

# Configurazione di CSSM su prem e registrazione delle licenze con ISE

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Installare CSM on-Prem su VMWARE ESXi.](#)

[Configurazione iniziale di CSSM locale.](#)

[Integrazione di CSM on-prem con Smart Account](#)

[OPZIONE 1: registrare il CSM on-prem tramite una connessione Internet.](#)

[OPZIONE 2: registrare il CSM on-prem senza una connessione Internet.](#)

[Integrazione di CSM On-Prem con ISE.](#)

[Crea certificati da CA di Windows.](#)

[Aggiungere record DNS in Windows Server.](#)

[Risoluzione dei problemi](#)

[Host/indirizzo IP non raggiungibile. \(Errore ISE\)](#)

[Servizio SSO: impossibile raggiungere Cisco. \(Errore in CSSM locale\)](#)

[Il nome comune nel CSR non è un nome host o un indirizzo IP risolvibile tramite DNS. Riprovare. \(Errore in CSM locale\)](#)

---

## 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

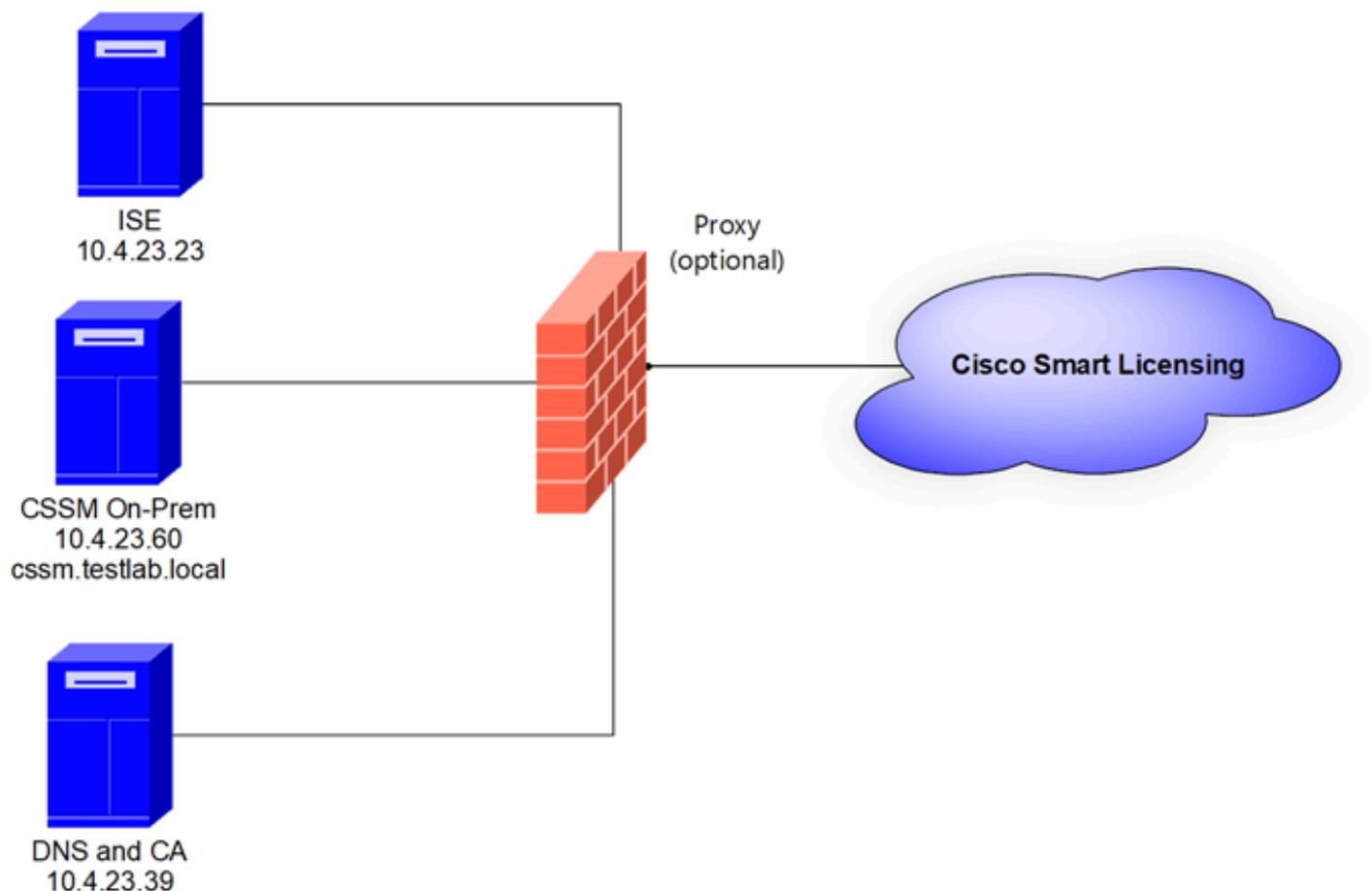
- Patch 2 di Identity Service Engine 3.2
- SSM On Prem 8.20234

- 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



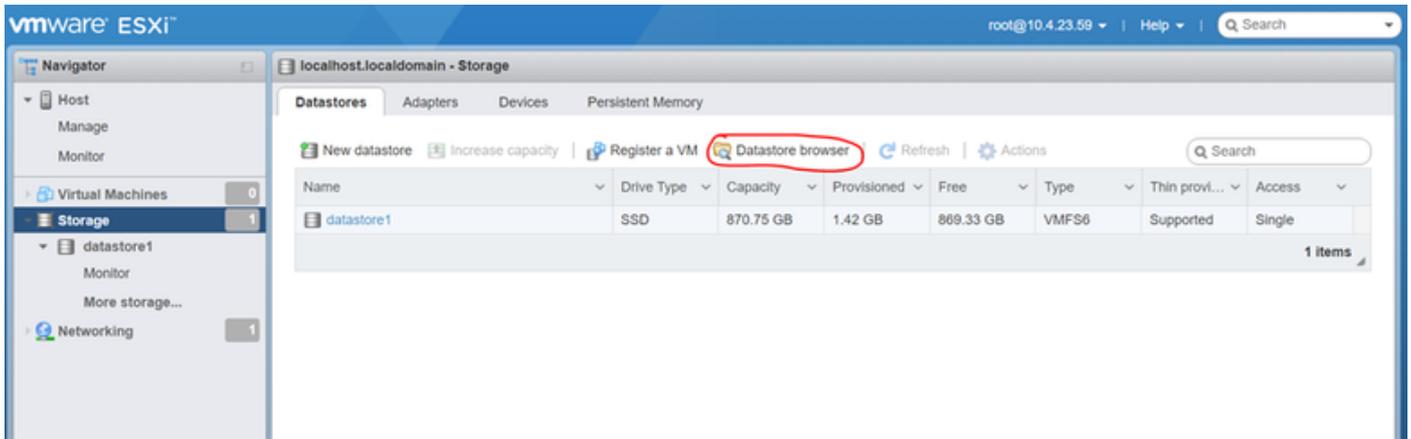
Topologia generale

### 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>

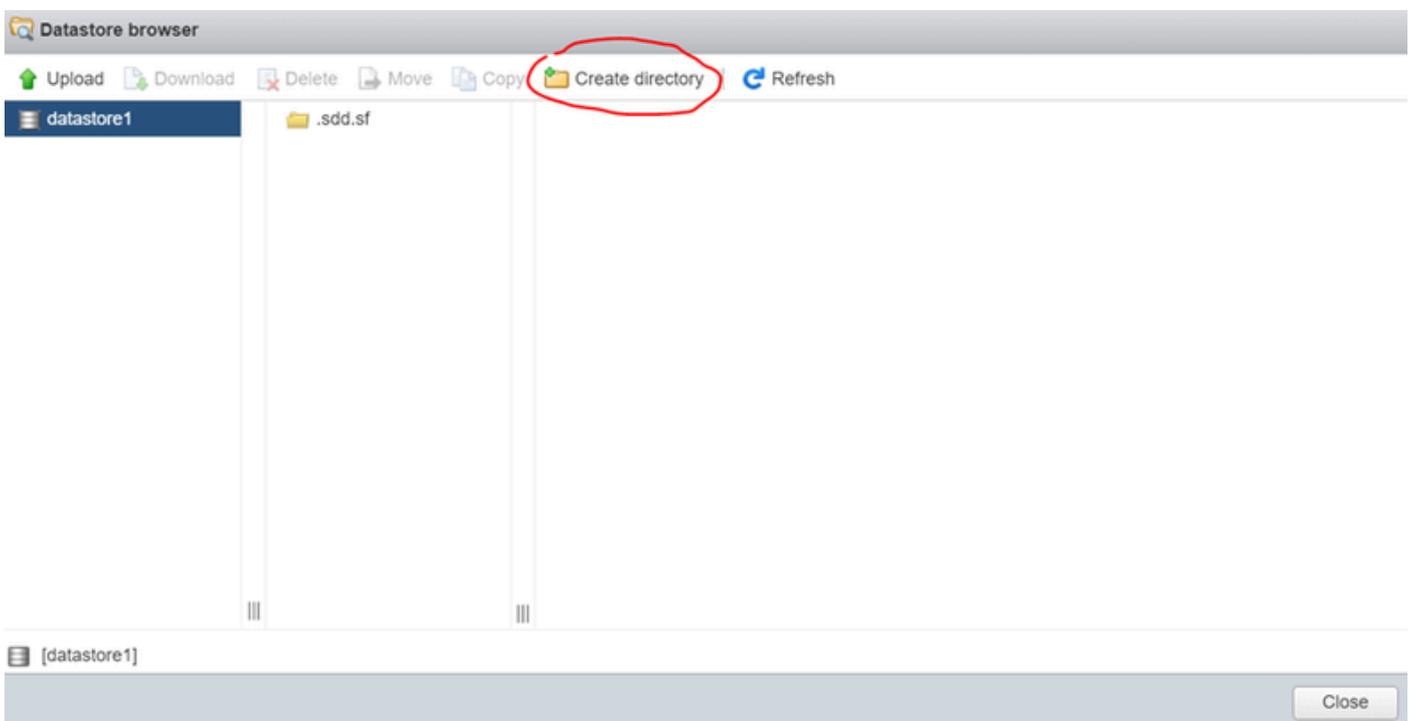
2. Caricare l'ISO in VMWARE ESXi.

Passare a Memoria > Browser archivio dati.



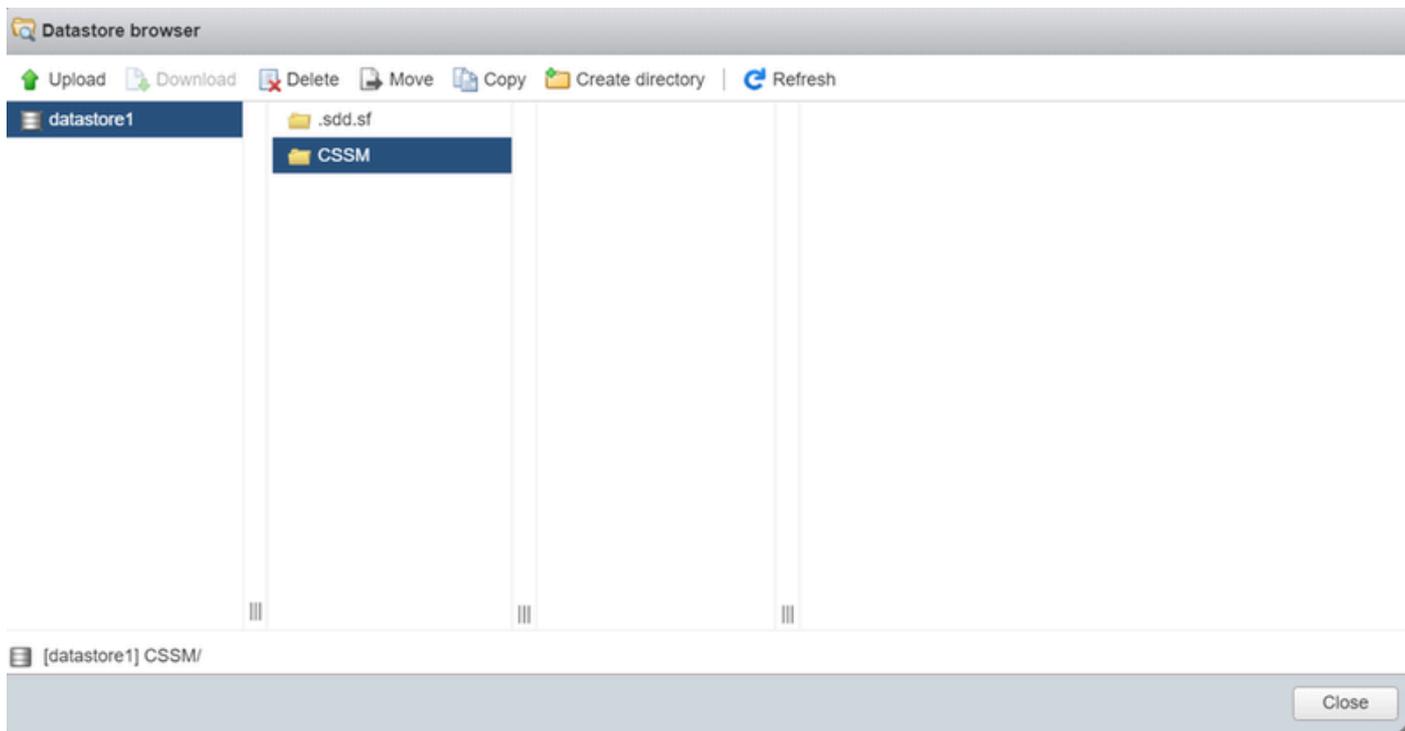
Sezione Data browser

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



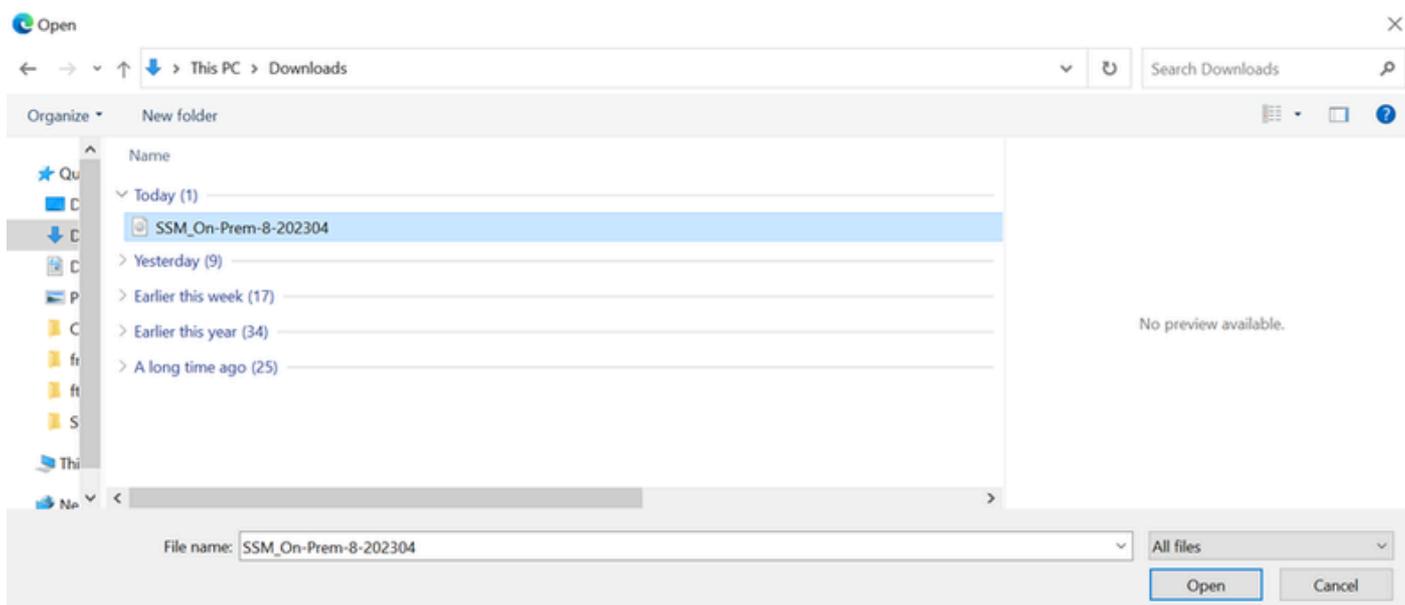
Creazione della directory

Nell'esempio seguente è stata creata la cartella CSSM:



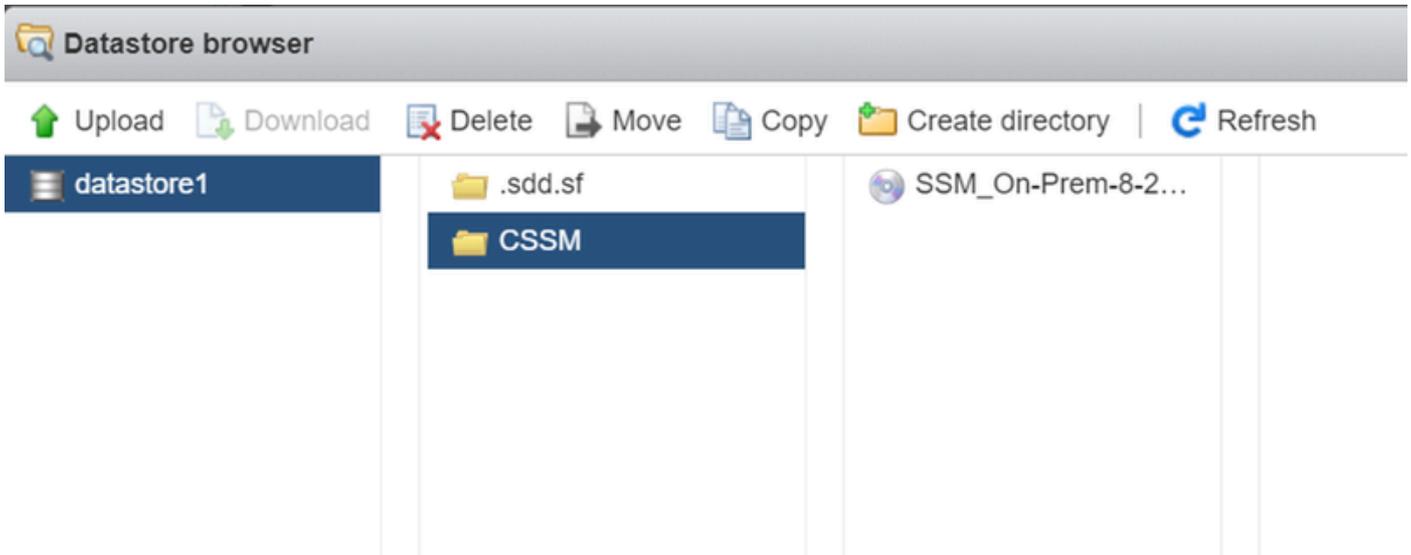
Creazione di cartelle

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



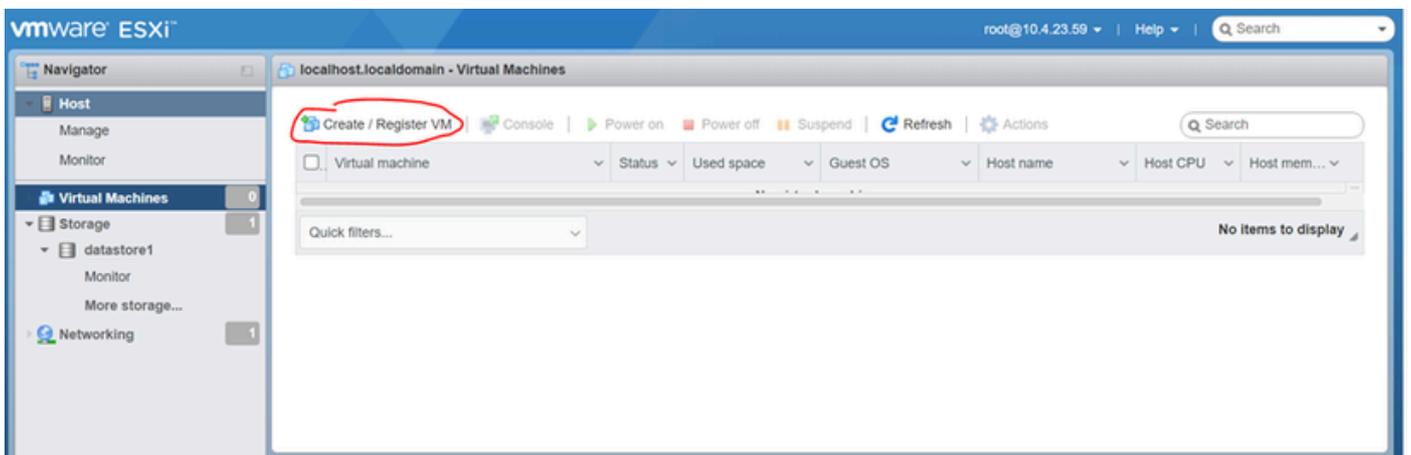
Caricamento ISO

Il file ISO si trova nella cartella CSSM:



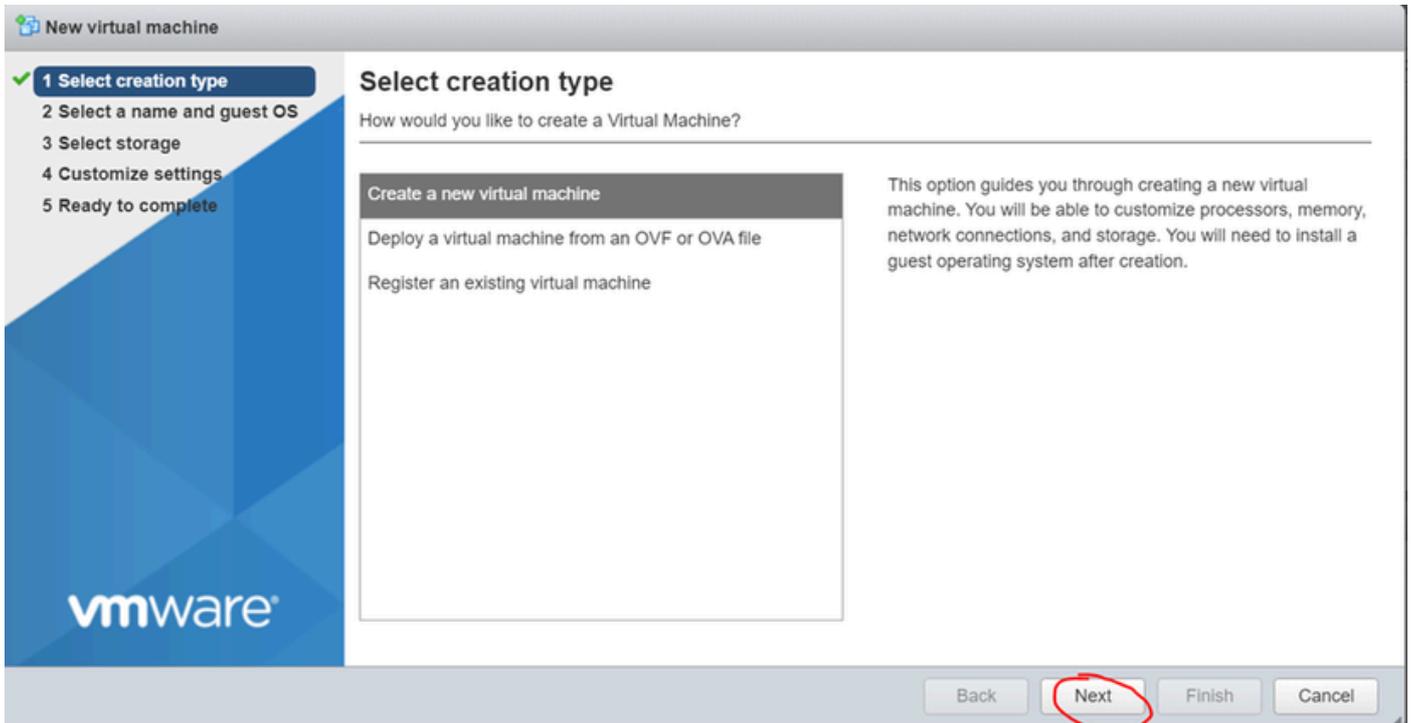
Caricamento ISO completato

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.

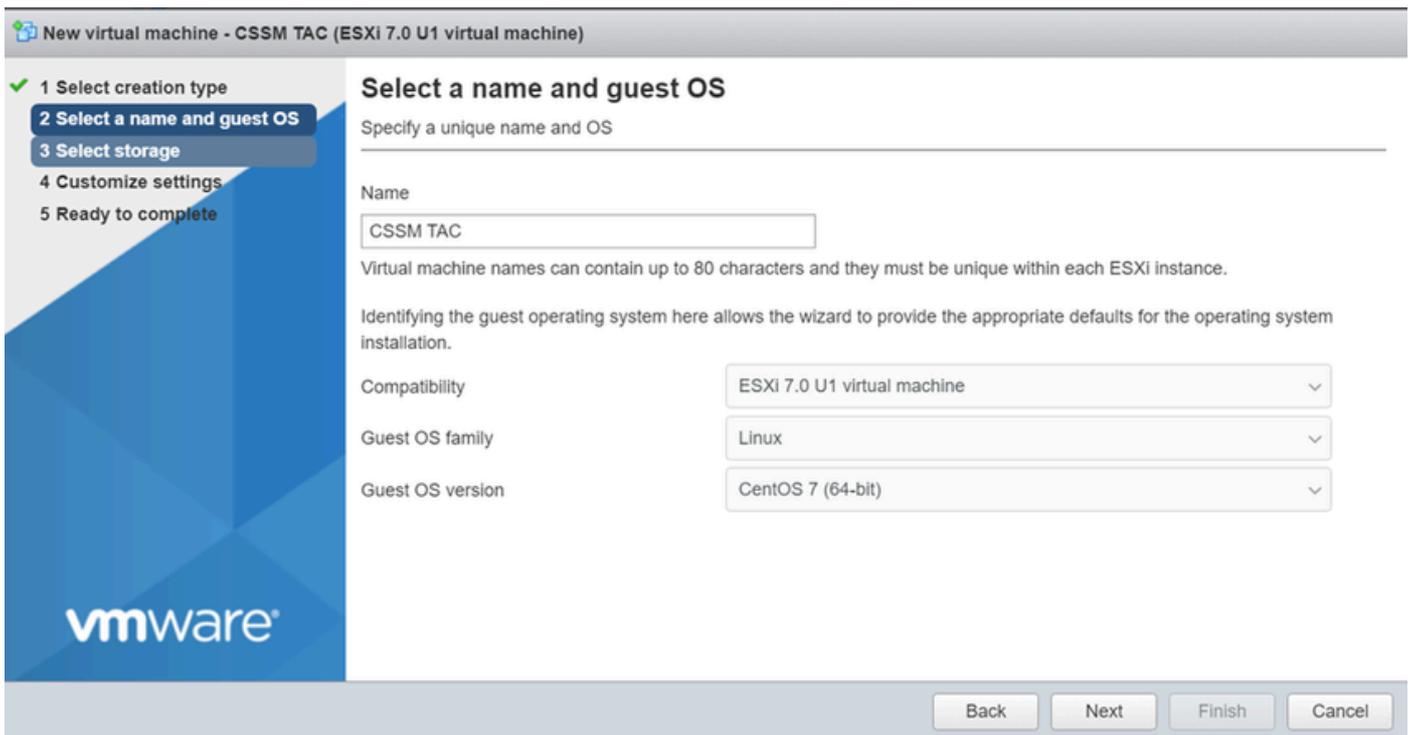


Creazione di una nuova VM fase 02

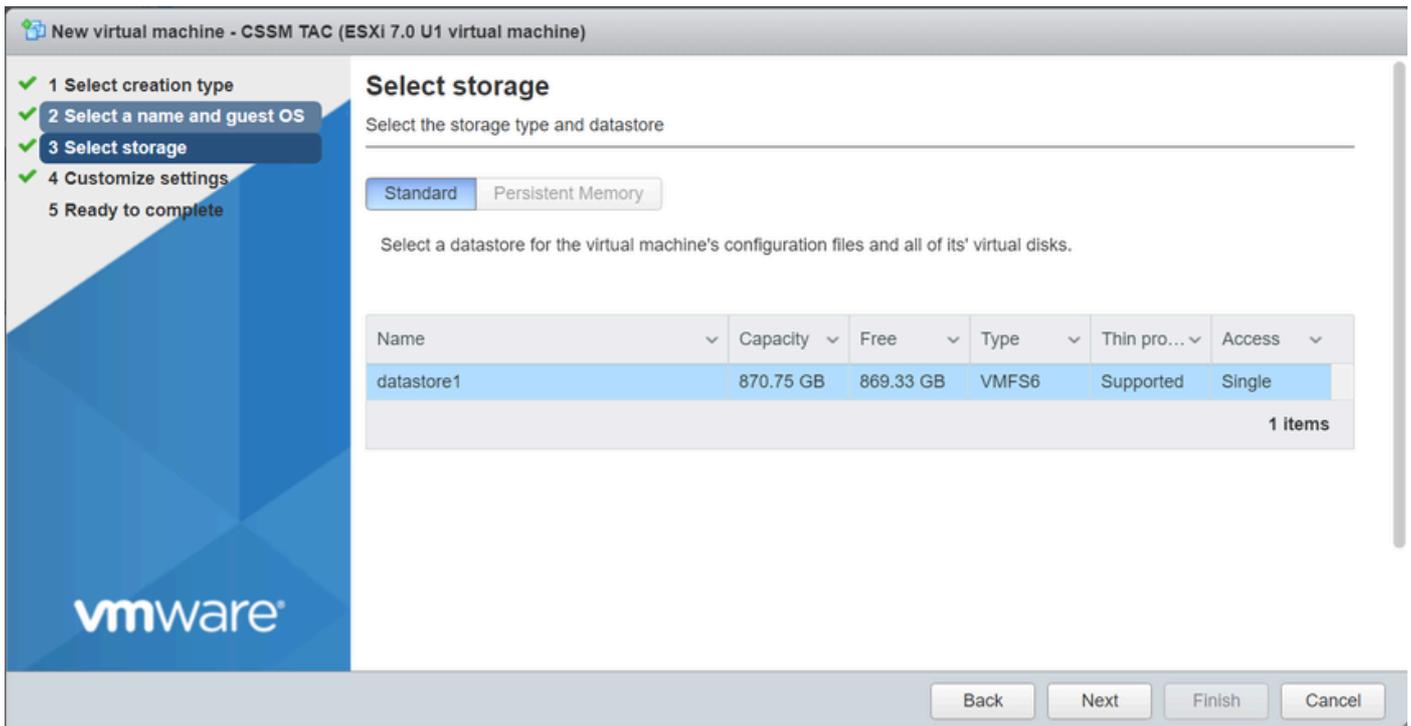
7. Quindi configurare i parametri successivi:

- 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).



## 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.

▼ CPU	4 ▼ ⓘ
Cores per Socket	1 ▼ Sockets: 1

Configurazione dei core

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

▼  Hard disk 1	200	GB	
Maximum Size	869.33 GB		
Location	[datastore1] CSSM TAC		<input type="button" value="Browse..."/>
Disk Provisioning	<input checked="" type="radio"/> Thin provisioned <input type="radio"/> Thick provisioned, lazily zeroed <input type="radio"/> Thick provisioned, eagerly zeroed		

Configurazione del disco

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

▼  Network Adapter 1	VM Network
Status	<input checked="" type="checkbox"/> Connect at power on
Adapter Type	E1000e

Configurazione delle impostazioni di rete

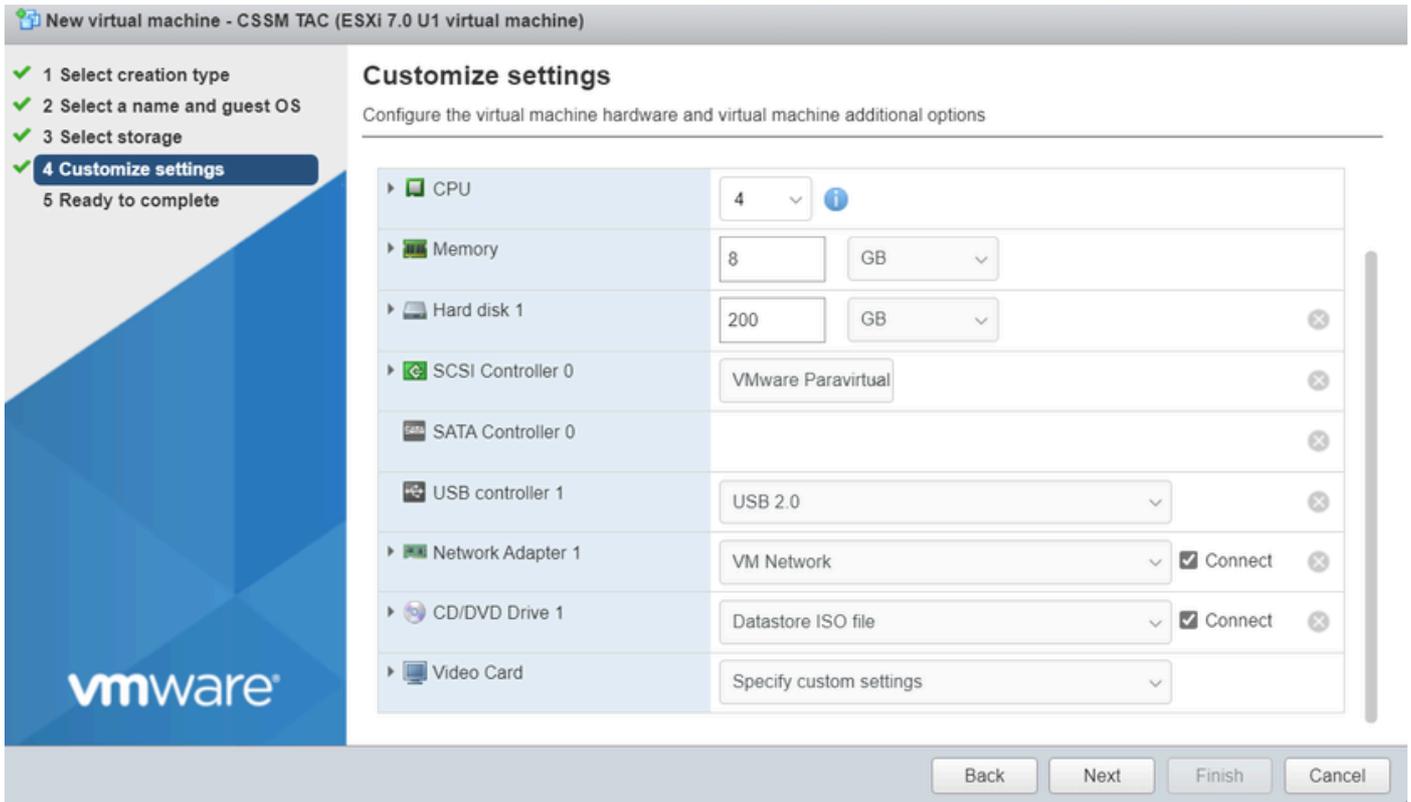
- Unità CD/DVD: scegliere "File ISO dei dati" e selezionare il file ISO.

**Datastore browser**

<b>datastore1</b> vmimages	.sdd.sf <b>CSSM</b>	SSM_On-Prem-8-2...	 SSM_On-Prem-8-2023... 2.92 GB Wednesday, July 26, 2...
-------------------------------	------------------------	--------------------	--

immagine ISO

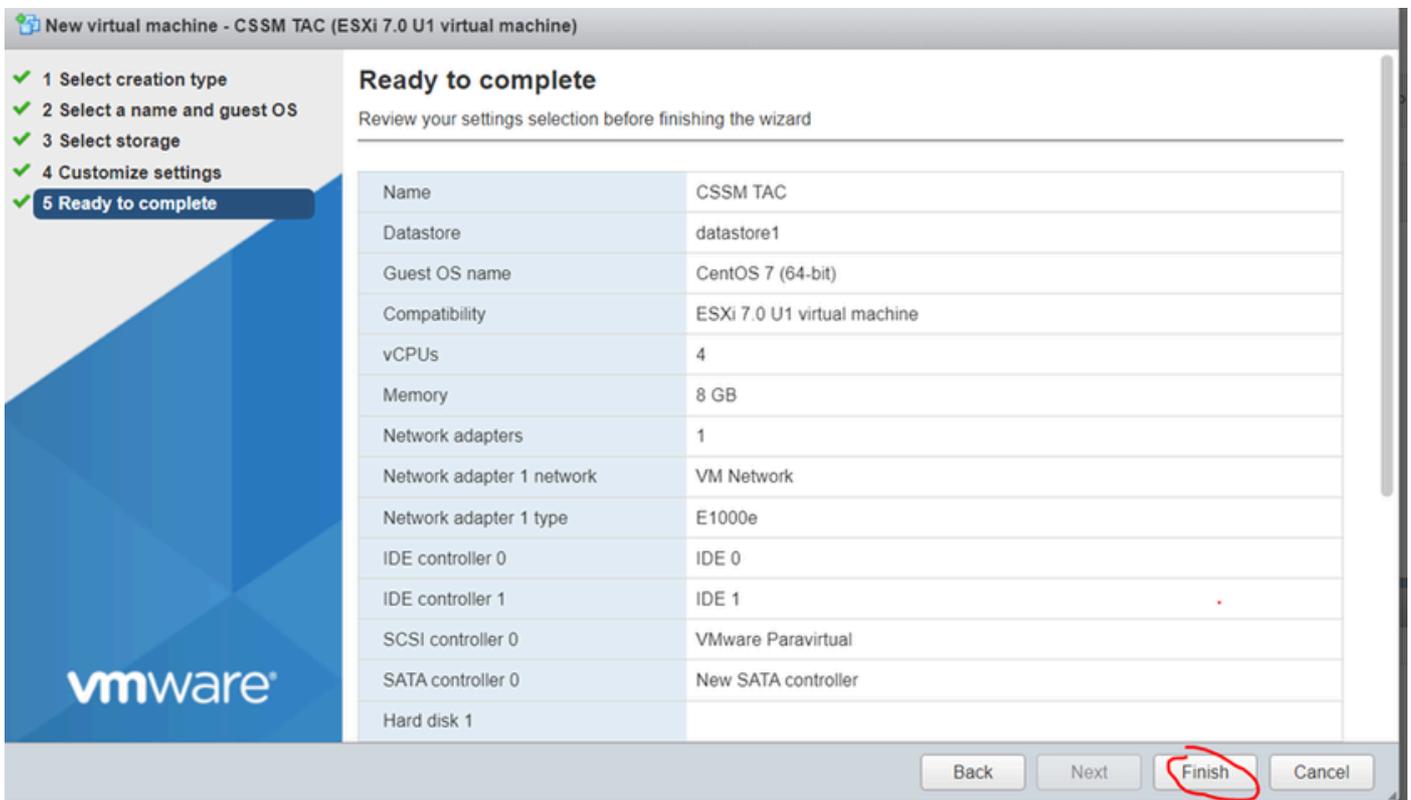
È possibile verificare il riepilogo delle impostazioni dopo aver completato i passaggi precedenti.



Riepilogo configurazione VM 01

Fare clic su Next (Avanti).

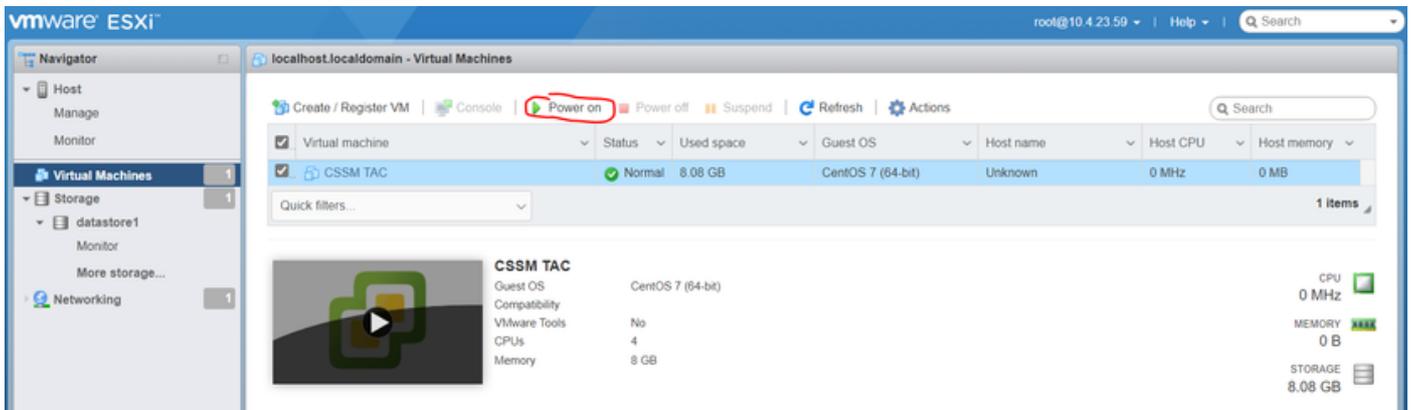
10. Fare clic su Fine.



Riepilogo configurazione VM 02

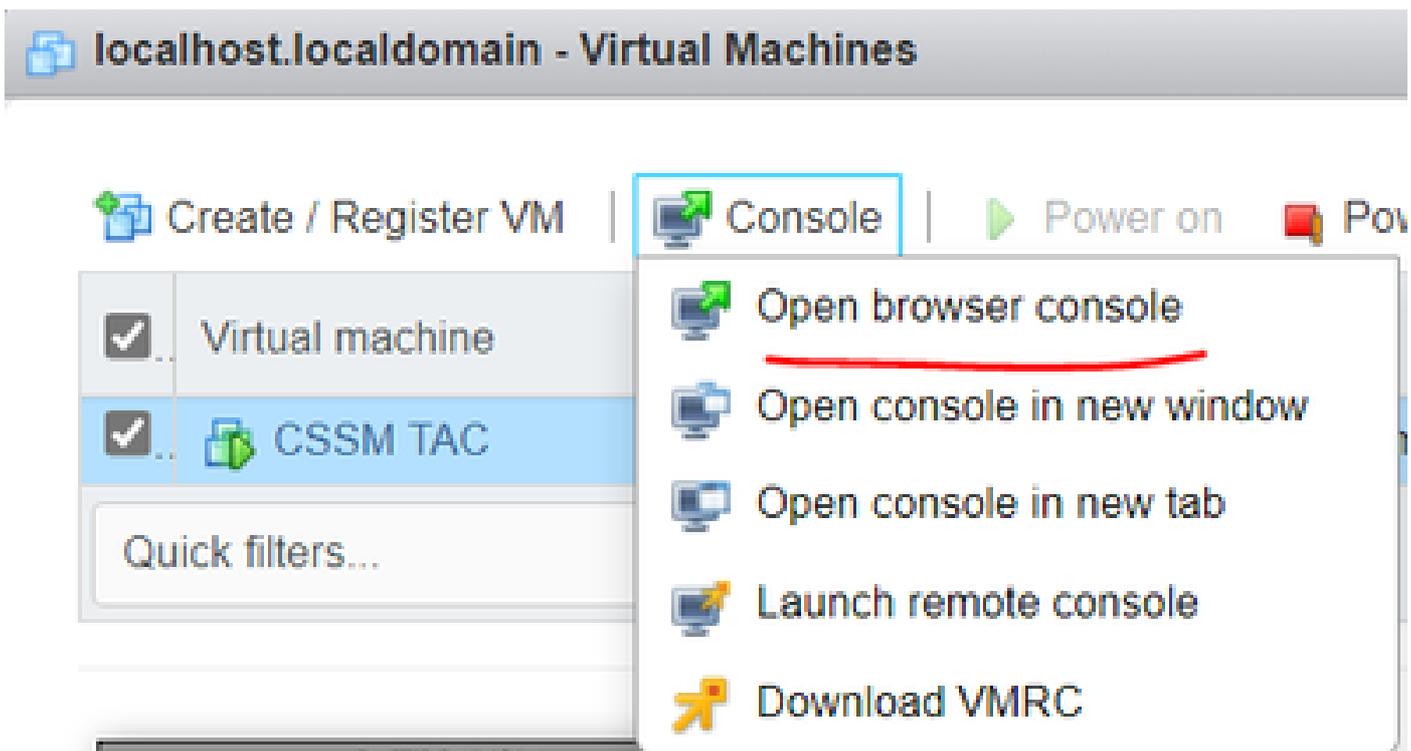
## Configurazione iniziale di CSSM locale.

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



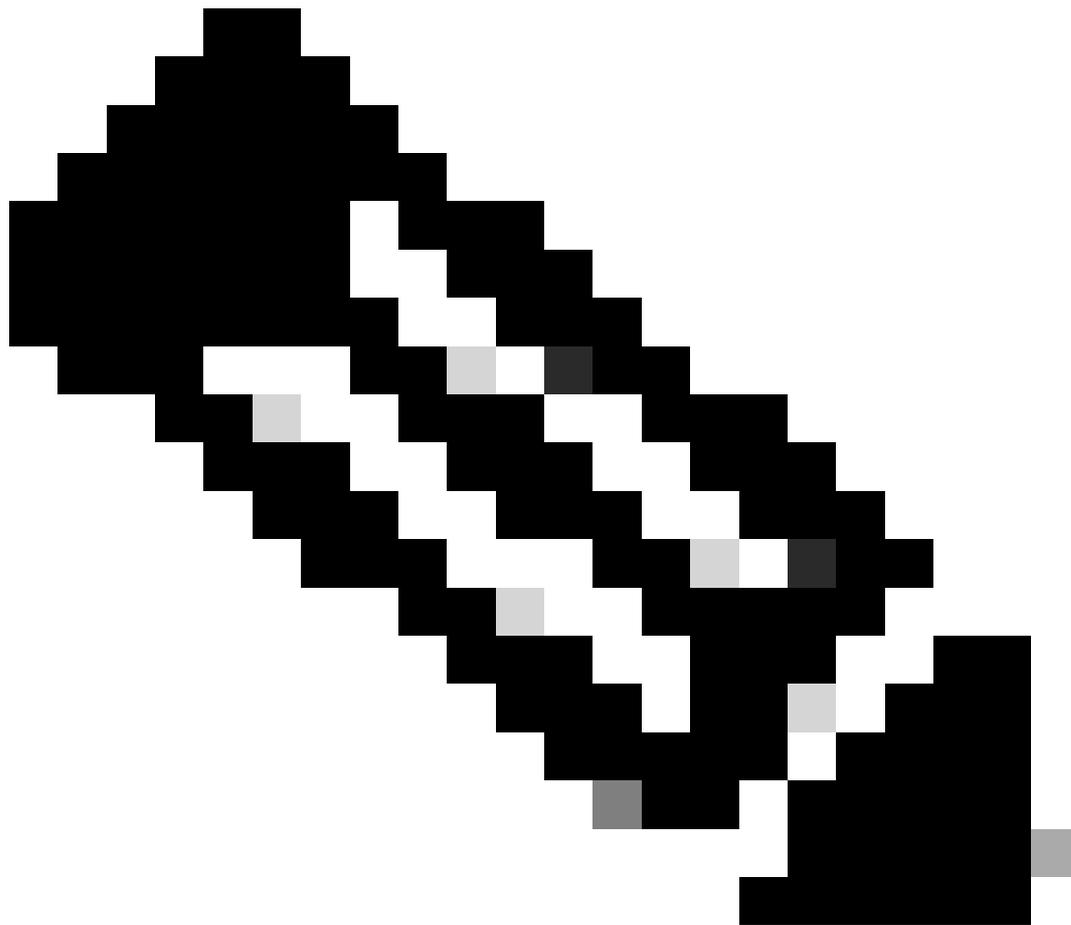
Opzione di accensione

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



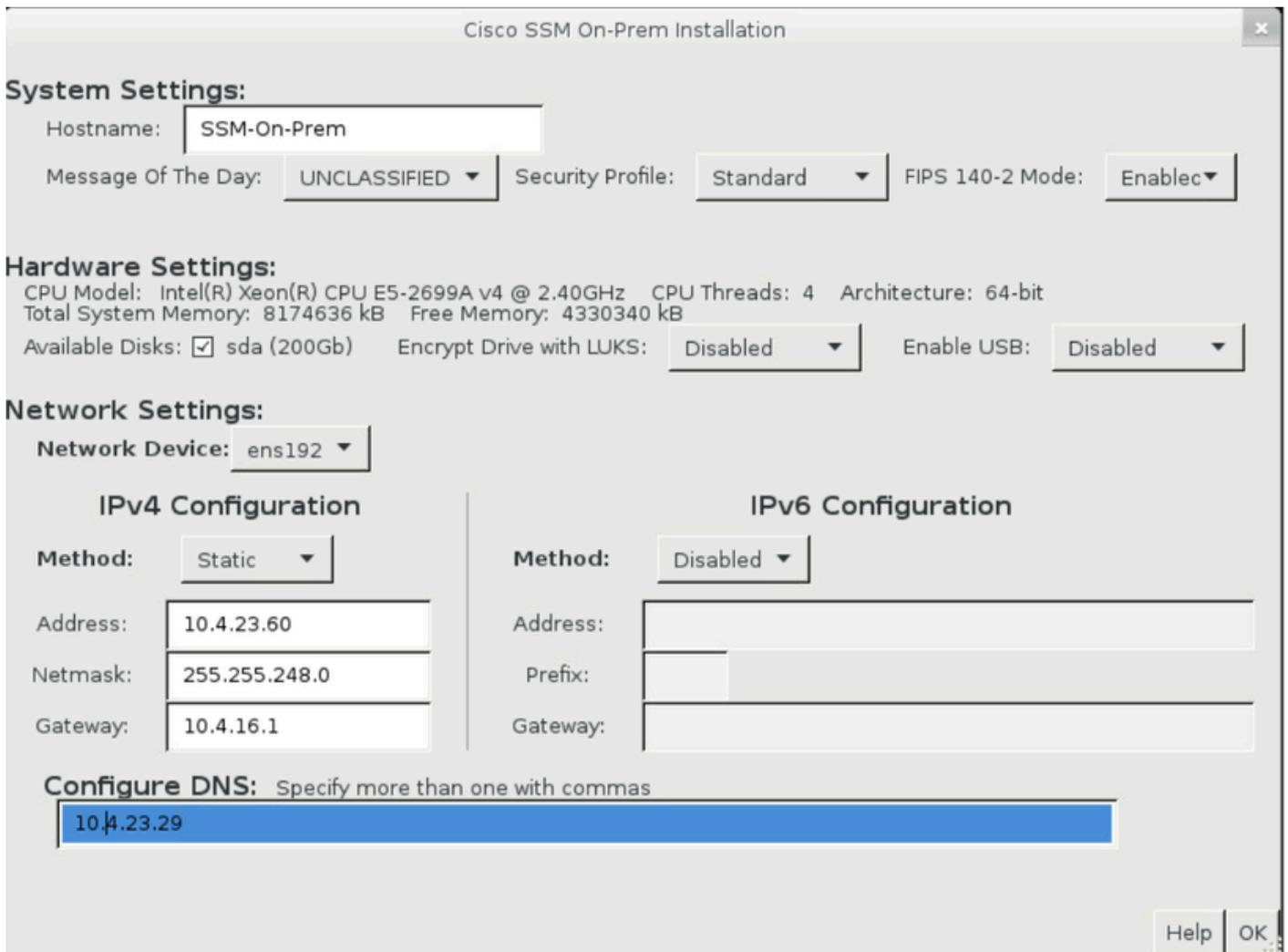
Opzioni per la gestione della VM

3. Configurare le impostazioni di rete.



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

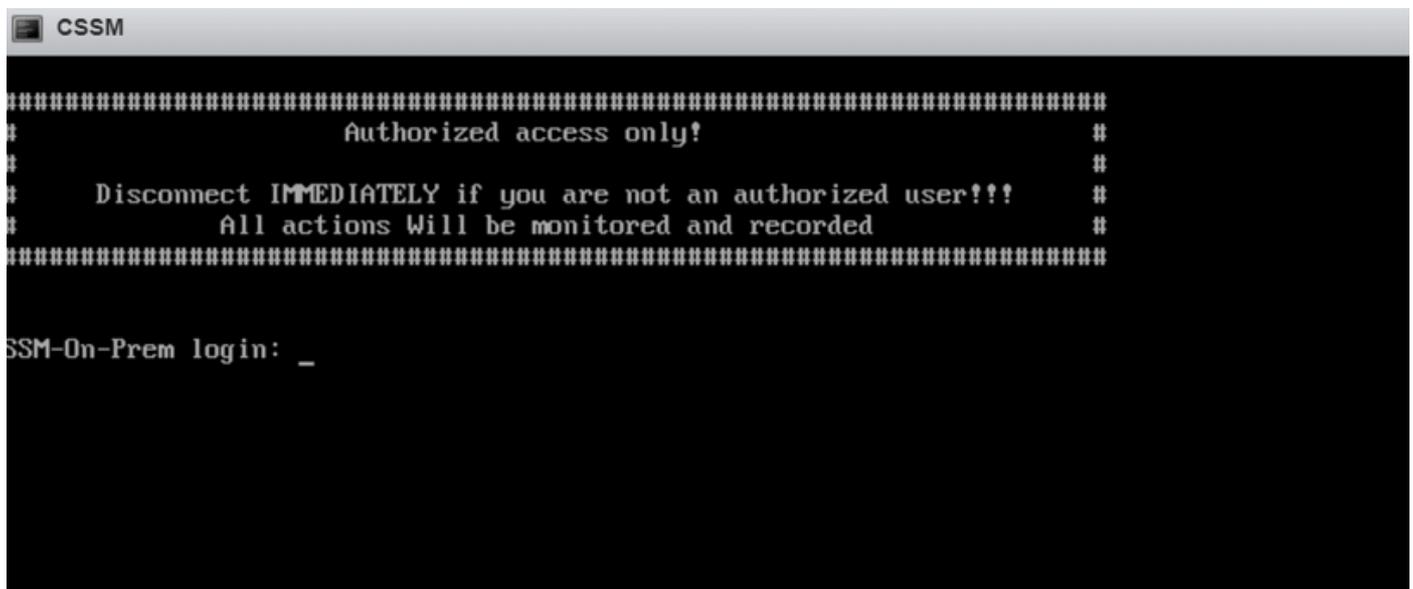
---



Configurazione delle impostazioni di rete CSM

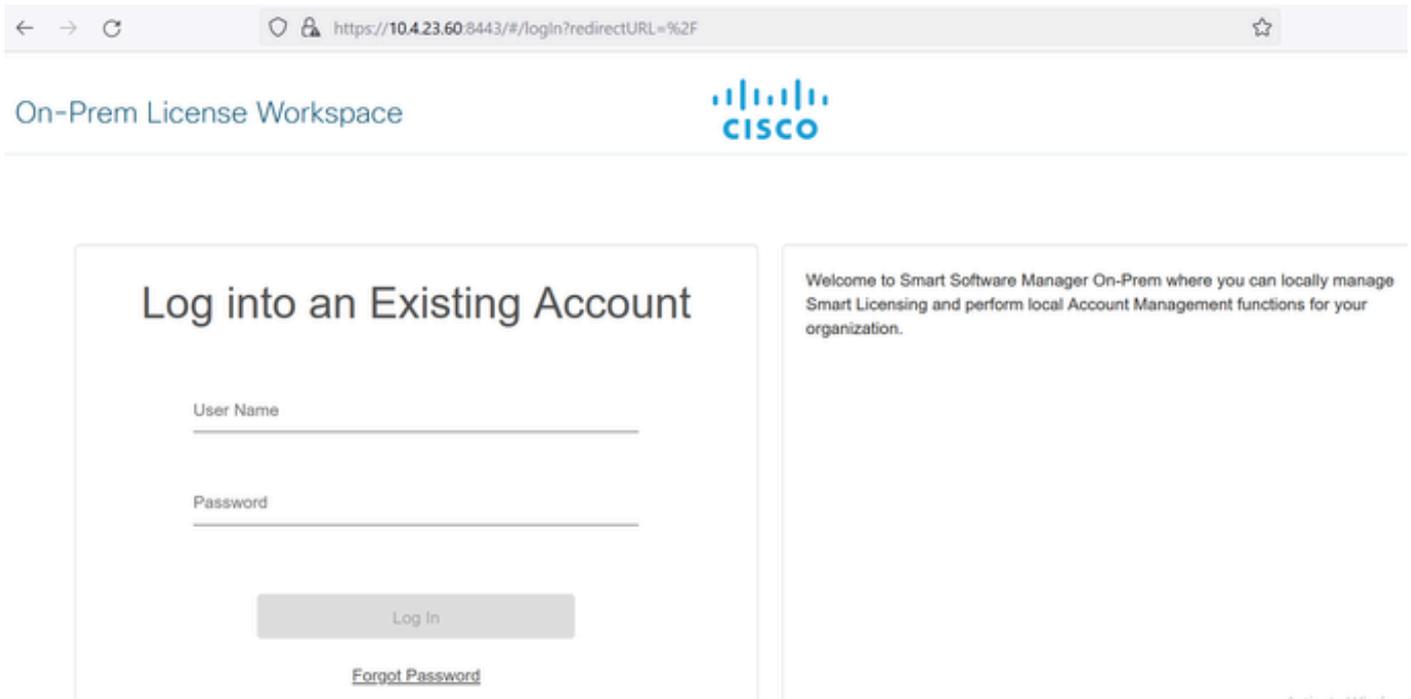
Fare clic su Ok per configurare la nuova password CLI.

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.

# Welcome to Cisco Smart Software Manager On-Prem

STEP 1 System Language Selection    STEP 2 Temporary Password Reset    **STEP 3 Host Common Name**    STEP 4 Review and Confirm

Products that support String SSL Cert Checking require the SSM On-Prem's "Host Common Name" to match the "destination" URL address. For example:

- Products using Smart Transport must use both the "license smart url" configuration and the "cssm.testlab.local" value in the URL string.
- Legacy products using Smart Call Home must use both the "destination address http" configuration and the "cssm.testlab.local" value in the URL string.

**If the above URLs do not match expectations, refer to the SSM On-Prem AdminWorkspace -> Security Widget to change the Host Common Name to the correct value.**

The option to configure alternative names (SAN) is available in Admin Console under Security -> Certificates and can be configured after the initial setup.

\* Host Common Name

cssm.testlab.local

Back Next

Configurazione nome comune host

## 9. Convalidare la configurazione e fare clic su Applica.

STEP 1 System Language Selection    STEP 2 Temporary Password Reset    STEP 3 Host Common Name    **STEP 4 Review and Confirm**

Once you click "Apply", you will be redirected to the login page where you will need to login with your new password. Please ensure you have securely stored your password for future logins.

### Review and Confirm

Language Selected: English  
Password Reset: Yes  
Host Common Name: sccmtac.ciscotac.com

Back Apply

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.

--	--

<p>Smart Software Manager</p> <p>Track and manage your licenses. Convert traditional licenses to Smart Licenses.</p> <p><b>Manage licenses &gt;</b></p>	<p>Download and Upgrade</p> <p>Download new software or updates to your current software.</p> <p>Access downloads &gt;</p>	<p>Traditional Licenses</p> <p>Generate and manage PAK-based and other device licenses, including demo licenses.</p> <p>Access LRP &gt;</p>
<p>Manage Smart Account</p> <p>Update your profile information and manage users.</p> <p>Manage account &gt;</p>	<p>EA Workspace</p> <p>Generate and manage licenses purchased through a Cisco Enterprise Agreement.</p> <p>Access EA Workspace &gt;</p>	<p>Manage Entitlements</p> <p>eDelivery, version upgrade, and more management functionality is now available in our new portal.</p> <p>Access MCE &gt;</p>

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.

The screenshot shows the Cisco Software Central interface. At the top, there is a navigation bar with the Cisco logo and search icons. Below it, a yellow banner displays a "Scheduled Downtime Notification" for License Registration Portal (LRP), Manage Smart Account & Account Administration, Plug-N-Play (PnP), and Smart Software Manager. The main content area is titled "Smart Software Licensing" and includes a breadcrumb "Cisco Software Central > Smart Software Licensing". A dropdown menu shows "InternalTestDemoAccount67.cisco.com". Below this, there are tabs for "Alerts", "Inventory", "Convert to Smart Licensing", "Reports", "Preferences", "On-Prem Accounts", and "Activity". The "Inventory" tab is selected. Underneath, there is a dropdown for "Virtual Account: AAA MEX TEST". At the bottom, there are tabs for "General", "Licenses", "Product Instances", and "Event Log". The "General" tab is active, showing a "Virtual Account" section with the following details:

Description:	Only for tests
Default Virtual Account:	No

Pagina Software Cisco

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

## Smart Software Manager On-Prem



**License**

Smart Licensing  
Track and manage Smart Licensing



**Administration**

[Request an Account](#)  
Get an Account for your organization. The Account must be approved by your System Administrator or System Operator before it can be used.

[Request Access to an Existing Account](#)  
Submit a request for access to an existing local Account. Approval must be granted by a Smart Account Administrator for your local Account.

[Manage Account](#)  
Modify the properties of your Accounts and associate existing User IDs with Accounts.

Menu principale CSSM.

5. Quindi selezionare Conti.

# On-Prem Admin Workspace

---

## Smart Software Manager On-Prem



Access  
Management



Settings



Accounts



Support  
Center



API Toolkit



Synchronization



Network



Users



Security

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.

## Account Registration

X

### Enter SSO Credentials

Username \*

otegoma@cisco.com

Password \*

●●●●●●●●●●

Submit

Approva.

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

## Account Registration

X

### Review Account Requests

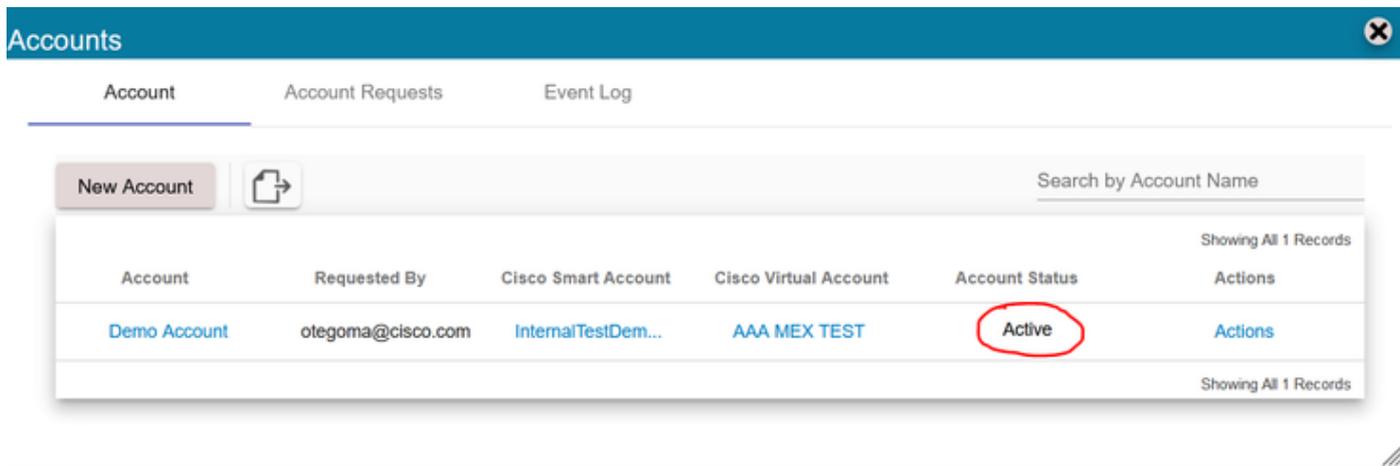
<b>Account Name</b>	Demo Account
<b>Cisco Smart Account</b>	InternalTestDemoAccount67.cisco.com ▼
<b>Cisco Virtual Account</b>	AAA MEX TEST ▼ ⓘ
<b>Requestor Email</b>	otegoma@cisco.com
<b>Request Date</b>	2023-Jul-27 15:00:31
<b>Message to Approver</b>	

Cancel

Next

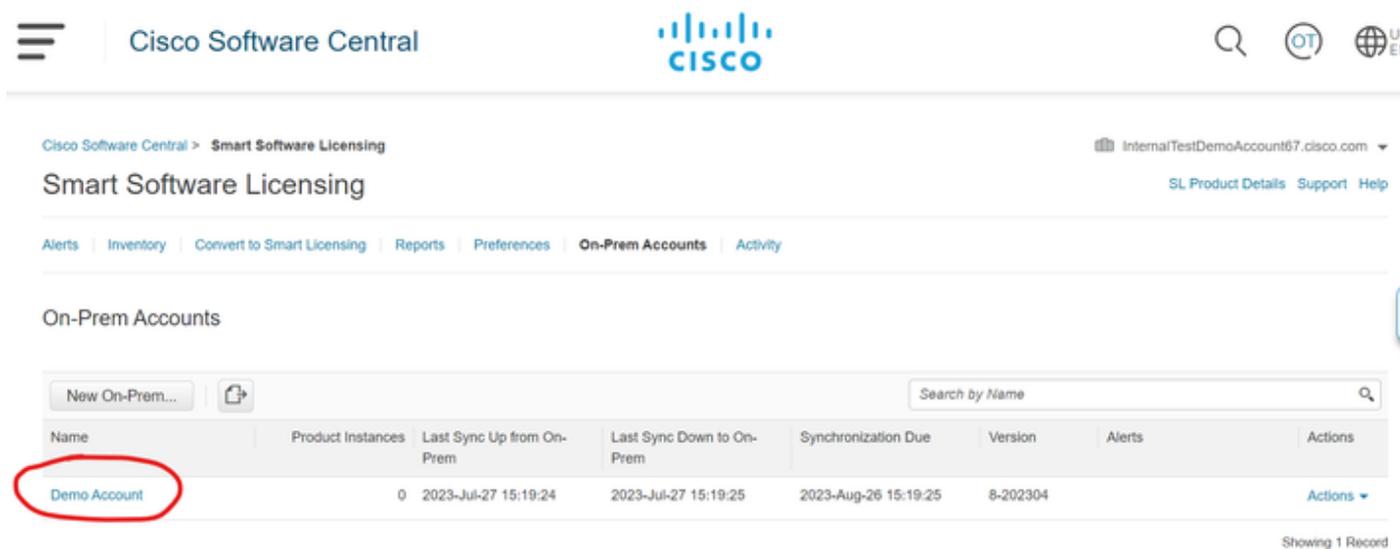
Registrazione account.

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.

## Manual Registration



1. Generate an Account Registration File using the button below and save the file to your PC

[Generate Registration File](#)

2. Register the Account with your Smart Account on Smart Software Manager

- Log into Cisco Smart Software Manager
- Navigate to the "Satellites" section of Smart Software Licensing and click the "New satellite..." button
- When prompted, upload the Account Registration File
- An Account Authorization File will be generated. Download the file to your PC

3. Upload this Account Authorization File below

Browse...

Upload

Registrazione manuale.

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

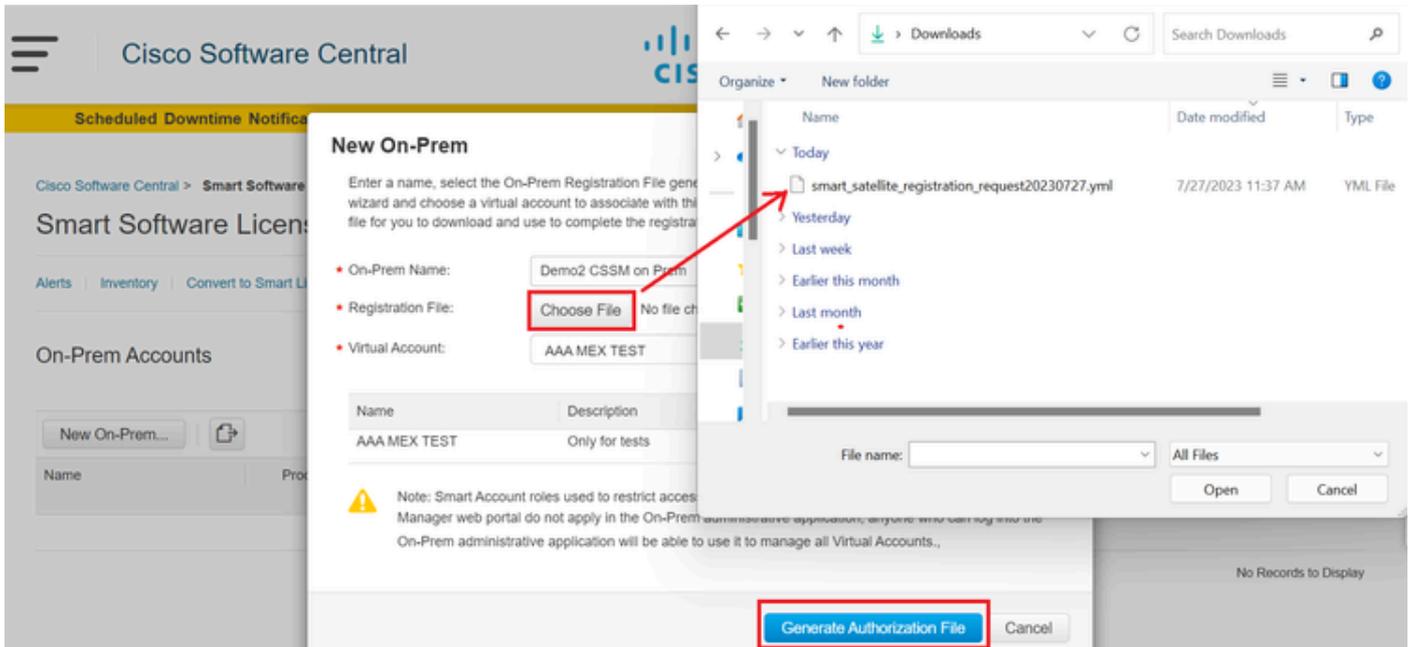
Fare clic su Nuovo in locale

The screenshot shows the Cisco Software Central interface. At the top, there is a navigation bar with the Cisco logo and the text 'Cisco Software Central'. Below this, the 'Smart Software Licensing' section is visible, with a breadcrumb trail 'Cisco Software Central > Smart Software Licensing'. The 'On-Prem Accounts' section is active, showing a table with columns for Name, Product Instances, Last Sync Up from On-Prem, Last Sync Down to On-Prem, Synchronization Due, Version, Alerts, and Actions. A 'New On-Prem...' button is circled in red. The table currently displays 'No Records Found'.

Aggiunta di nuovi elementi locali.

Configurare quindi i parametri successivi:

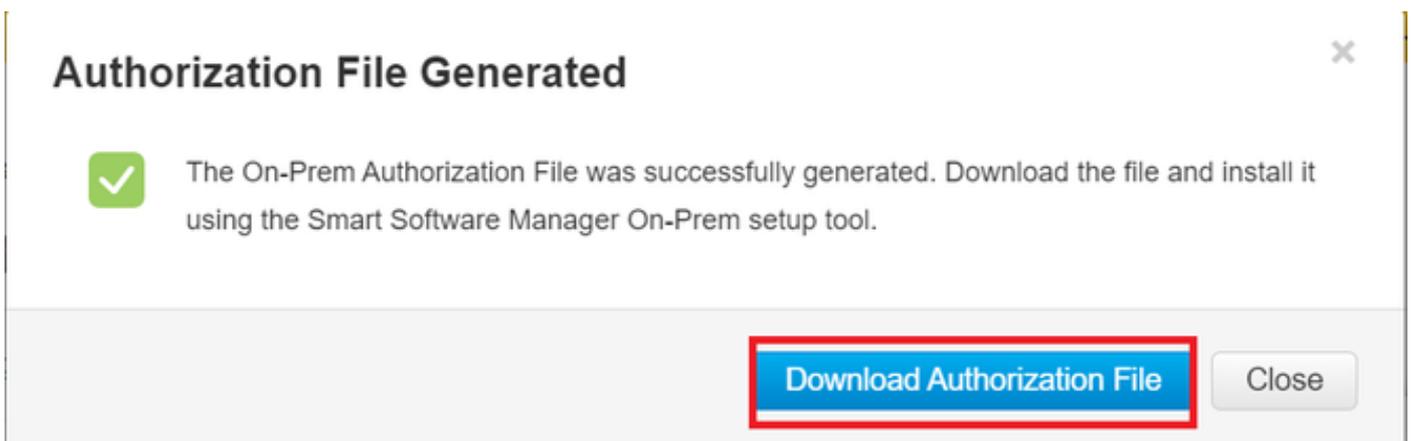
- Nome locale: nome personalizzato del nuovo registro.
- File di registrazione: fare clic su Scegli file e selezionare la richiesta di registrazione.
- Account virtuale: incollare il nome dell'account virtuale.



File di autorizzazione.

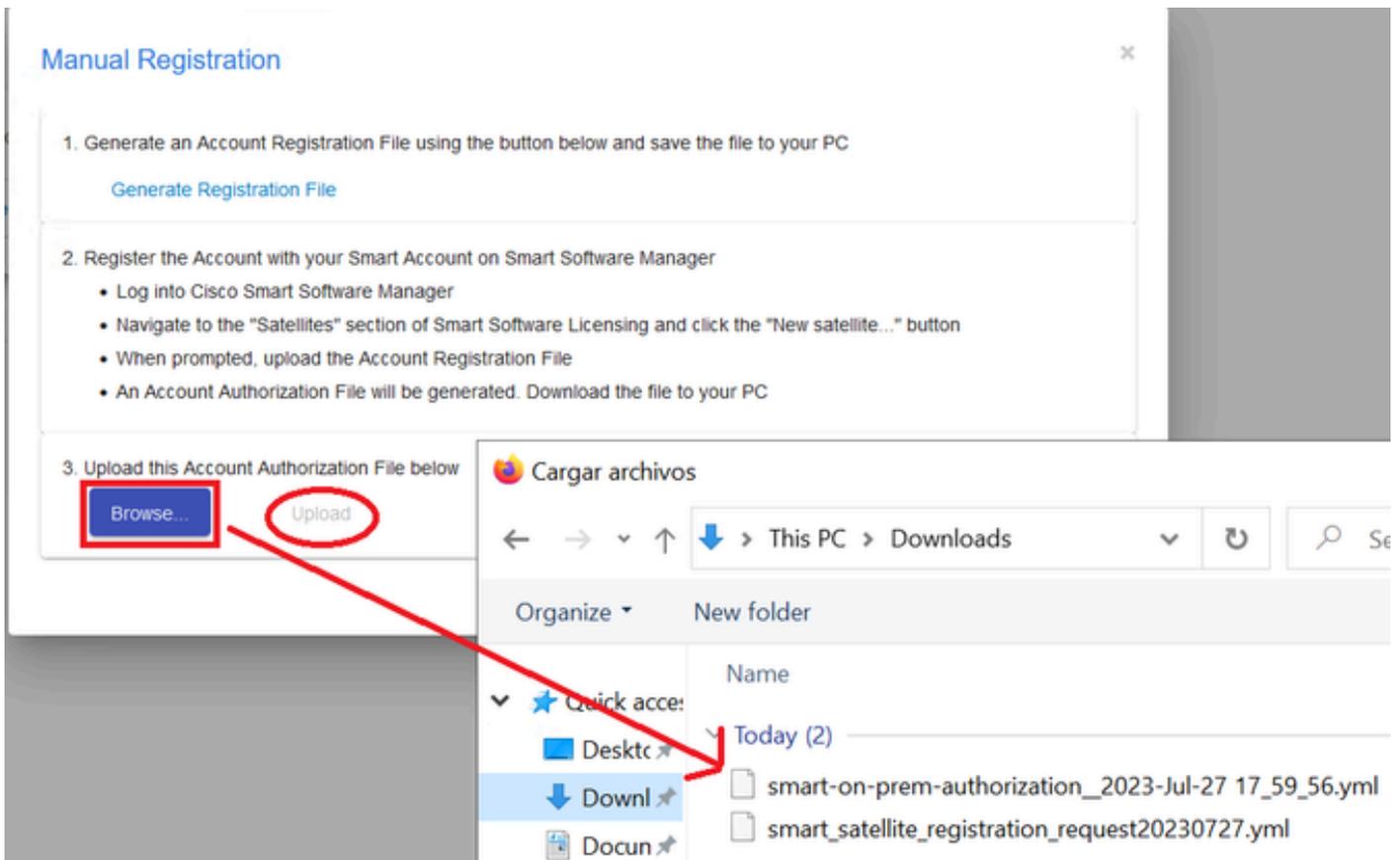
E fare clic su Genera file di autorizzazione.

Scaricare quindi il file di autorizzazione.



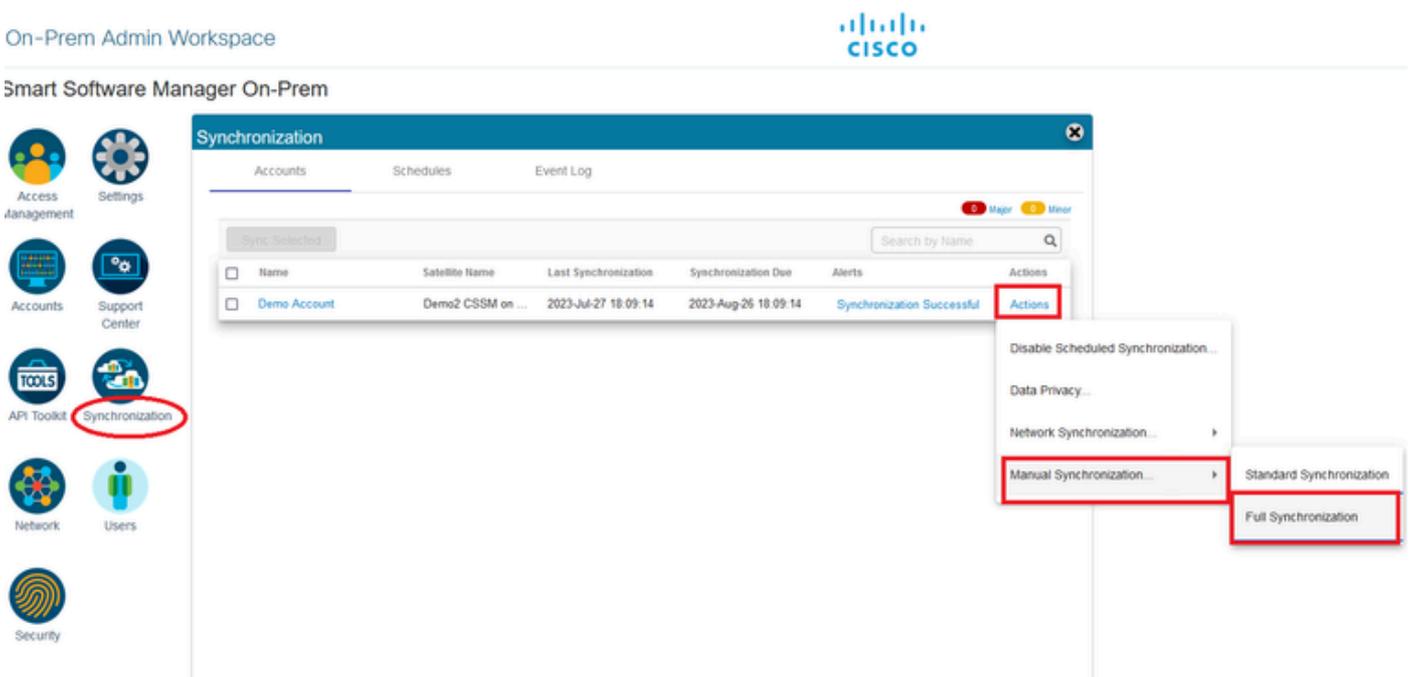
Download del file di autorizzazione.

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.



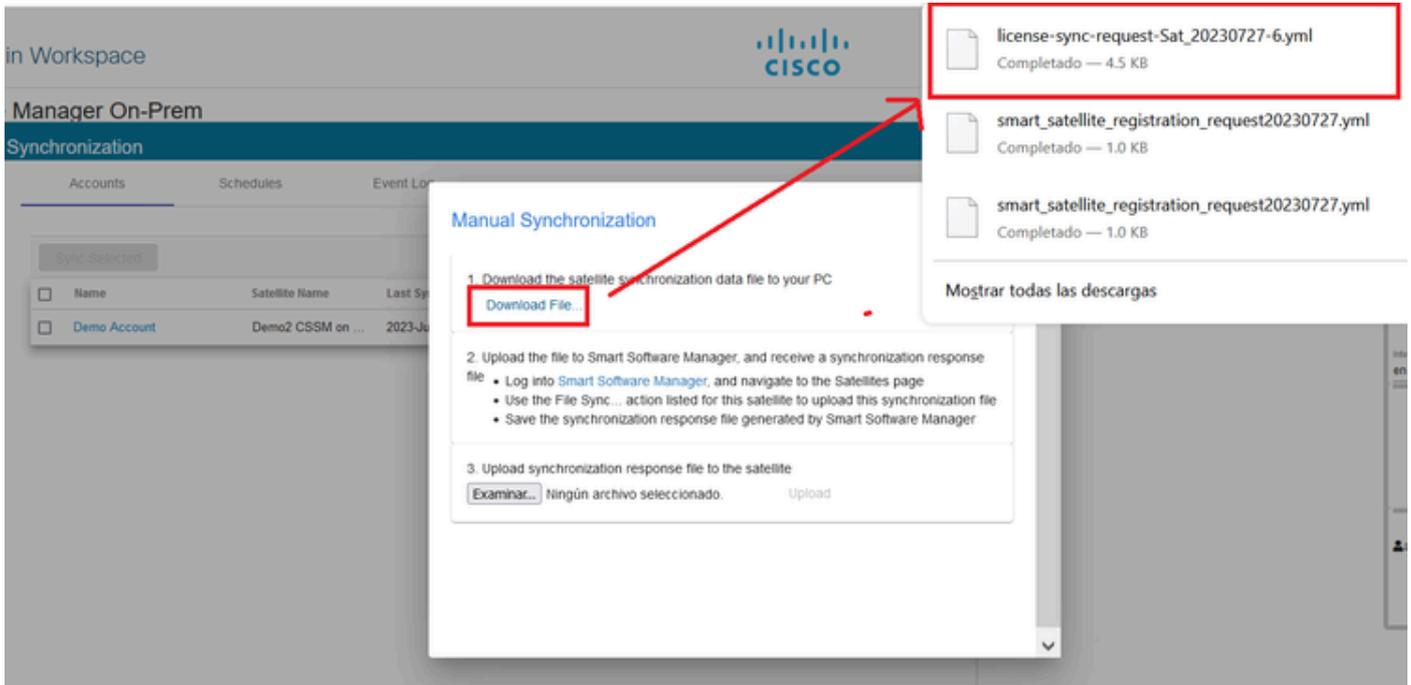
Caricamento del file di autorizzazione.

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



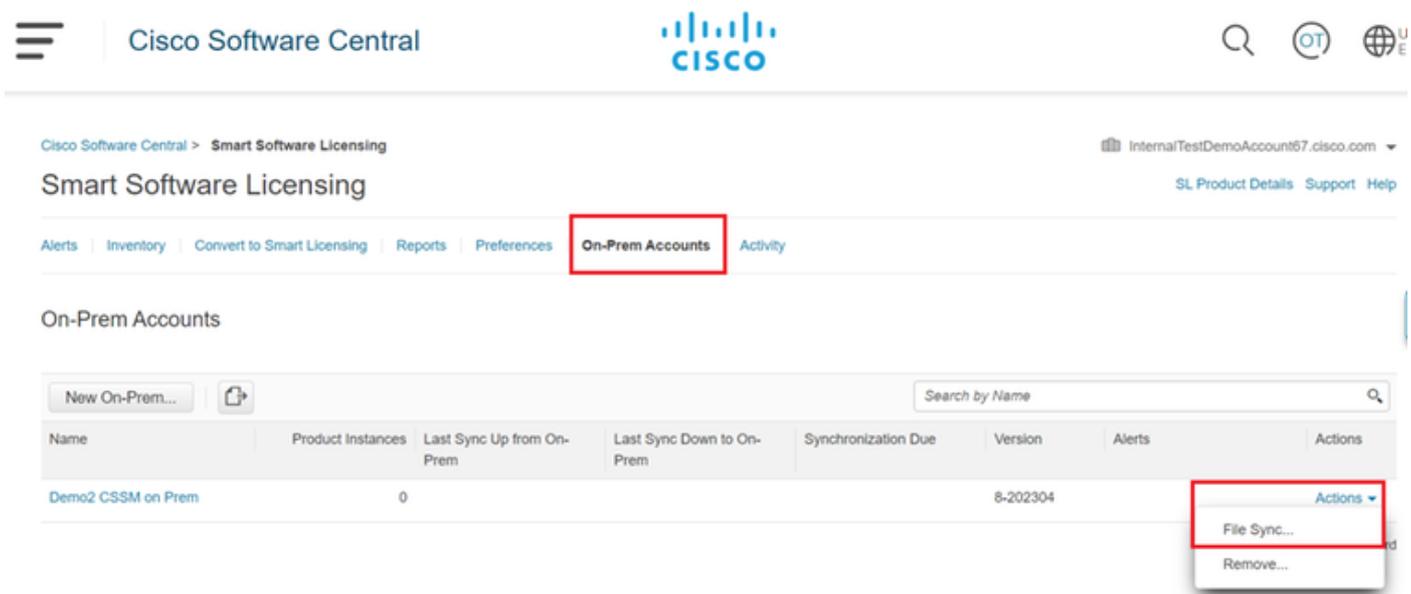
Sincronizzazione manuale

Scaricare il file di richiesta Sync.



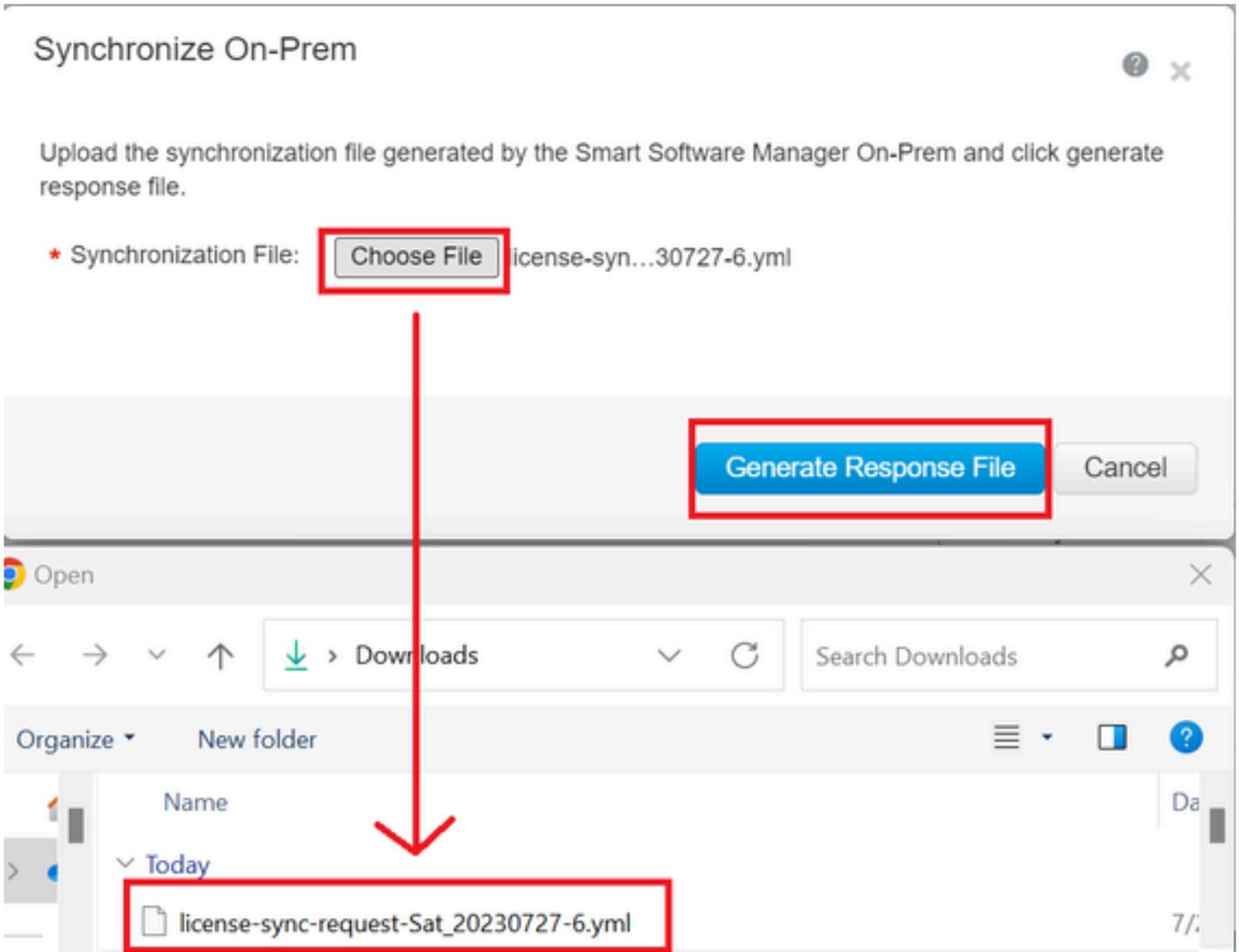
Scaricamento file in corso.

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



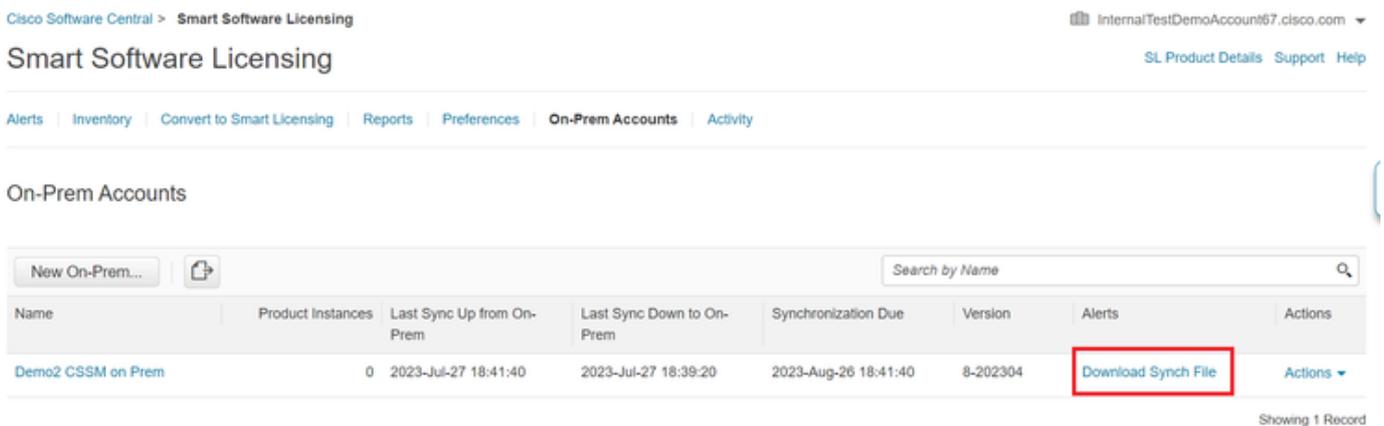
Caricamento file in corso. Sincronizza.

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



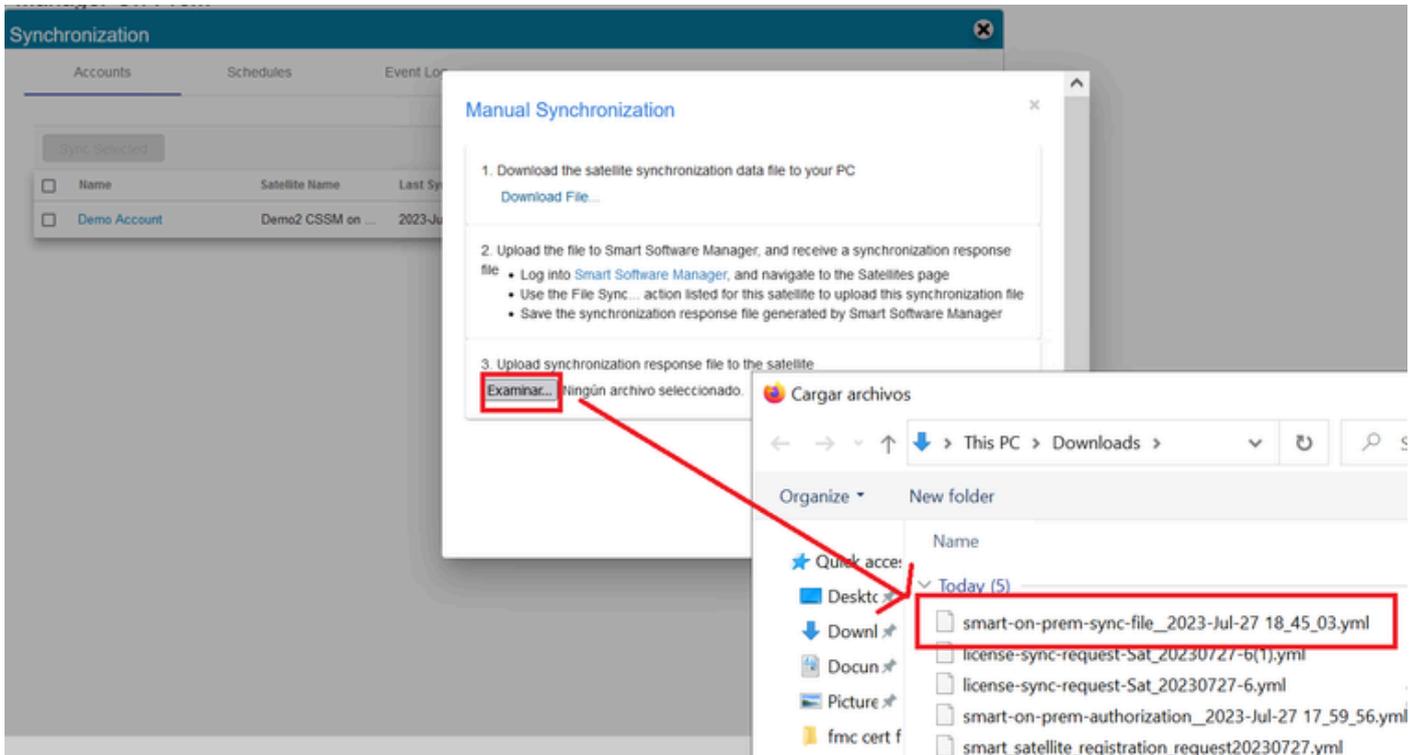
Generare un file di risposta.

Quindi fare clic su Scarica file di risposta di sincronizzazione



Sincronizza file.

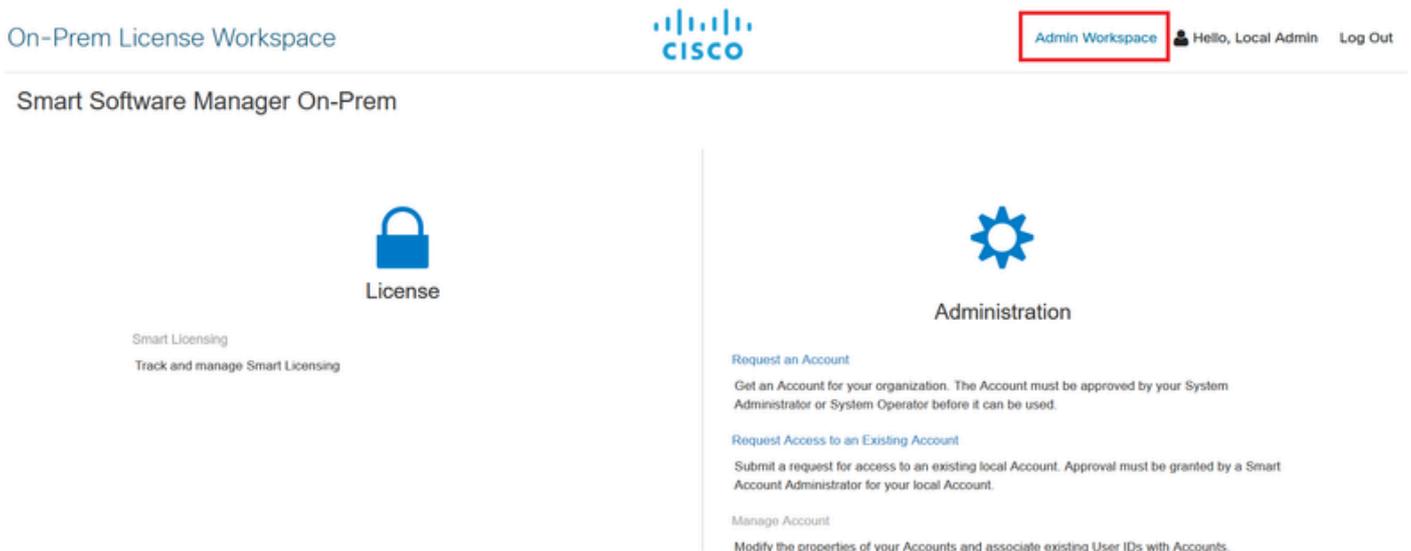
Infine, caricare il file di risposta Synch nel CSM in sede.



Sincronizzazione completata.

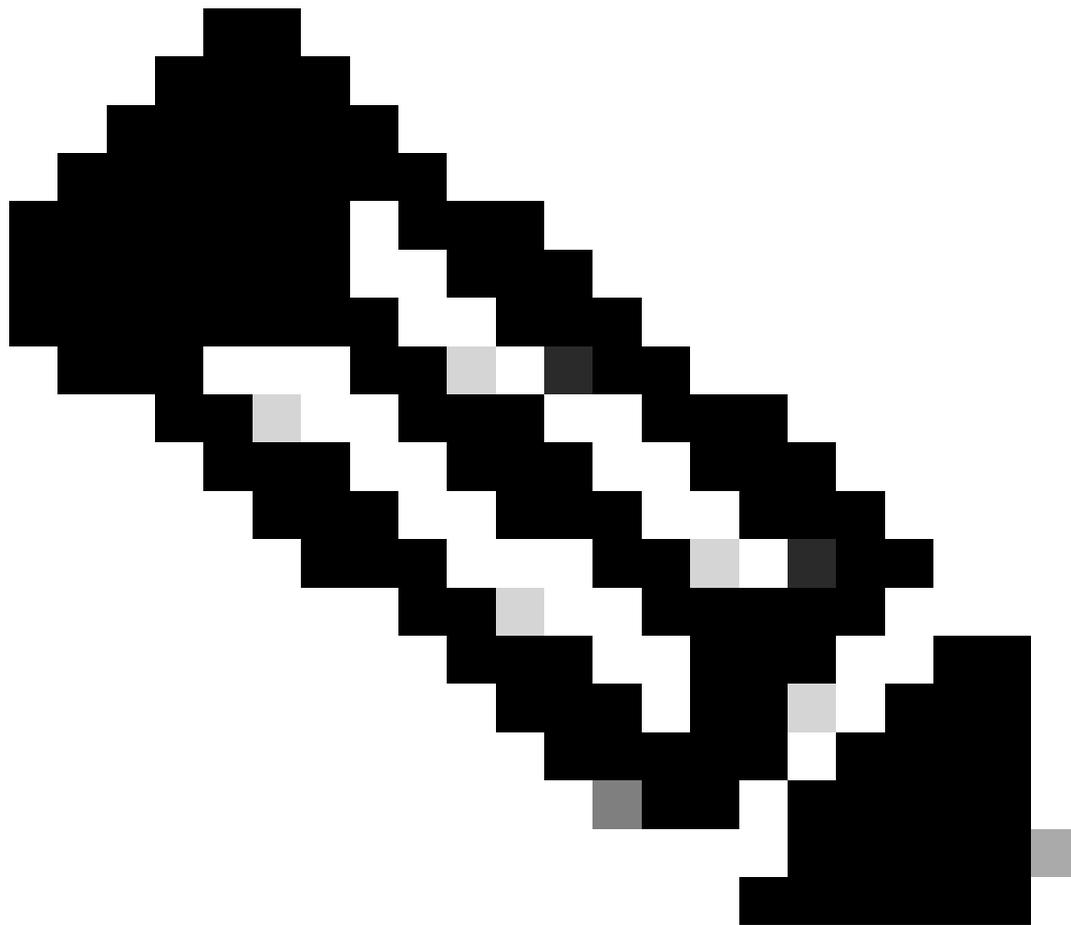
## Integrazione di CSM On-Prem con ISE.

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



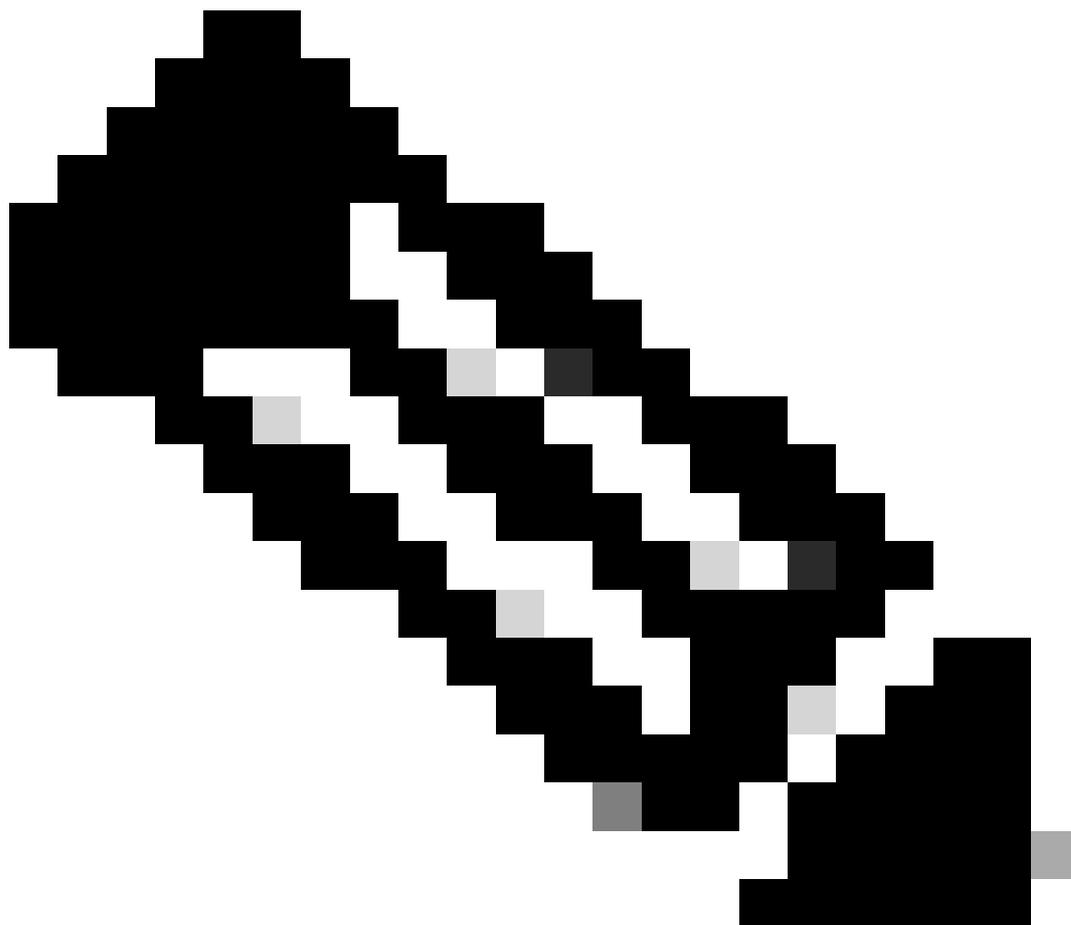
Menu principale CSSM.

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.

---

Security

Account Password Certificates Event Log

Product Certificate

Host Common Name  
cssm.testlab.local

Subject Alternative Name

Save

NOTE: The Host Common Name is typically composed of Host + Domain Name(FQDN) and will look like "www.yoursite.com" or "yoursite.com". The SSL Server Certificate used for product communications is specific to the Common Name that has been issued at the Host. Therefore, the Common Name must match the Web address you will use to configure the Cisco Product when connecting to SSM On-Prem. The Common name is a part of the Subject Alternative Name by default. If you change the Common Name or add Subject Alternative Name, you must resynchronize your Local Account in order for Cisco to issue a new product certificate(TG cert).

Browser Certificate

Add Generate CSR

localhost  
(Default Certificate) EXPIRATION DATE: 2025-JUL-16

CA Certificates

Add

Description	Subject	Expires On	Created	Actions
No Records Found				

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.

## Generate CSR

Common Name	<b>cssm.testlab.local</b>
Organizational Unit	<b>Testlab</b>
Country	<b>Mexico</b>
State/Province	<b>Mexico City</b>
City/Locality	<b>Mexico City</b>
Organization	<b>SEC AAA</b>
Key Size	<b>2048</b>
Subject Alternative Name	<b>cssm.testlab.local</b>

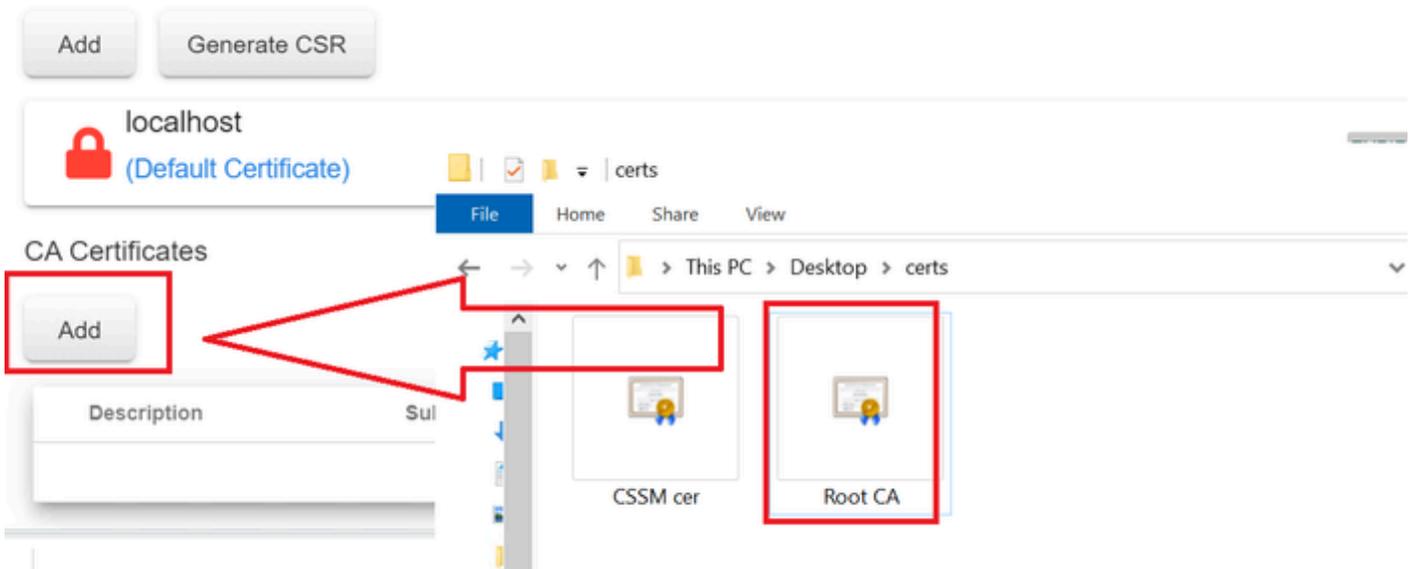
**Generate**

Cancel

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.

## Browser Certificate



Caricamento della CA radice.

Fare clic su Continua.



Please note that if you are uploading **LDAP Server Certificate**, it is mandatory to reboot your SSM On-Prem server for the certificate to take effect and thus allowing secure communication with the server.

Below are the commands for non-HA(standalone) deployments:

1. Execute "reboot" command in Onprem-console  
ssh admin@<IP>  
onprem-console  
reboot

For HA deployments

1. Execute reboot command on active node in onprem-console. After failover, ensure that DB replication has started. If you wish to restore the previous active node, execute another reboot, after verifying replication has started.

The active node is the node that is serving the virtual IP of the cluster.

Proceed

Opzione Continua.

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

## Upload Certificate

\* Description:

\* Certificate:

CA radice descrizione.

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

Browser Certificate

localhost  
(Default Certificate)

CA Certificates

File Home Share View

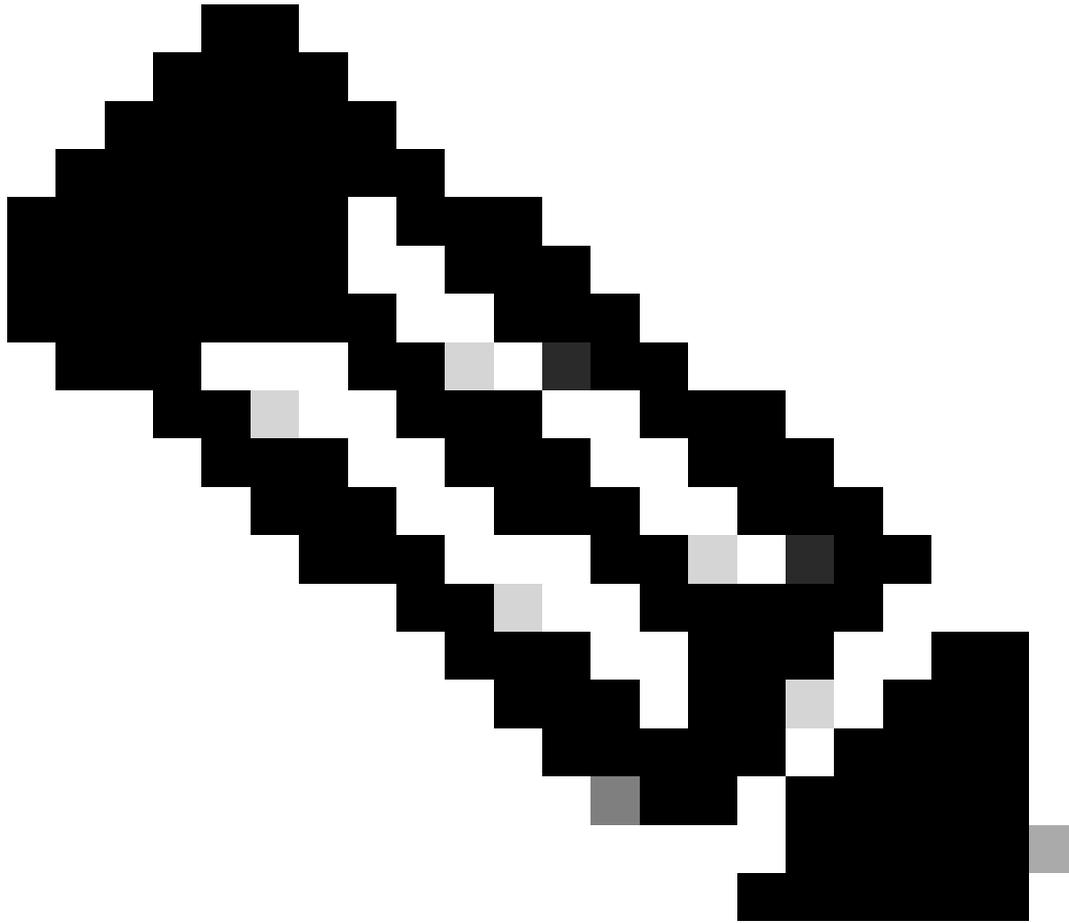
Desktop > certs

2 items

Search by Description

Description	Subject	Expires On	Created	Actions
RootCA	/DC=com/DC=ciscotac/CN=ci	2026-Jul-24 09:26:34	2023-Jul-30 19:41:06	Actions

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.

#### Browser Certificate

Add

Generate CSR



cssm.testlab.local

EXPIRATION DATE: 2025-JUL-16

#### CA Certificates

Add

Search by Description

Description

Subject

Expires On

Created

Actions

RootCA

/DC=local/DC=testlab/CN=tes 2027-Apr-14 22:51:26

2024-Jul-16 21:18:52

[Actions](#)

Convalida dei certificati.

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

On-Prem Admin Workspace

CISCO

Licensing Workspace Log Out

Smart Software Manager On-Prem

Access Management Network Support Center

Accounts Security Synchronization

API Toolkit Settings Users

System Health

Good Your machine is working well

Server Name SSM-On-Prem  
Version 8-202304  
Uptime 3 days

Resource Monitor Percentage

CPU |  
RAM |  
DISK |

Interface  
ens192 ↑ 6.9 MB/s ↓ 37 KB/s

Recent Alerts

Pagina Workspace.

### 10. passare a Smart Licensing.

On-Prem License Workspace

CISCO

Admin Workspace Hello, Local Admin Log Out

Smart Software Manager On-Prem

Demo Account

License

Smart Licensing  
Track and manage Smart Licensing

Administration

Request an Account  
Get an Account for your organization. The Account must be approved by your System Administrator or System Operator before it can be used.

Request Access to an Existing Account  
Submit a request for access to an existing local Account. Approval must be granted by a Smart Account Administrator for your local Account.

Pagina delle licenze CSM Smart

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

# Smart Licensing

- Alerts
- Inventory**
- Convert to Smart Licensing
- Reports
- Preferences
- Activity

Local Virtual Account: [Default](#)

- General**
- Licenses
- Product Instances
- SL Using Policy
- Event Log

## Local Virtual Account

Description: This is the default virtual account created during company account creation.  
Default Local Virtual Account: Yes

## Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this Local Virtual Account. For products that support Smart Transport, you must configure the "license smart uri" on the product to use the [Smart Transport Registration URL](#). For products that support Smart Licensing Using Policy that use csu as transport, you must configure the "license smart transport csu" to use the [CSLU Transport URL](#). For legacy products that still use Smart Call Home, you must configure the "destination address http" on the product to use the [Smart Call Home Registration URL](#). The recommended method is Smart Transport. Please consult your Products Configuration Guide for setting the destination URL value.

**New Token...**

Nuova opzione token.

## 12. Selezionare Create Token e copiarlo.

### Create Registration Token



This dialog will generate the token required to register your product instances with your Account .

Local Virtual Account: **Default**

Description:

Expire After:  Days  
*Enter a value between 1 and 9999, but Cisco recommends a maximum of 30 days*

Max. Number of Uses:   
*The token will be expired when either the expiration or the maximum uses is reached.*

Allow export-controlled functionality on the products registered with this token

**Create Token** Cancel

Creazione del nuovo token.



## CSSM configuration

Security

Account Password Certificates Event Log

Product Certificate

Host Common Name  
cssm.testlab.local

Subject Alternative Name

Save

NOTE: The Host Common Name is typically composed of Host + Domain Name(FQDN) and will look like "www.yoursite.com" or "yoursite.com". The SSL Server Certificate used for product communications is specific to the Common Name that has been issued at the Host. Therefore, the Common Name must match the Web address you will use to configure the Cisco Product when connecting to SSM On-Prem. The Common name is a part of the Subject Alternative Name by default. If you change the Common Name or add Subject Alternative Name, you must resynchronize your Local Account in order for Cisco to issue a new product certificate(TG cert).

Browser Certificate

Add Generate CSR

cssm.testlab.local EXPIRATION DATE: 2025-JUL-18

## ISE configuration

Connection Method  
SSM On-Prem server

SSM On-Prem server Host  
cssm.testlab.local

Note: Cisco Support Diagnostics will not work with SSM On-Prem server registration.

Tier  
 Essential  Advantage  Premier  Device Admin

Virtual Appliance  
 ISE VM License

This enables the ISE features for the purchased licenses to be tracked by Cisco Smart Licensing.

By clicking Register you will agree to the Terms&Conditions. You can download Terms&Conditions on [Smart Licensing Resources](#).

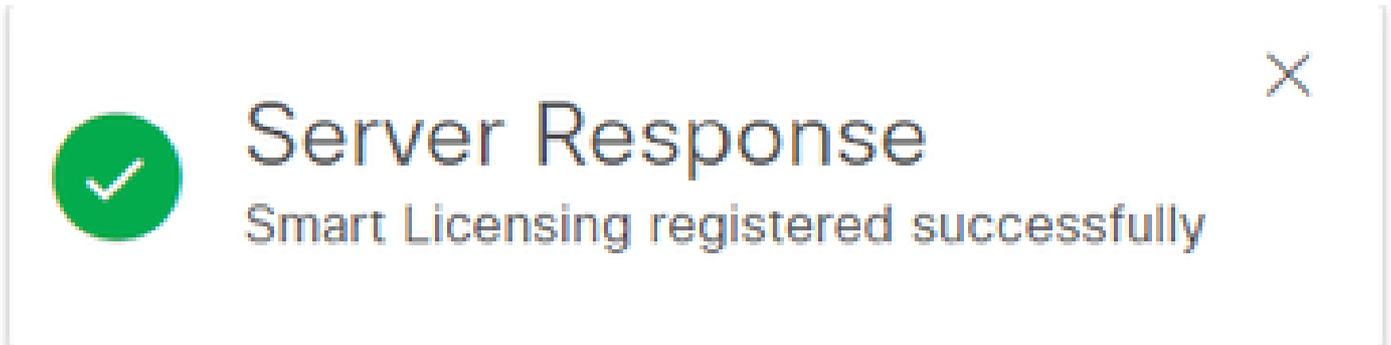
Cancel Register

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.

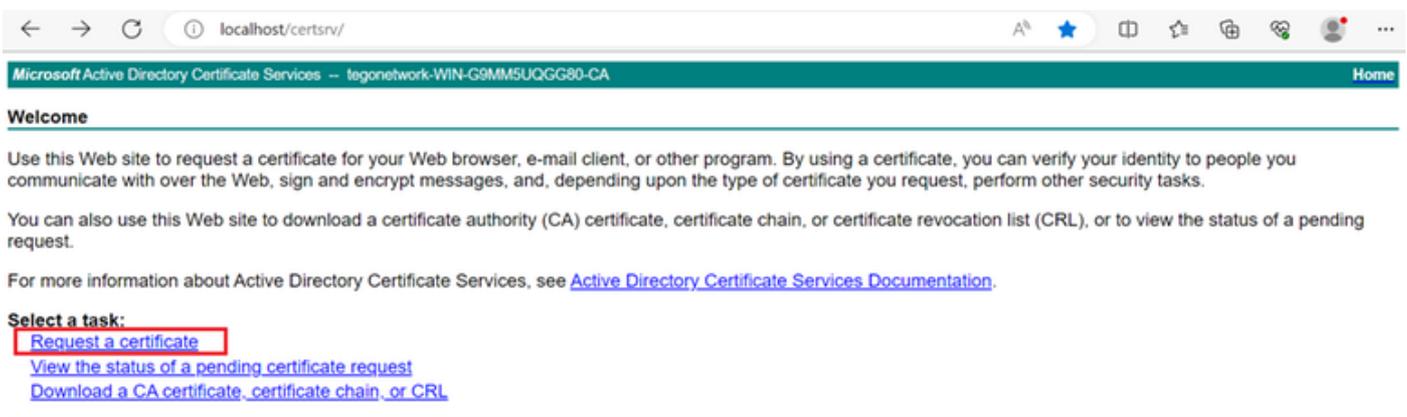


Registrazione completata.

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).



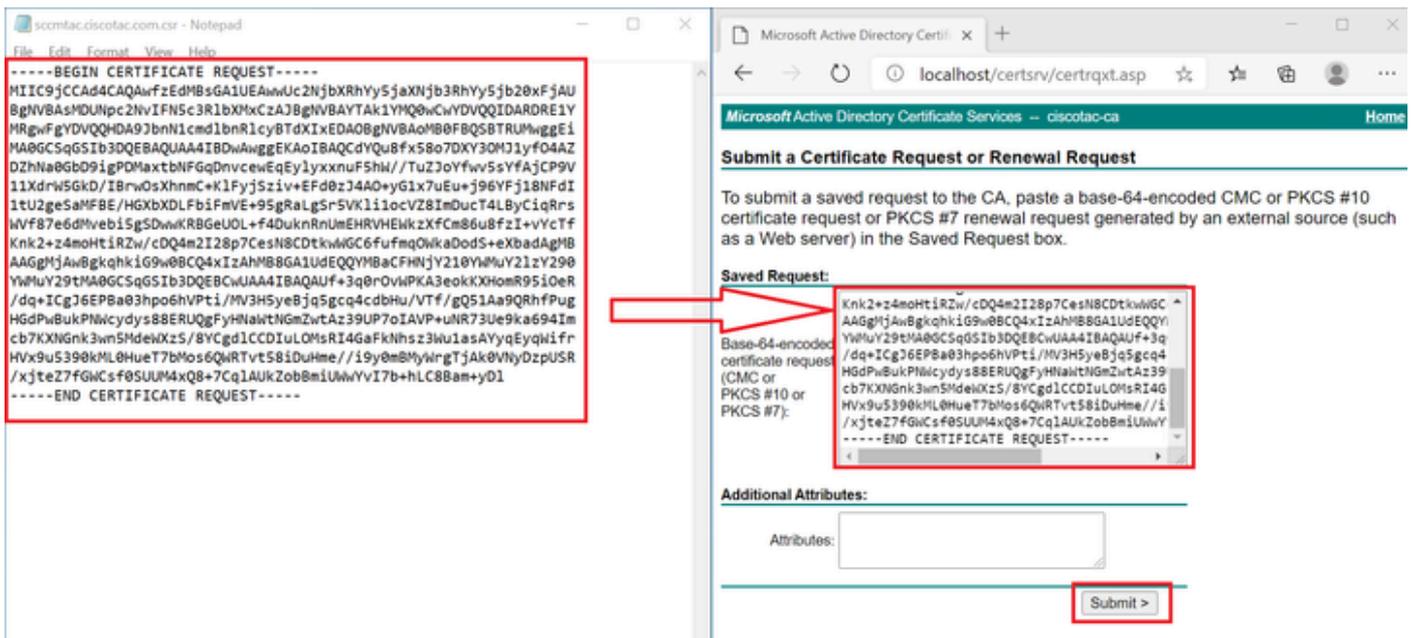
Richiedi certificato.

3. Fare clic su Richiesta avanzata certificati.



Richiesta avanzata di certificati.

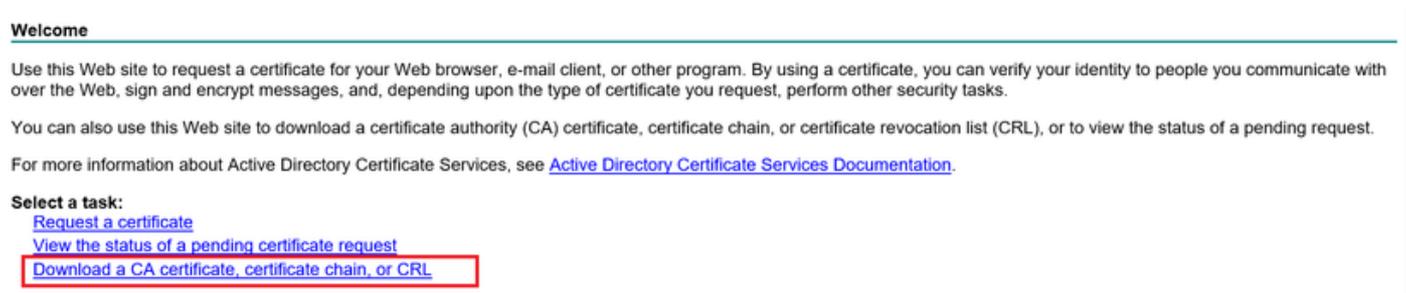
4. Aprire il CSR generato in precedenza. Copiare quindi le informazioni e incollarle su Richiesta salvata.



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.

## Download a CA Certificate, Certificate Chain, or CRL

---

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [ciscotac-ca]

Encoding method:

DER  
 Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

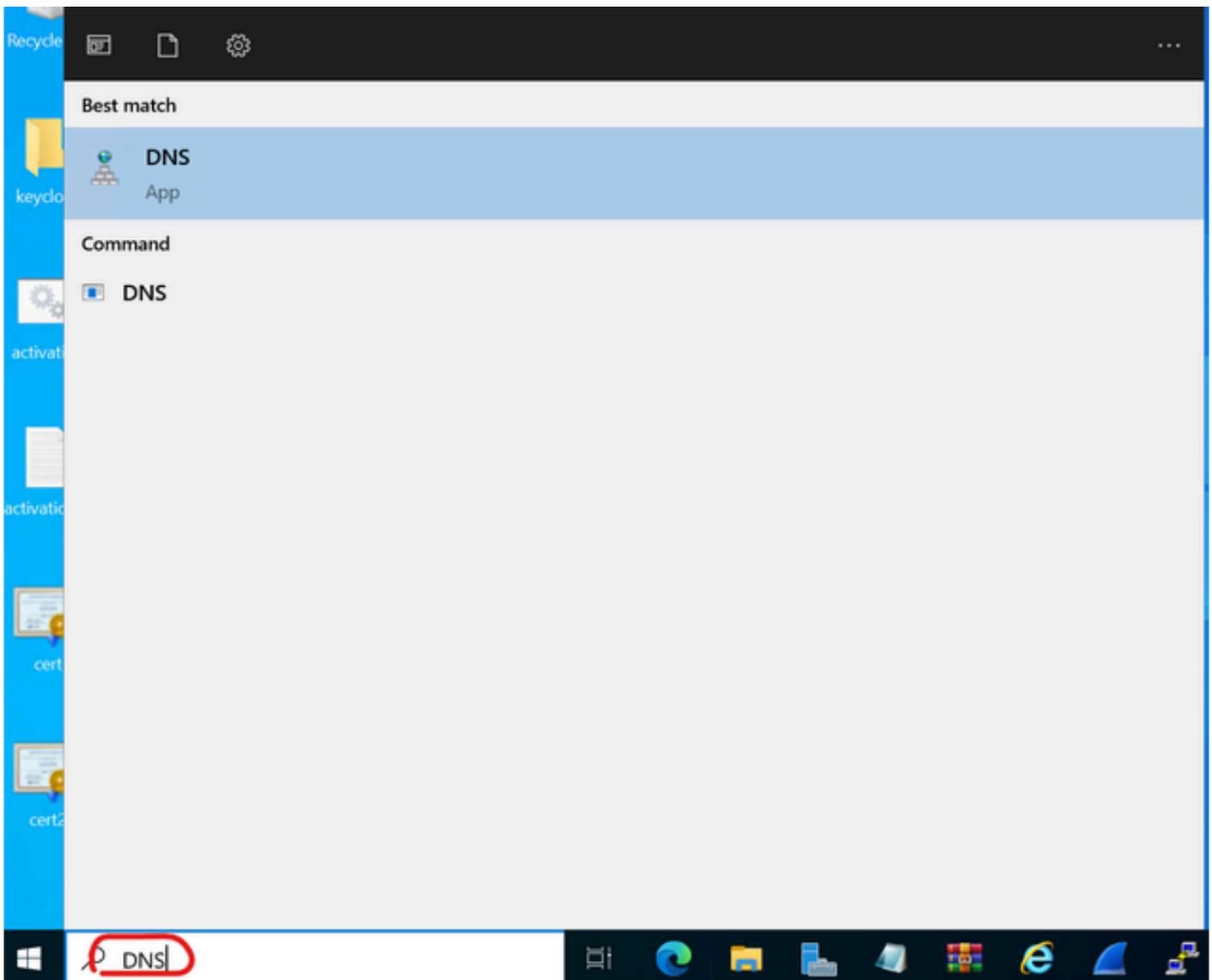
---

Base 64.

Aggiungere record DNS in Windows Server.

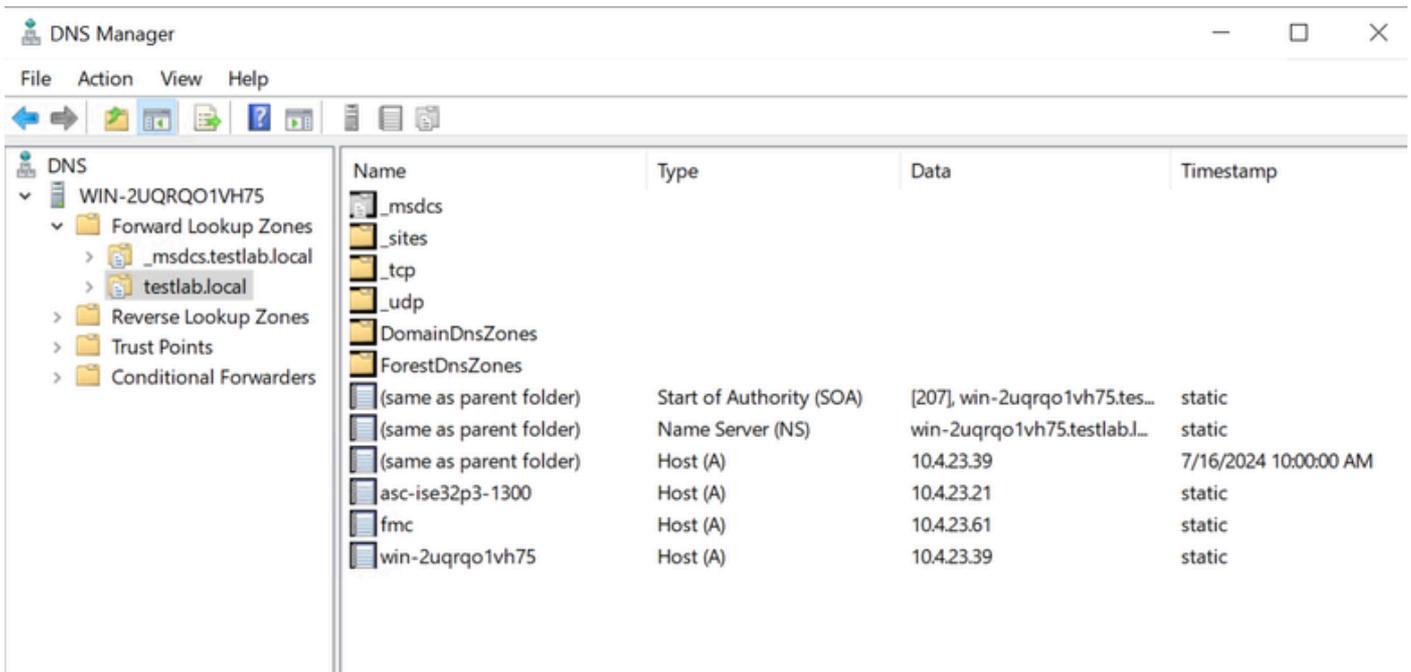
Se l'utente è l'amministratore, aggiungere gli FQDN ISE e CSM.

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.



Gestore DNS.

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).