

Configure CSSM on Prem and Register Licenses with ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Install CSSM On-Prem on VMWARE ESXi](#)

[Initial Configuration of CSSM On-Prem](#)

[Integrate CSSM On-Prem with Smart Account](#)

[OPTION 1: Register your CSSM On-Prem through Internet connection](#)

[OPTION 2: Register your CSSM On-Prem without an Internet connection](#)

[Integrate CSSM On-Prem with ISE](#)

[Create certificates from Windows CA](#)

[Add DNS records on Windows Server](#)

[Troubleshoot](#)

[Host/IP Address is not reachable.\(Error on ISE\)](#)

[SSO service: Unable to reach Cisco.\(Error on CSSM On-Prem\)](#)

[The Common Name in the CSR is not a DNS-resolvable hostname or IP address. please try again.\(Error on CSSM On-Prem\)](#)

Introduction

This document describes the integration of **CSSM On-Prem** with **Cisco Identity Service Engine (ISE)** and **Cisco Smart Account**, ensuring a seamless setup.

Prerequisites

Requirements

ISE **3.X**

Cisco Smart Software Manager(CSSM) **Version 8** Release **202304 +**

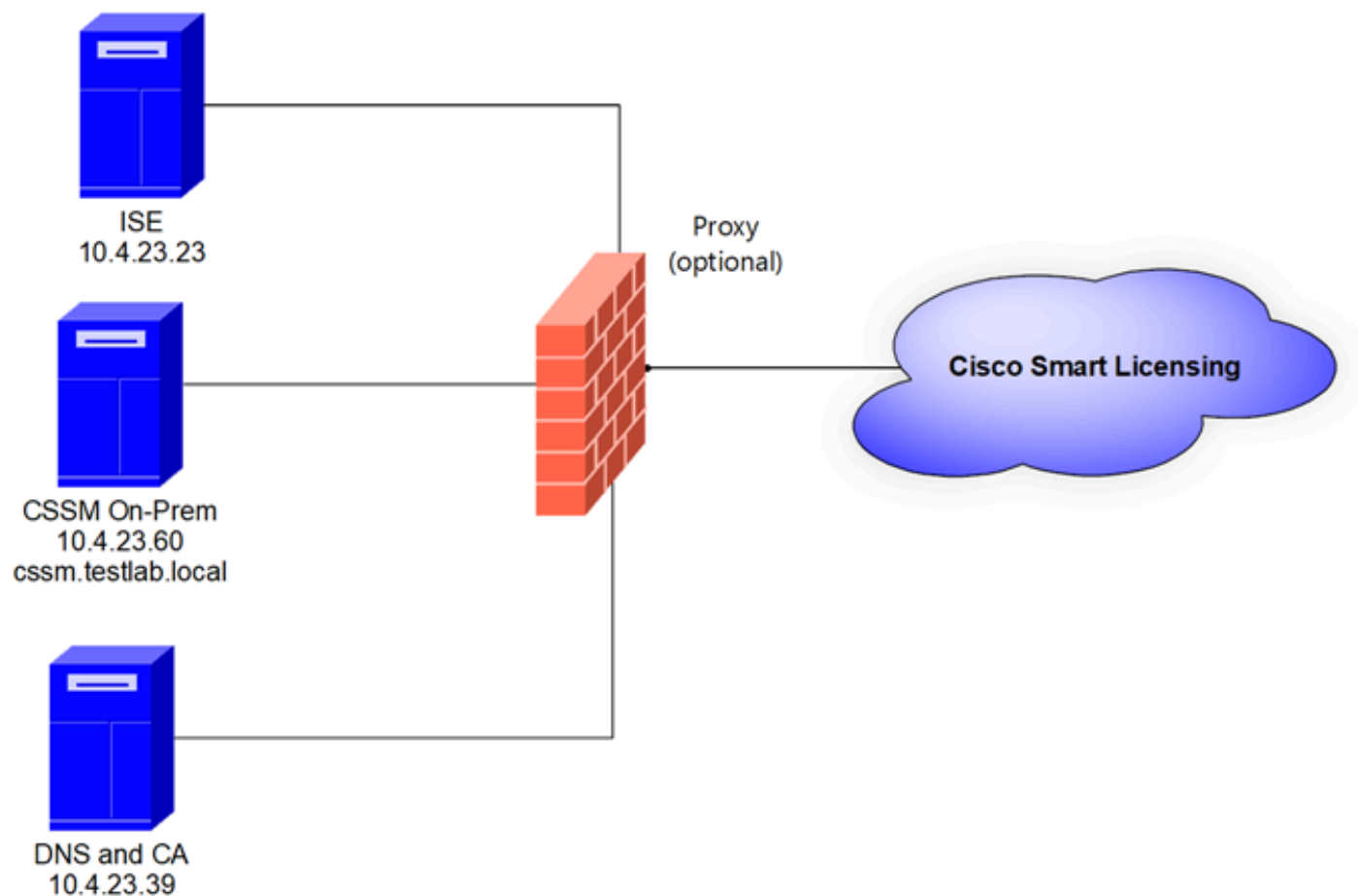
Components Used

- Identity Service Engine **3.2 patch 2**
- SSM On Prem **8.20234**
- Windows Active Directory 2016 (**DNS** and **Certificate Authority** services)
- VMWare ESXi **version 7**

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



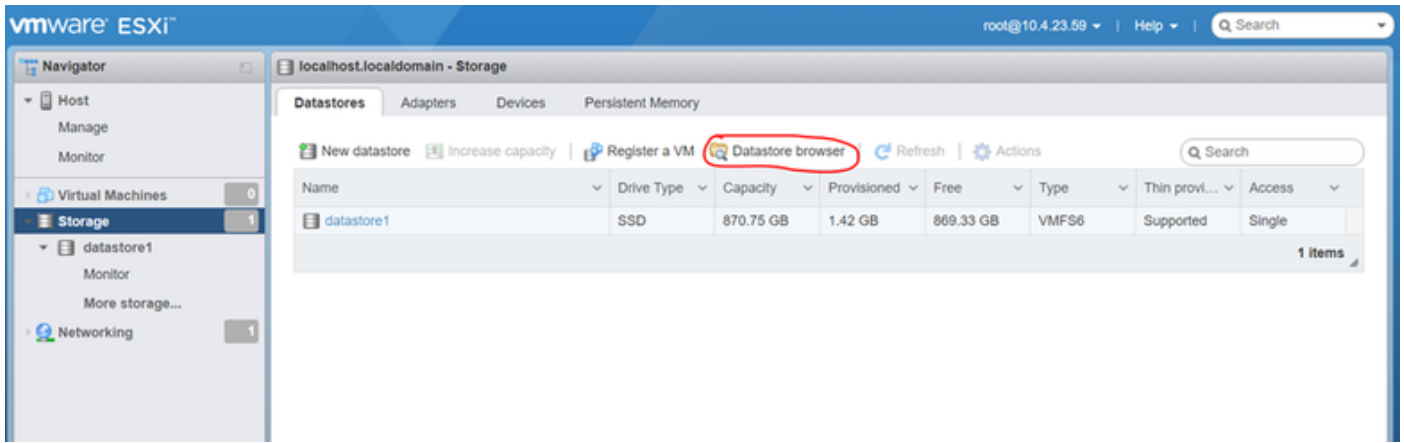
General topology

Install CSSM On-Prem on VMWARE ESXi.

1. Download the **Cisco IOS®**. You can use the next link: <https://software.cisco.com/download/home/286285506/type/286326948/release/8-202304>

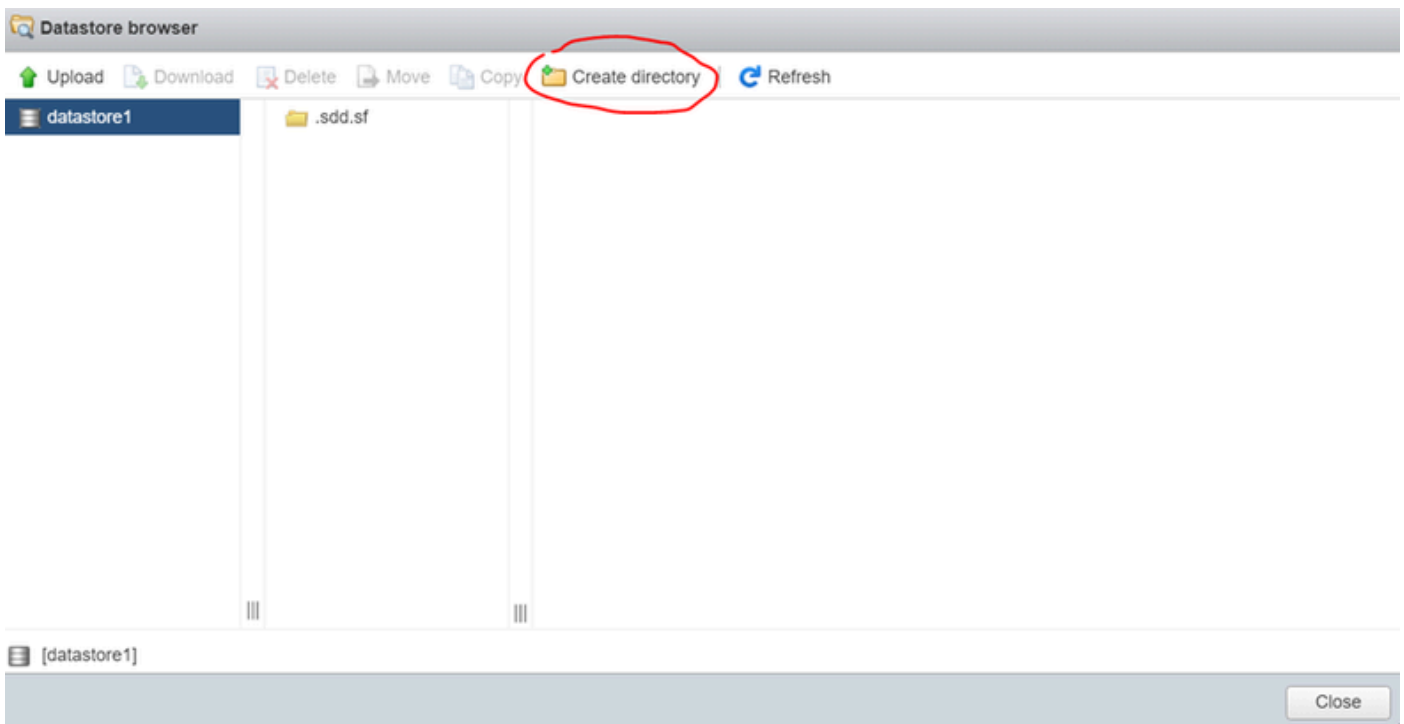
2. Upload the **ISO** in **VMWARE ESXi**.

Navigate to **Storage > Datastore Browser**.



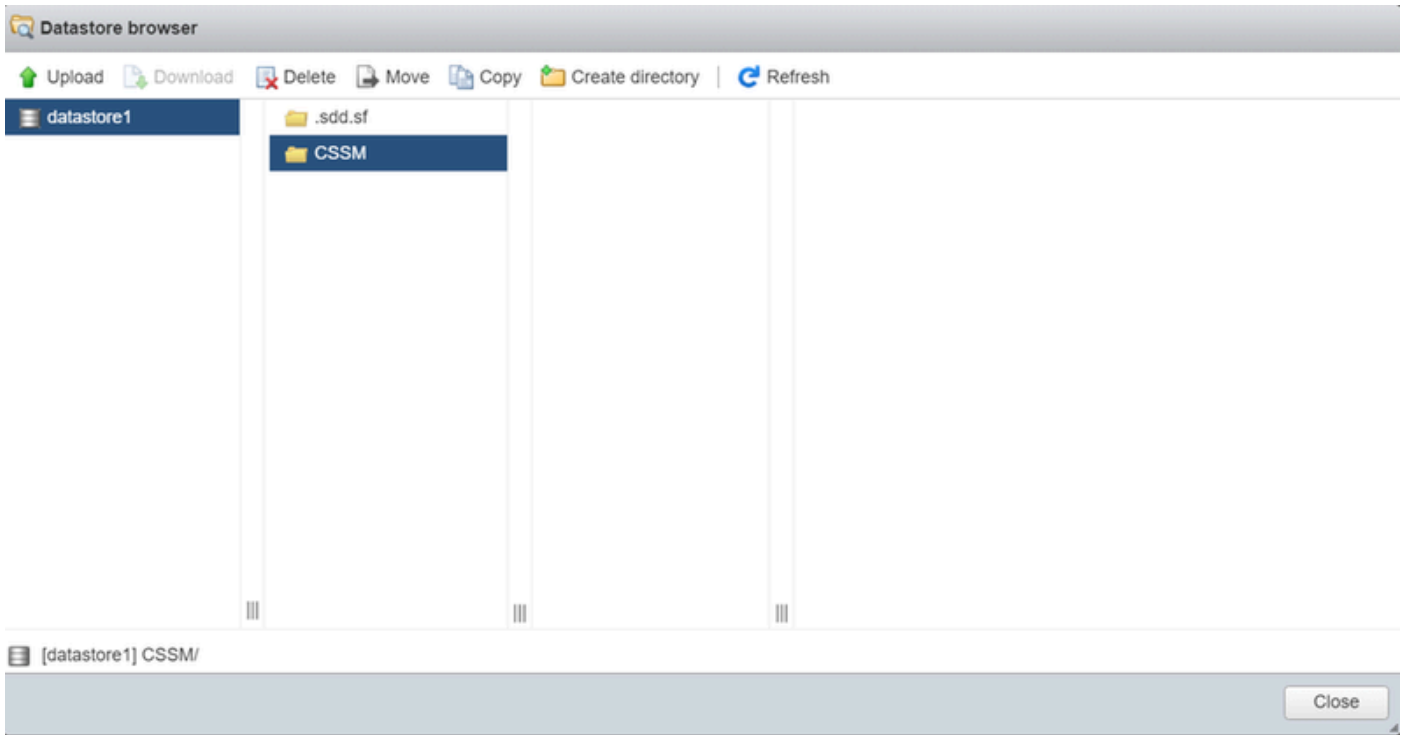
Data browser section

3. Click **Create Directory** to create a new folder (optional).



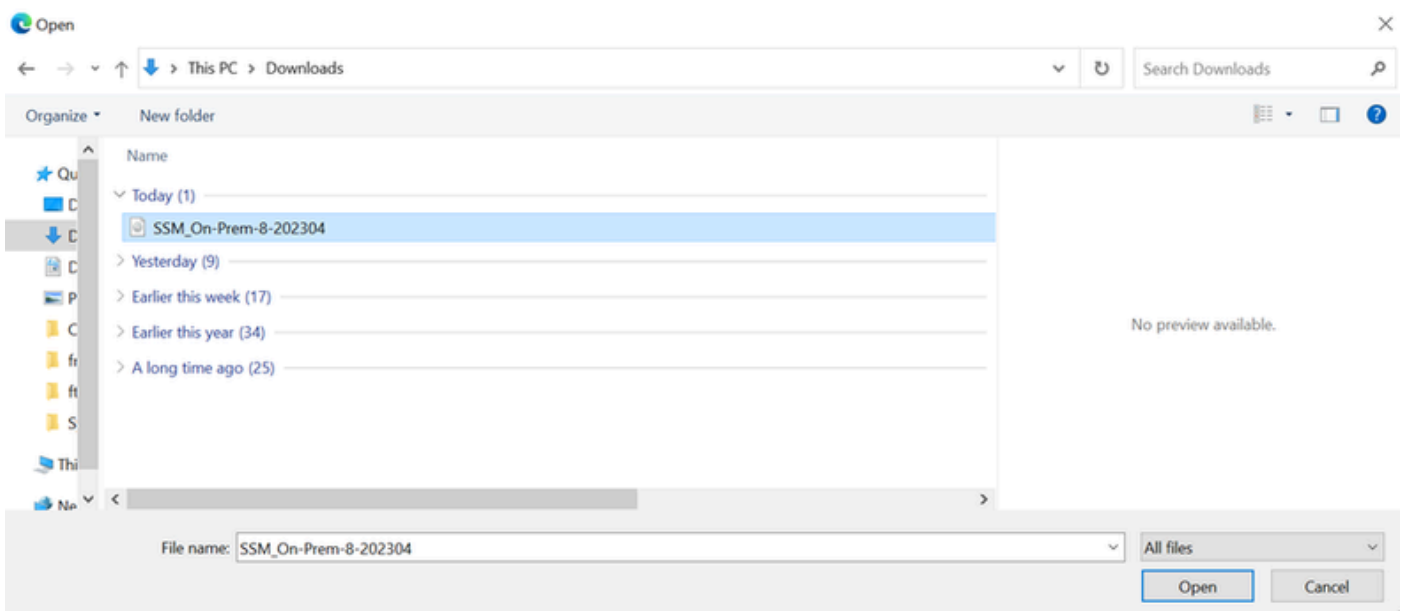
Creation of directory

In this example, the **CSSM** folder was created:



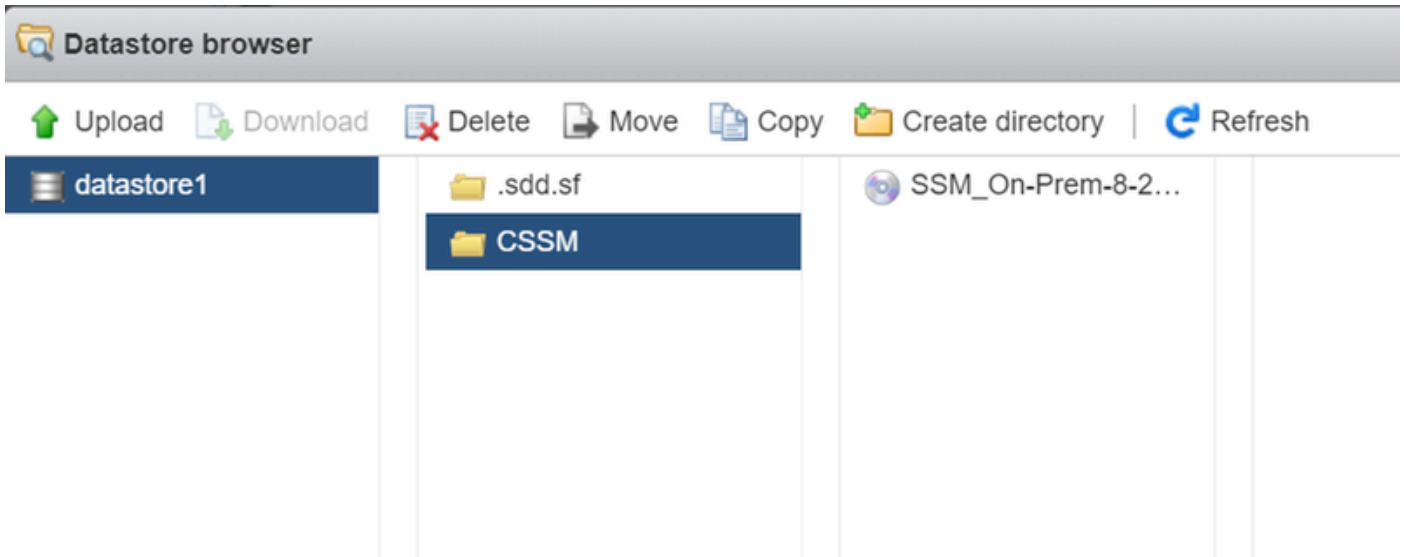
Creation of folders

4. Click **Upload** and then choose your **ISO** file.



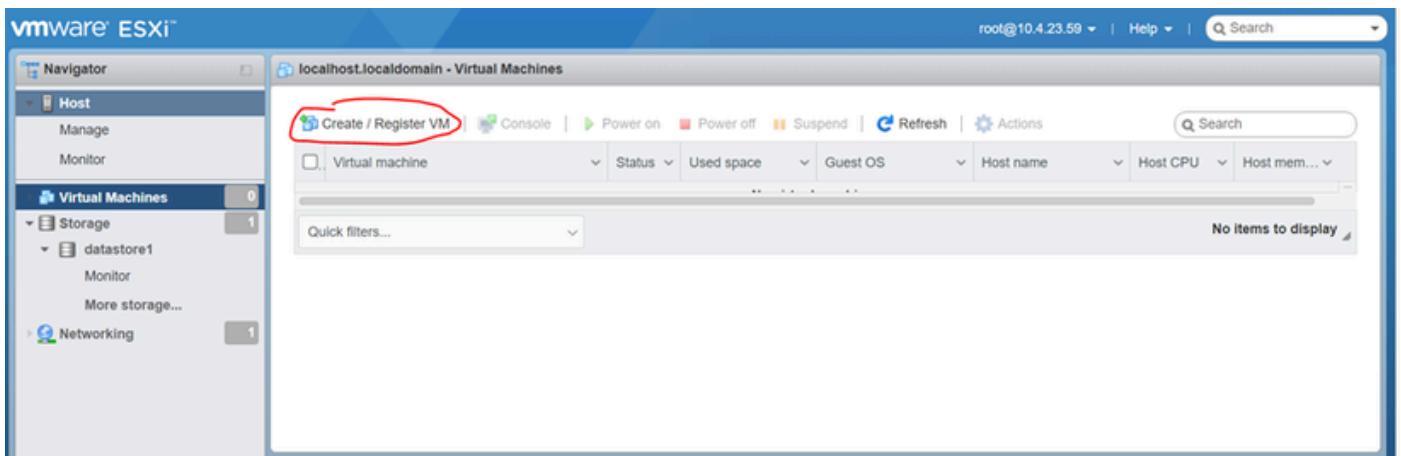
Uploading ISO

Now the **ISO** file is in the **CSSM** folder:



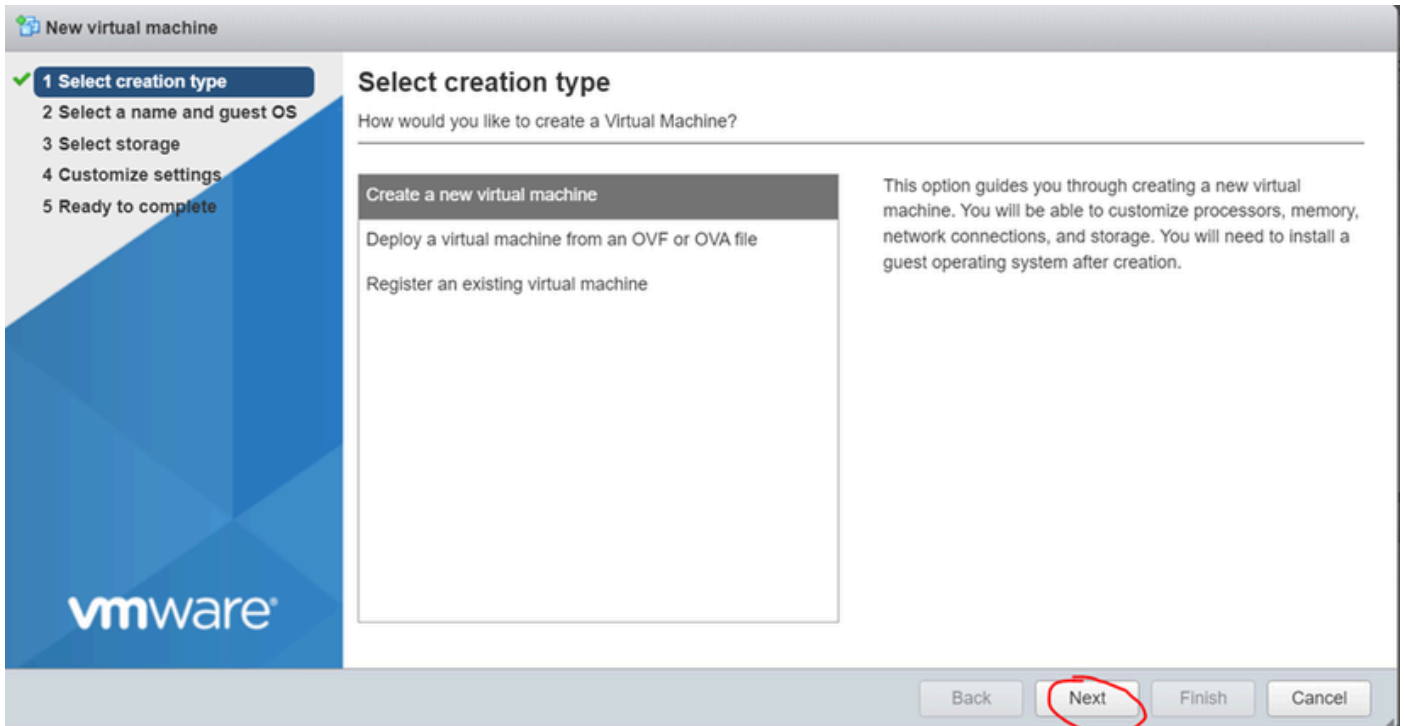
The ISO upload is completed

5. Create the Virtual Machine. navigate to **Virtual Machine > Create / Register VM.**



Creating a new VM step 01

6. Choose **Create a new virtual machine** and click **next**.

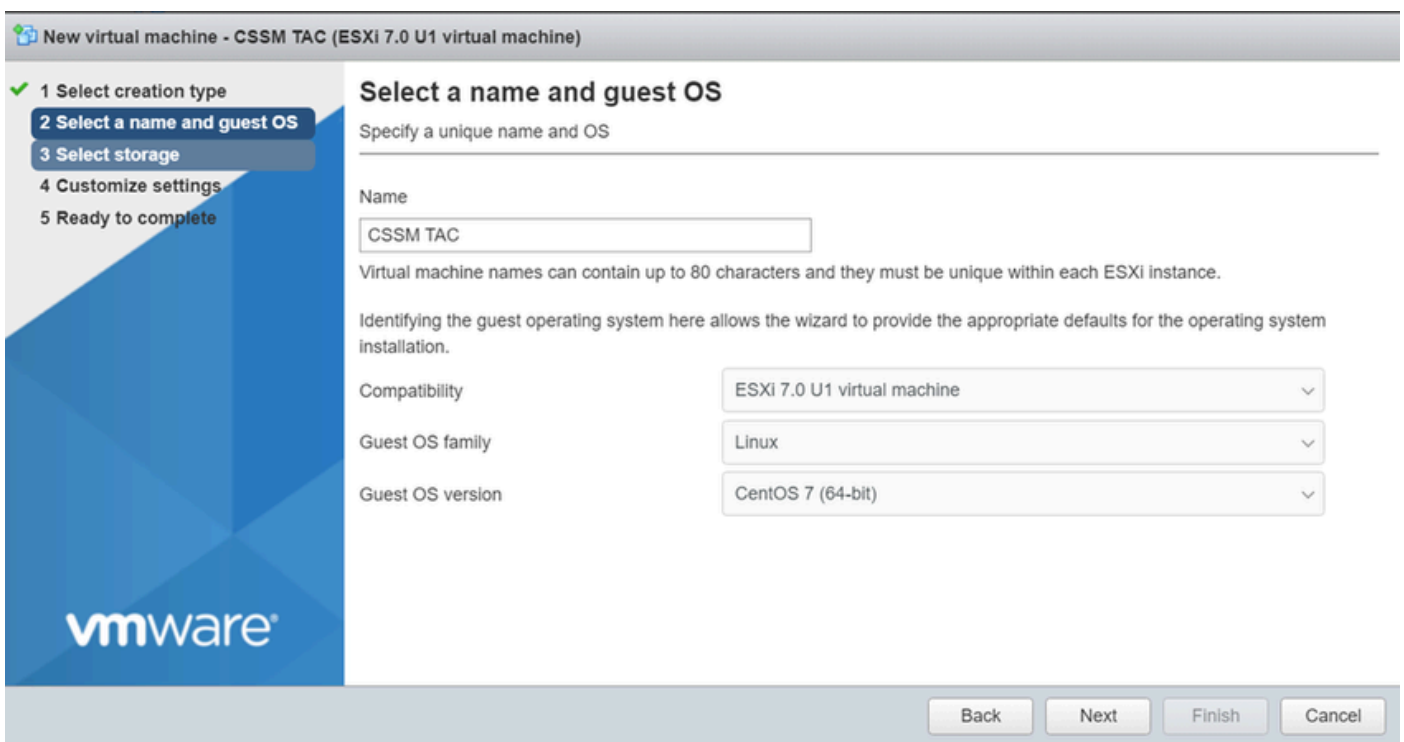


Creating a new VM step 02

7. Then configure the next parameters:

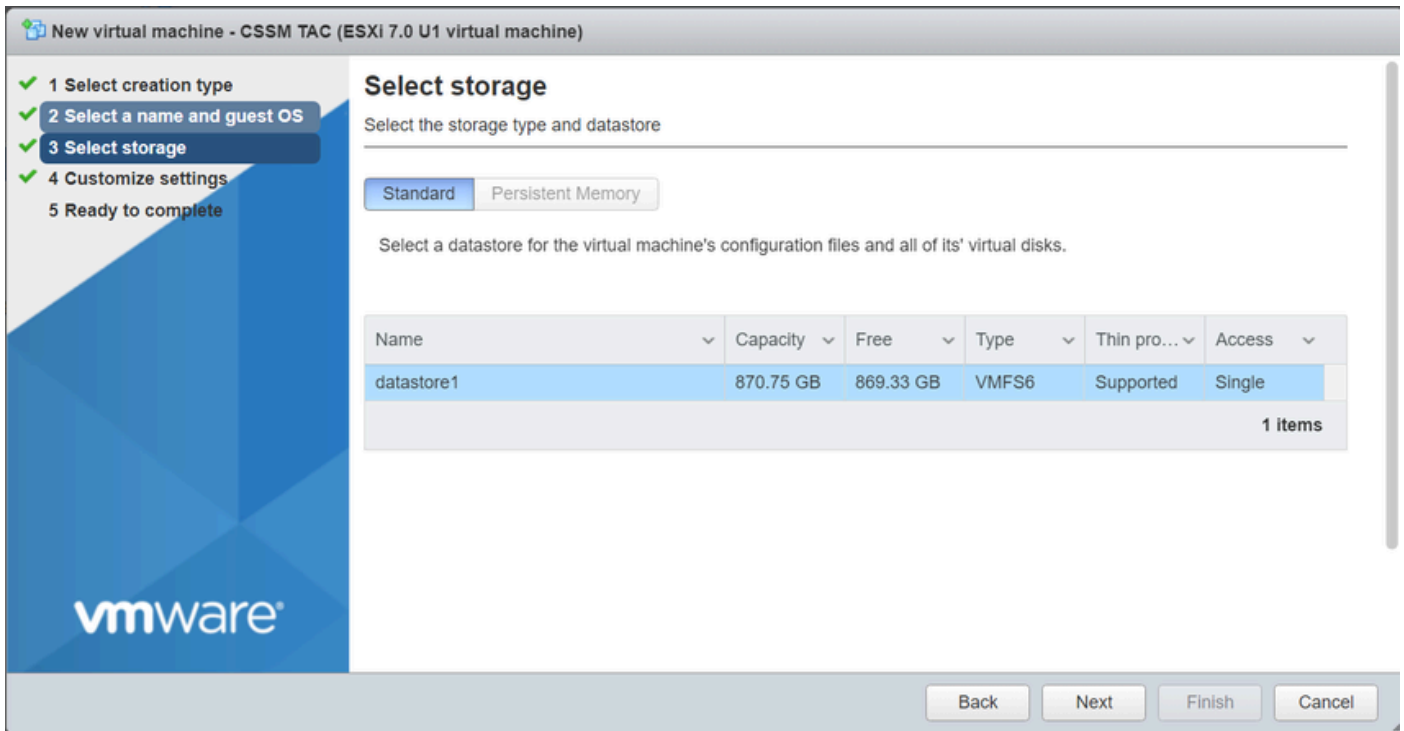
- **Name:** Enter the name of your virtual machine.
- **Compatibility:** Select either ESXi 6.0 or later or ESXi 6.5 or later.
- **Guest OS family:** Linux.
- **Guest OS version:** Choose either CentOS 7 (64 bit) or Other 2.6x Linux (64 bit)

Click **next**.



VM name and IOS

8. Select your **storage** and click **next**.



Storage list

9. Configure the next parameters:

- **CPU: 4 as minimum.** The actual vCPU setting depends on your scale requirement



Note: The amount of cores per socket needs to be set to 1 regardless of the number of virtual sockets selected. For example, a 4 vCPU configuration needs to be configured as 4 sockets and 1 core per socket.

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

Configuration of Cores

- **Memory:** 8 GB
- **Hard Disk:** 200 GB and verify provisioning is set to **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		

Configuration of disk

- **Network Adapter:** Select E1000 adapter type and select **Connect at Power On**.

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

Configuration of network settings

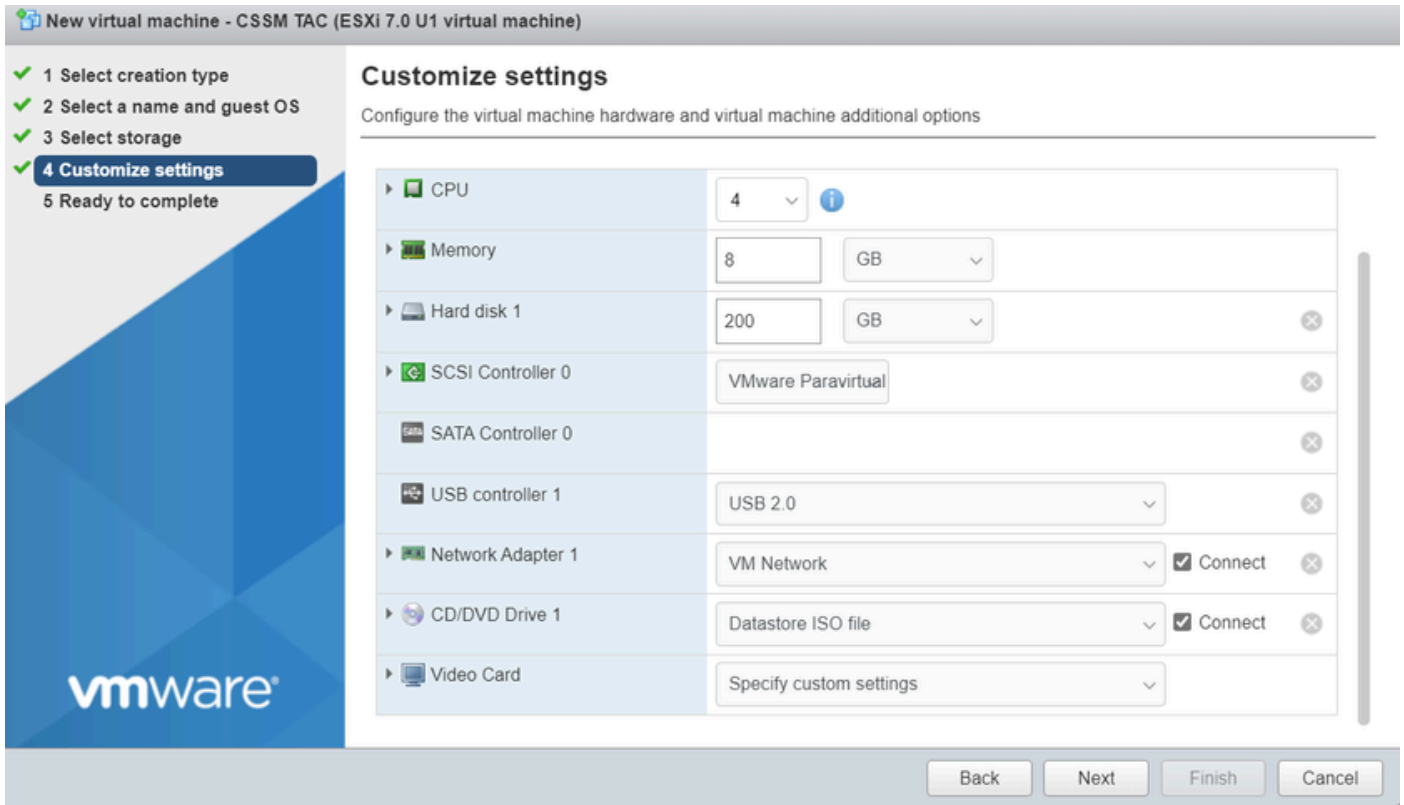
- **CD / DVD Drive:** Choose “**Data ISO file**” and select the **ISO** file.

Datastore browser

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

ISO image

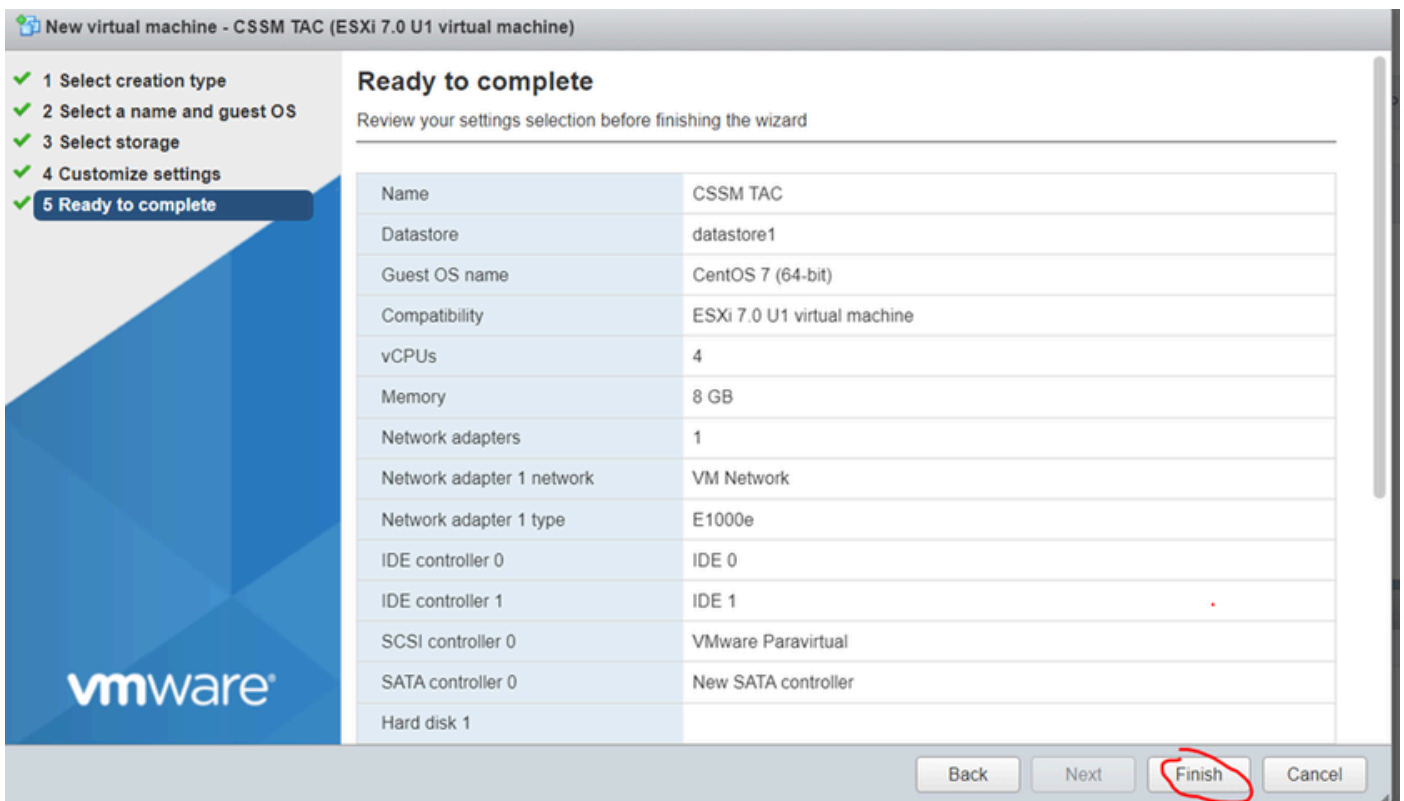
You can verify the summary of the settings once you have completed the previous steps.



Summary VM configuration 01

Click **next**.

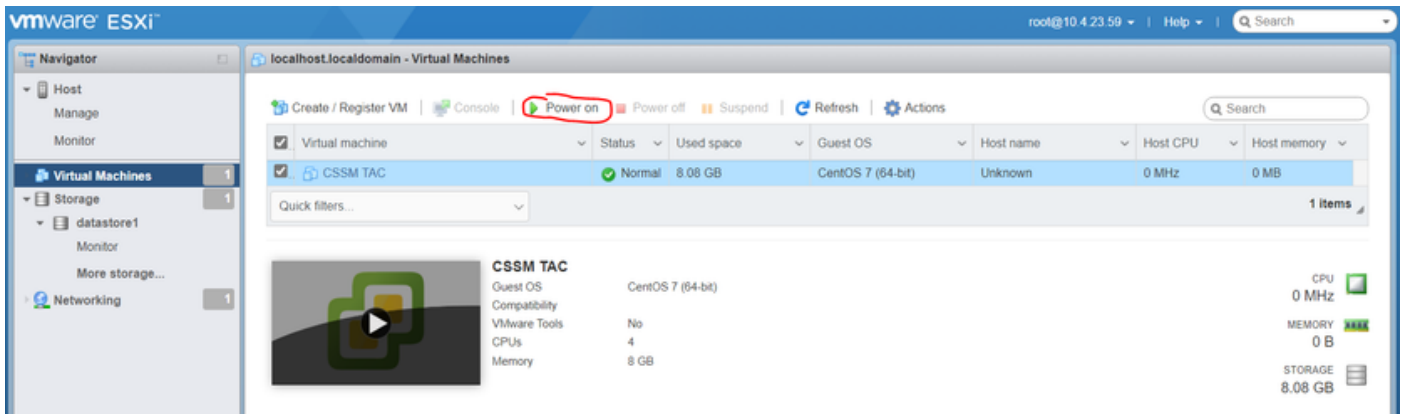
10. Click **Finish**.



Summary VM configuration 02

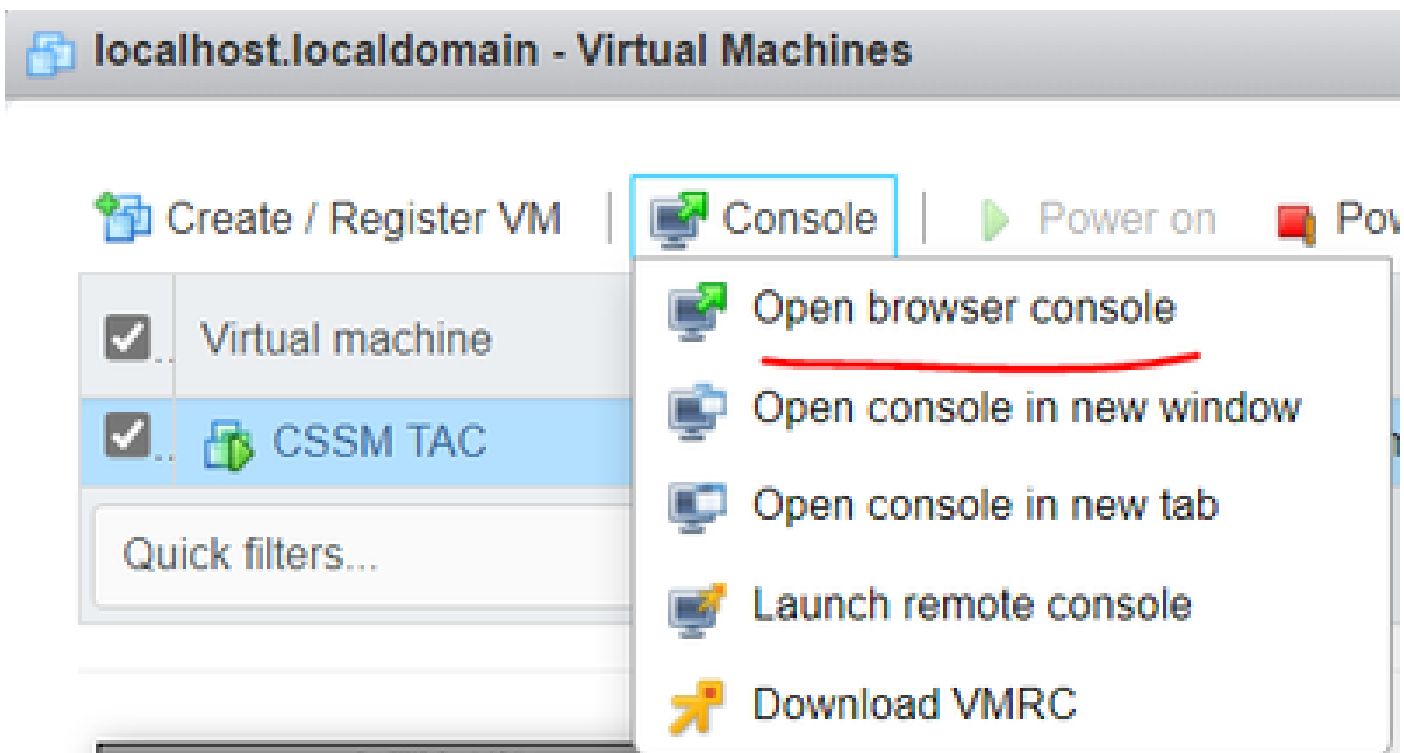
Initial Configuration of CSSM On-Prem .

1. In **VMWARE ESXi**, navigate to **Virtual Machines** and select your VM and then click **Power On**.



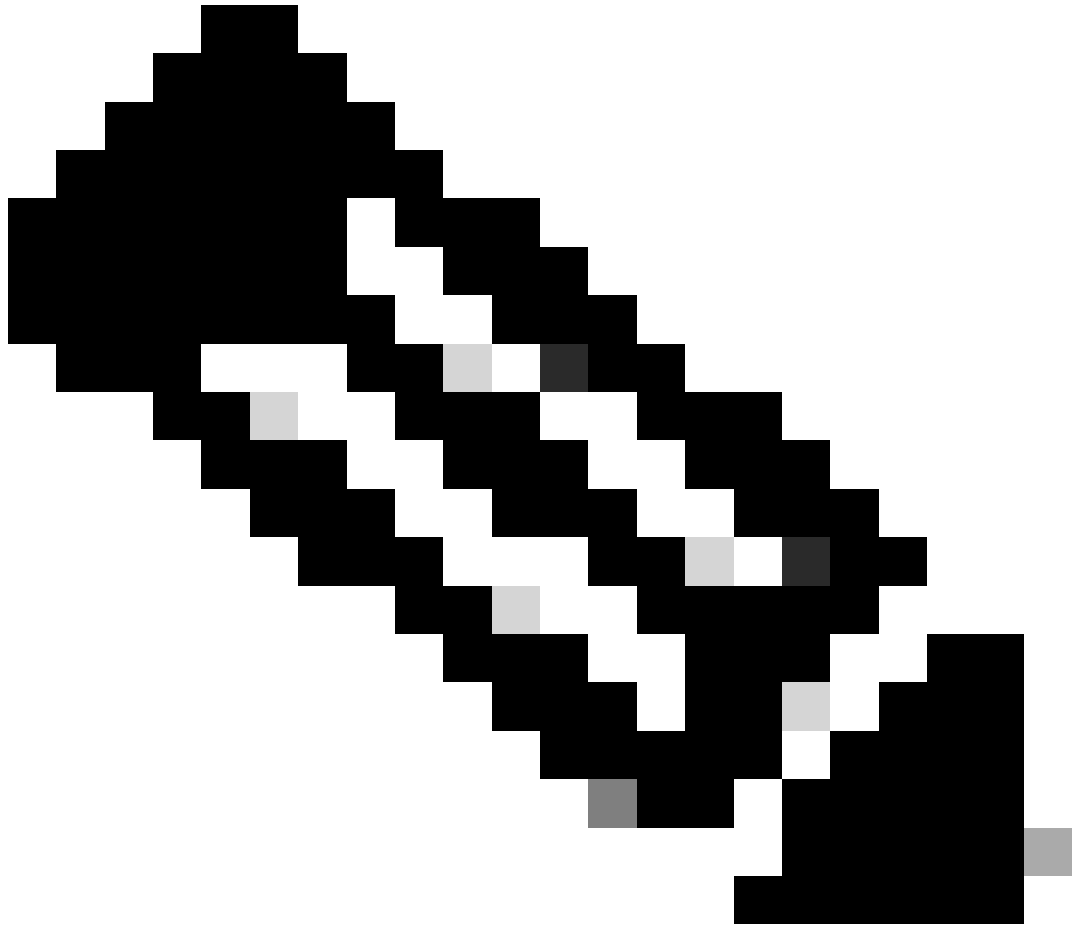
Power on option

2. You have multiple options to manage the VM console. Select **Console > Open browser console**.



Options to manage the VM

3. Configure your **network settings**.



Note: It's important to configure the **IP address** of the DNS Server that resolves the **CSSM FQDN**.

Cisco SSM On-Prem Installation

System Settings:
 Hostname:
 Message Of The Day: Security Profile: FIPS 140-2 Mode:

Hardware Settings:
 CPU Model: Intel(R) Xeon(R) CPU E5-2699A v4 @ 2.40GHz CPU Threads: 4 Architecture: 64-bit
 Total System Memory: 8174636 kB Free Memory: 4330340 kB
 Available Disks: sda (200Gb) Encrypt Drive with LUKS: Enable USB:

Network Settings:
 Network Device:

IPv4 Configuration	IPv6 Configuration
Method: <input type="text" value="Static"/>	Method: <input type="text" value="Disabled"/>
Address: <input type="text" value="10.4.23.60"/>	Address: <input type="text"/>
Netmask: <input type="text" value="255.255.248.0"/>	Prefix: <input type="text"/>
Gateway: <input type="text" value="10.4.16.1"/>	Gateway: <input type="text"/>

Configure DNS: Specify more than one with commas

Configuration of CSSM network settings

Click **Ok** to configure your new **CLI password**.

4. Then the installation process starts and is finished until you can see the access prompt.

```

CSSM
#####
#                               Authorized access only!                               #
#                               #                                                       #
# Disconnect IMMEDIATELY if you are not an authorized user!!!                       #
# All actions Will be monitored and recorded                                         #
#####
SSM-On-Prem login: _

```

CSSM initial configuration completed

5. Open a browser and enter **https://<ip_address_CSSM>**.

CSSM login page

Use the default credentials:

Username: **admin**

Password: **CiscoAdmin!2345**

6. Select your language.

7. Create a new **GUI password**.

8. Configure the **Host Common Name**. (example: *hostname.yourdomain*).

*In this case, the `cssm.testlab.local` was configured as **Host Common Name**.*

Welcome to Cisco Smart Software Manager On-Prem

9. Validate your configuration and click **Apply**.

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**

CSSM initial settings completed.

Integrate CSSM On-Prem with Smart Account

You need to associate your **Smart Account** with your **CSSM On Prem Server**.

1. Open your **Cisco Smart Account** using the next link:

<https://software.cisco.com/>

2. Then choose **Manage Licenses** under the **Smart Software Manager** section.

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

3. Navigate to **Inventory** and copy the name of your **Smart Account name** and **Virtual Account**. In

this guide, this is InternalTestDemoAccount67 and AAA MEX TEST.

Cisco Software Central

Scheduled Downtime Notification - License Registration Portal (LRP), Manage Smart Account & Account Administration, Plug-N-Play (PnP), Smart Software Manager

Cisco Software Central > Smart Software Licensing

InternalTestDemoAccount67.cisco.com

SL Product Details Support Help

Alerts **Inventory** Convert to Smart Licensing Reports Preferences On-Prem Accounts Activity

Virtual Account: AAA MEX TEST

General Licenses Product Instances Event Log

Virtual Account

Description: Only for tests

Default Virtual Account: No

Software Cisco page

4. Open the **CSSM GUI** and select the **Admin Workspace** option.

On-Prem License Workspace

Admin Workspace Hello, Local Admin Log Out

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.

Main CSSM menu.

5. Then select **Accounts**.

On-Prem Admin Workspace

Smart Software Manager On-Prem



Access
Management



Settings



Accounts



Support
Center



API Toolkit



Synchronization



Network



Users



Security

: The next steps describe the procedure to install the GUI certificate in the CSSM. If you want to protect the management connection to your GUI CSSM by using a certificate signed by your personal **Certification Authority (CA)** you need to check the next steps. Otherwise, check directly the step 9.

The screenshot shows the 'Security' configuration page with the 'Certificates' tab selected. Under 'Product Certificate', the 'Host Common Name' is 'cssm.testlab.local'. Under 'Browser Certificate', the 'Generate CSR' button is highlighted. A 'localhost' certificate is listed with an expiration date of 2025-JUL-16. The 'CA Certificates' section is empty.

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				

CSR option.

3. Then enter your personal information. Be aware the **Subject Alternative Name** is created automatically by using the same value as the **Common Name**. The **CSR** is downloaded automatically after clicking **Generate**.

Generate CSR

Common Name	<input type="text" value="cssm.testlab.local"/>
Organizational Unit	<input type="text" value="Testlab"/>
Country	<input type="text" value="Mexico"/>
State/Province	<input type="text" value="Mexico City"/>
City/Locality	<input type="text" value="Mexico City"/>
Organization	<input type="text" value="SEC AAA"/>
Key Size	<input type="text" value="2048"/>
Subject Alternative Name	<input type="text" value="cssm.testlab.local"/>

CSR details.

- 4. Sign the CSR:** For more information check the “[Create certificates from Windows CA.](#)” on this document.
- 5. Upload the root CA certificate.**

Browser Certificate

Add Generate CSR

localhost
(Default Certificate)

File Home Share View

certs

This PC > Desktop > certs

CA Certificates

Add

Description Sul

CSSM cer

Root CA

Uploading Root CA.

Click **Proceed**.



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

Proceed option.

6. Enter a description and choose the **root certificate** and click **Ok**.

Upload Certificate

* Description:

* Certificate: Root CA.cer

Description root CA.

7. Upload the CSR signed by the CA (**CSSM Identity Certificate**).

Browser Certificate

localhost (Default Certificate)

CA Certificates

2 items

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

Uploading CSSM Identity Cert.

Note: NOTE: In our case, the **Intermediate certificate** does not exist in our CA. However, if you use an **intermediate certificate** in your architecture, the **intermediate certificate** is mandatory.

8. Then, confirm that both certificates have been installed.

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](#)

Certificates validation.

9. Create a token on the SSM On-Prem: Select **licensing Workspace**.

Workspace page.

10. navigate to **Smart Licensing**.

CSSM Smart licensing page

11. Look for your **Local Virtual Account**, then click **New Token** and click **Proceed**.

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 cslu as transport, you must configure the "license smart transport cslu" 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...

New token option.

12. Select **Create Token** and copy it.

Create Registration Token



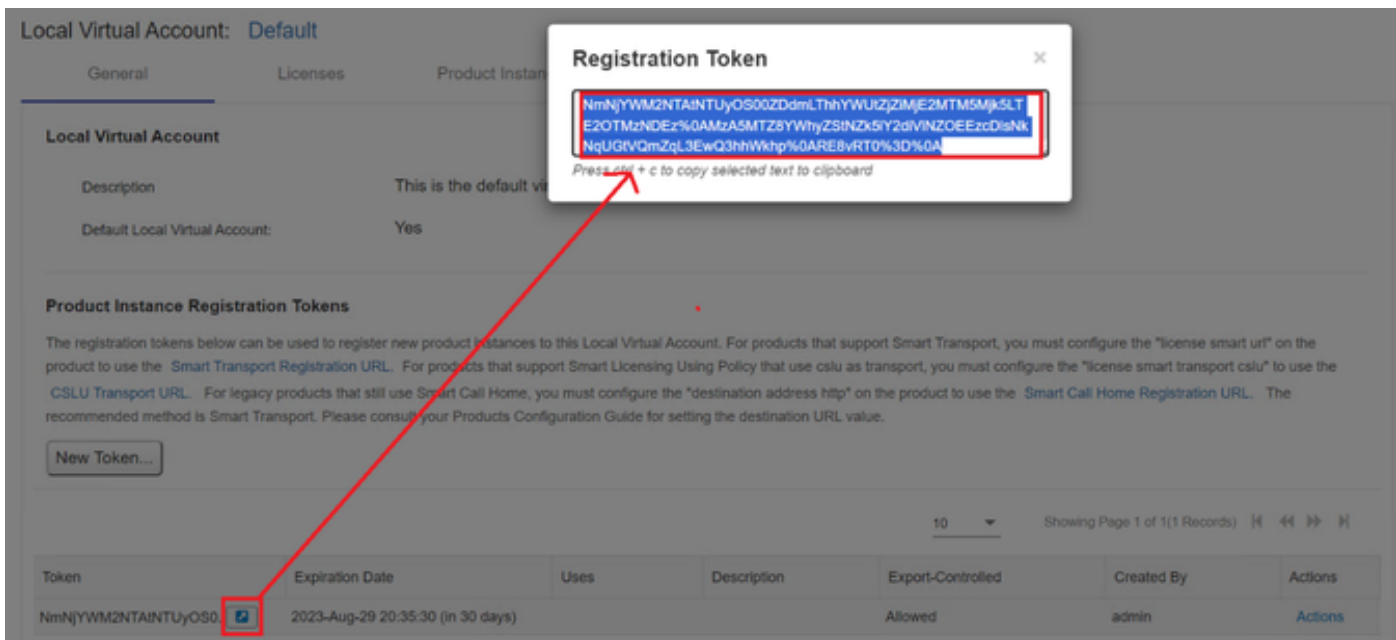
This dialog will generate the token required to register your product instances with your Account .

Local Virtual Account	Default
Description	<input type="text"/>
Expire After	<input type="text" value="30"/> Days <i>Enter a value between 1 and 9999, but Cisco recommends a maximum of 30 days</i>
Max. Number of Uses	<input type="text"/> <i>The token will be expired when either the expiration or the maximum uses is reached.</i>

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

Create Token

Creation of new token.



Token details.

13. Open the **ISE GUI** and navigate to **Administration > Systems > Licensing**, then click **Registration details**, select the **SSM On-Prem server Host** method, and paste **the token**.

License Type

Choose Registration Details to acquire pre-purchased license entitlements. Choose Permanent License Reservation to enable all Cisco ISE licenses. Enter the required details to enable Cisco ISE licenses. When you click Register, you agree to the terms and conditions detailed in [Smart Licensing Resources](#).

Smart Licensing Registration
 Permanent License Reservation
 Specific License Reservation
 Registration Details

When you register Cisco ISE in the [Cisco Smart Software Manager portal](#), a unique ID called the Registration Token is displayed in the portal. Copy the registration token displayed in the CSSM portal and paste it here.

Registration Token

NmNjYWM2NTAINTUyOS00ZDdmLThhYWU

Registration of licenses.

14. Enter the **SSM On-Prem FQDN** on **SSM On-Prem server Host** and click **Register**.

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](#).

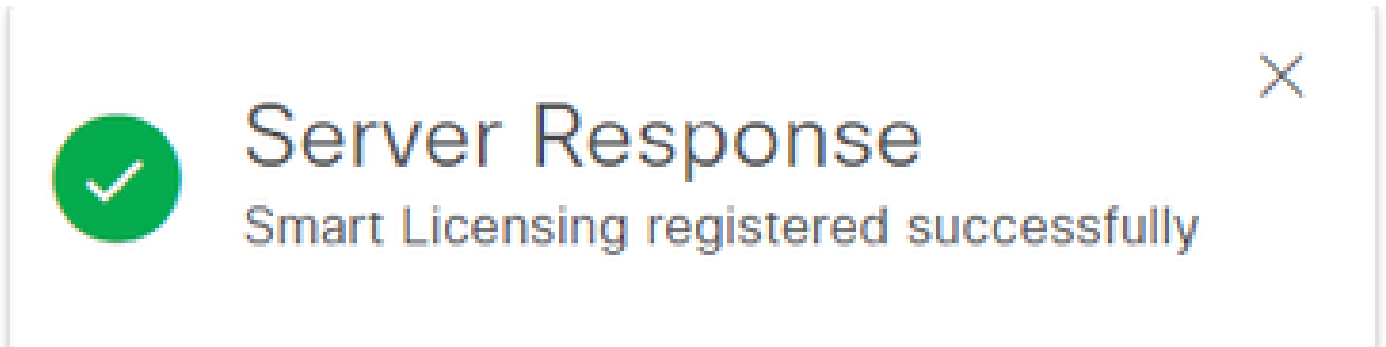
Cancel Register

CSSM and ISE settings.

Note: It's important to have the **hostname + domain** configured on the **Host Common Name** because ISE uses this parameter in order to establish a connection with the CSSM. You can use an

IP address instead of the **hostname + domain**, however the recommendation is to use the **hostname + domain**

15. And finally, the registration has been completed.

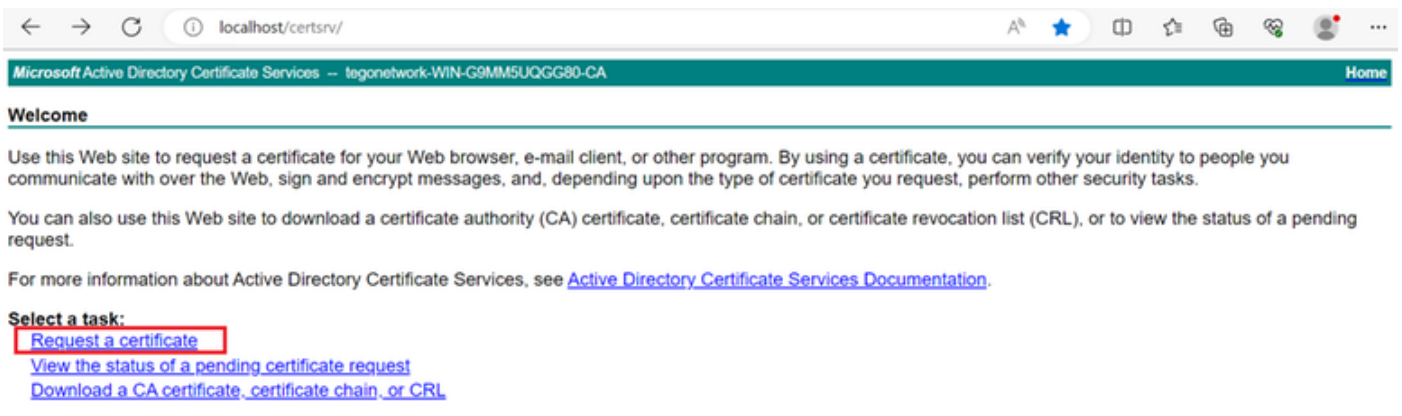


Registration completed.

Create certificates from Windows CA.

If you are the administrator of the Certificate Authority, you must do the next:

1. Open a web browser and navigate to <http://localhost/certsrv/>
2. Click on **Request a certificate**.



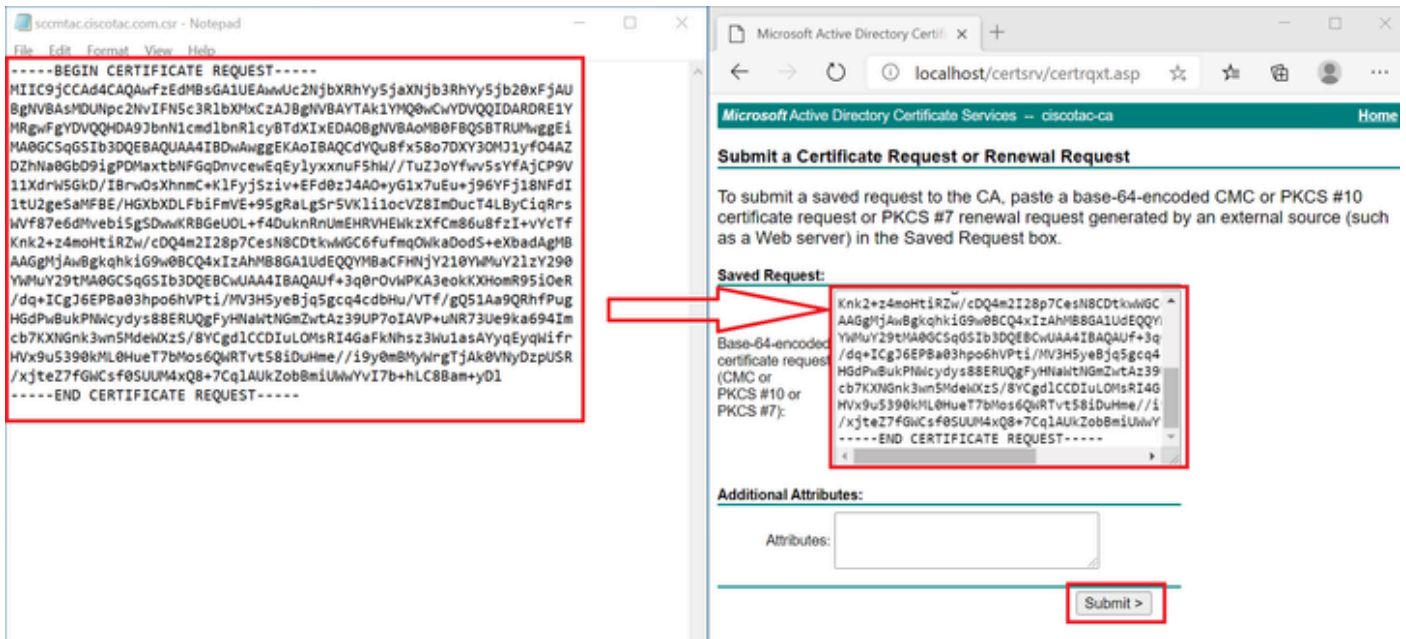
Request certificate.

3. Click **advanced certificate request**.



Advanced certificate request.

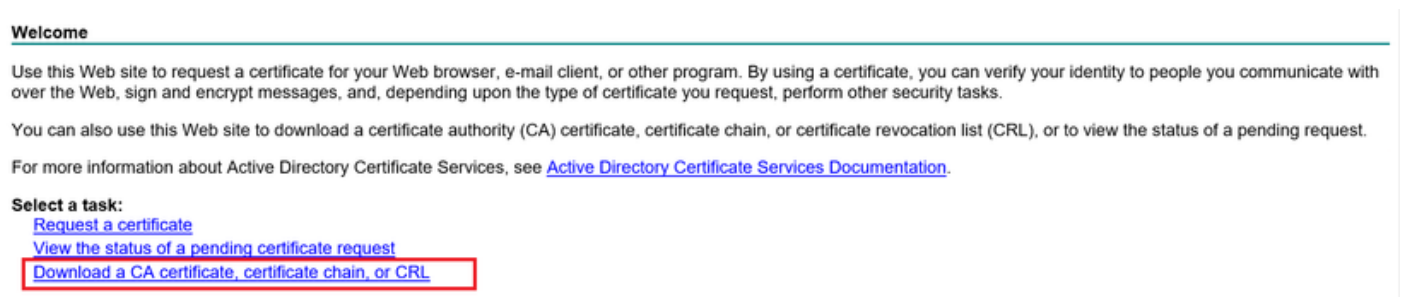
4. Open the CSR generated previously. Then copy the information and paste it on **Saved request**.



Submit certificate.

After clicking **Submit** the certificate is downloaded automatically.

5. Now download the CA certificate root. navigate back to <http://localhost/certsrv/> and select **Download a CA Certificate, Certificate Chain, or CRL**.



Download root CA.

6. Download the **CA certificate** by using the **encoding method as 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.

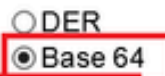
CA certificate:

Current [ciscotac-ca]



Encoding method:

DER
 Base 64



[Download CA certificate](#)

[Download CA certificate chain](#)

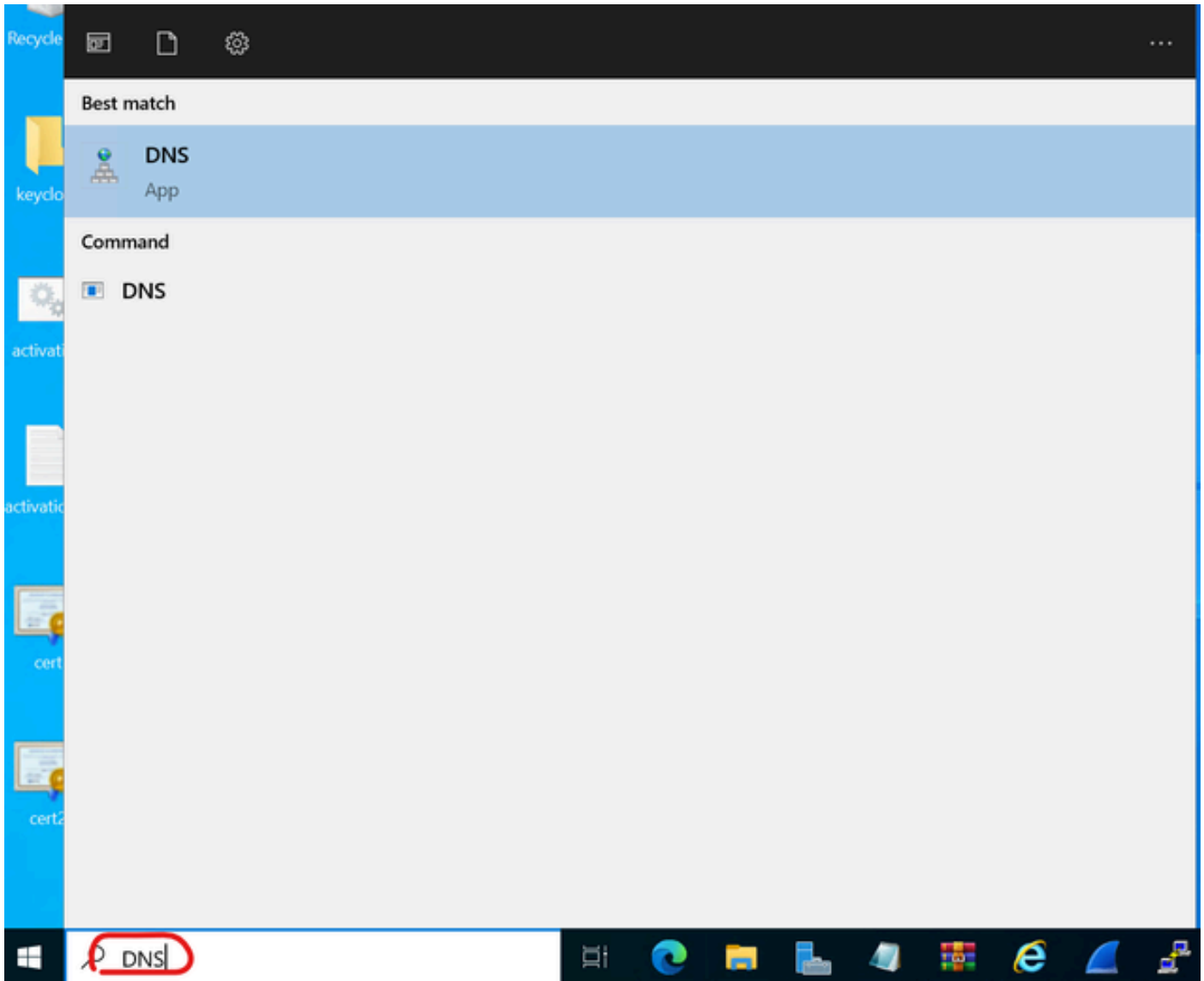
[Download latest base CRL](#)

Base 64 option.

Add DNS records on Windows Server.

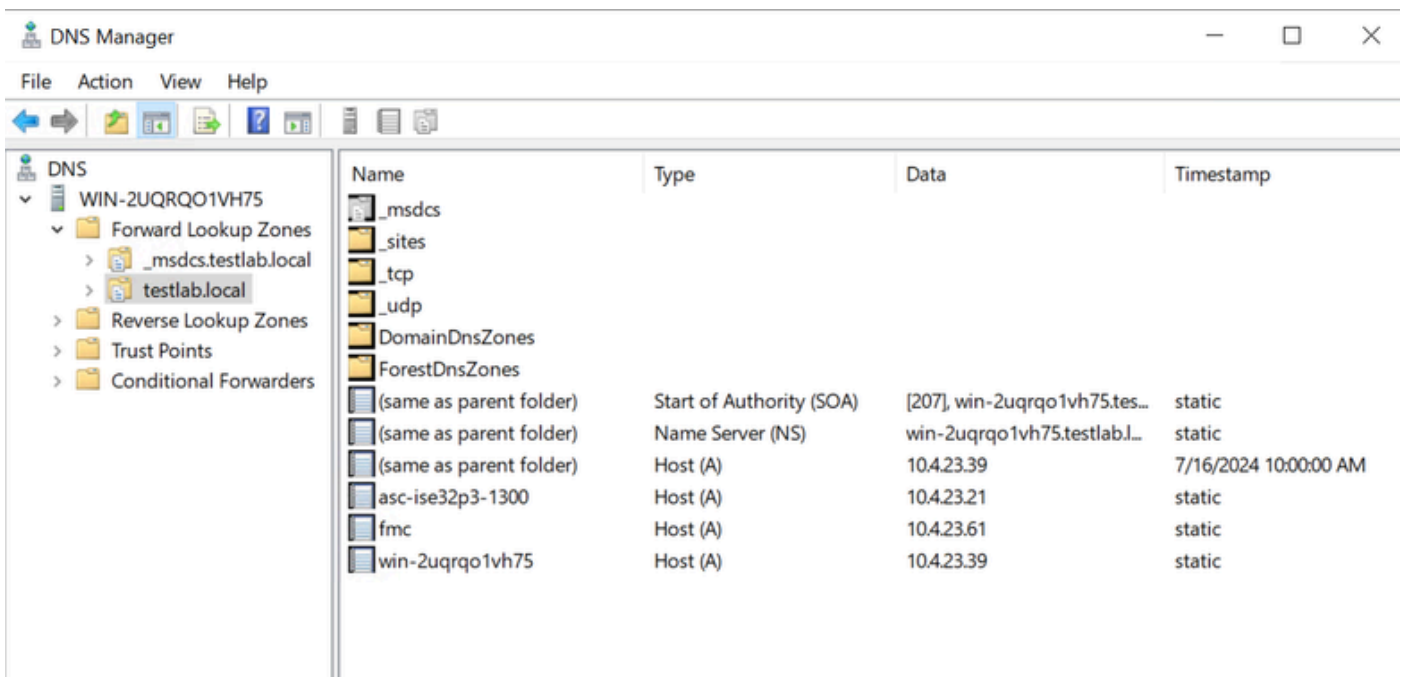
If you are the administrator, add the ISE and CSSM FQDNs.

1. Open the **DNS Manager**: Type “DNS” on the Windows finder and open the DNS app.



DNS option.

2. Navigate to **Forward Lookup Zones** > And choose your domain.



DNS manager.

3. Right-click on a black space over the screen and select “**New Host (A or 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

