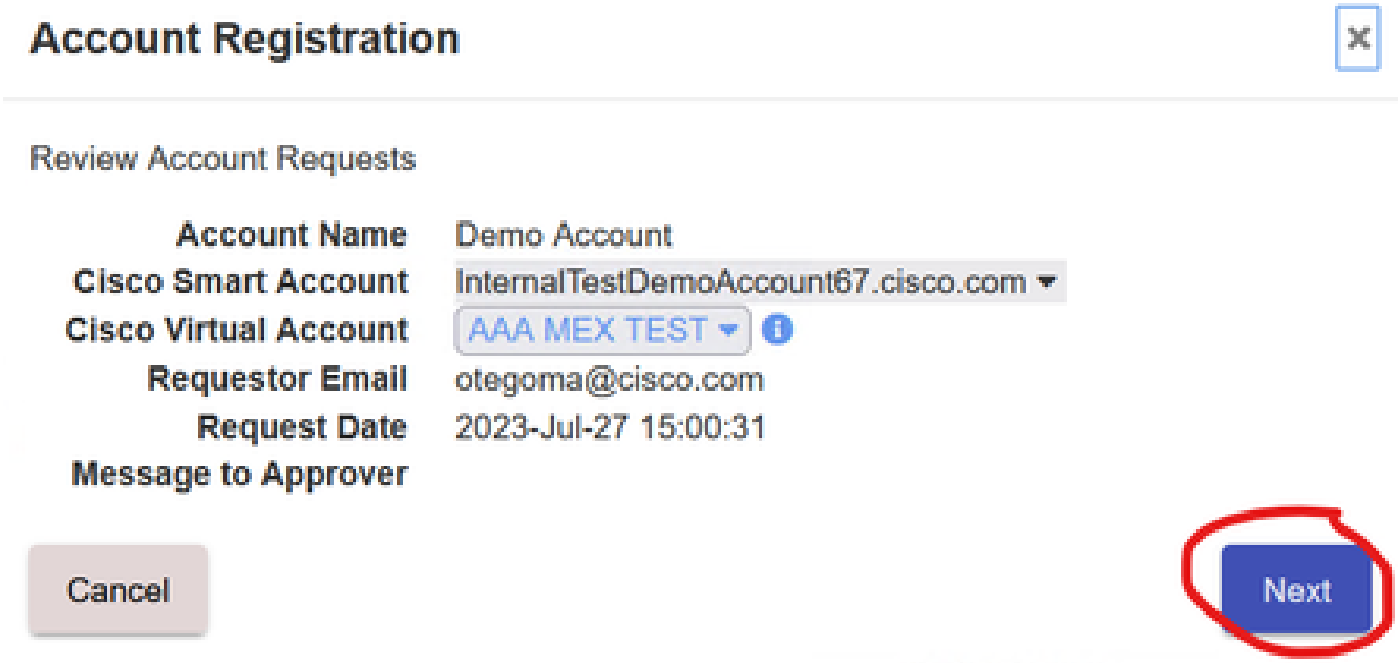
OPZIONE 1: registrare il CSM on-prem tramite una connessione Internet.

1. Se si sceglie Approva, è necessario immettere il nome utente e la password dello Smart Account Cisco e fare clic su Invia.



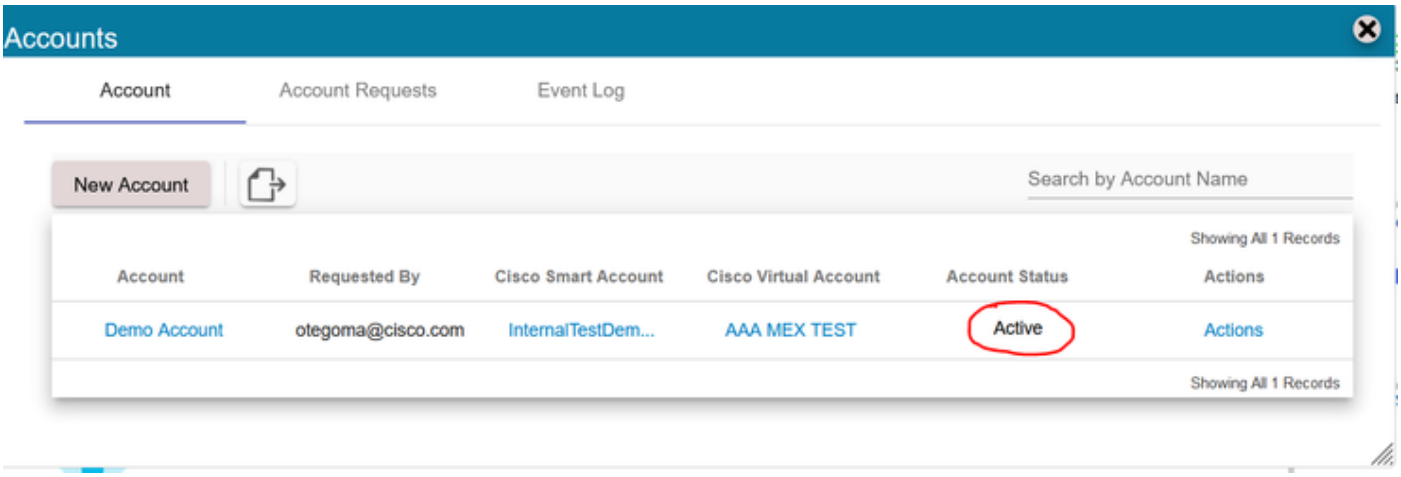
Approva.

Quindi fai clic su avanti per accettare la registrazione dell'account.



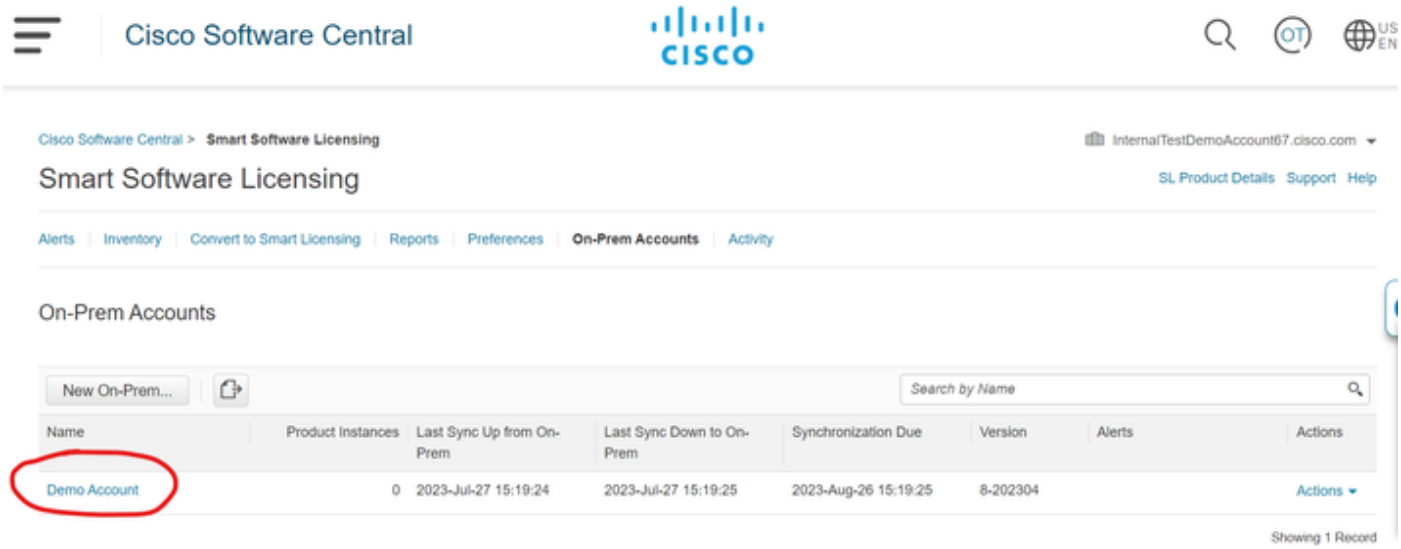
Registrazione account.

Per confermare lo stato della registrazione, passare a Account e lo stato dell'account deve essere attivo.



Stato account.

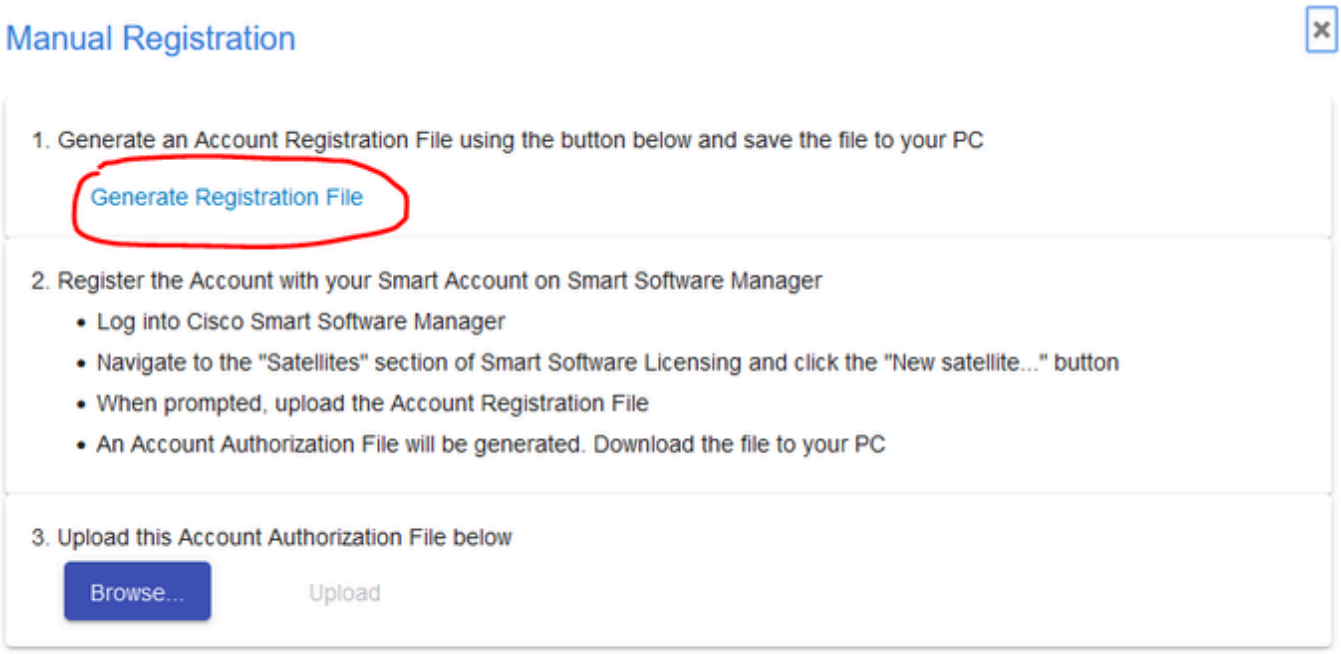
Aprire lo Smart Account (https://software.cisco.com/). Selezionare quindi l'opzione Conti locali per visualizzare il nuovo registro.



In Conto Prem.

OPZIONE 2: registrare il CSM on-prem senza una connessione Internet.

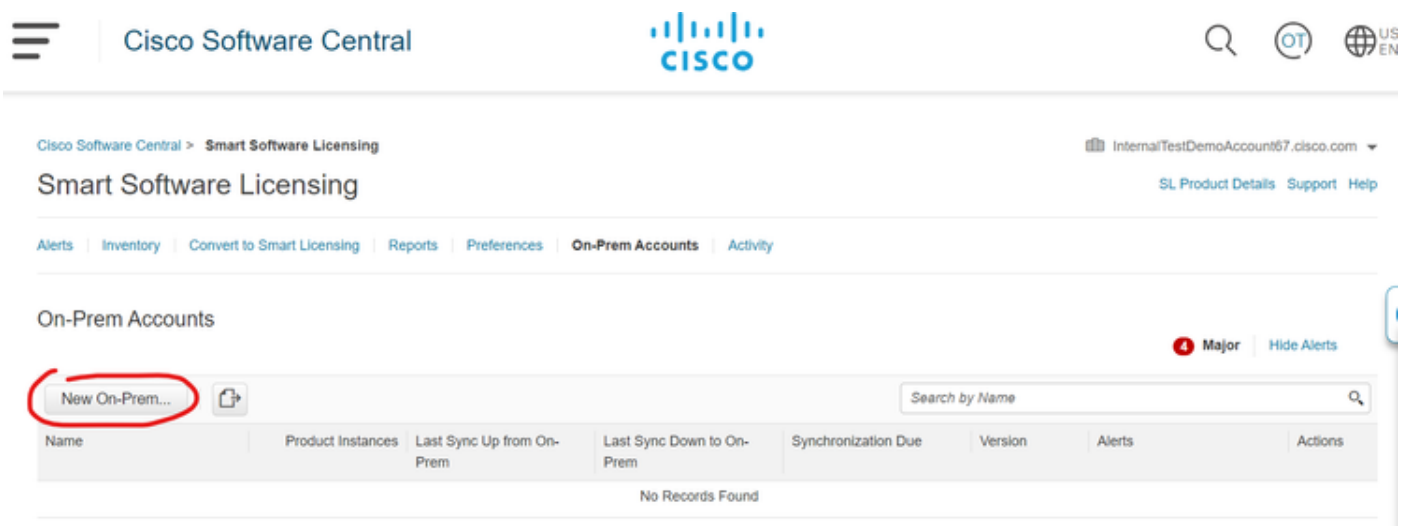
Se si sceglie Registrazione manuale, fare clic su Genera file di registrazione. In questo modo viene creata una richiesta di registrazione che verrà scaricata nel computer.



Registrazione manuale.

Aprire quindi lo Smart Account (https://software.cisco.com/) e passare a Account locali.

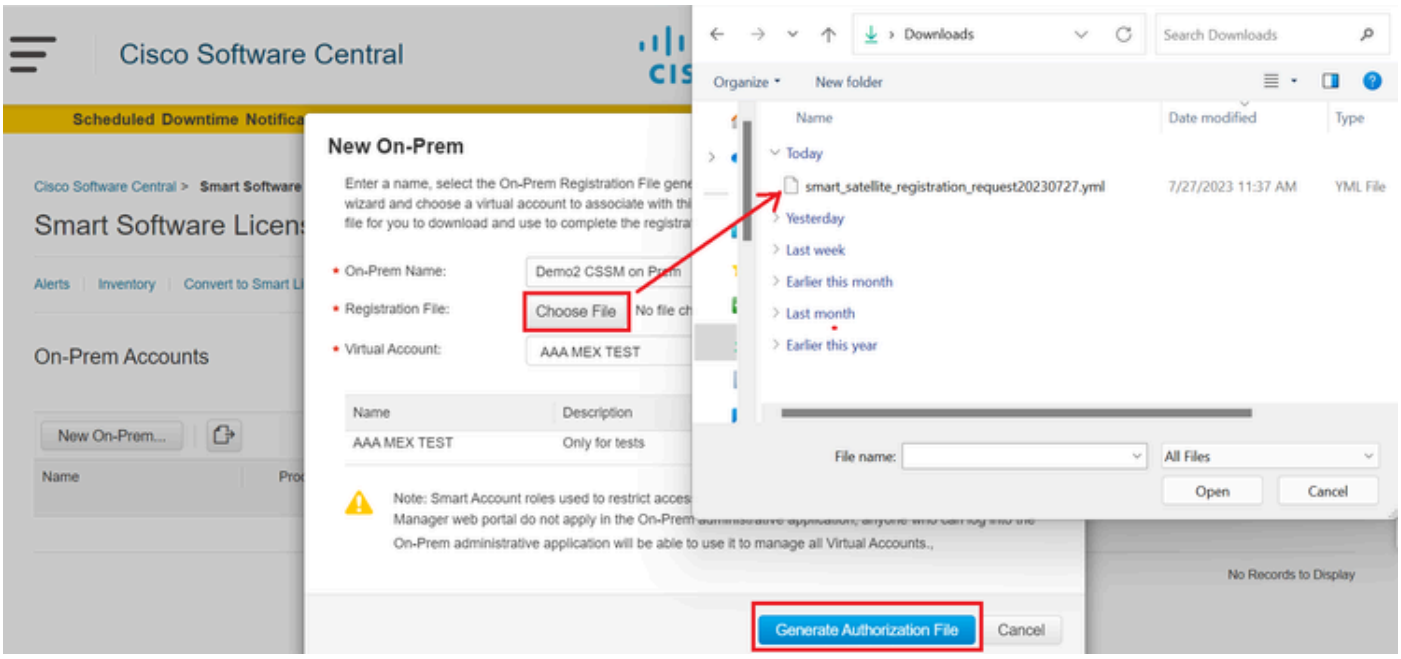
Fare clic su Nuovo in locale



Aggiunta di nuovi elementi locali.

Configurare quindi i parametri successivi:

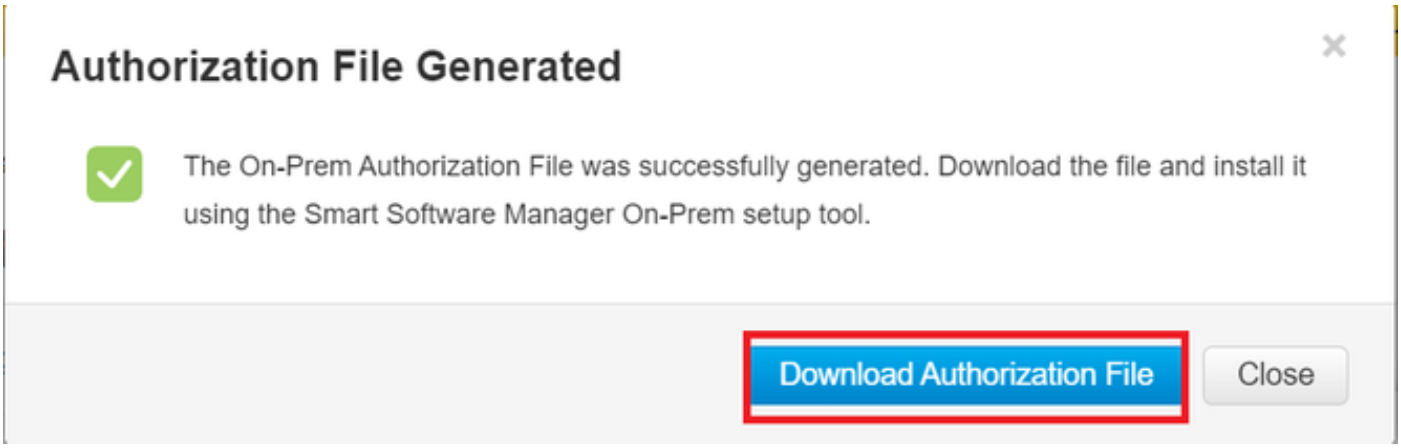
- Nome locale: nome personalizzato del nuovo registro.
- File di registrazione: fare clic su Scegli file e selezionare la richiesta di registrazione.
- Account virtuale: incollare il nome dell'account virtuale.



File di autorizzazione.

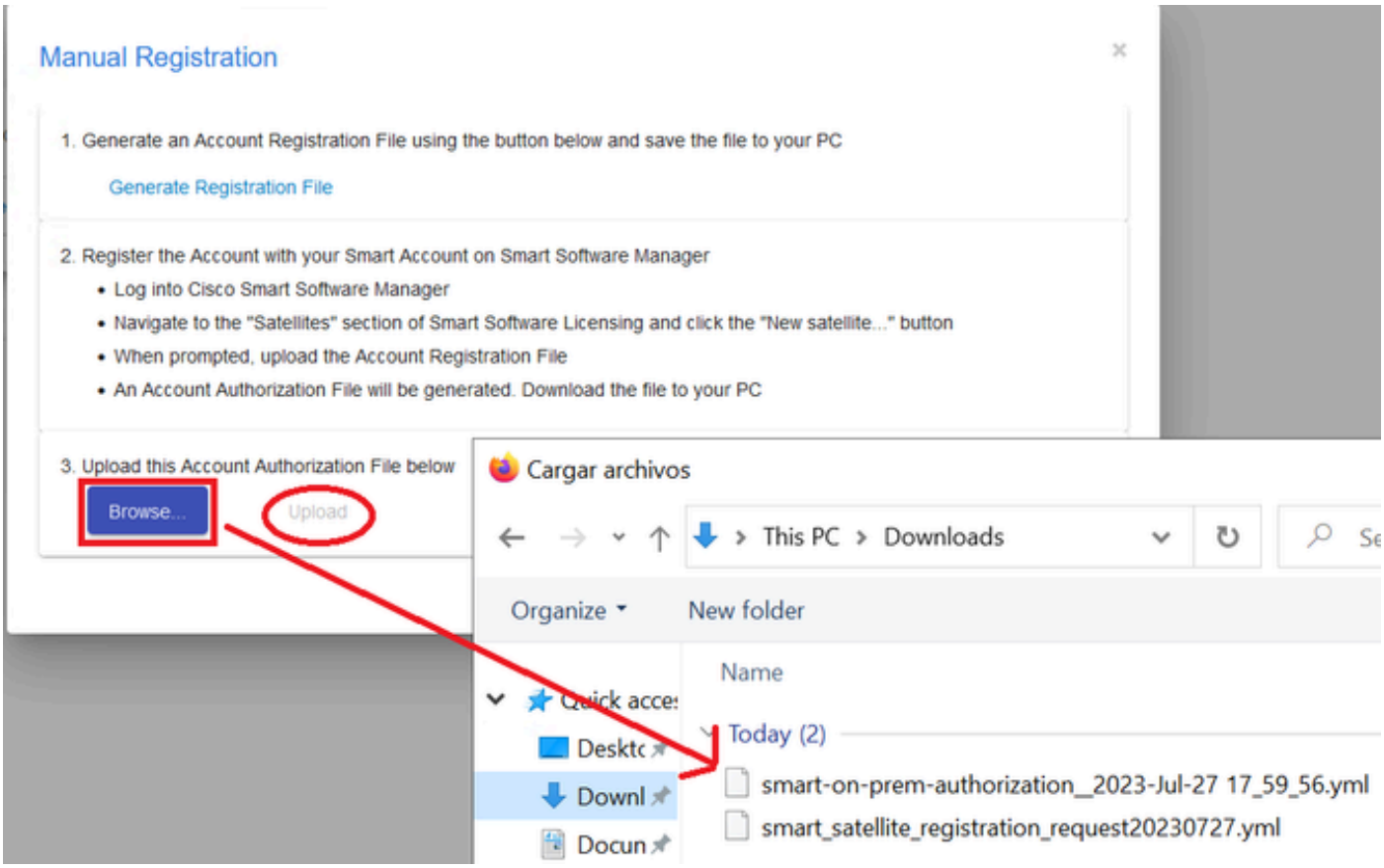
E fare clic su Genera file di autorizzazione.

Scaricare quindi il file di autorizzazione.



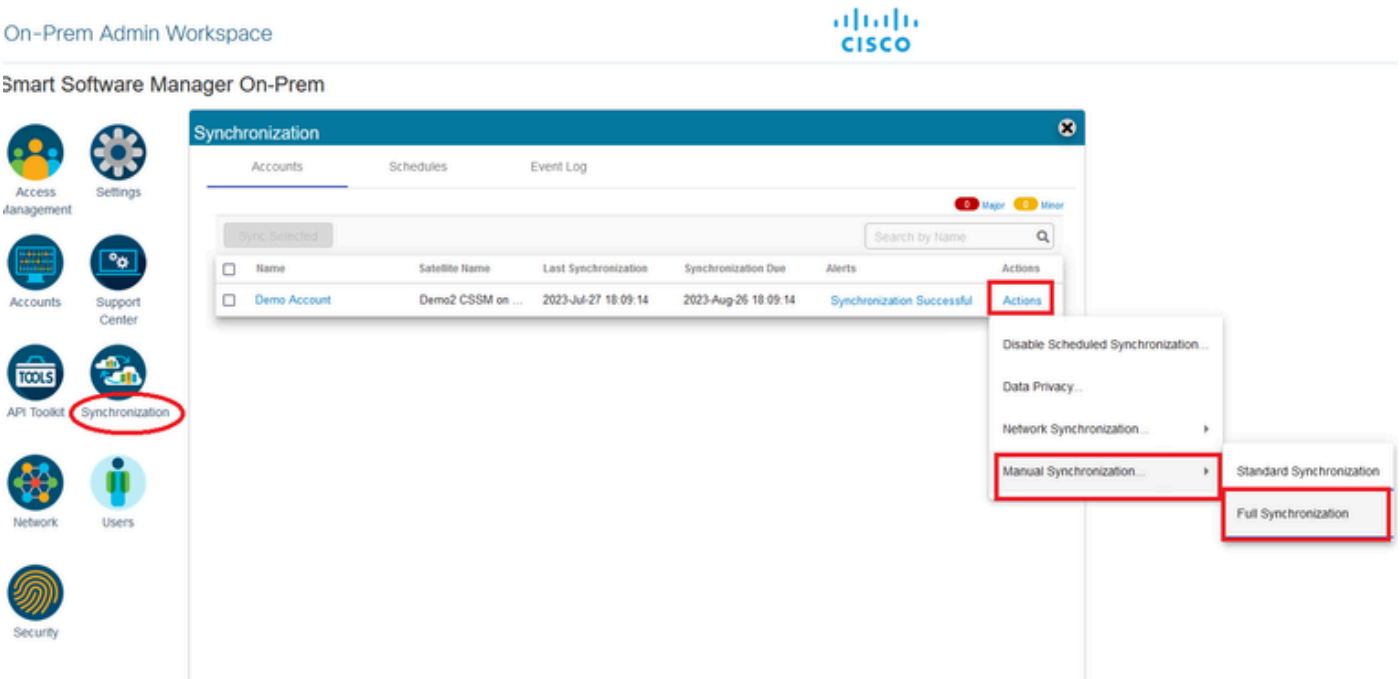
Download del file di autorizzazione.

Aprire l'interfaccia utente di CSM per caricare il file di autorizzazione. Fare clic su Sfoglia, scegliere il file e quindi fare clic su Carica.



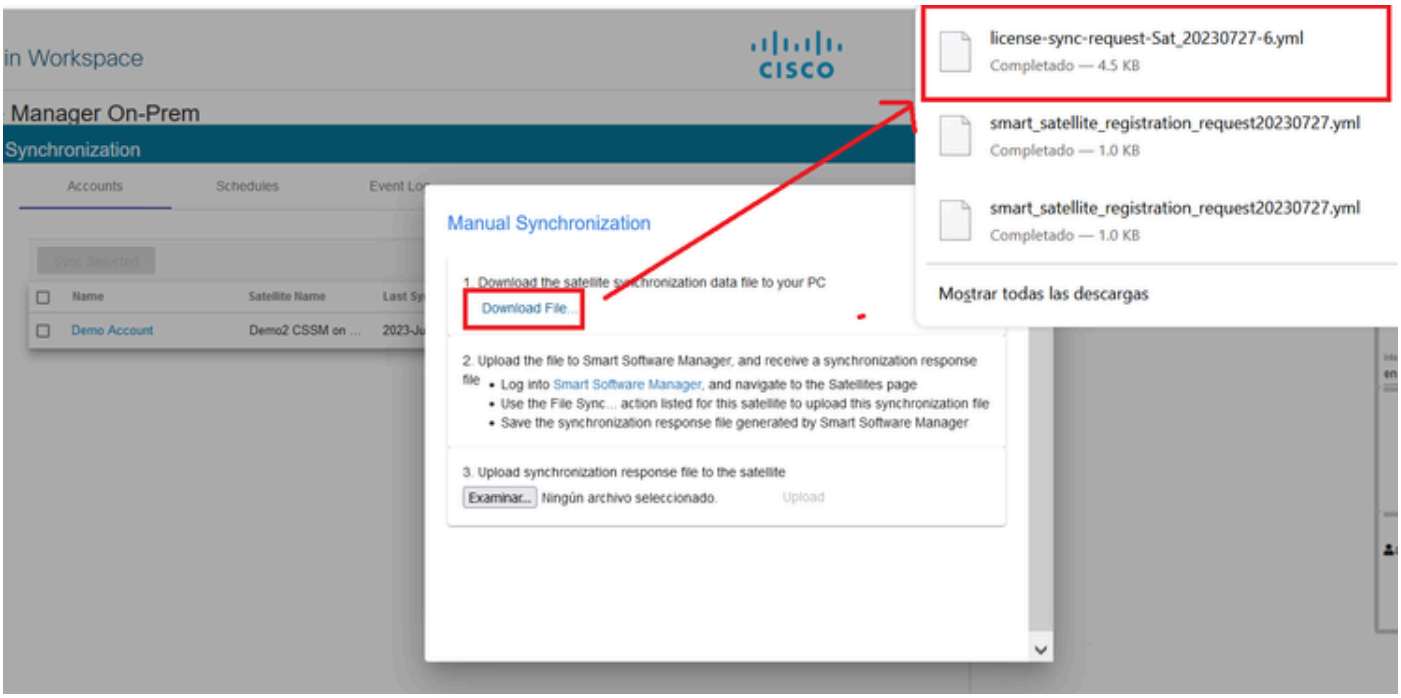
Caricamento del file di autorizzazione.

Passare quindi a Sincronizzazione e fare clic su Azioni > Sincronizzazione manuale > Sincronizzazione completa.



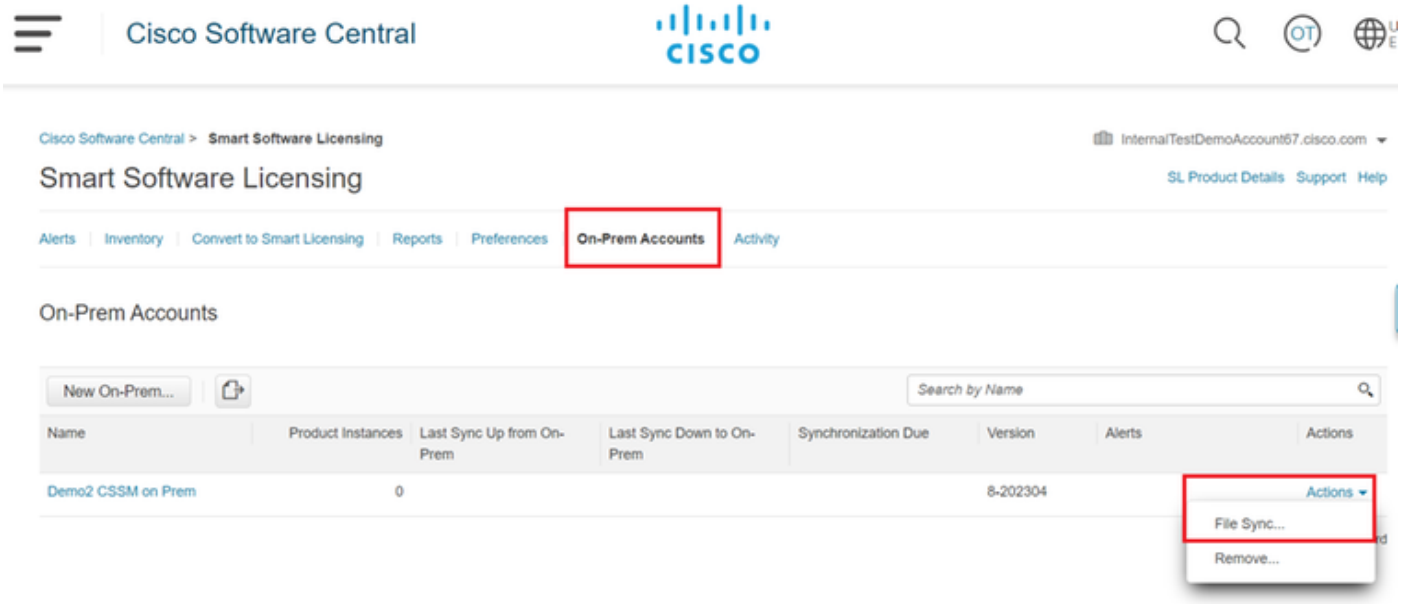
Sincronizzazione manuale

Scaricare il file di richiesta Sync.



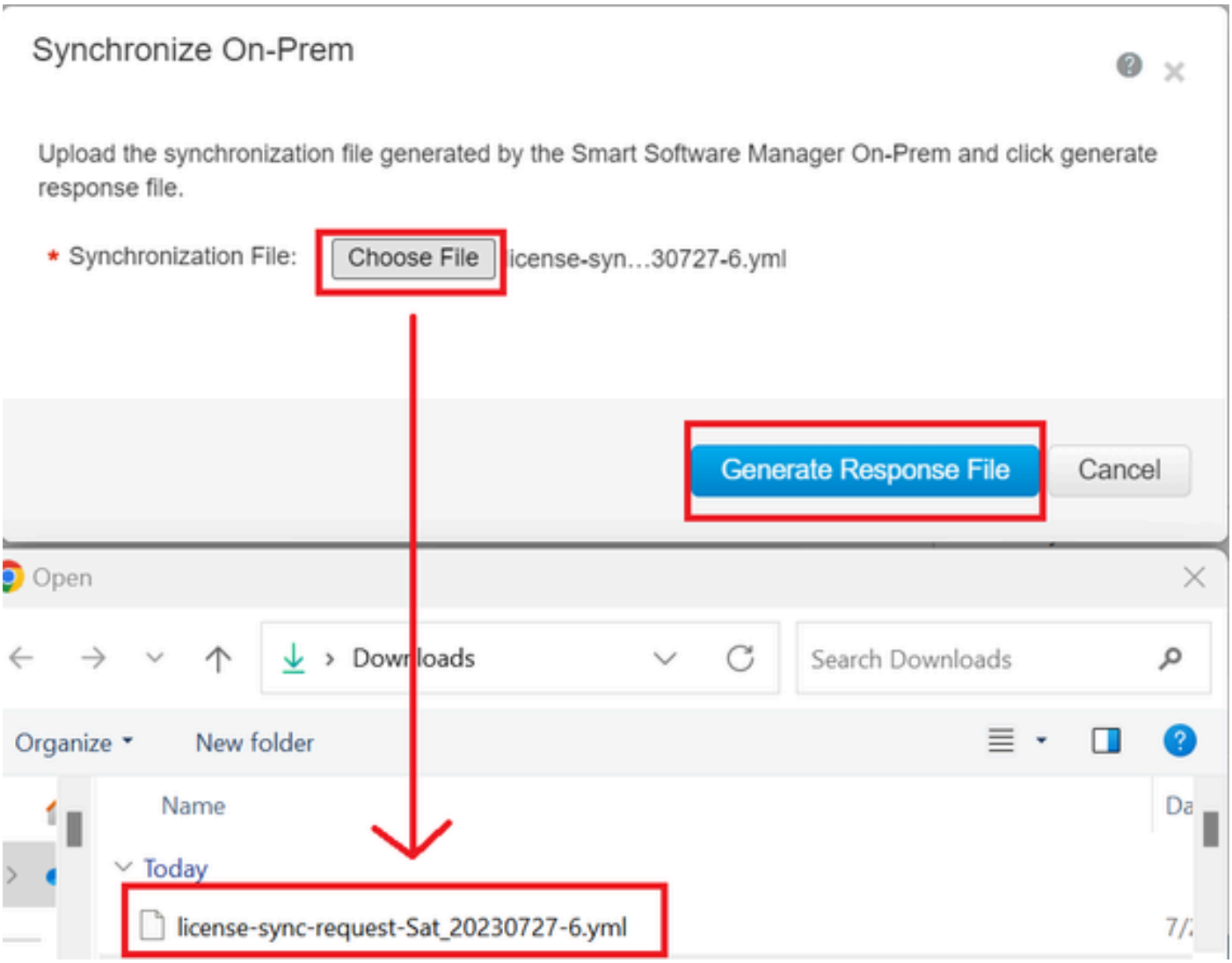
Scaricamento file in corso.

Aprire lo Smart Account e selezionare Account locale, quindi cercare il nome locale CSM nell'elenco e fare clic su Azioni > Sincronizzazione file



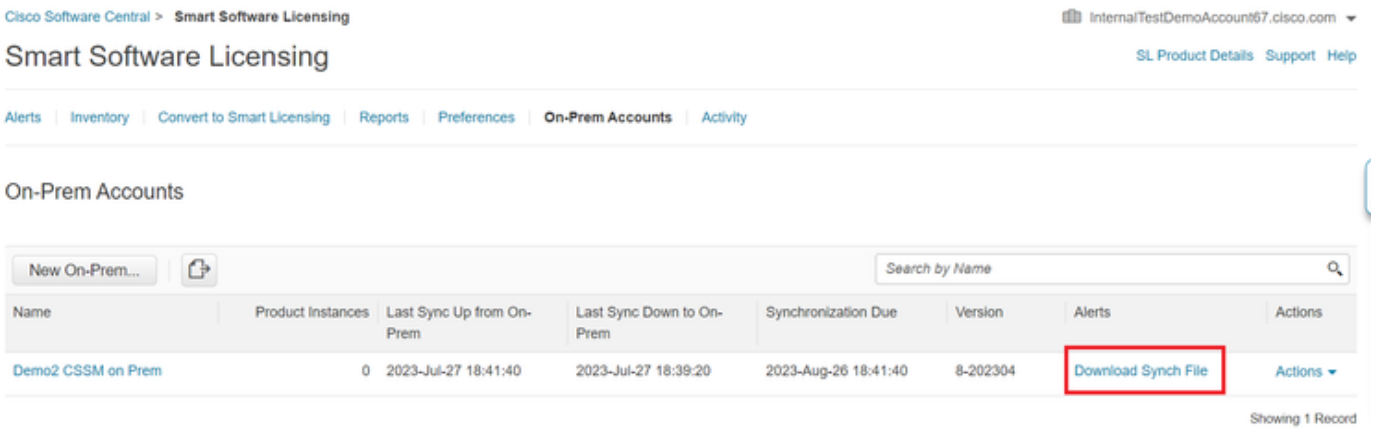
Caricamento file in corso. Sincronizza.

Caricare quindi il file di richiesta Sync e fare clic su Genera file di risposta.



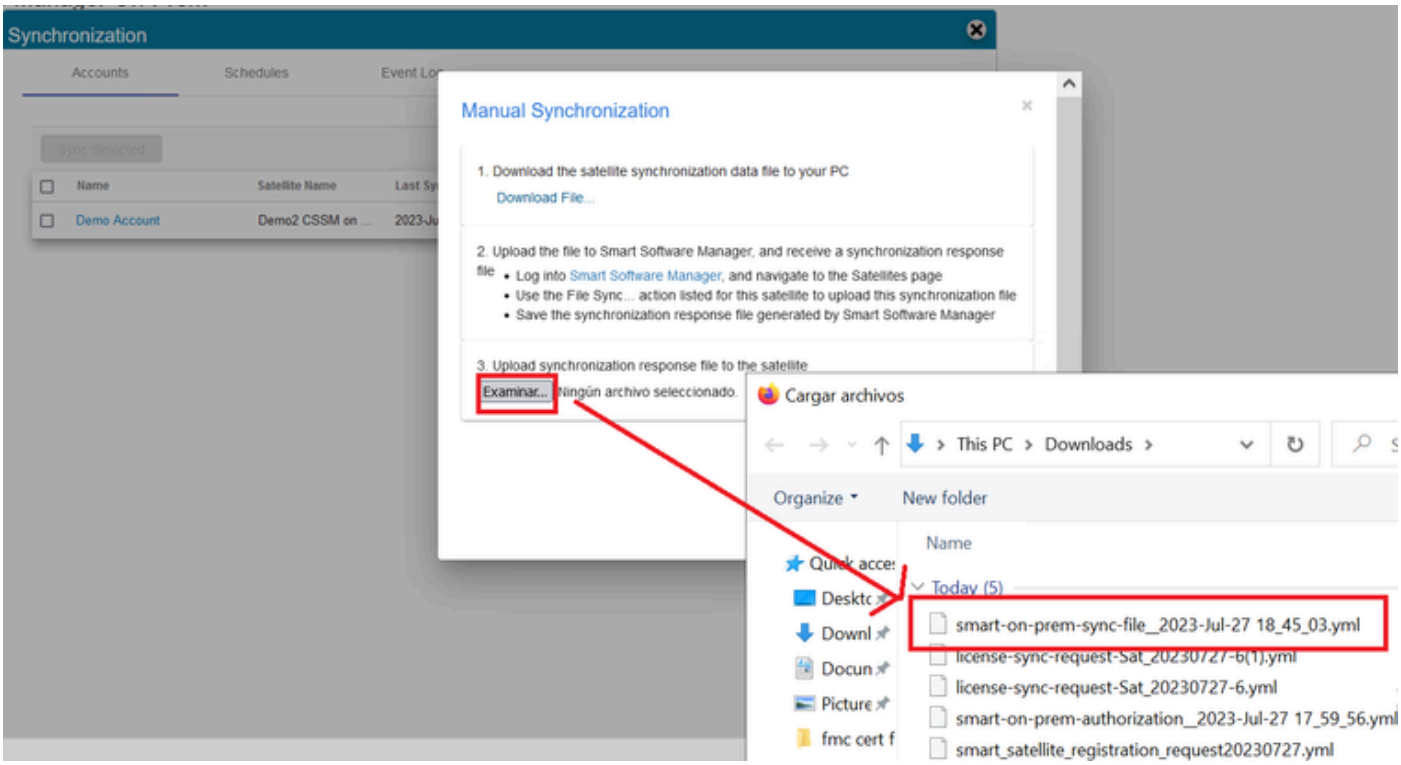
Generare un file di risposta.

Quindi fare clic su Scarica file di risposta di sincronizzazione



Sincronizza file.

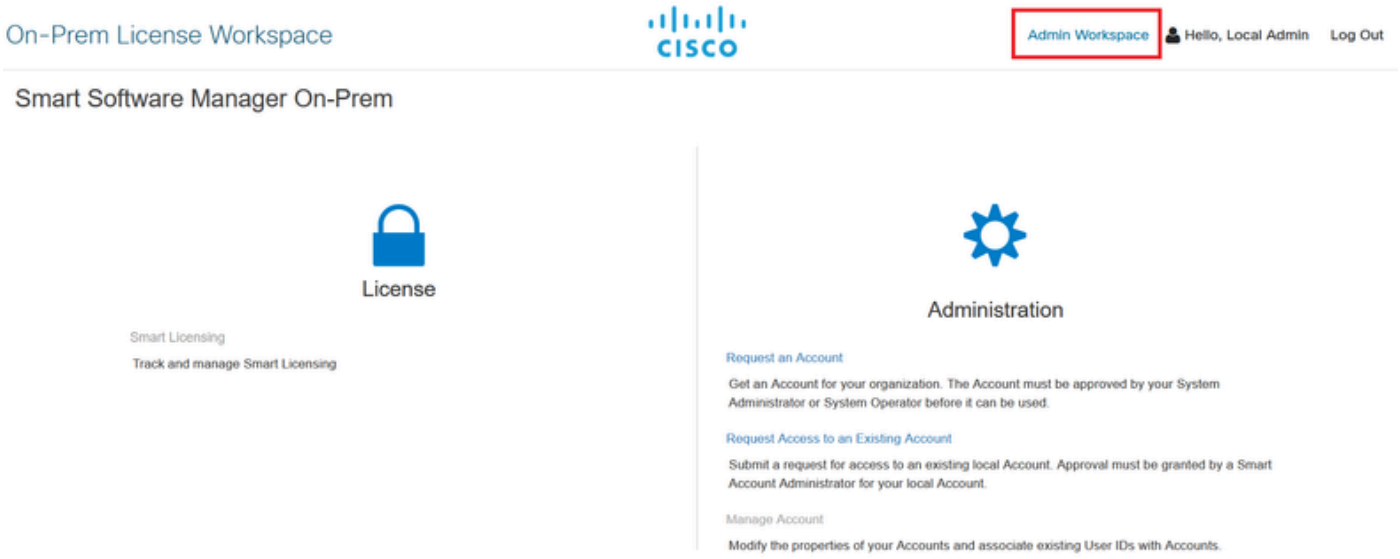
Infine, caricare il file di risposta Synch nel CSM in sede.



Sincronizzazione completata.

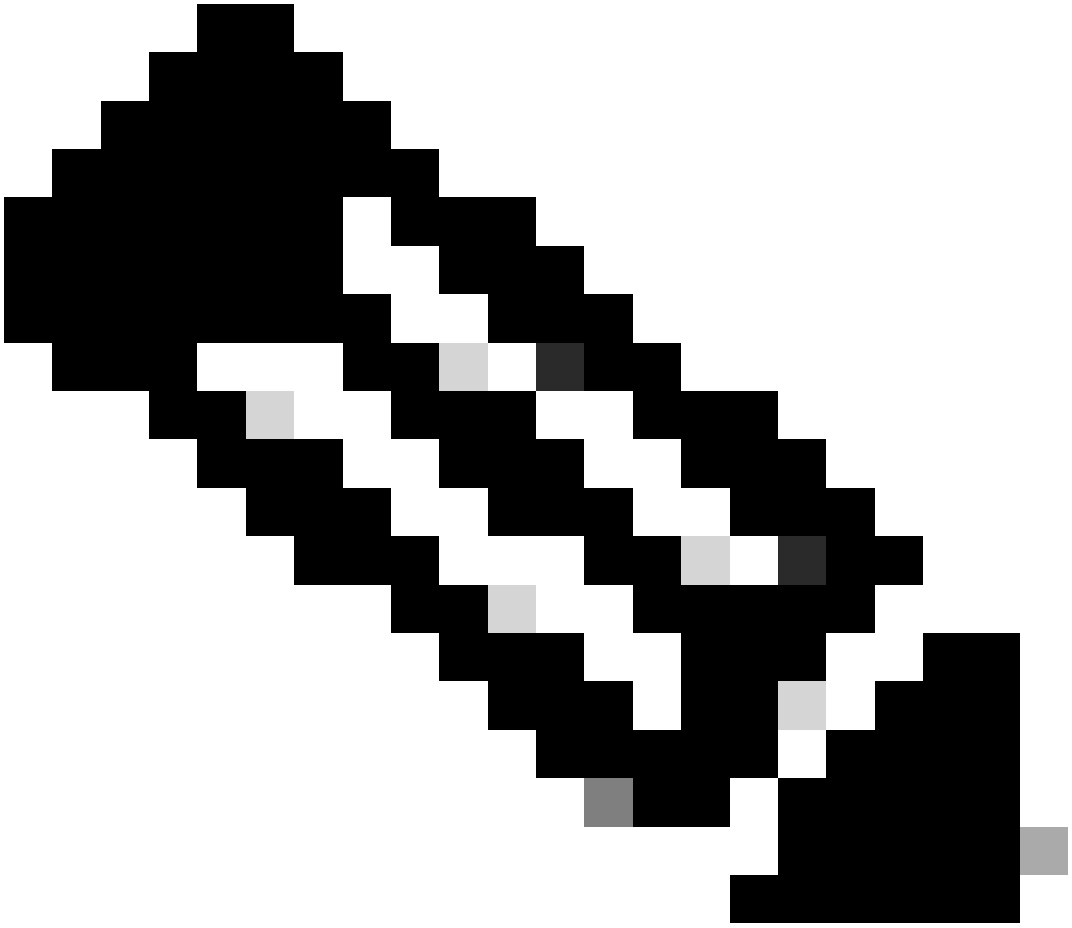
Integrazione di CSM On-Prem con ISE.

1. Aprire l'interfaccia utente di CSM e selezionare Admin Workspace.

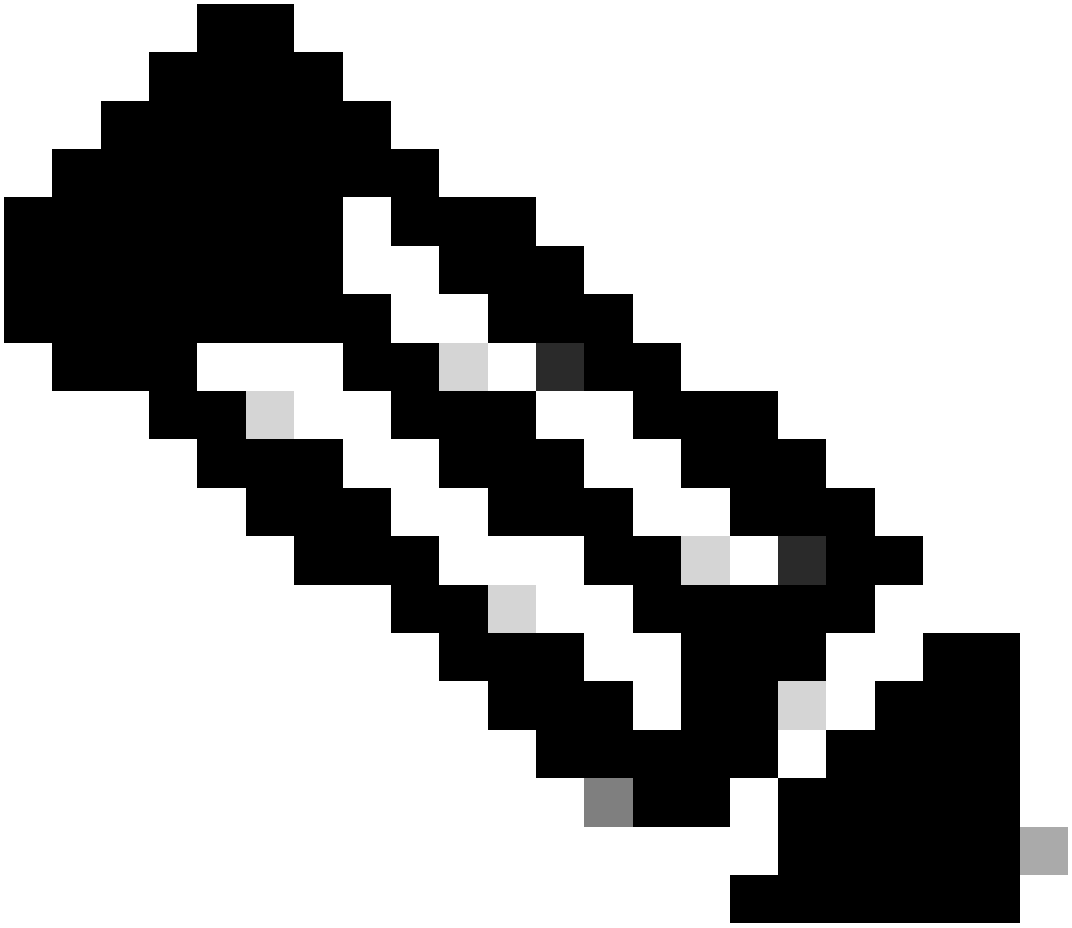


Menu principale CSSM.

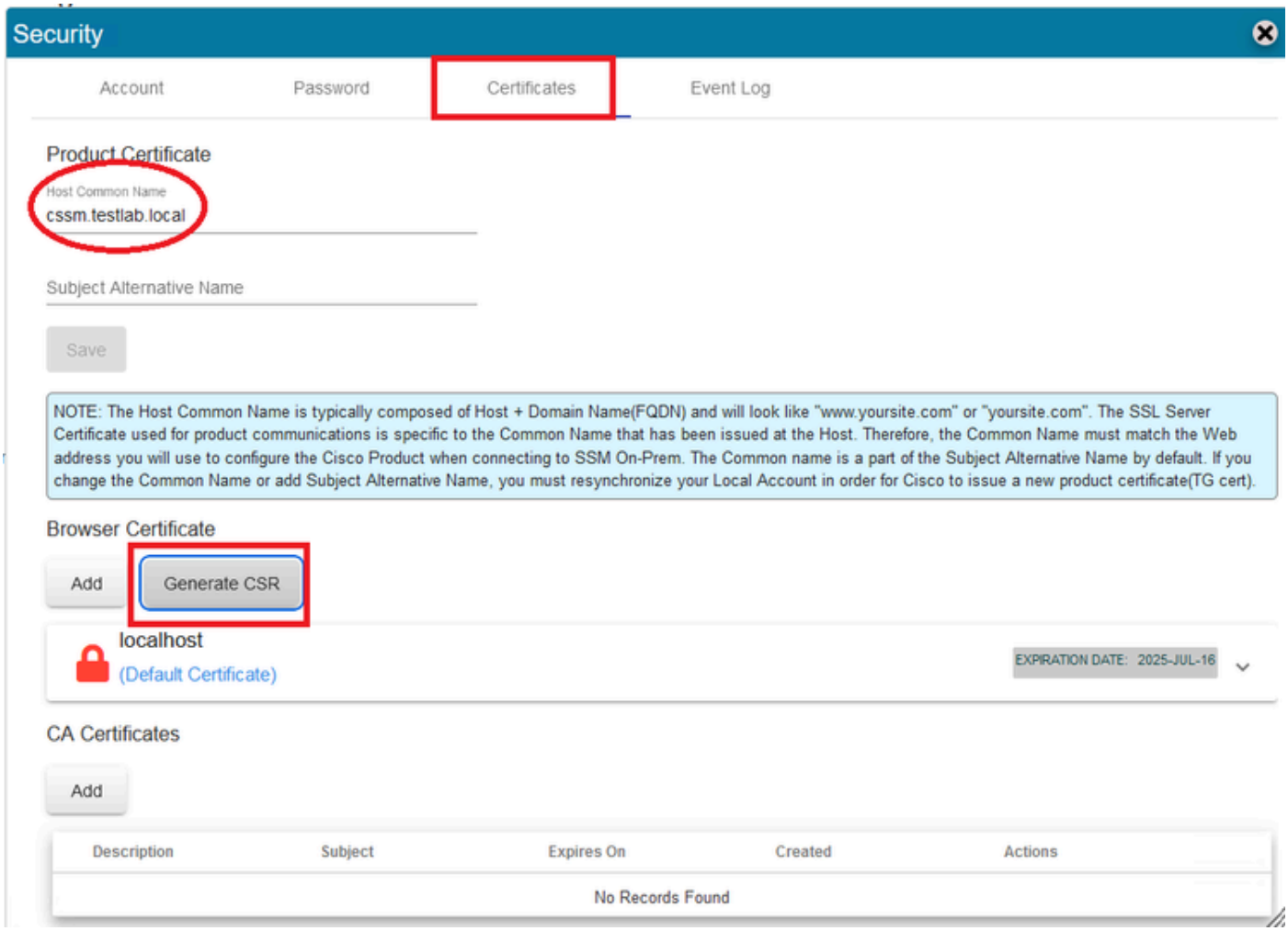
2. Selezionare Sicurezza > Certificati > Genera CSR



Nota: è importante configurare il nome host + dominio sul nome comune host perché ISE utilizza questo parametro per stabilire una connessione con il CSM. È possibile utilizzare un indirizzo IP anziché il nome host + dominio, tuttavia si consiglia di utilizzare il nome host + dominio

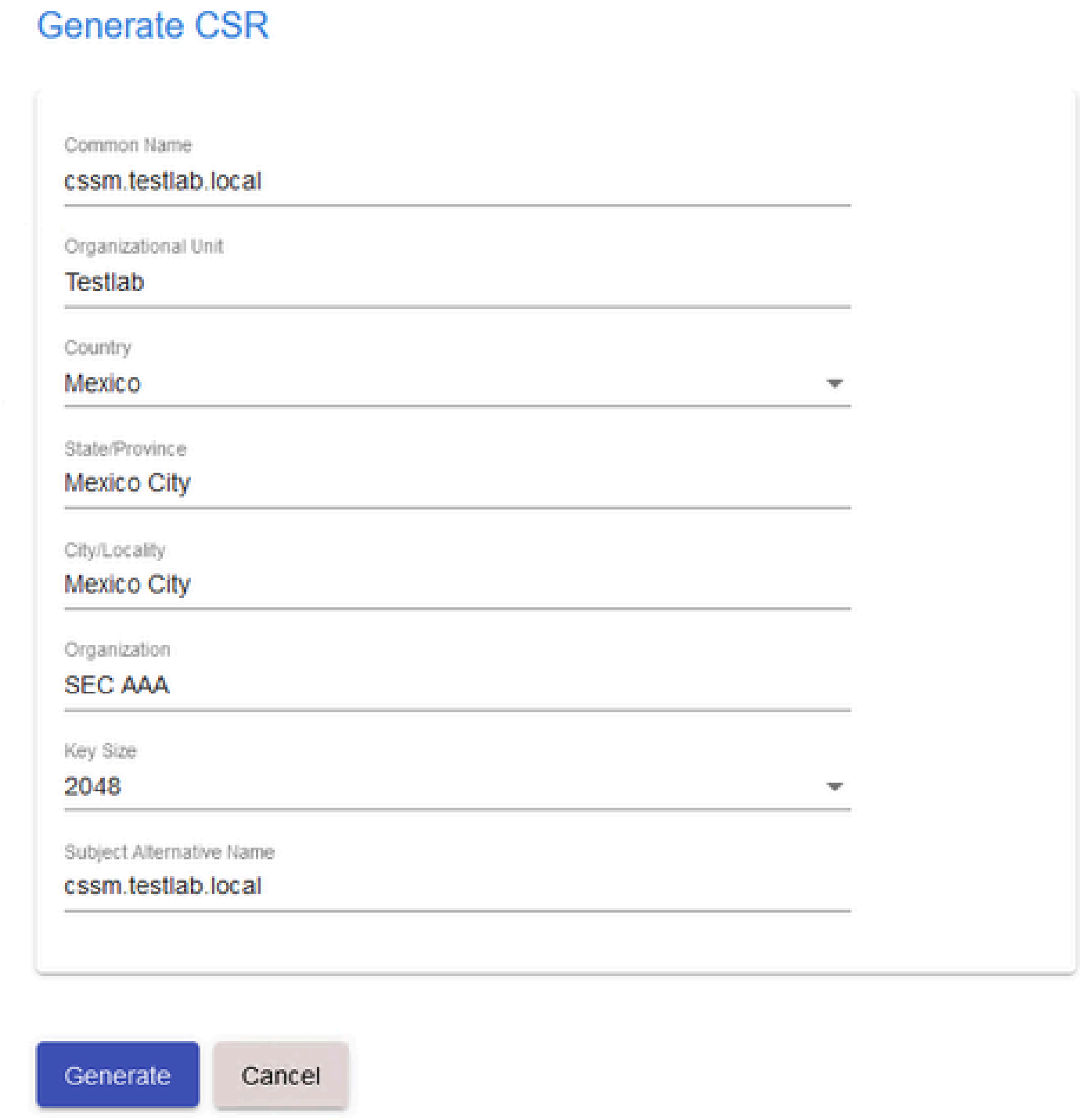


Nota: i passaggi successivi descrivono la procedura per installare il certificato GUI nel CSM. Se si desidera proteggere la connessione di gestione al CSM GUI utilizzando un certificato firmato dall'Autorità di certificazione (CA) personale, è necessario verificare i passaggi successivi. In caso contrario, controllare direttamente il punto 9.



Opzione CSR.

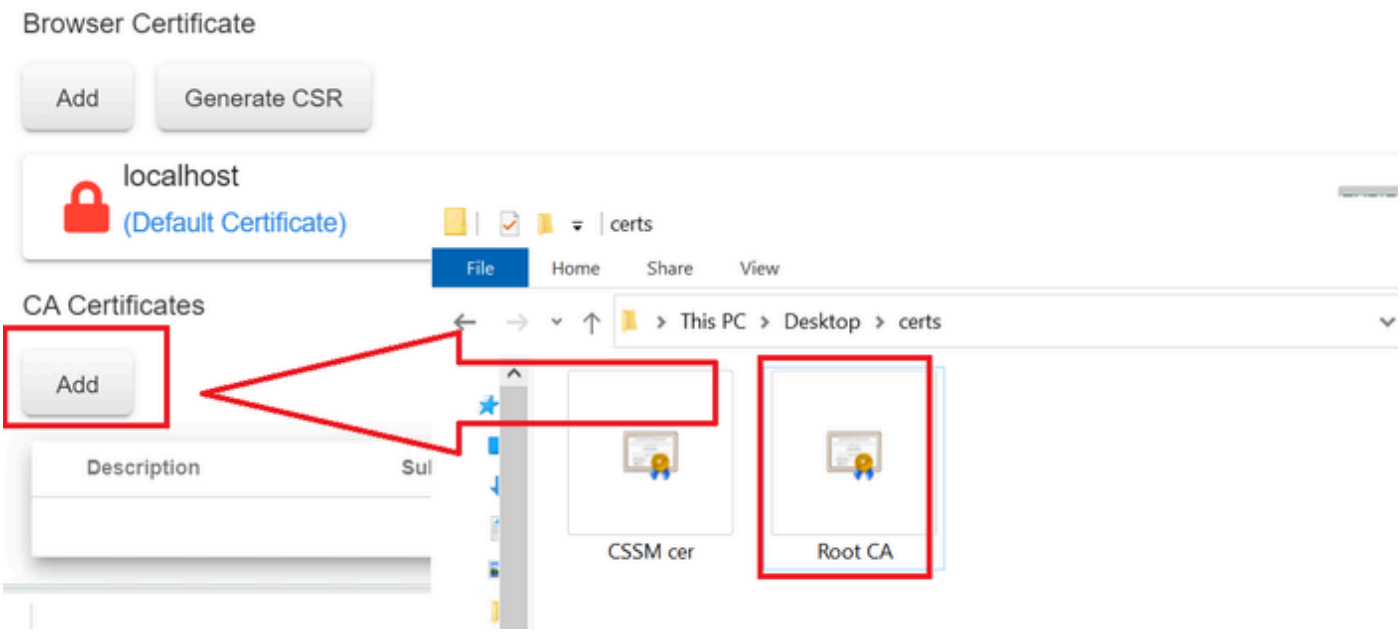
3. Immettere quindi le informazioni personali. Tenere presente che il Nome alternativo soggetto viene creato automaticamente utilizzando lo stesso valore del Nome comune. Il CSR viene scaricato automaticamente dopo aver fatto clic su Genera.



Dettagli CSR.

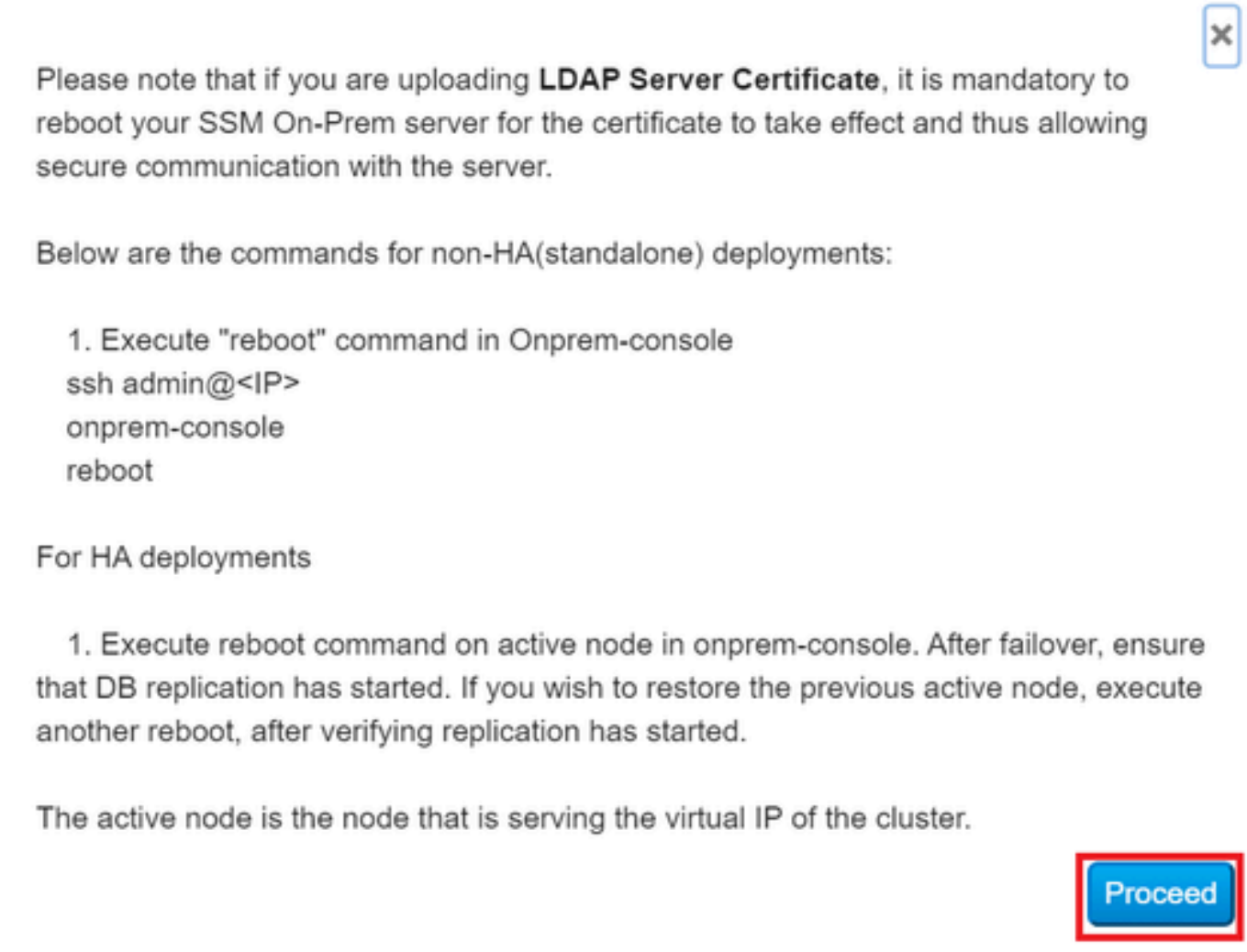
4. Firmare il CSR: per ulteriori informazioni, vedere la sezione "Creazione di certificati da un'autorità di certificazione Windows" in questo documento.

5. Caricare il certificato CA radice.



Caricamento della CA radice.

Fare clic su Continua.

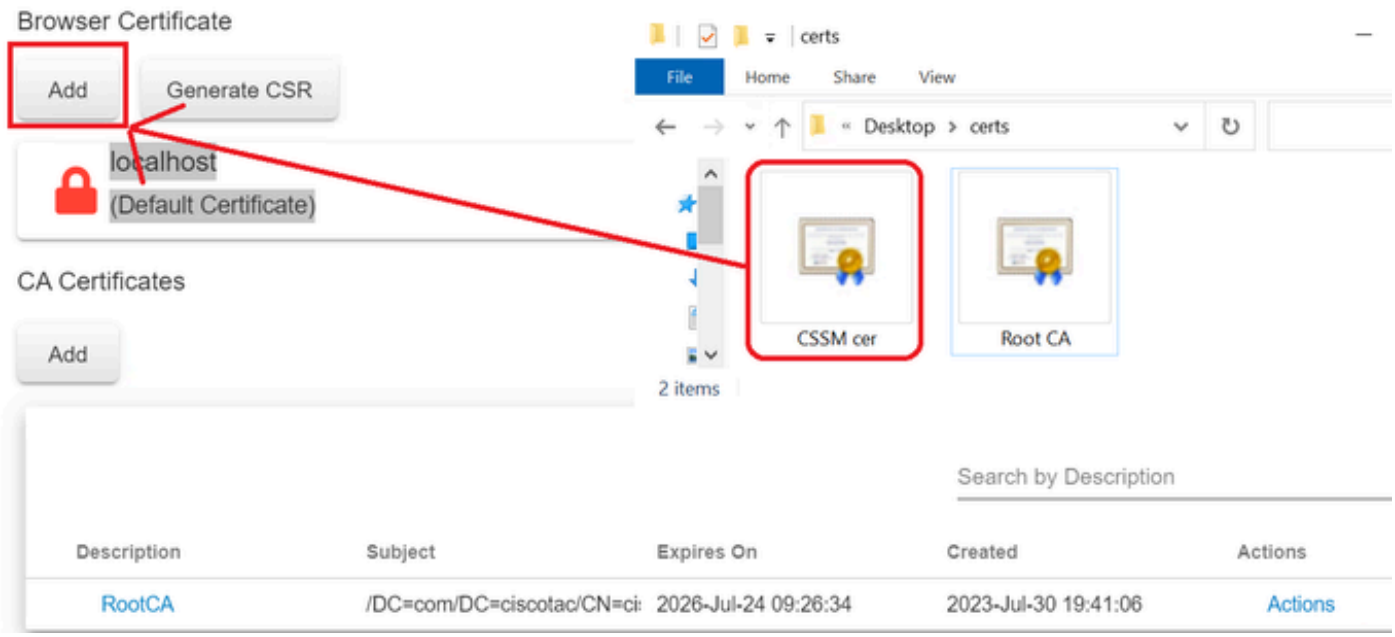


Opzione Continua.

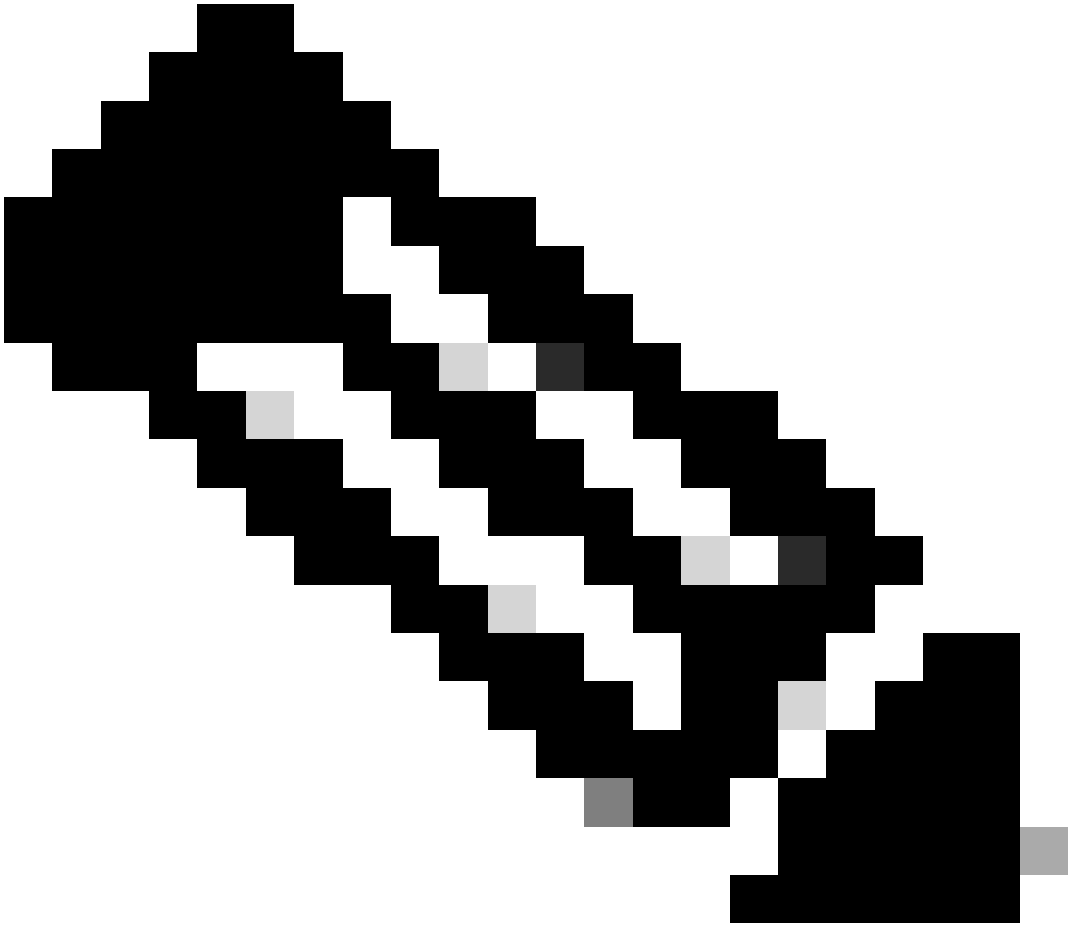
6. Immettere una descrizione e scegliere il certificato radice, quindi fare clic su OK.

CA radice descrizione.

7. Caricare il CSR firmato dalla CA (Certificato di identità CSM).

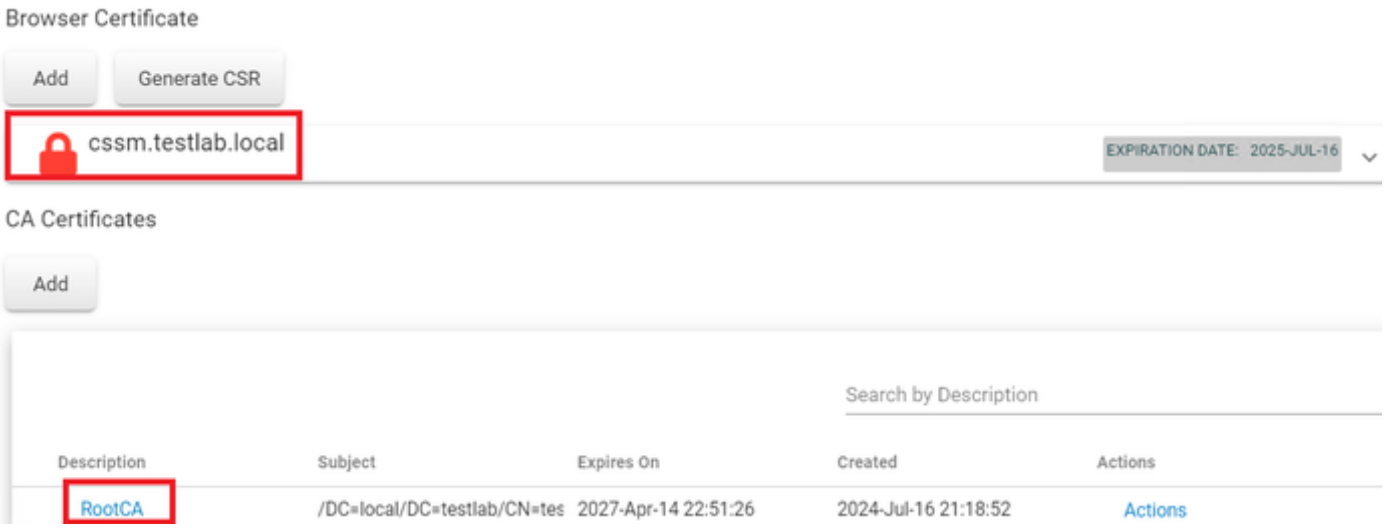


Caricamento del certificato di identità CSM.



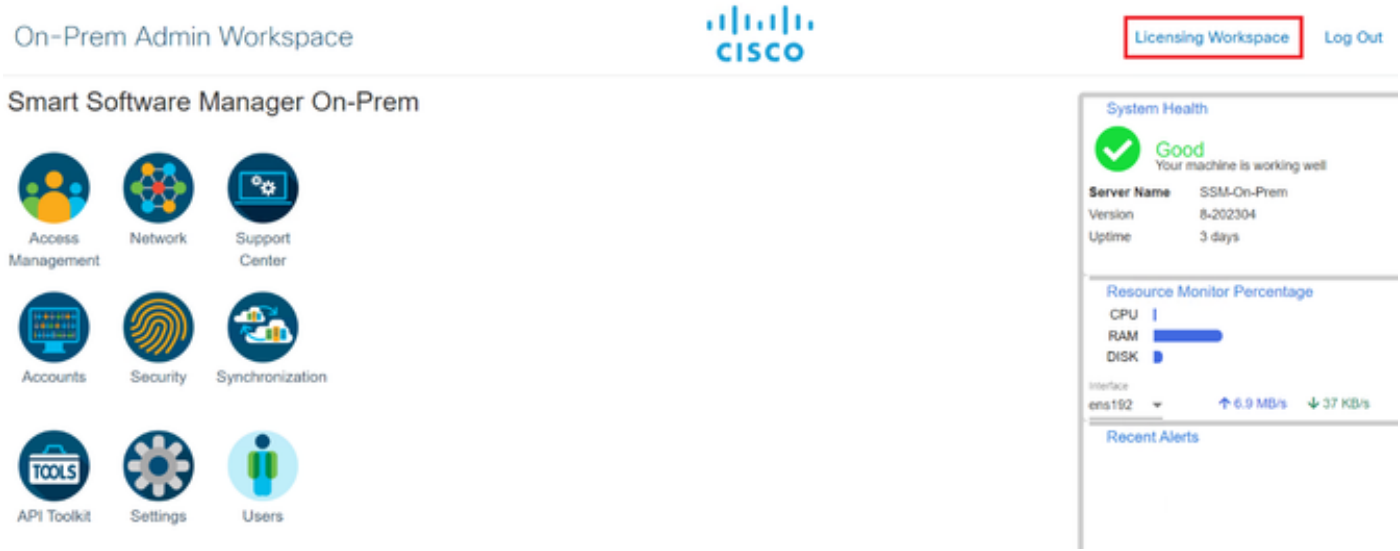
Nota: nel nostro caso, il certificato intermedio non esiste nella nostra CA. Se tuttavia si utilizza un certificato intermedio nell'architettura, il certificato intermedio è obbligatorio.

8. Confermare quindi che entrambi i certificati siano stati installati.



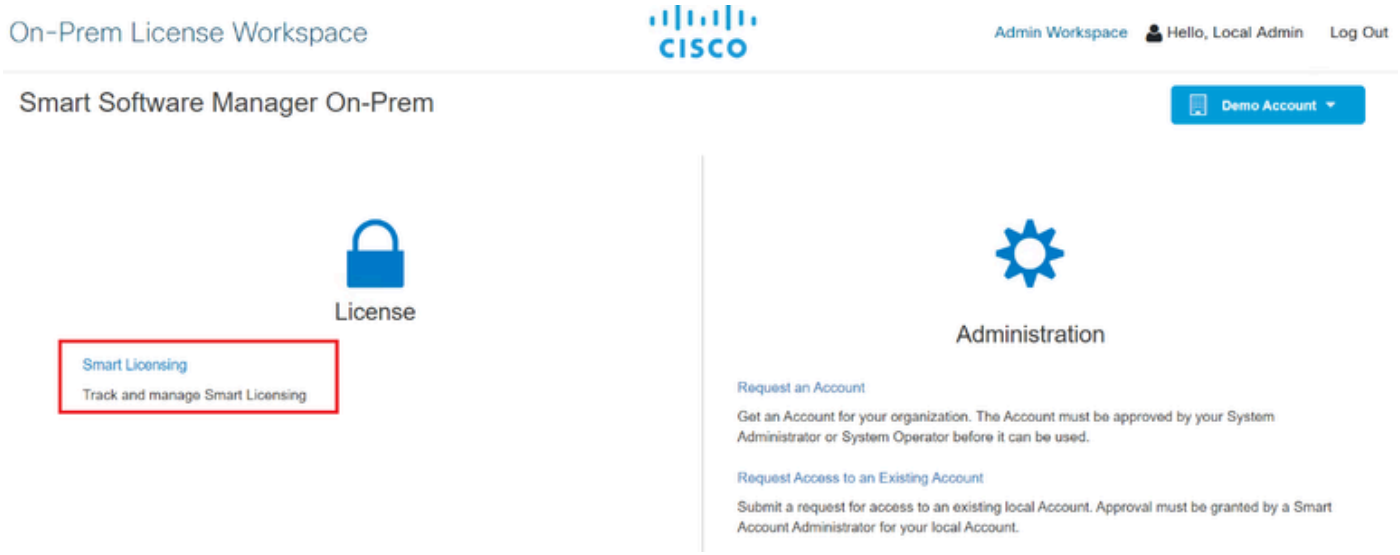
Convalida dei certificati.

9. Creare un token nell'area di lavoro locale SSM: selezione licenze.



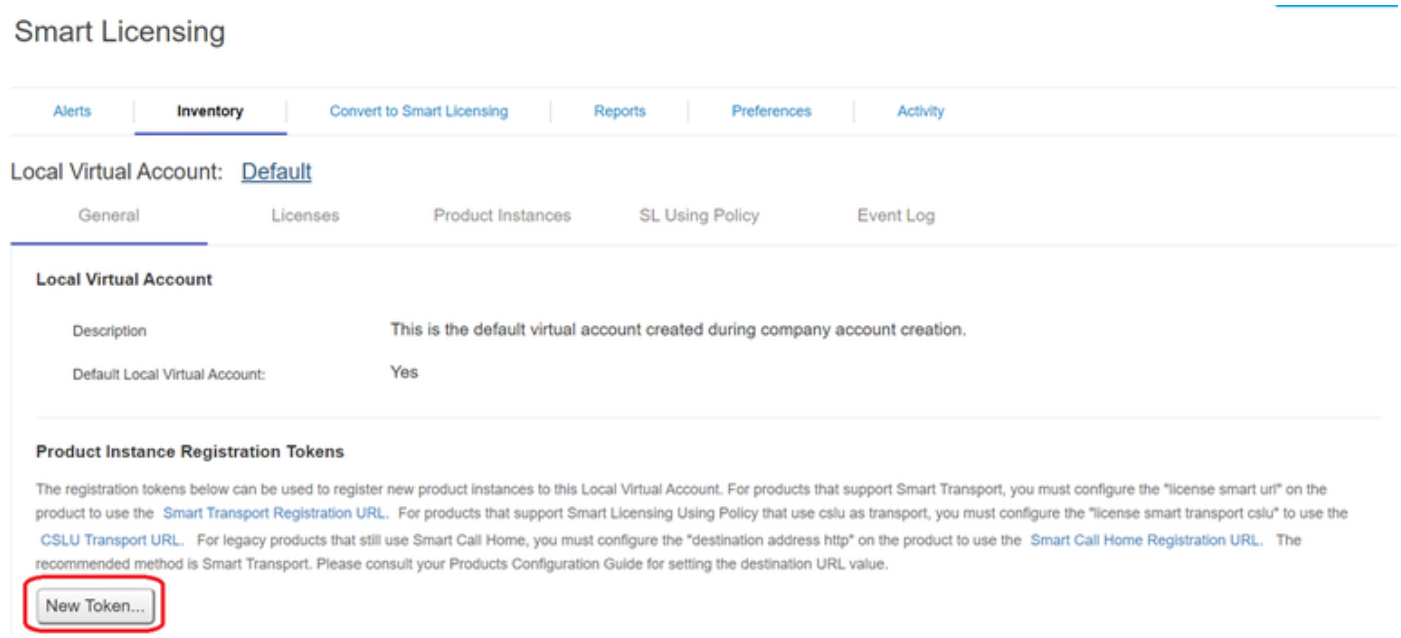
Pagina Workspace.

10. passare a Smart Licensing.



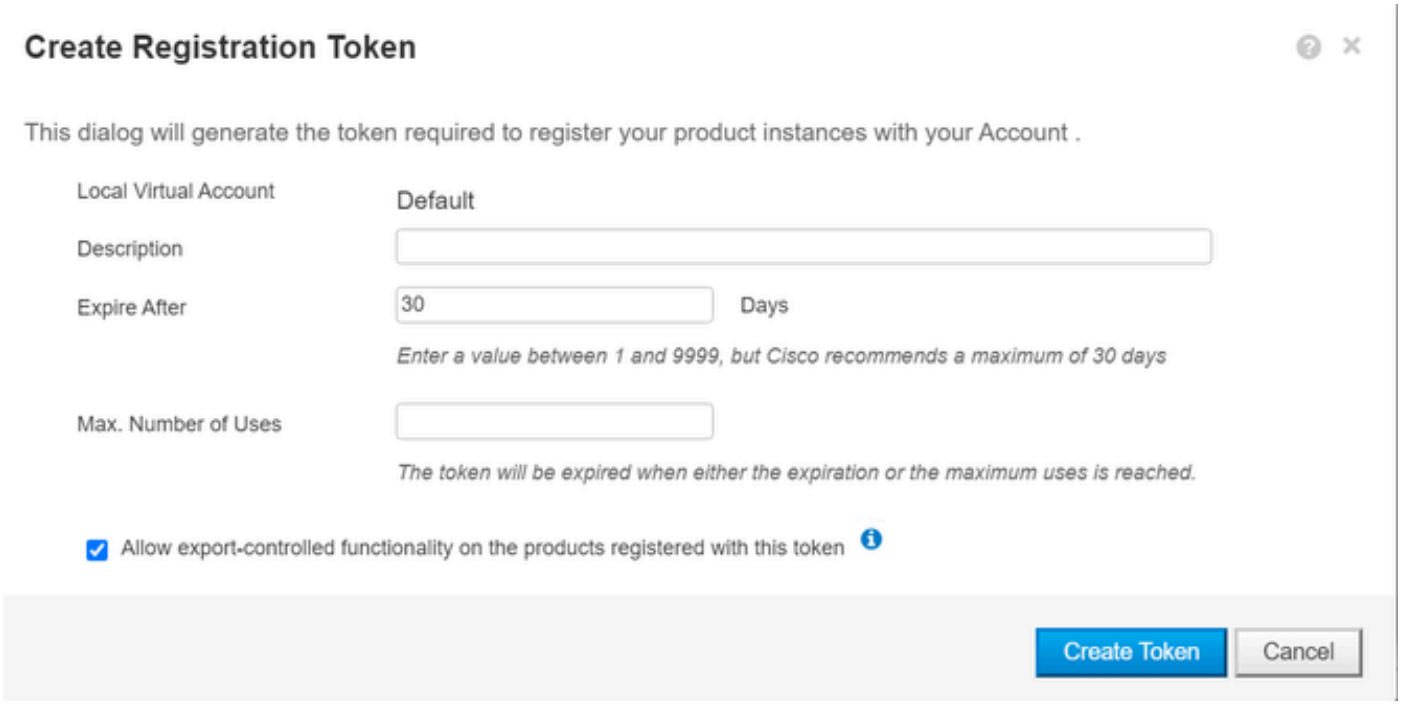
Pagina delle licenze CSM Smart

11. Cercare l'account virtuale locale, quindi fare clic su Nuovo token e su Continua.

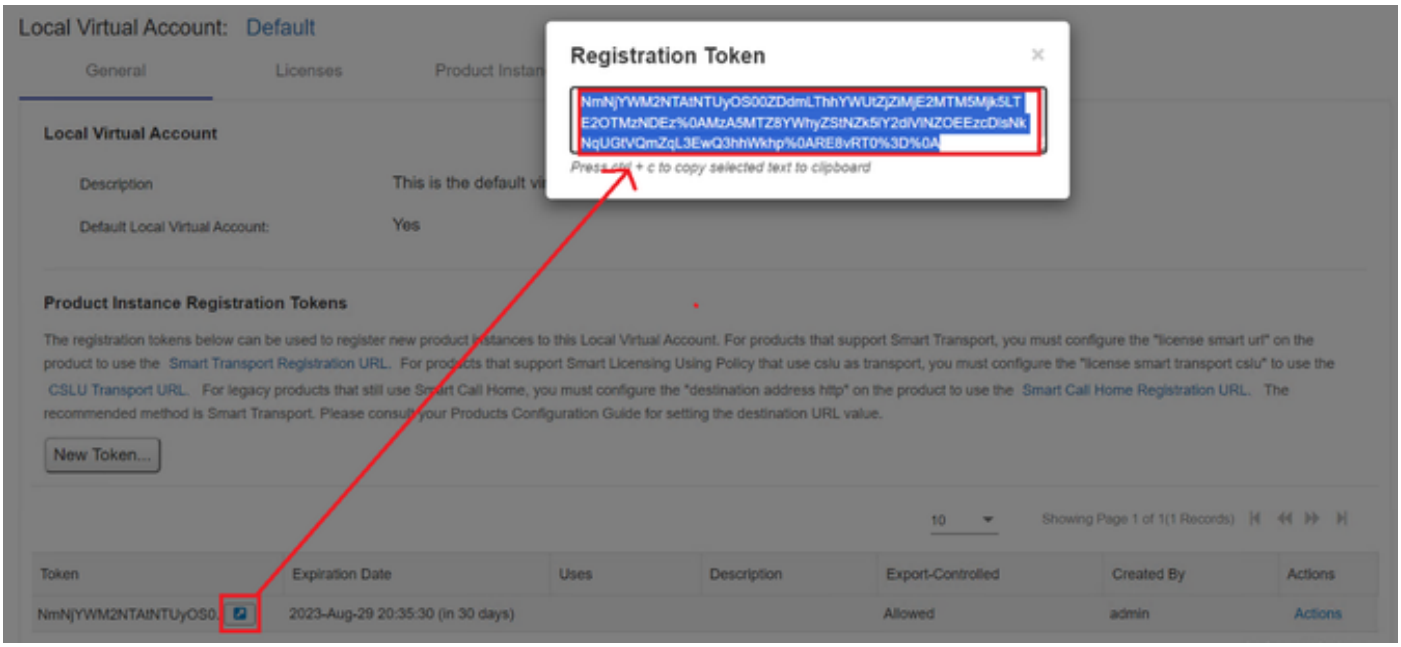


Nuova opzione token.

12. Selezionare Create Token e copiarlo.

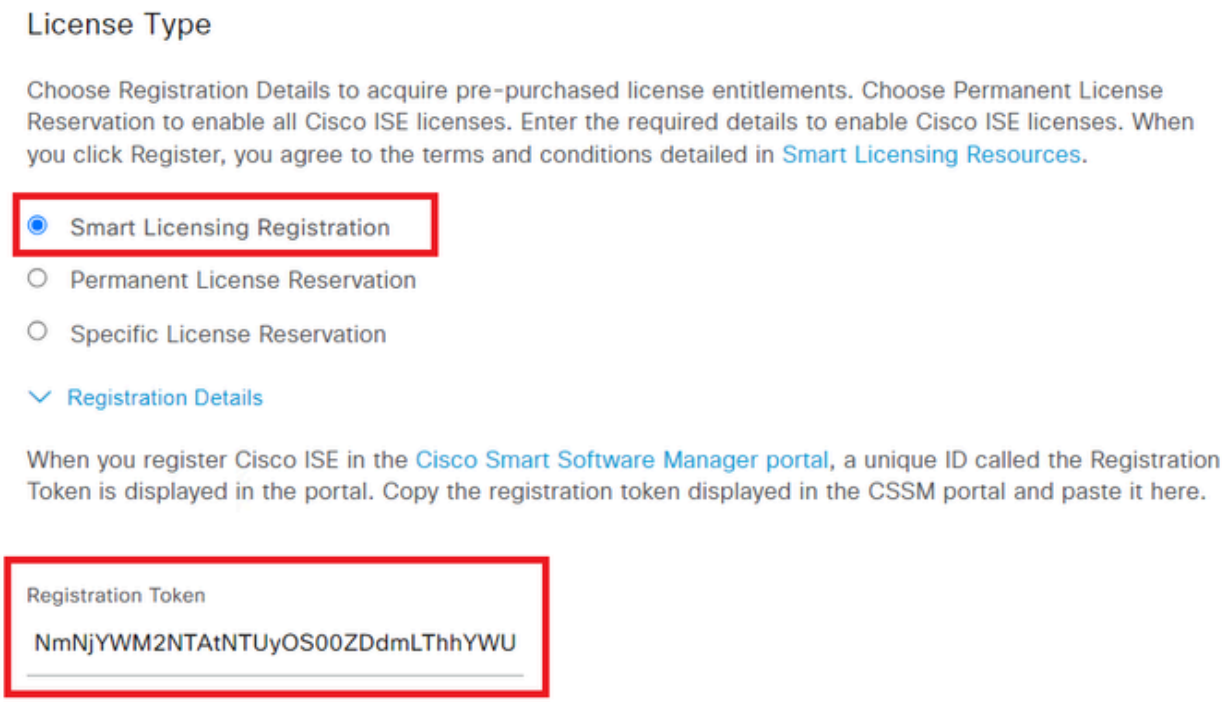


Creazione del nuovo token.



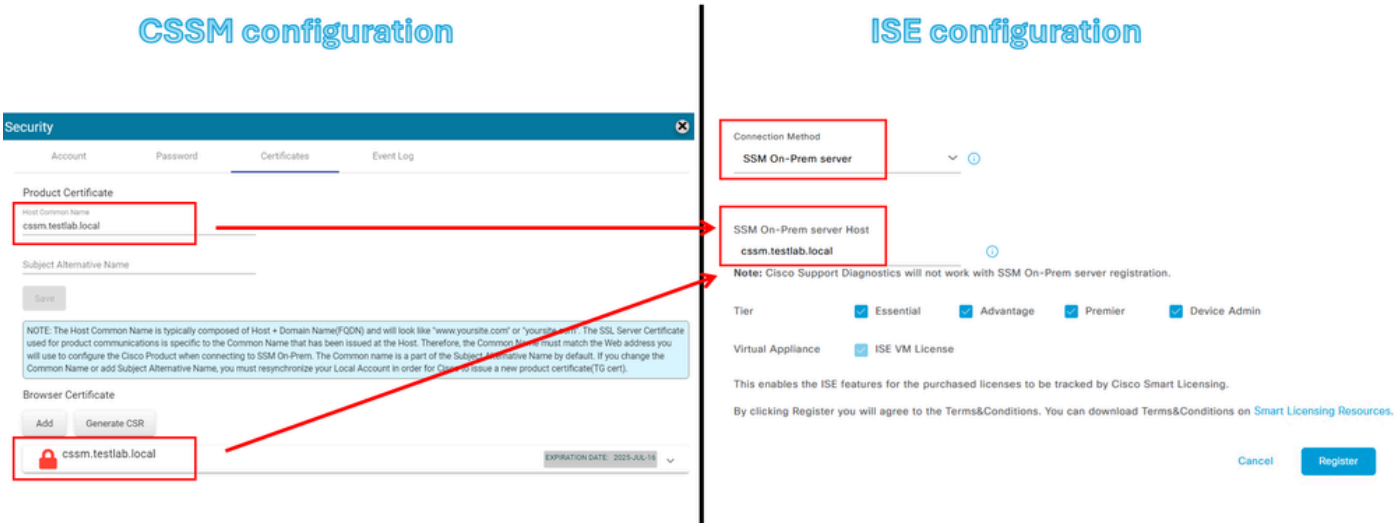
Dettagli token.

13. Aprire la GUI di ISE e selezionare Amministrazione > Sistemi > Licenze, quindi fare clic su Dettagli registrazione, selezionare il metodo host del server locale SSM, quindi incollare il token.

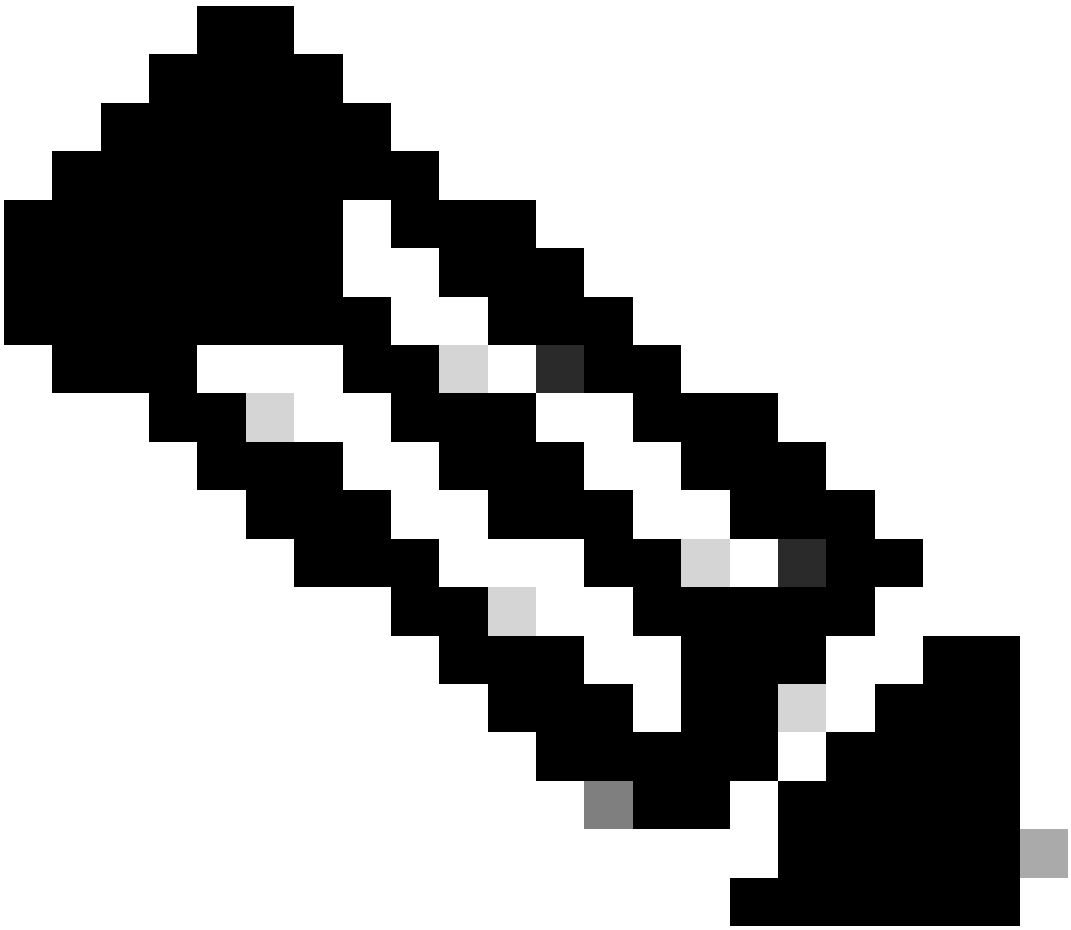


Registrazione delle licenze.

14. Immettere l'FQDN locale di SSM sull'host del server locale SSM e fare clic su Registra.



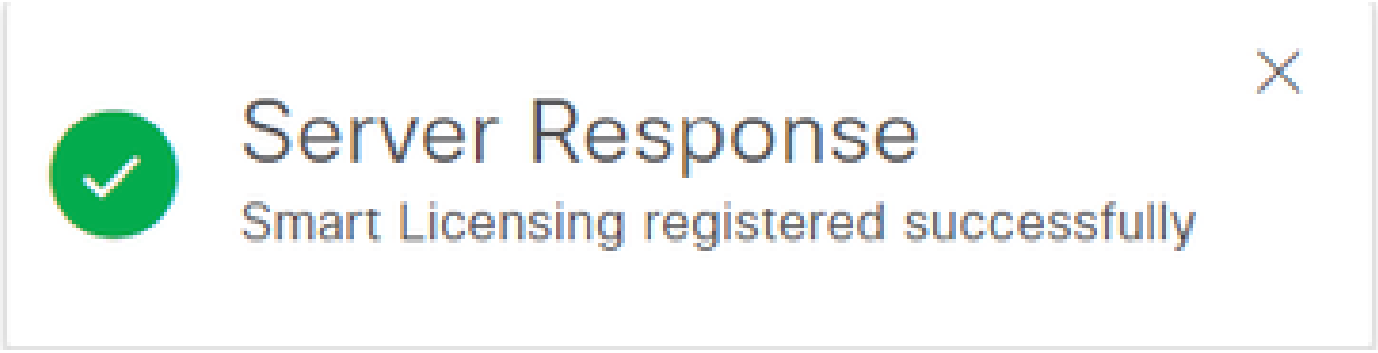
Impostazioni CSSM e ISE.



Nota: è importante configurare il nome host + dominio sul nome comune host perché ISE utilizza questo parametro per stabilire una connessione con il CSM. È possibile utilizzare

un indirizzo IP al posto di hostname + domain, tuttavia si consiglia di utilizzare hostname + domain

15. Infine, la registrazione è stata completata.

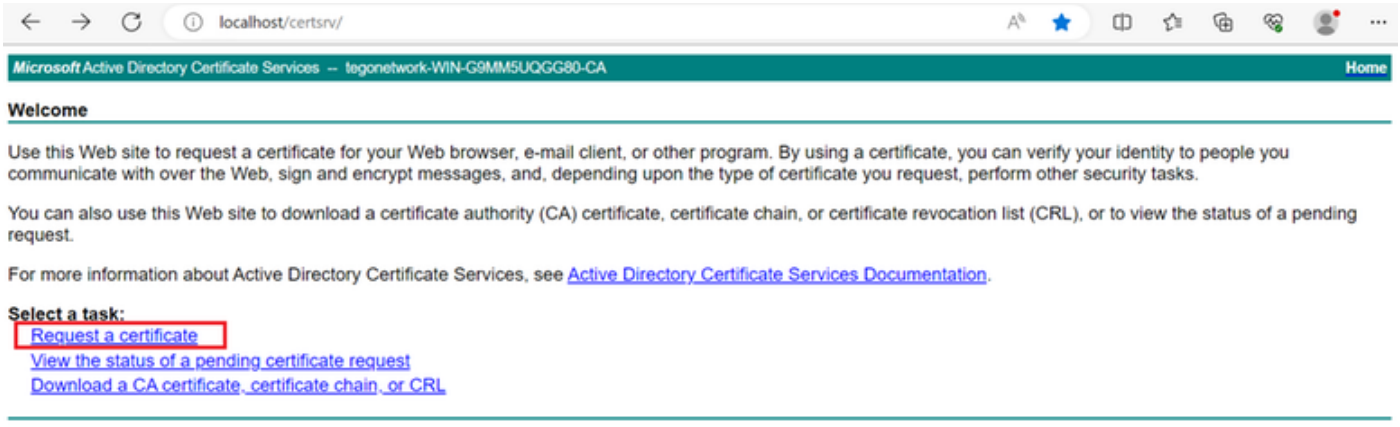


Registrazione completata.

Crea certificati da CA di Windows.

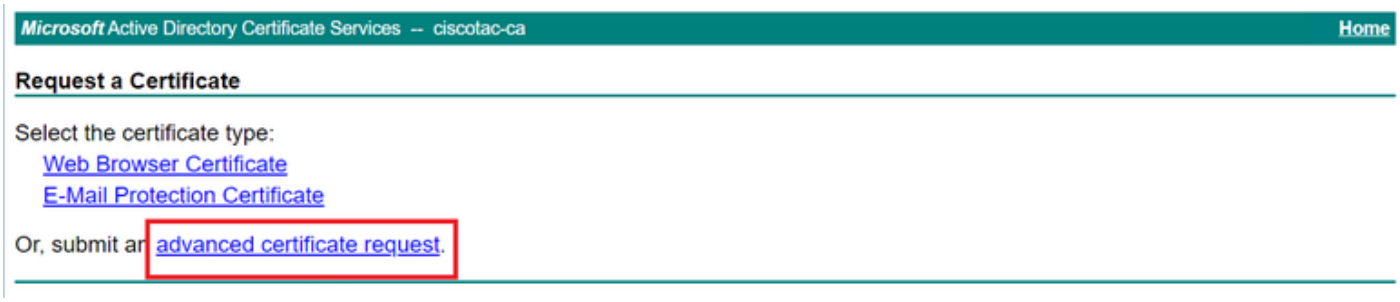
L'amministratore dell'Autorità di certificazione deve eseguire le operazioni seguenti:

1. Aprire un browser Web e passare a http://localhost/certsrv/
2. Fare clic su Request a certificate (Richiedi certificato).



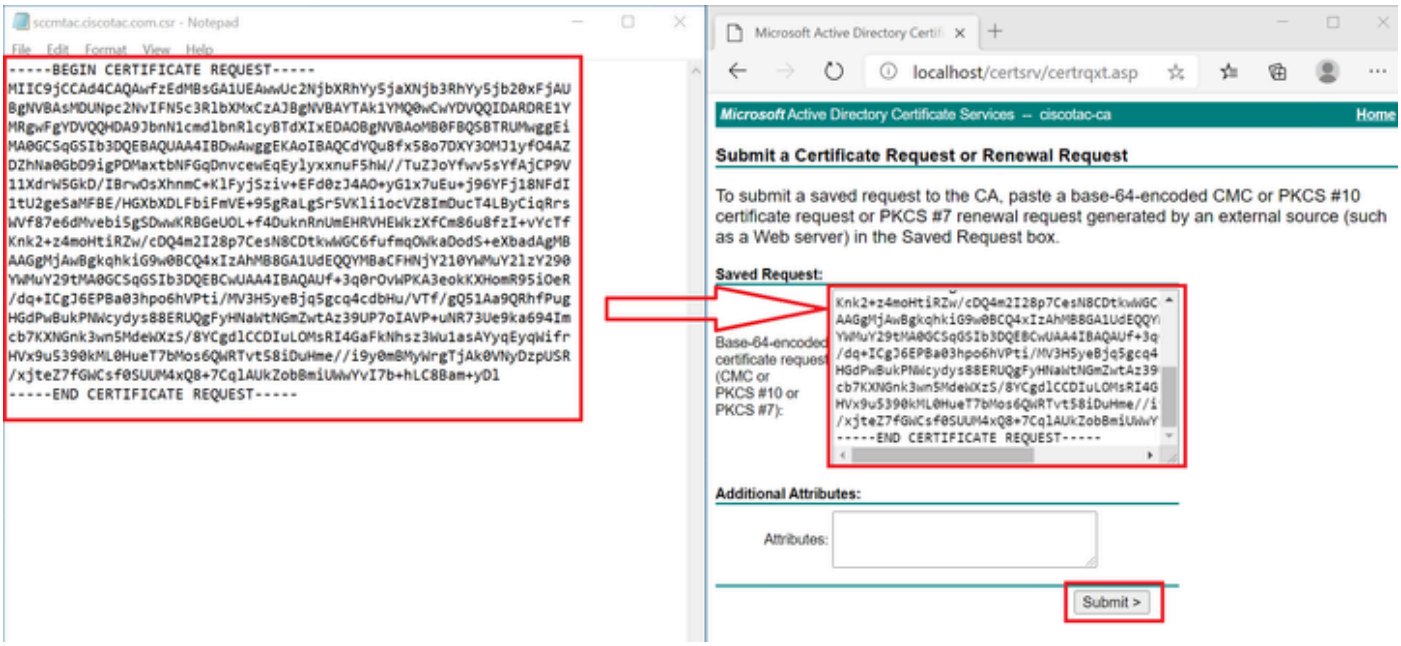
Richiedi certificato.

3. Fare clic su Richiesta avanzata certificati.



Richiesta avanzata di certificati.

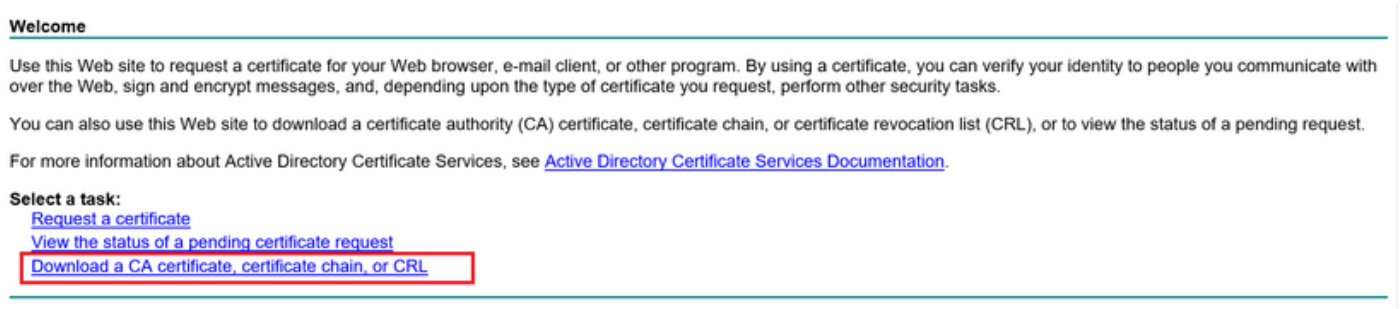
4. Aprire il CSR generato in precedenza. Copiare quindi le informazioni e incollarle su Richiesta salvata.



Invia certificato.

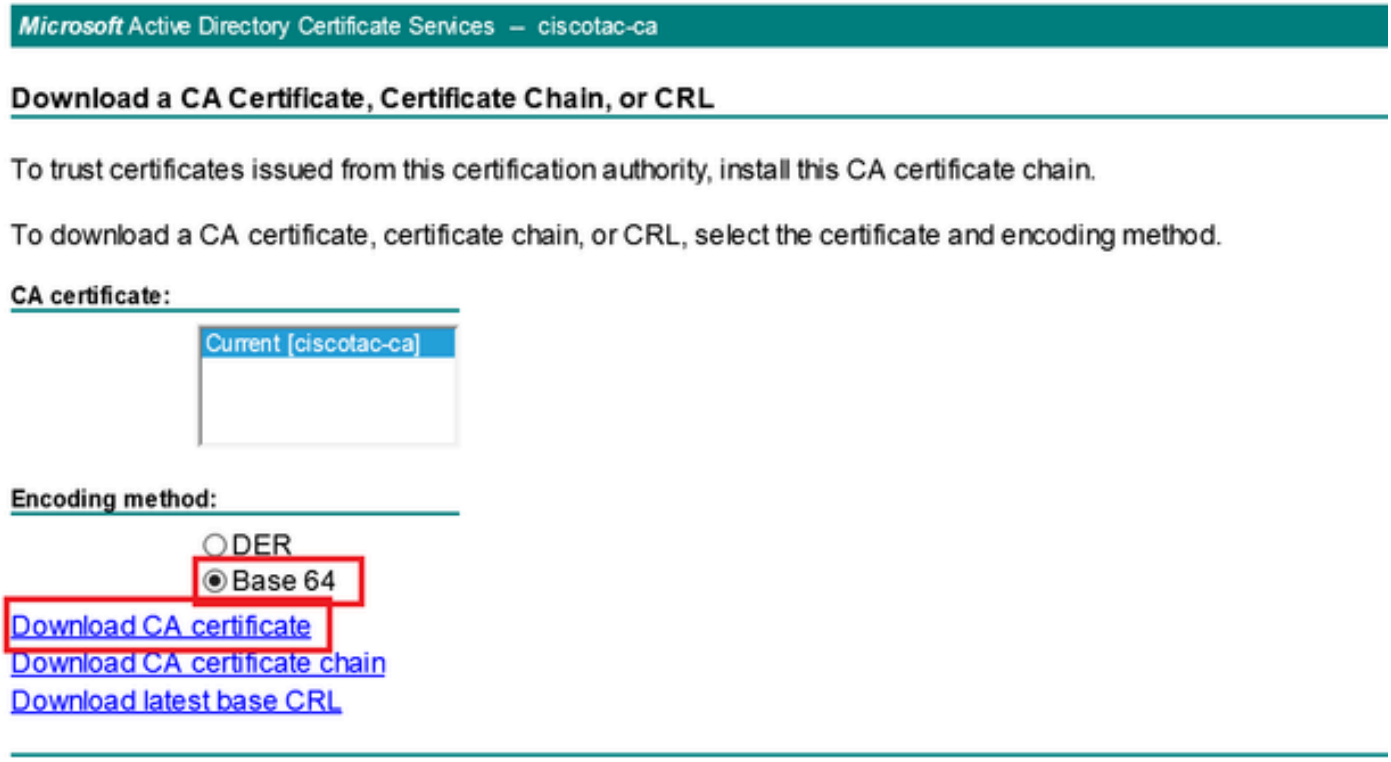
Dopo aver fatto clic su Invia, il certificato viene scaricato automaticamente.

5. Scaricare la radice del certificato CA. Tornare a http://localhost/certsrv/ e selezionare Download a CA Certificate, Certificate Chain o CRL.



Scaricare la CA radice.

6. Scaricare il certificato CA utilizzando il metodo di codifica Base64.

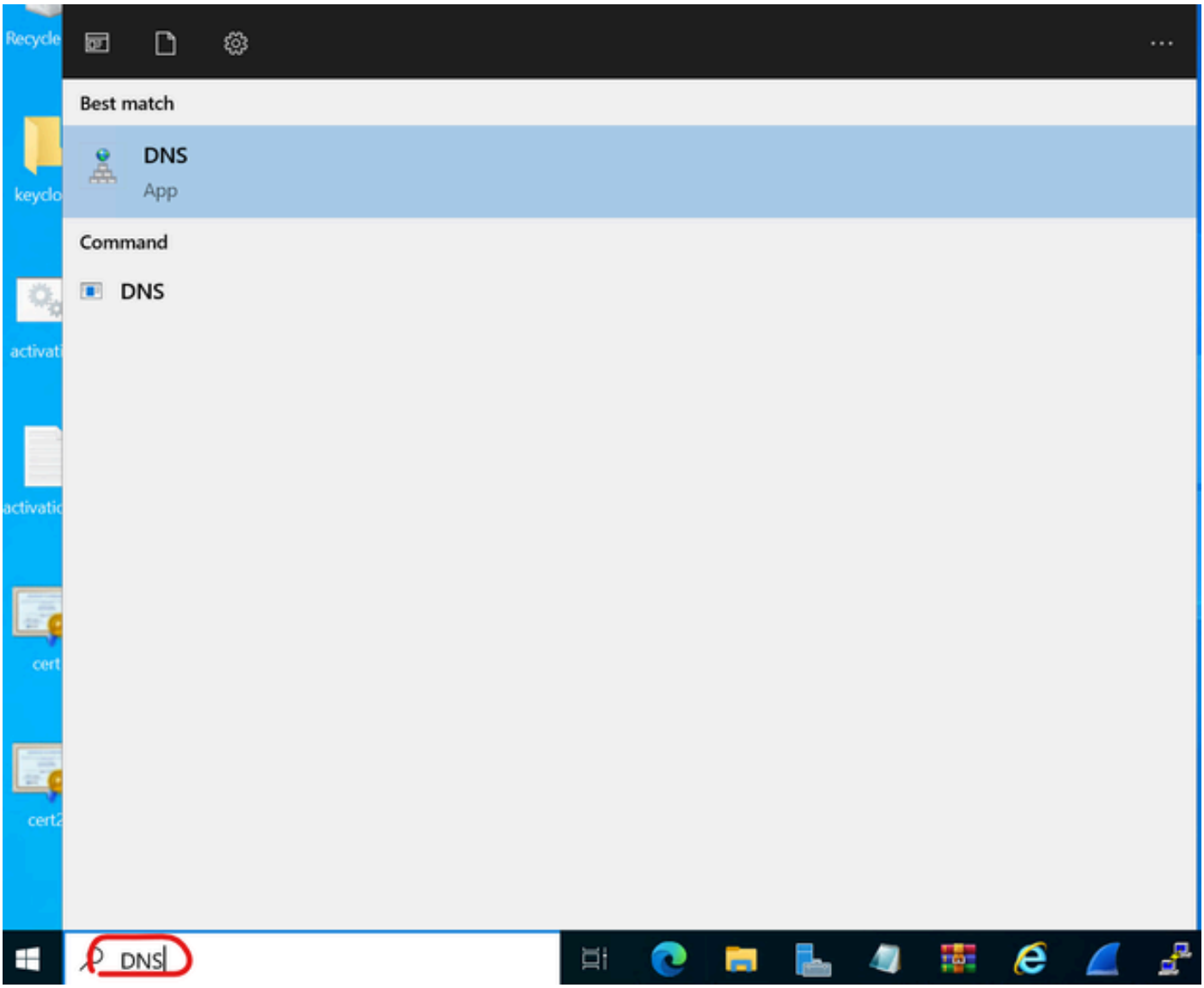


Base 64.

Aggiungere record DNS in Windows Server.

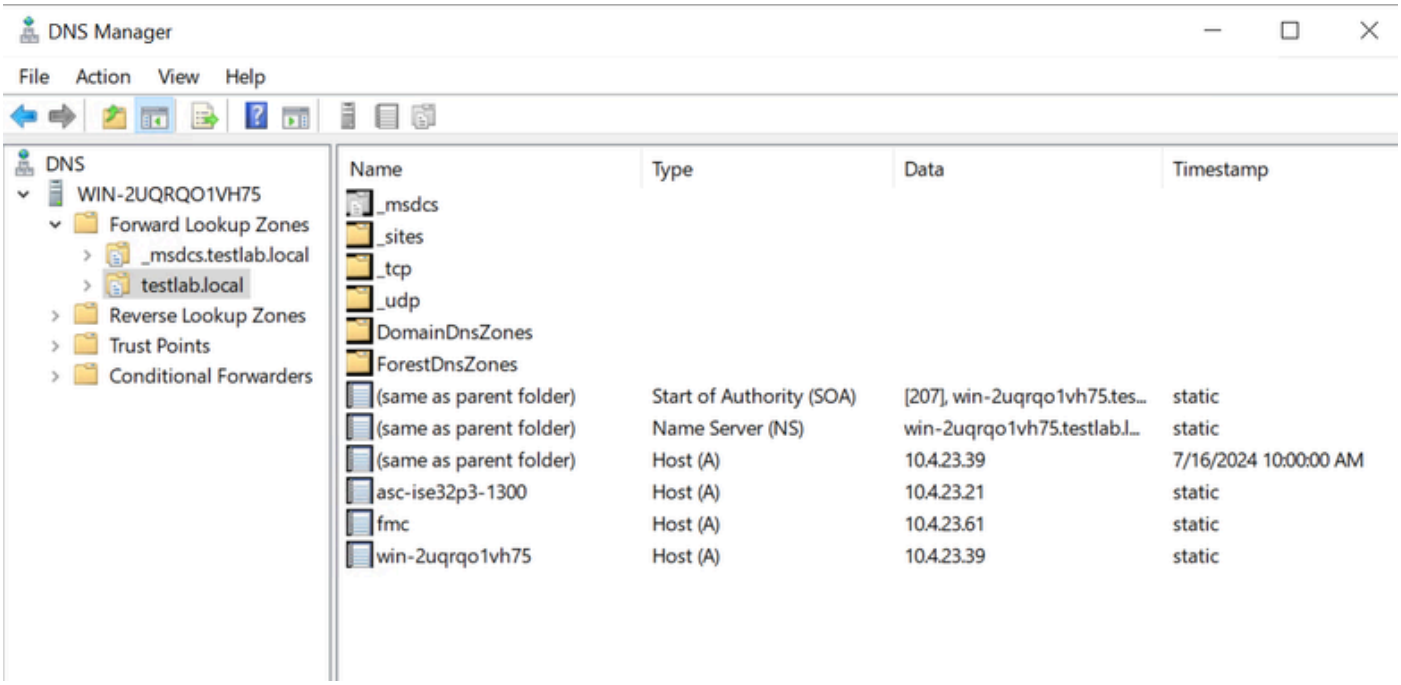
Se l'utente è l'amministratore, aggiungere gli FQDN ISE e CSM.

1. Aprire Gestore DNS: digitare "DNS" nel Finder di Windows e aprire l'app DNS.

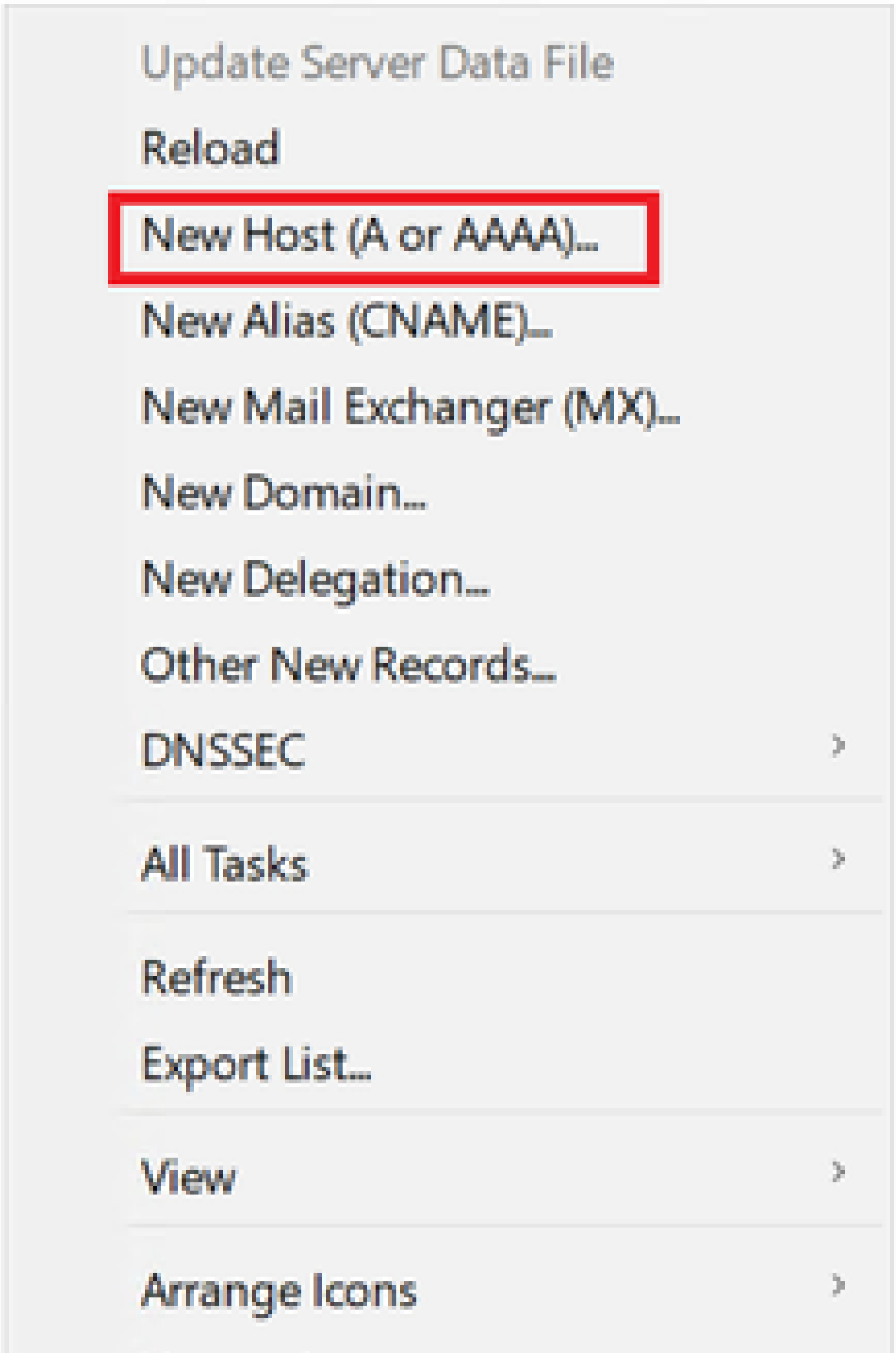


Opzione DNS.

2. Passare a Zone di ricerca diretta > E scegliere il dominio.



3. Fare clic con il pulsante destro del mouse su uno spazio nero e selezionare "New Host (A or AAAA)" (Nuovo host (A o AAAA)


Update Server Data File
Reload
New Host (A or AAAA)...
New Alias (CNAME)...
New Mail Exchanger (MX)...
New Domain...
New Delegation...
Other New Records...
DNSSEC
All Tasks
Refresh
Export List...
View
Arrange Icons

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).