

Configuration de CSSM sur Prem et enregistrement des licences avec ISE

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Installez CSSM On-Prem sur VMWARE ESXi.](#)

[Configuration initiale de CSSM On-Prem.](#)

[Intégration de CSSM On-Prem avec un compte Smart](#)

[OPTION 1 : Enregistrez votre module CSSM On-Prem via une connexion Internet.](#)

[OPTION 2 : Enregistrez votre module CSSM On-Prem sans connexion Internet.](#)

[Intégration de CSSM On-Prem avec ISE.](#)

[Créer des certificats à partir de Windows CA.](#)

[Ajoutez des enregistrements DNS sur Windows Server.](#)

[Dépannage](#)

[L'hôte/l'adresse IP n'est pas accessible.\(Erreur sur ISE\)](#)

[Service SSO : impossible d'atteindre Cisco. \(Erreur sur CSSM On-Prem\)](#)

[Le nom commun dans le CSR n'est pas un nom d'hôte ou une adresse IP pouvant être résolu par DNS. veuillez réessayer.\(Erreur sur CSSM On-Prem\)](#)

Introduction

Ce document décrit l'intégration de CSSM On-Prem avec Cisco Identity Service Engine (ISE) et Cisco Smart Account, assurant une configuration transparente.

Conditions préalables

Exigences

ISE 3.X

Cisco Smart Software Manager (CSSM) version 8 version 202304 +

Composants utilisés

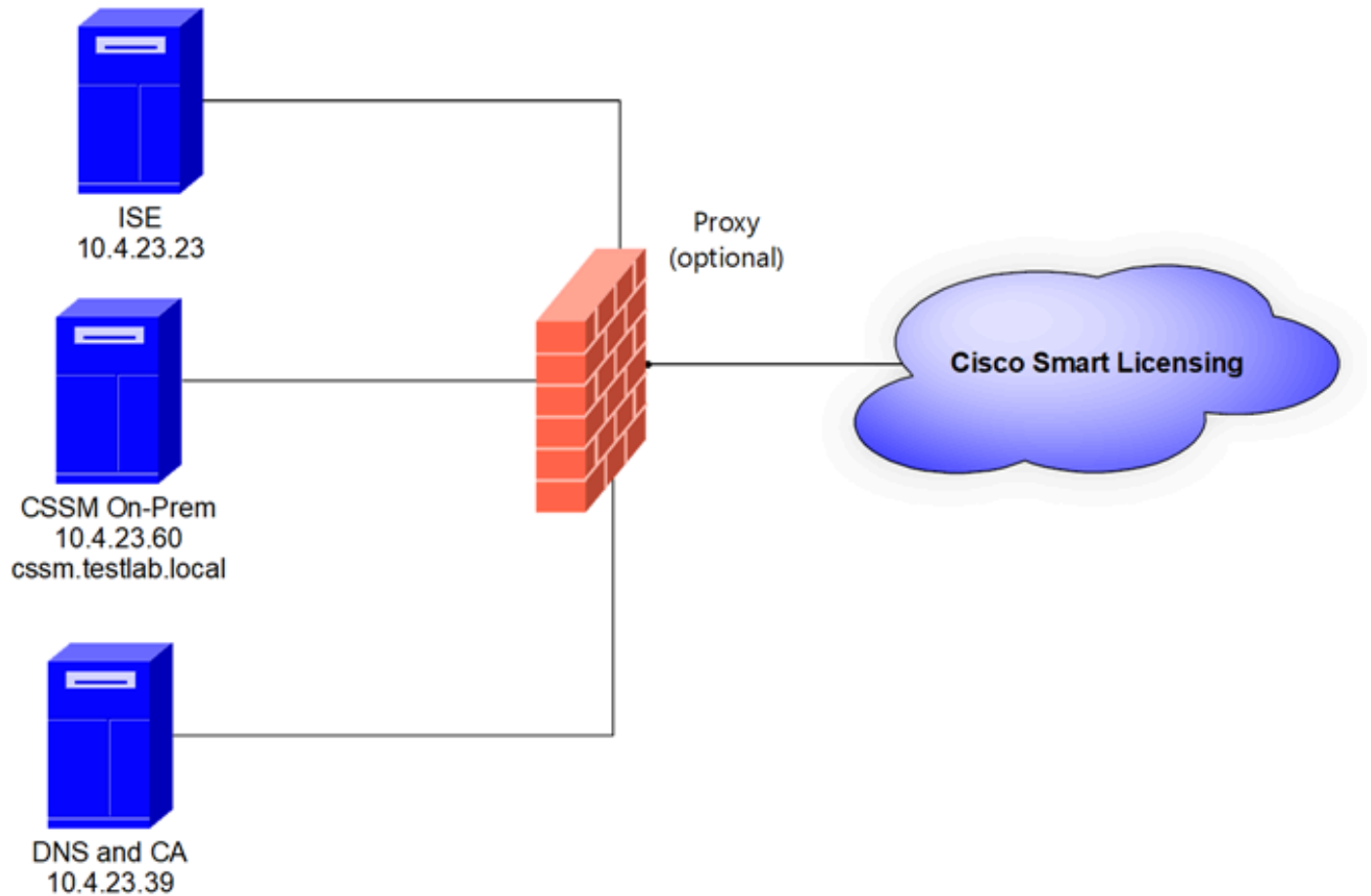
- Identity Service Engine 3.2, correctif 2
- SSM sur Prem 8.20234

- Windows Active Directory 2016 (services DNS et Certificate Authority)
- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme du réseau



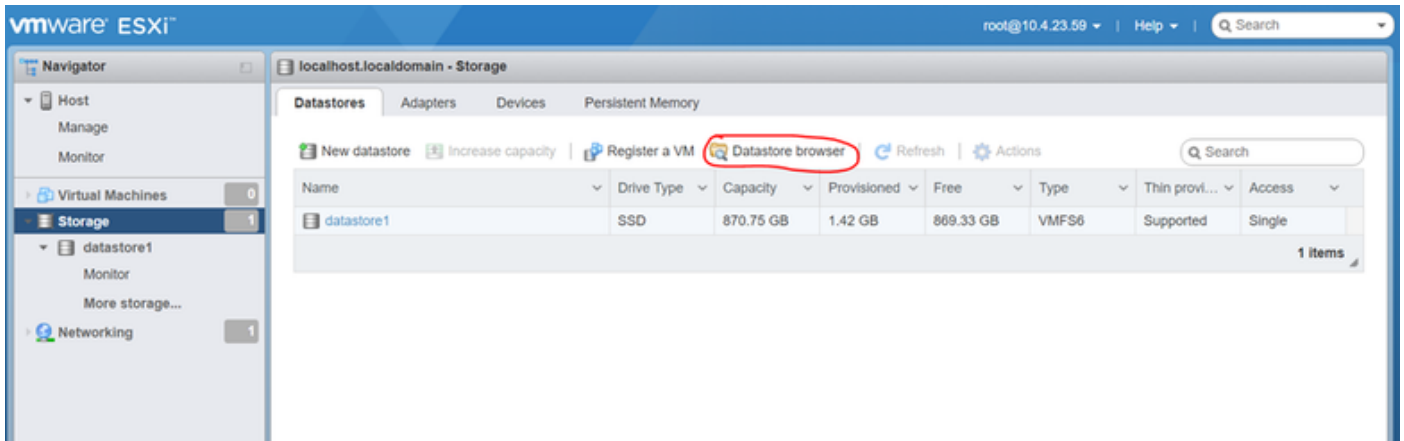
Topologie générale

Installez CSSM On-Prem sur VMWARE ESXi.

1. Téléchargez le logiciel Cisco IOS®. Vous pouvez utiliser le lien suivant :
<https://software.cisco.com/download/home/286285506/type/286326948/release/8-202304>

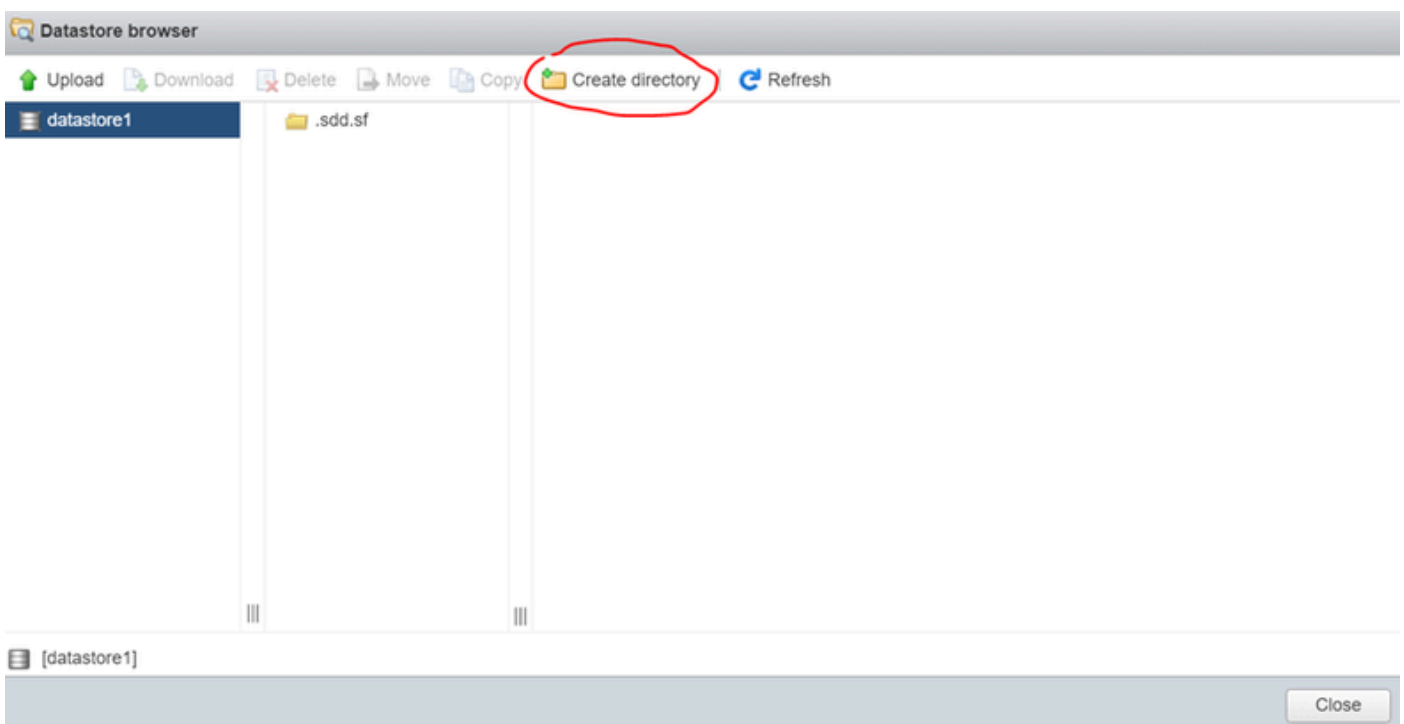
2. Téléchargez l'ISO dans VMWARE ESXi.

Accédez à Stockage > Navigateur de data store.



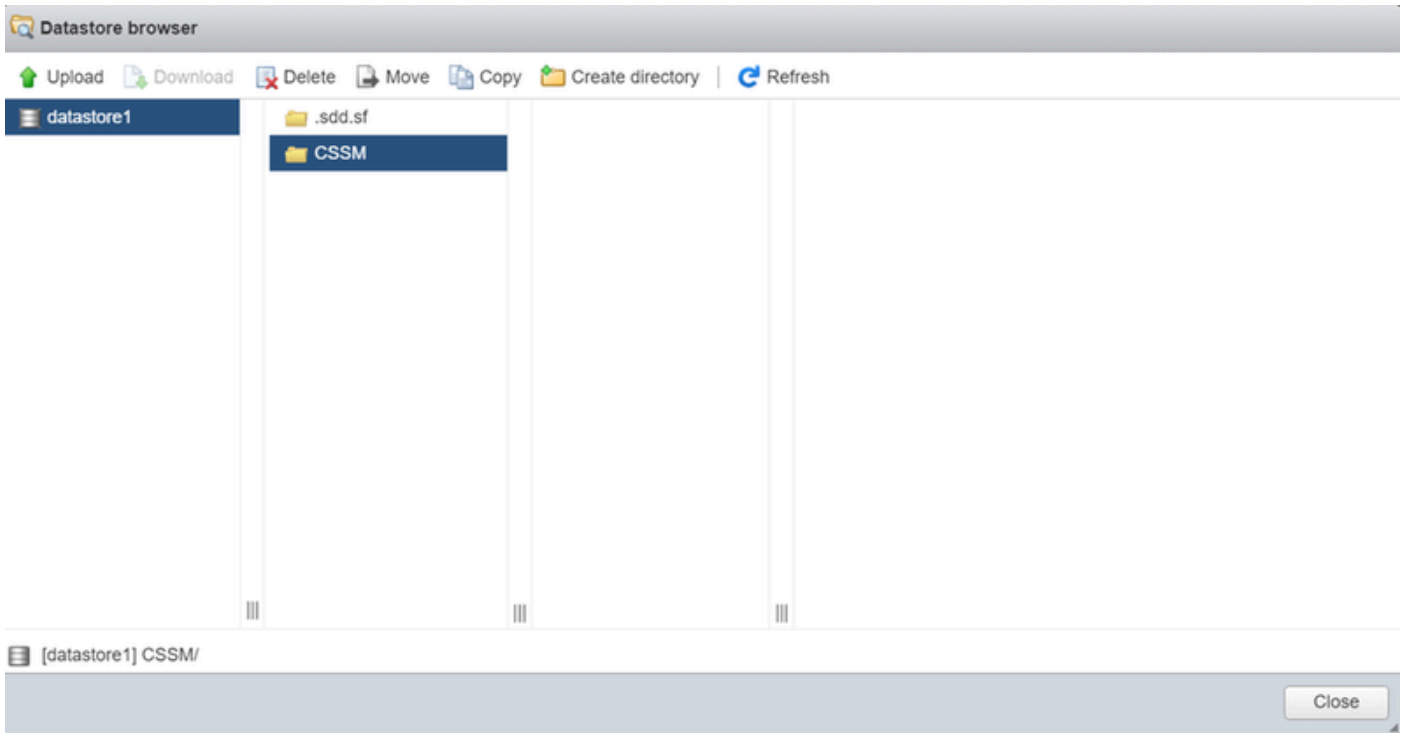
Section Navigateur de données

3. Cliquez sur Créer un répertoire pour créer un nouveau dossier (facultatif).



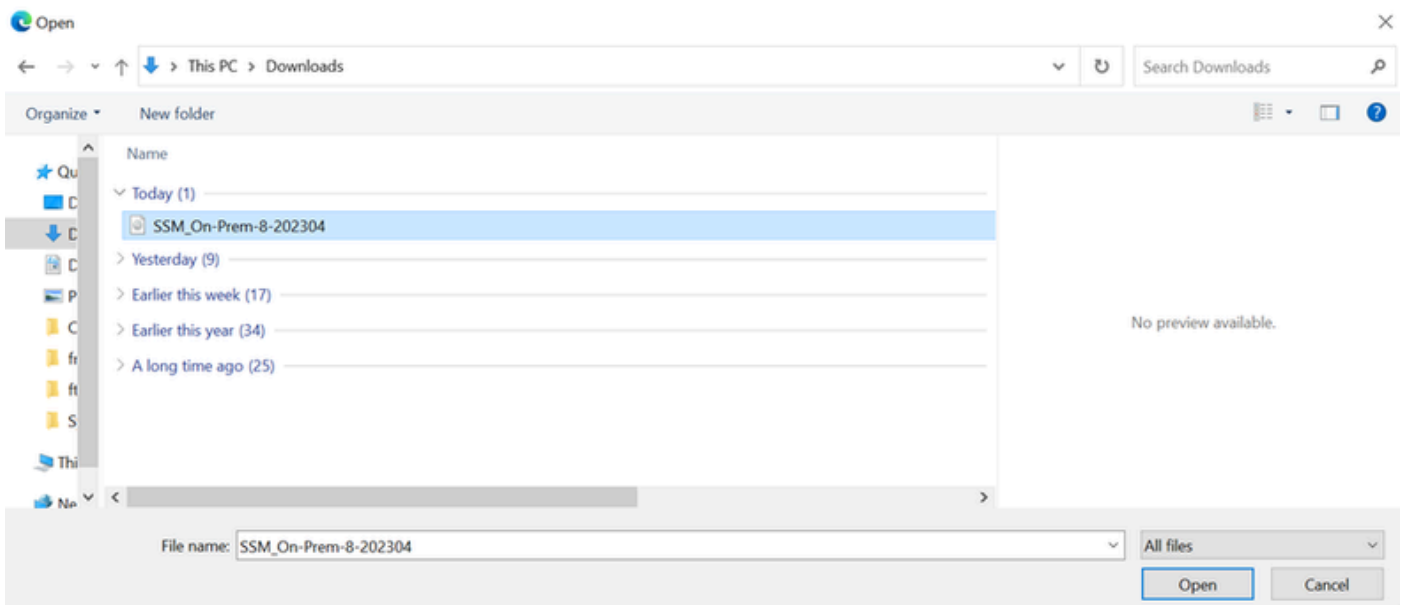
Création du répertoire

Dans cet exemple, le dossier CSSM a été créé :



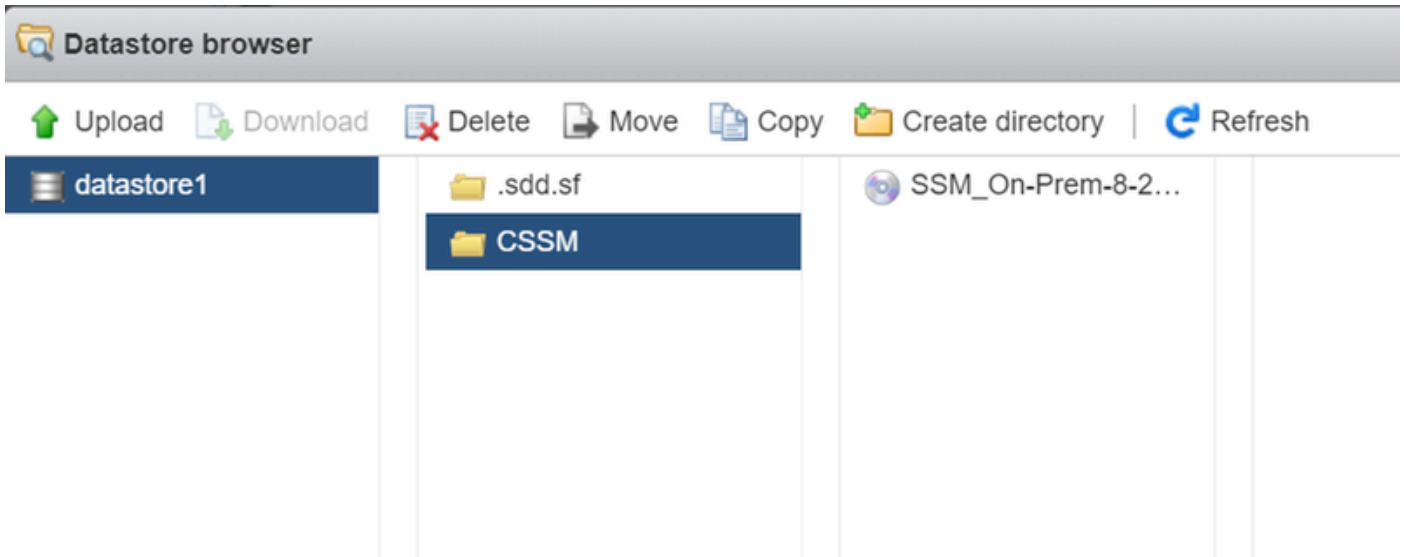
Création de dossiers

4. Cliquez sur Upload, puis choisissez votre fichier ISO.



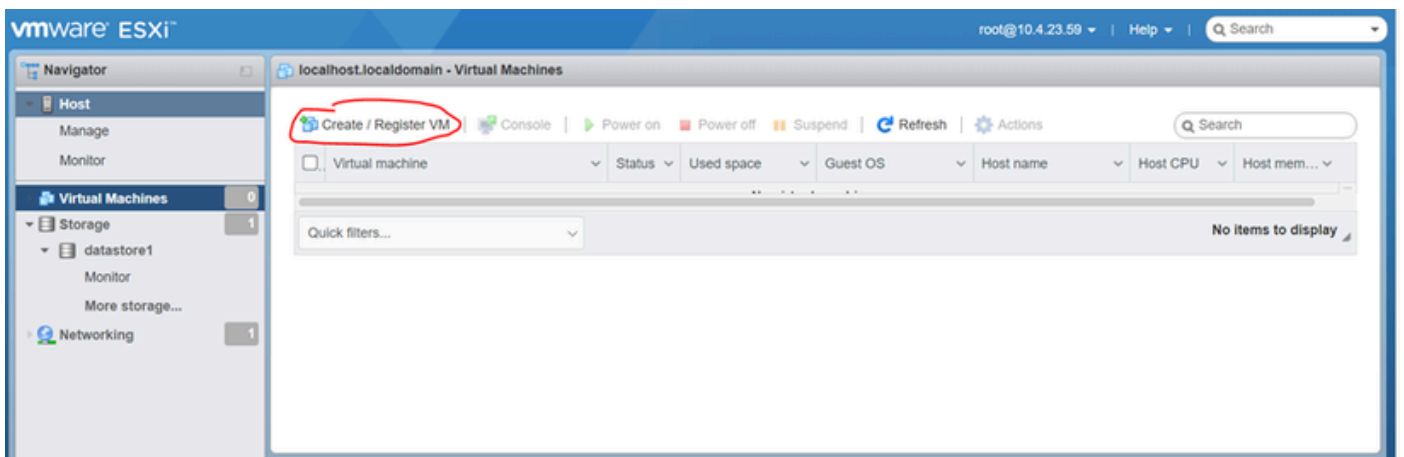
Téléchargement ISO

Le fichier ISO se trouve désormais dans le dossier CSSM :



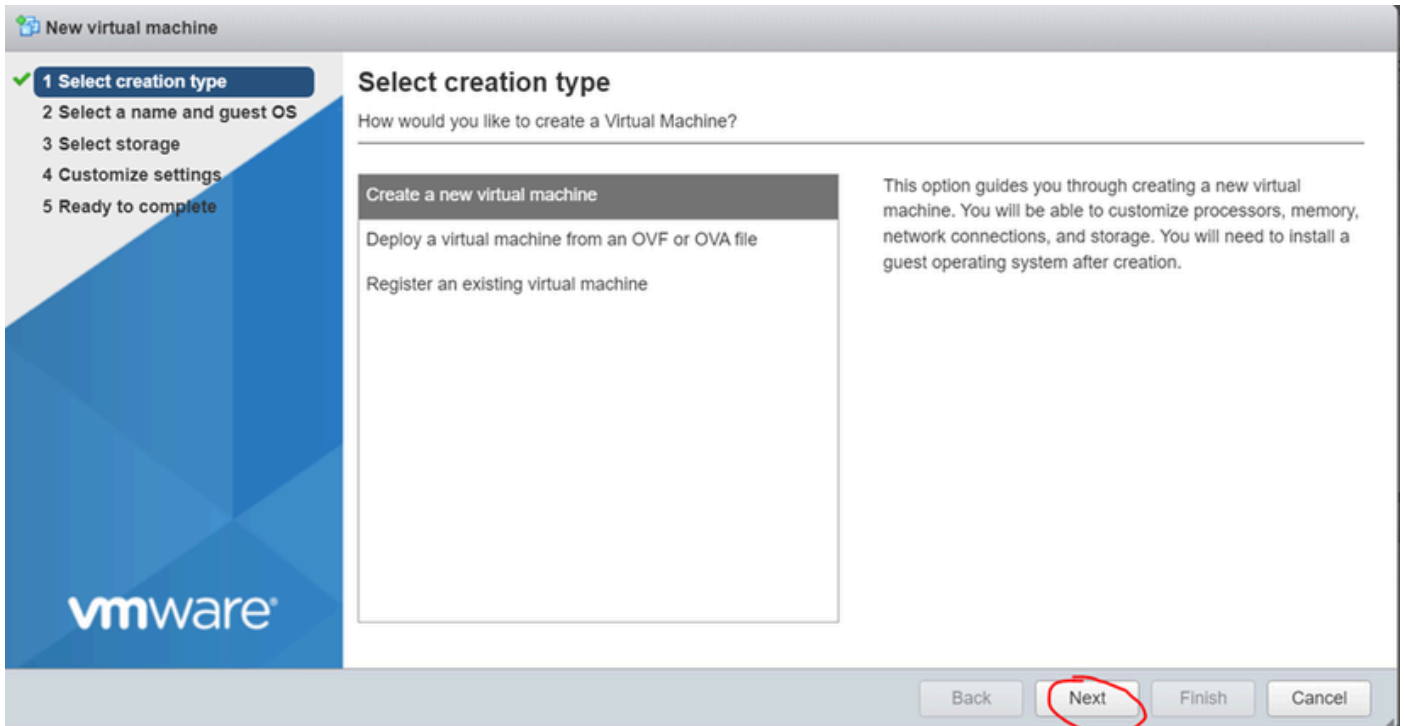
Le téléchargement ISO est terminé

5. Créez la machine virtuelle. accédez à Machine virtuelle > Créer / Enregistrer la machine virtuelle.



Création d'une nouvelle VM, étape 01

6. Choisissez Create a new virtual machine et cliquez sur next.



Création d'une nouvelle VM, étape 02

7. Configurez ensuite les paramètres suivants :

- Name : saisissez le nom de votre ordinateur virtuel.
- Compatibilité : sélectionnez ESXi 6.0 ou version ultérieure ou ESXi 6.5 ou version ultérieure.
- Famille de systèmes d'exploitation invités : Linux.
- Version du système d'exploitation invité : choisissez CentOS 7 (64 bits) ou Other 2.6x Linux (64 bits)

Cliquez sur Next (Suivant).

New virtual machine - CSSM TAC (ESXi 7.0 U1 virtual machine)

1 Select creation type
2 Select a name and guest OS
 3 Select storage
 4 Customize settings
 5 Ready to complete

Select a name and guest OS

Specify a unique name and OS

Name

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility

Guest OS family

Guest OS version

Back Next Finish Cancel

Nom de VM et IOS

8. Sélectionnez votre stockage et cliquez sur next.

New virtual machine - CSSM TAC (ESXi 7.0 U1 virtual machine)

1 Select creation type
 2 Select a name and guest OS
3 Select storage
 4 Customize settings
 5 Ready to complete

Select storage

Select the storage type and datastore

Standard Persistent Memory

Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	870.75 GB	869.33 GB	VMFS6	Supported	Single

1 items

Back Next Finish Cancel

Liste de stockage

9. Configurez les paramètres suivants :

- UC : 4 au minimum. Le paramètre de vCPU réel dépend de vos exigences d'évolutivité



Remarque : la quantité de coeurs par socket doit être définie sur 1, quel que soit le nombre de sockets virtuels sélectionnés. Par exemple, une configuration à 4 processeurs virtuels doit être configurée avec 4 sockets et 1 coeur par socket.

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

Configuration des coeurs

- Mémoire : 8 Go
- Disque dur : 200 Go et vérifiez que le provisionnement est défini sur Provisionnement léger.

▼ 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 du disque

- Carte réseau : sélectionnez le type de carte E1000 et Connect at Power On (Connexion à la mise sous tension).

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

Configuration des paramètres réseau

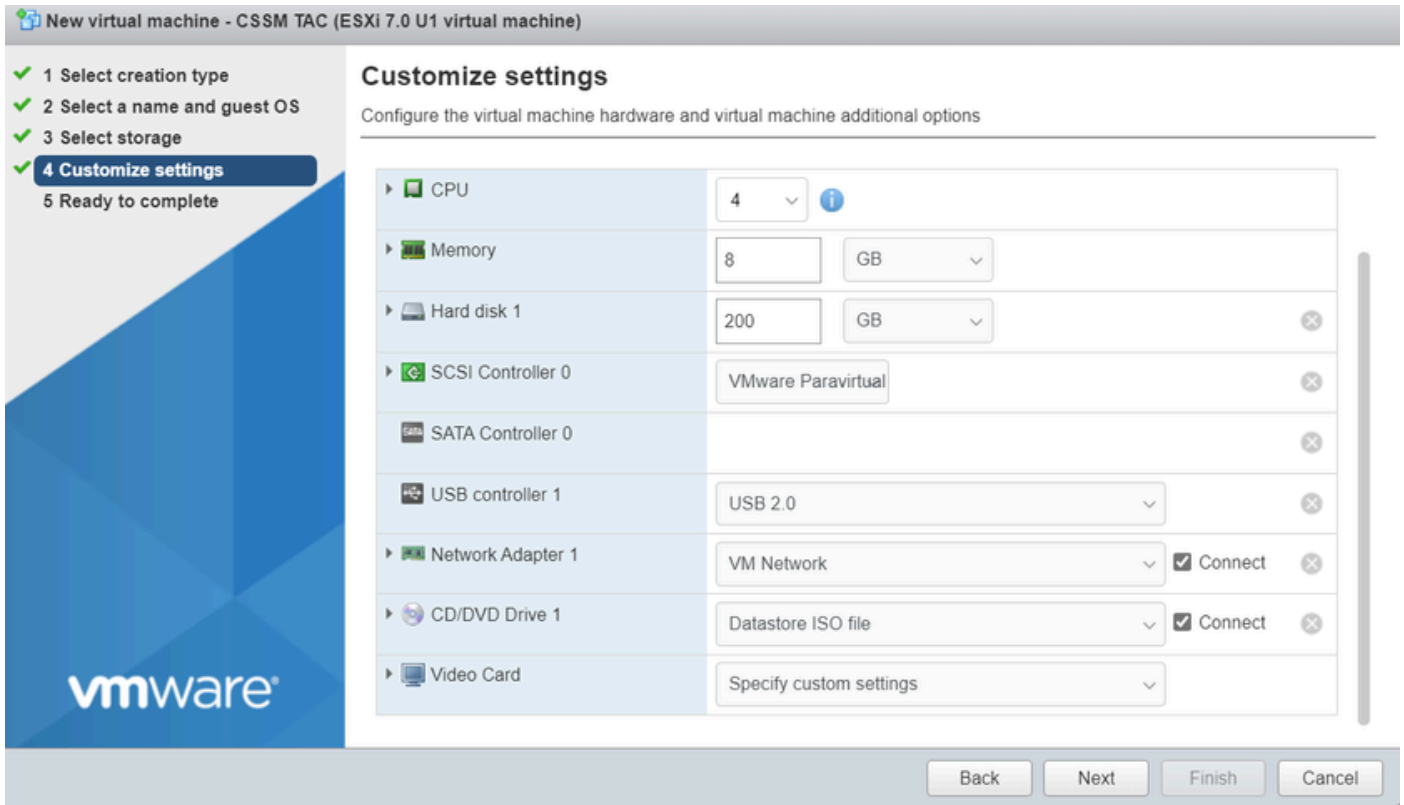
- Lecteur de CD / DVD : Choisissez «Data ISO file» et sélectionnez le fichier ISO.

Datastore browser

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

image ISO

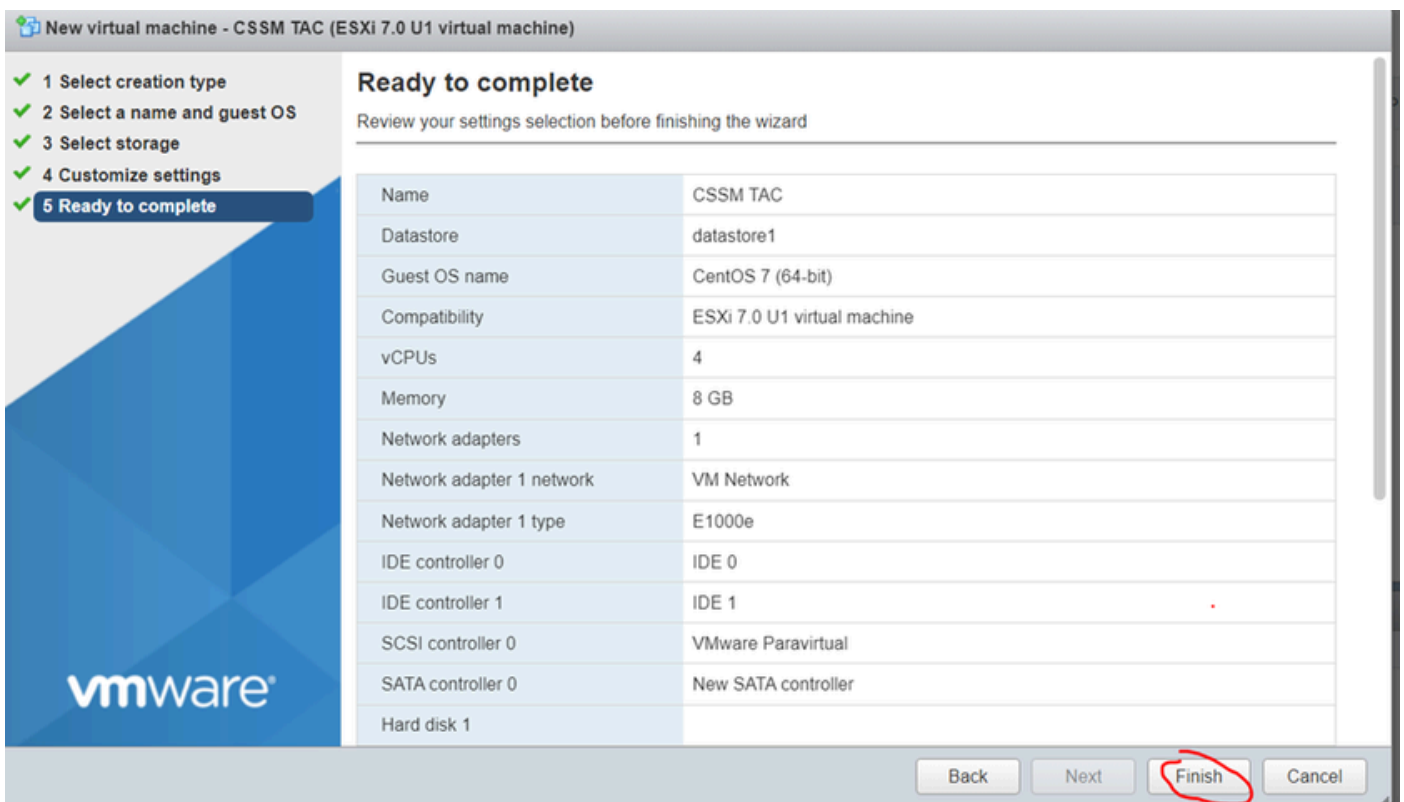
Vous pouvez vérifier le résumé des paramètres une fois que vous avez terminé les étapes précédentes.



Récapitulatif de la configuration VM 01

Cliquez sur Next (Suivant).

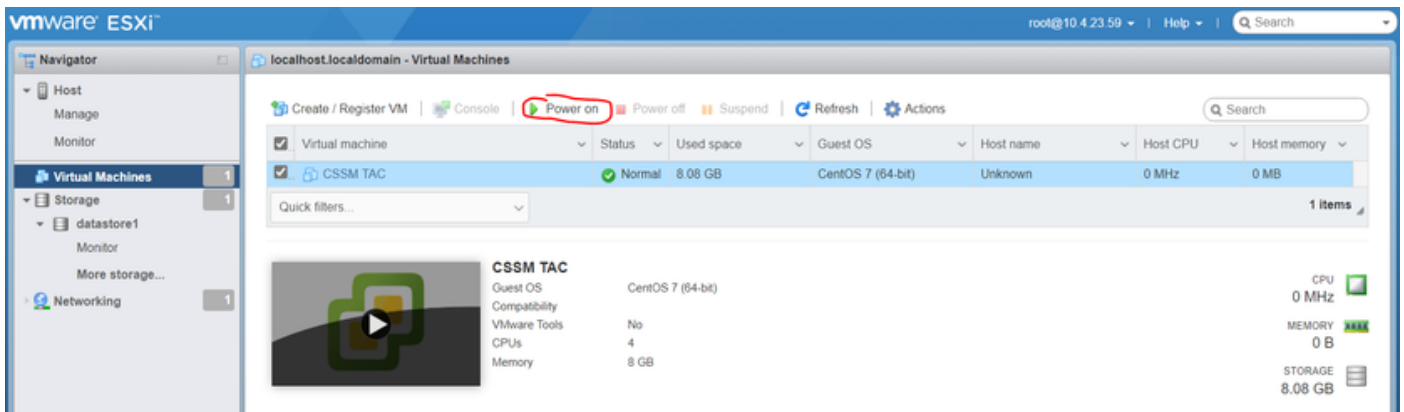
10. Cliquez sur Terminer.



Récapitulatif de la configuration VM 02

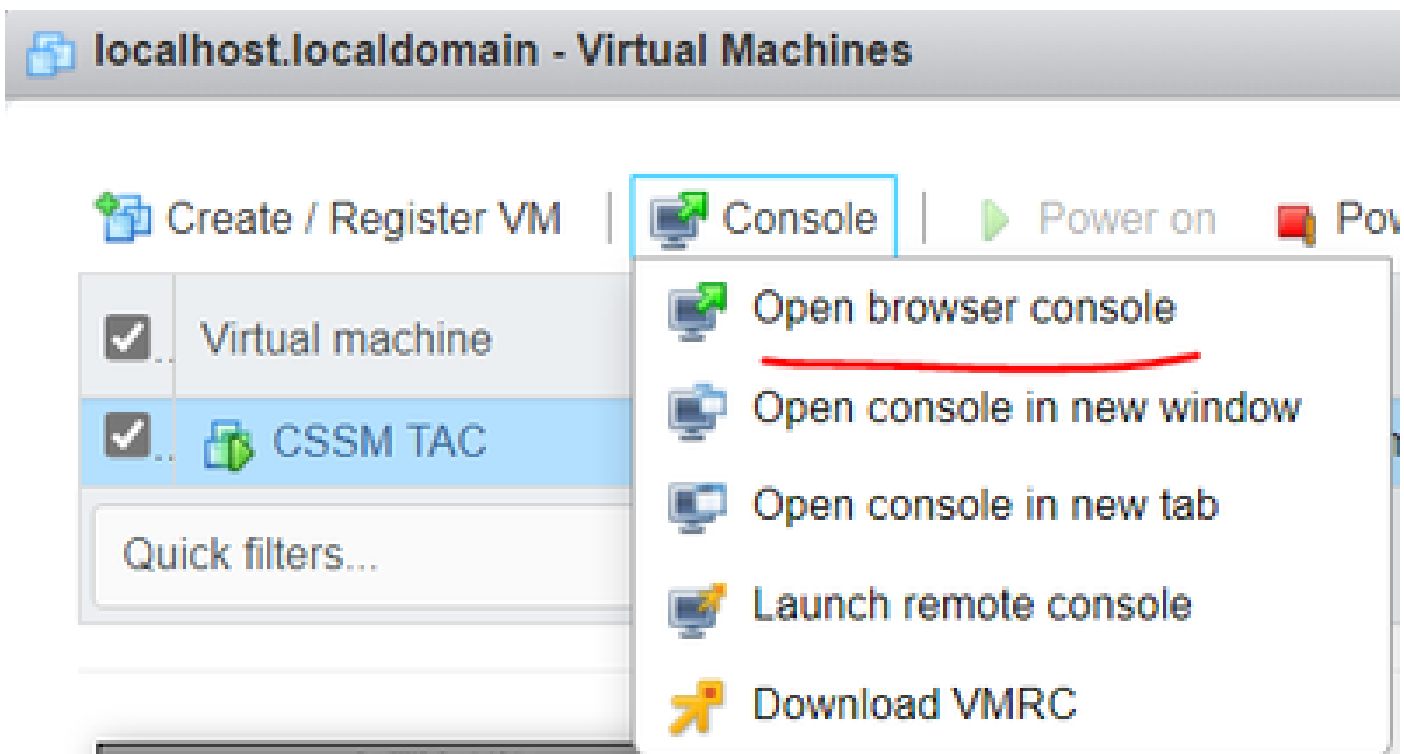
Configuration initiale de CSSM On-Prem .

1. Dans VMWARE ESXi, accédez à Machines virtuelles et sélectionnez votre machine virtuelle, puis cliquez sur Mise sous tension.



Option de mise sous tension

2. Vous disposez de plusieurs options pour gérer la console de VM. Sélectionnez Console > Ouvrir la console du navigateur.



Options de gestion de la VM

3. Configurez vos paramètres réseau.



Remarque : il est important de configurer l'adresse IP du serveur DNS qui résout le nom de domaine complet du CSSM.

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 des paramètres réseau CSSM

Cliquez sur Ok pour configurer votre nouveau mot de passe CLI.

4. Le processus d'installation démarre et se termine jusqu'à ce que vous voyiez l'invite d'accès.

```

CSSM
#####
#                               #
#           Authorized access only!           #
#                               #
# Disconnect IMMEDIATELY if you are not an authorized user!!! #
#           All actions Will be monitored and recorded           #
#                               #
#####

SSM-On-Prem login: _

```

Configuration initiale CSSM terminée

5. Ouvrez un navigateur et entrez `https://<ip_address_CSSM>`.



Log into an Existing Account

User Name

Password

Log In

[Forgot Password](#)

Welcome to Smart Software Manager On-Prem where you can locally manage Smart Licensing and perform local Account Management functions for your organization.

Page de connexion CSSM

Utilisez les informations d'identification par défaut :

Nom d'utilisateur : admin

Mot de passe : CiscoAdmin ! 2345

6. Sélectionnez votre langue.
7. Créez un nouveau mot de passe GUI.
8. Configurez le nom commun de l'hôte. (exemple : nomhôte.votredomaine).

Dans ce cas, cssm.testlab.local a été configuré en tant que nom commun d'hôte.

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

9. Validez votre configuration et cliquez sur 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

Paramètres initiaux du CSSM terminés.

Intégration de CSSM On-Prem avec un compte Smart

Vous devez associer votre compte Smart à votre CSSM On Prem Server.

1. Ouvrez votre compte Cisco Smart en cliquant sur le lien suivant :

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

2. Choisissez ensuite Manage Licenses dans la section Smart Software Manager.

<p>Smart Software Manager</p> <p>Track and manage your licenses. Convert traditional licenses to Smart Licenses.</p> <p style="color: #0070c0; text-decoration: underline;">Manage licenses ></p>	<p>Download and Upgrade</p> <p>Download new software or updates to your current software.</p> <p style="color: #0070c0; text-decoration: underline;">Access downloads ></p>	<p>Traditional Licenses</p> <p>Generate and manage PAK-based and other device licenses, including demo licenses.</p> <p style="color: #0070c0; text-decoration: underline;">Access LRP ></p>
<p>Manage Smart Account</p> <p>Update your profile information and manage users.</p> <p style="color: #0070c0; text-decoration: underline;">Manage account ></p>	<p>EA Workspace</p> <p>Generate and manage licenses purchased through a Cisco Enterprise Agreement.</p> <p style="color: #0070c0; text-decoration: underline;">Access EA Workspace ></p>	<p>Manage Entitlements</p> <p>eDelivery, version upgrade, and more management functionality is now available in our new portal.</p> <p style="color: #0070c0; text-decoration: underline;">Access MCE ></p>
<p>Option Gérer les licences</p>		

3. Accédez à Inventaire et copiez le nom de votre compte Smart ainsi que celui de votre compte virtuel. Dans ce guide, il s'agit de InternalTestDemoAccount67 et de 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

Page Software Cisco

4. Ouvrez l'interface utilisateur graphique de CSSM et sélectionnez l'option Admin Workspace.

On-Prem License Workspace

CISCO

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.

Menu principal CSSM.

5. Sélectionnez ensuite Comptes.

On-Prem Admin Workspace

Smart Software Manager On-Prem



Access
Management



Settings



Accounts



Support
Center



API Toolkit



Synchronization



Network



Users



Security

utilisez cette option pour enregistrer le service CSSM On-Prem avec votre compte Smart via Internet.

- Rejeter : abandonne la demande.
- Manual Registration (Enregistrement manuel) : utilisez cette option pour enregistrer le service CSSM On-Prem avec votre compte Smart sans Internet.

OPTION 1 : Enregistrez votre module CSSM On-Prem via une connexion Internet.

1. Si vous choisissez Approve, vous devez entrer votre nom d'utilisateur et votre mot de passe de votre compte Smart Cisco et cliquer sur Submit.

Account Registration

X

Enter SSO Credentials

Username *

otegoma@cisco.com

Password *

●●●●●●●●●●

Submit

Approuver l'option

Cliquez ensuite sur next pour accepter l'enregistrement du compte.

Account Registration

X

Review Account Requests

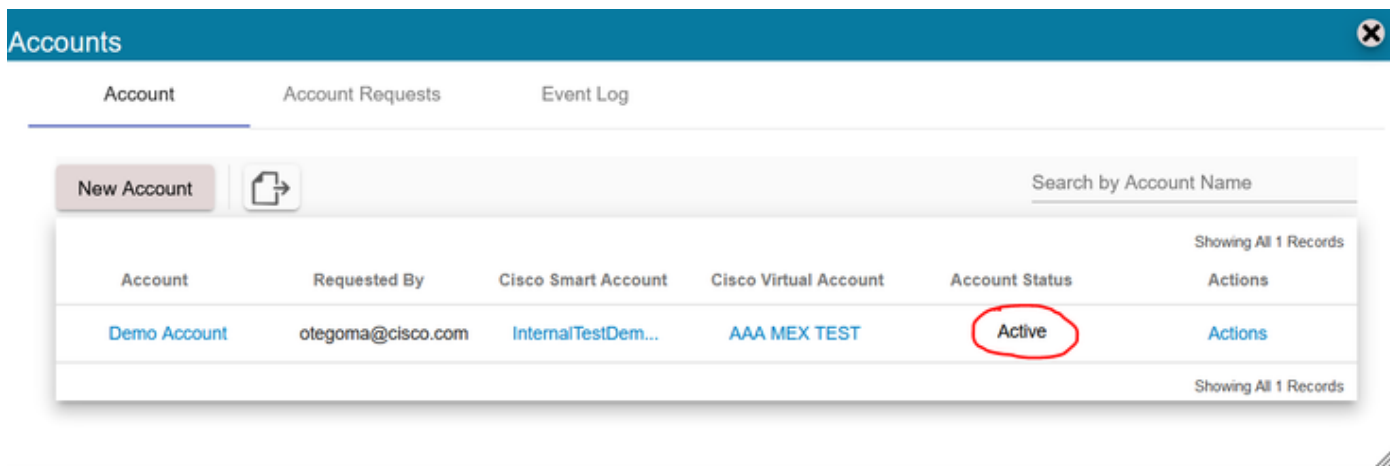
Account Name	Demo Account
Cisco Smart Account	InternalTestDemoAccount67.cisco.com ▼
Cisco Virtual Account	AAA MEX TEST ▼ ⓘ
Requestor Email	otegoma@cisco.com
Request Date	2023-Jul-27 15:00:31
Message to Approver	

Cancel

Next

Enregistrement du compte.

Pour confirmer le statut de l'inscription, accédez à Compte et le statut du compte doit être actif.



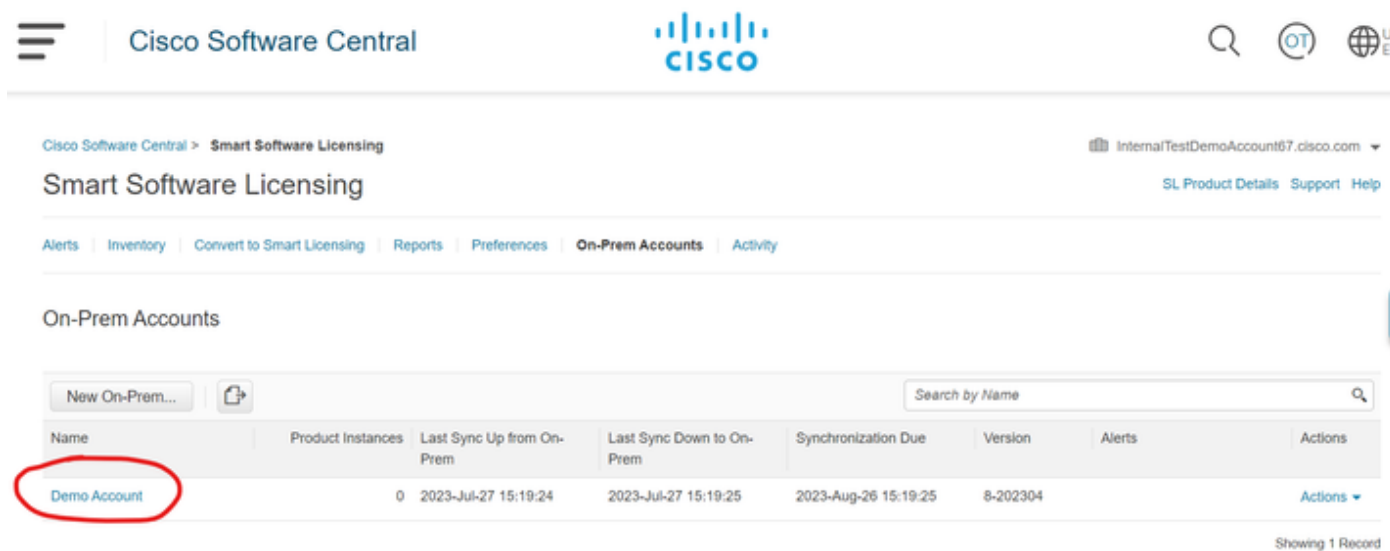
The screenshot shows the 'Accounts' page in Cisco Software Central. It features a navigation bar with 'Account', 'Account Requests', and 'Event Log'. Below the navigation bar, there is a 'New Account' button and a search bar labeled 'Search by Account Name'. A table displays the account details:

Account	Requested By	Cisco Smart Account	Cisco Virtual Account	Account Status	Actions
Demo Account	olegoma@cisco.com	InternalTestDem...	AAA MEX TEST	Active	Actions

The 'Active' status in the 'Account Status' column is circled in red. The table also indicates 'Showing All 1 Records' at the top right and bottom right.

Statut du compte.

Ouvrez maintenant votre compte Smart (<https://software.cisco.com/>). Sélectionnez ensuite l'option On-Prem Accounts pour afficher le nouveau registre.



The screenshot shows the 'Cisco Software Central' interface. The main header includes the Cisco logo and navigation icons. The page title is 'Smart Software Licensing'. Below the title, there are navigation links: 'Alerts', 'Inventory', 'Convert to Smart Licensing', 'Reports', 'Preferences', 'On-Prem Accounts', and 'Activity'. The 'On-Prem Accounts' section is active, showing a table with one account listed: 'Demo Account'. The 'Demo Account' is circled in red.

Name	Product Instances	Last Sync Up from On-Prem	Last Sync Down to On-Prem	Synchronization Due	Version	Alerts	Actions
Demo Account	0	2023-Jul-27 15:19:24	2023-Jul-27 15:19:25	2023-Aug-26 15:19:25	8-202304		Actions

The table also indicates 'Showing 1 Record' at the bottom right.

Sur le compte Prem.

OPTION 2 : Enregistrez votre module CSSM On-Prem sans connexion Internet.

Si vous choisissez Enregistrement manuel, cliquez sur Générer un fichier d'enregistrement. Cette opération crée une demande d'enregistrement qui va être téléchargée sur votre ordinateur.

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

Enregistrement manuel.

Ouvrez ensuite votre compte Smart (<https://software.cisco.com/>) et accédez à Comptes sur site.

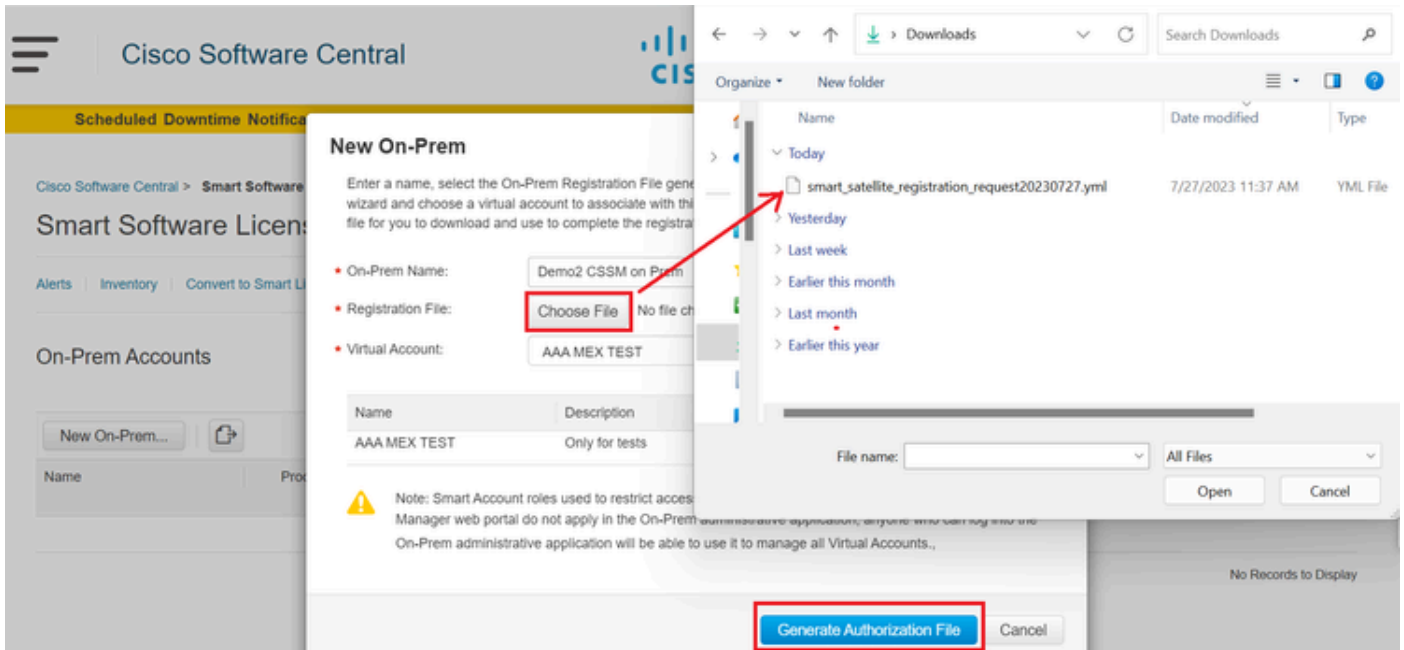
Cliquez sur Nouveau sur site

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 main content area is titled 'Smart Software Licensing' and includes a breadcrumb trail: 'Cisco Software Central > Smart Software Licensing'. The 'On-Prem Accounts' section is active, displaying 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 shows 'No Records Found'.

Ajout d'un nouveau serveur sur site.

Configurez ensuite les paramètres suivants :

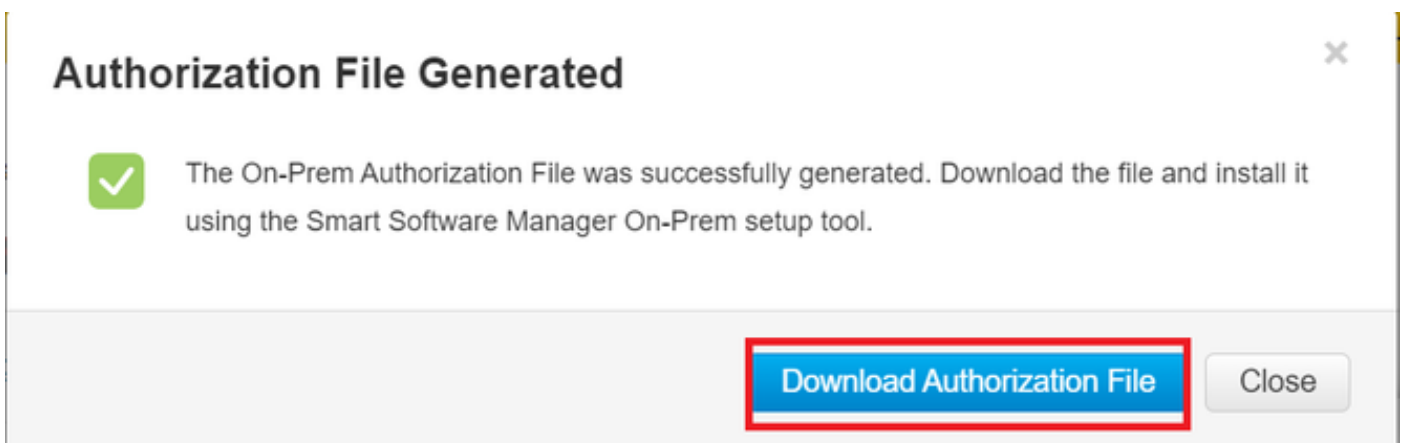
- On-Prem Name : il s'agit d'un nom personnalisé du nouveau registre.
- Registration File : cliquez sur Choose File et sélectionnez la demande d'enregistrement.
- Virtual Account : collez votre nom de compte virtuel.



Fichier d'autorisation.

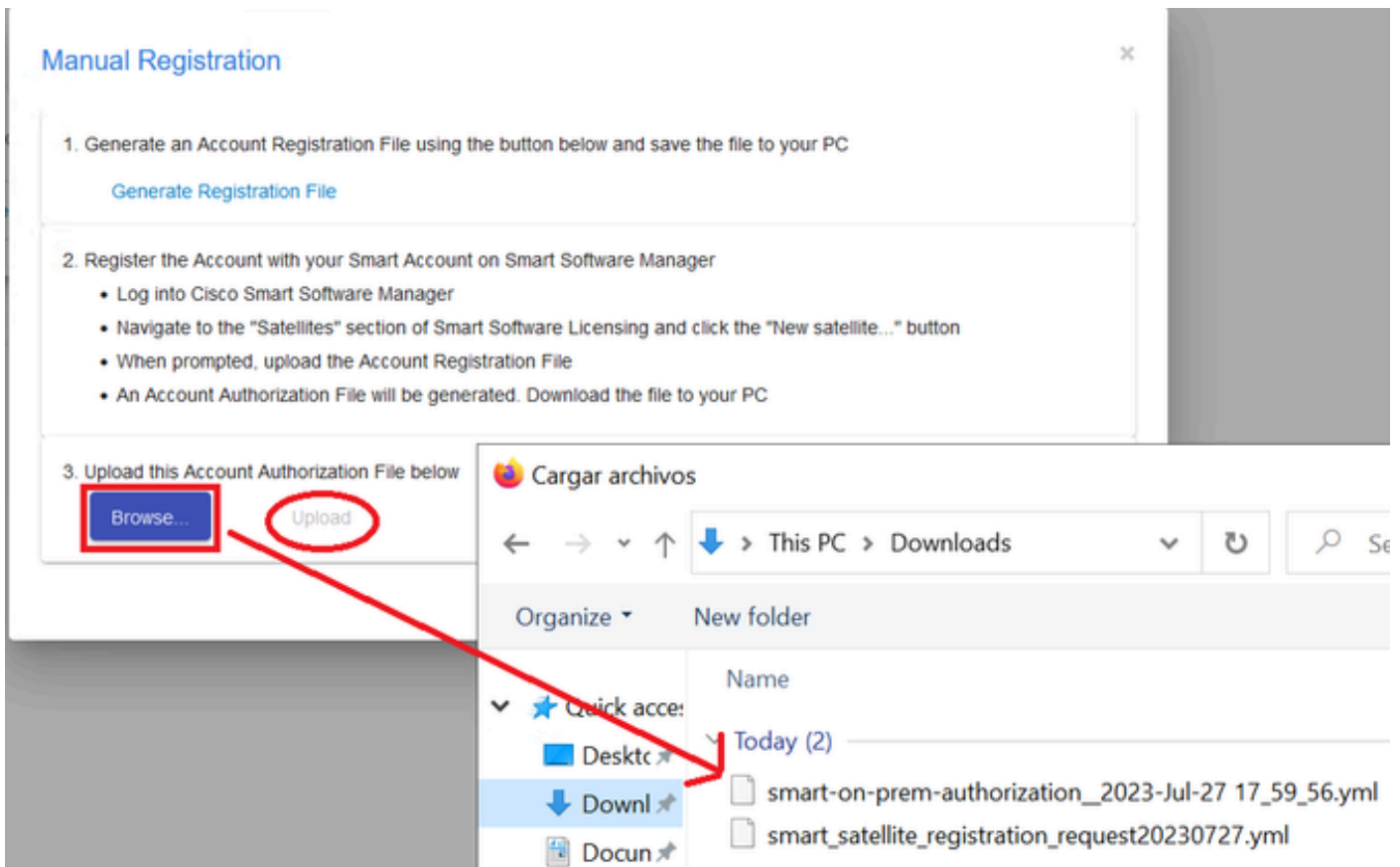
Et cliquez sur Generate Authorization File.

Téléchargez ensuite le fichier d'autorisation.



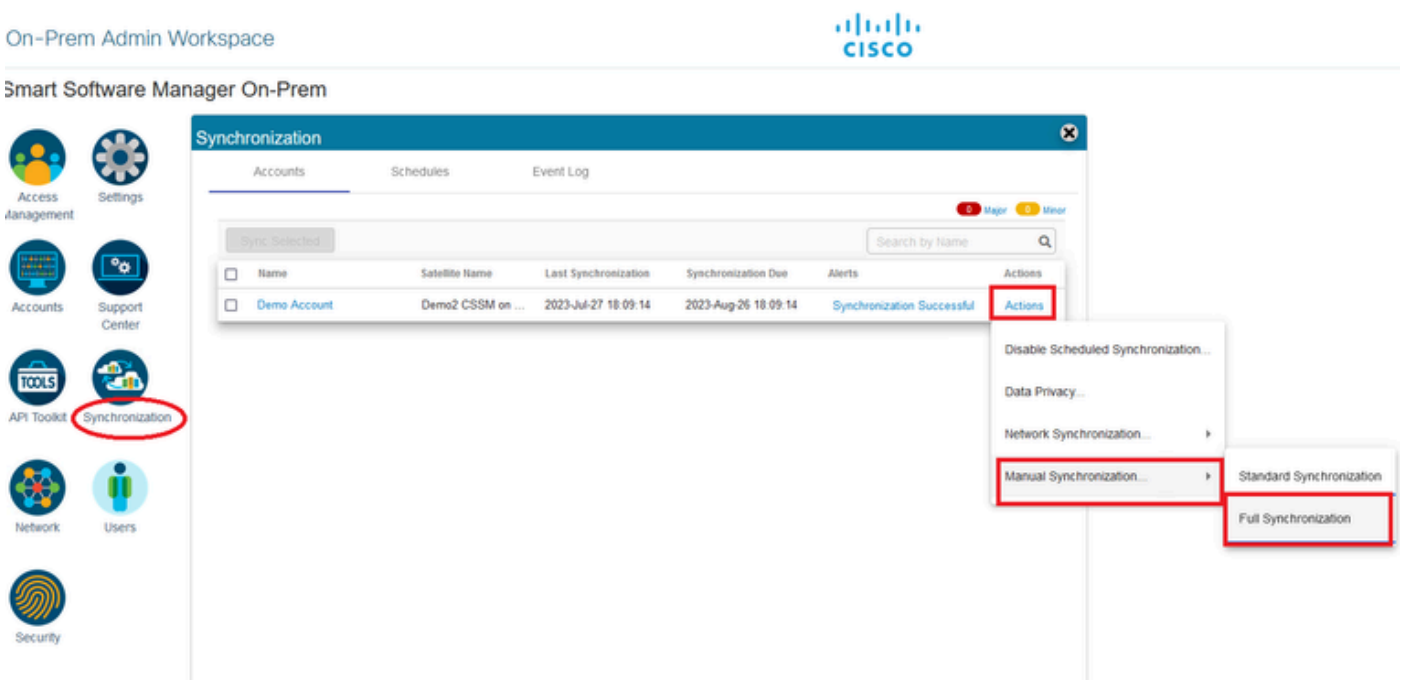
Téléchargement du fichier d'autorisation.

Ouvrez l'interface utilisateur graphique de CSSM pour télécharger le fichier d'autorisation. Cliquez sur Browse, choisissez le fichier, puis cliquez sur Upload.



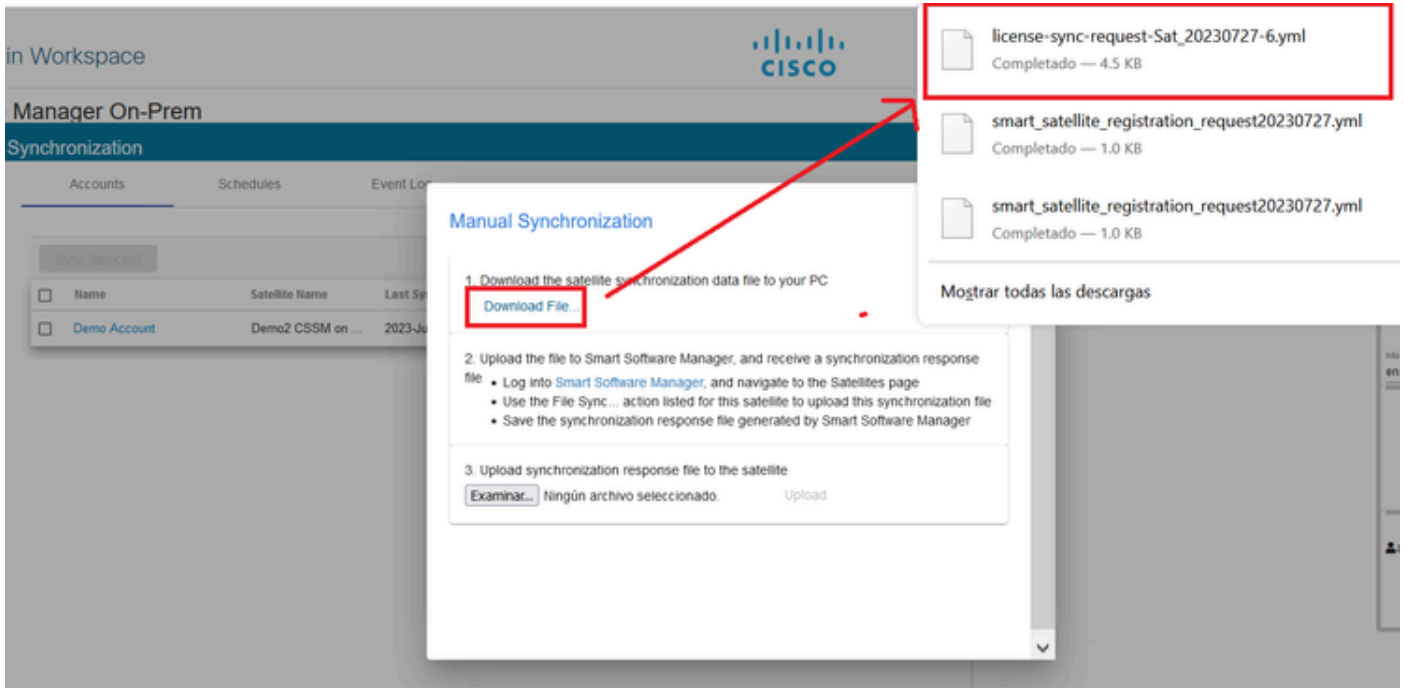
Téléchargement du fichier d'autorisation.

Accédez ensuite à Synchronization et cliquez sur Actions > Manual Synchronization > Full Synchronization.



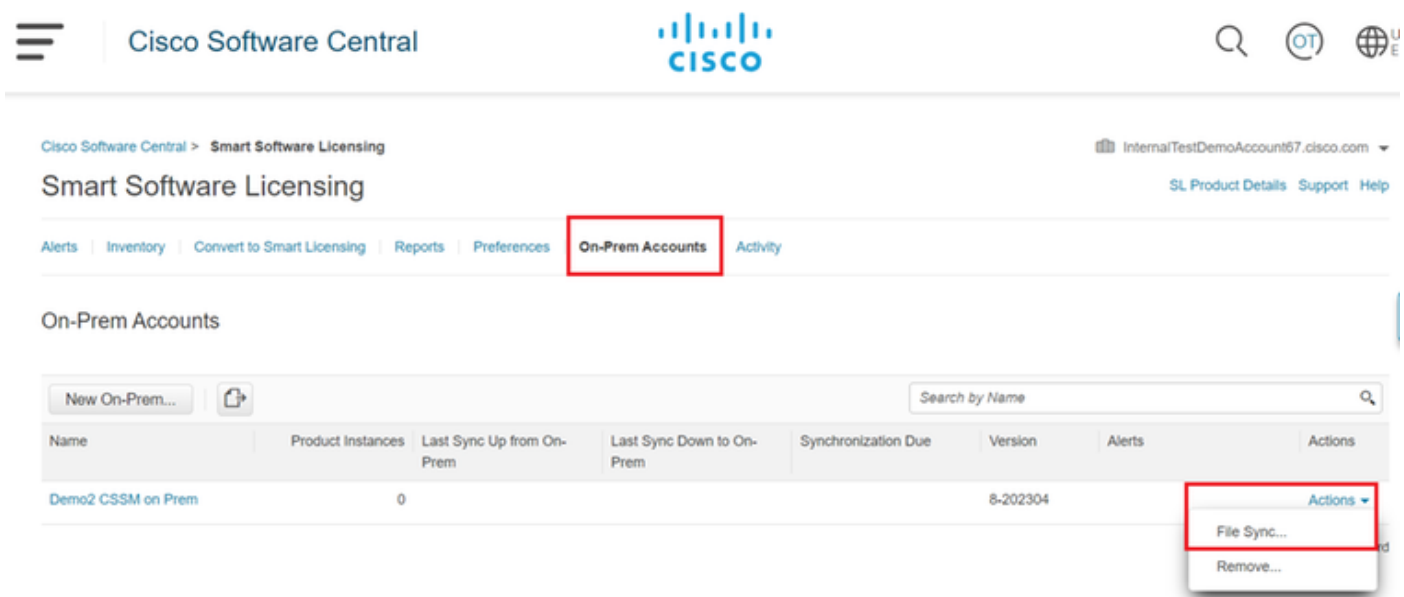
Synchronisation manuelle.

Téléchargez le fichier de demande de synchronisation.



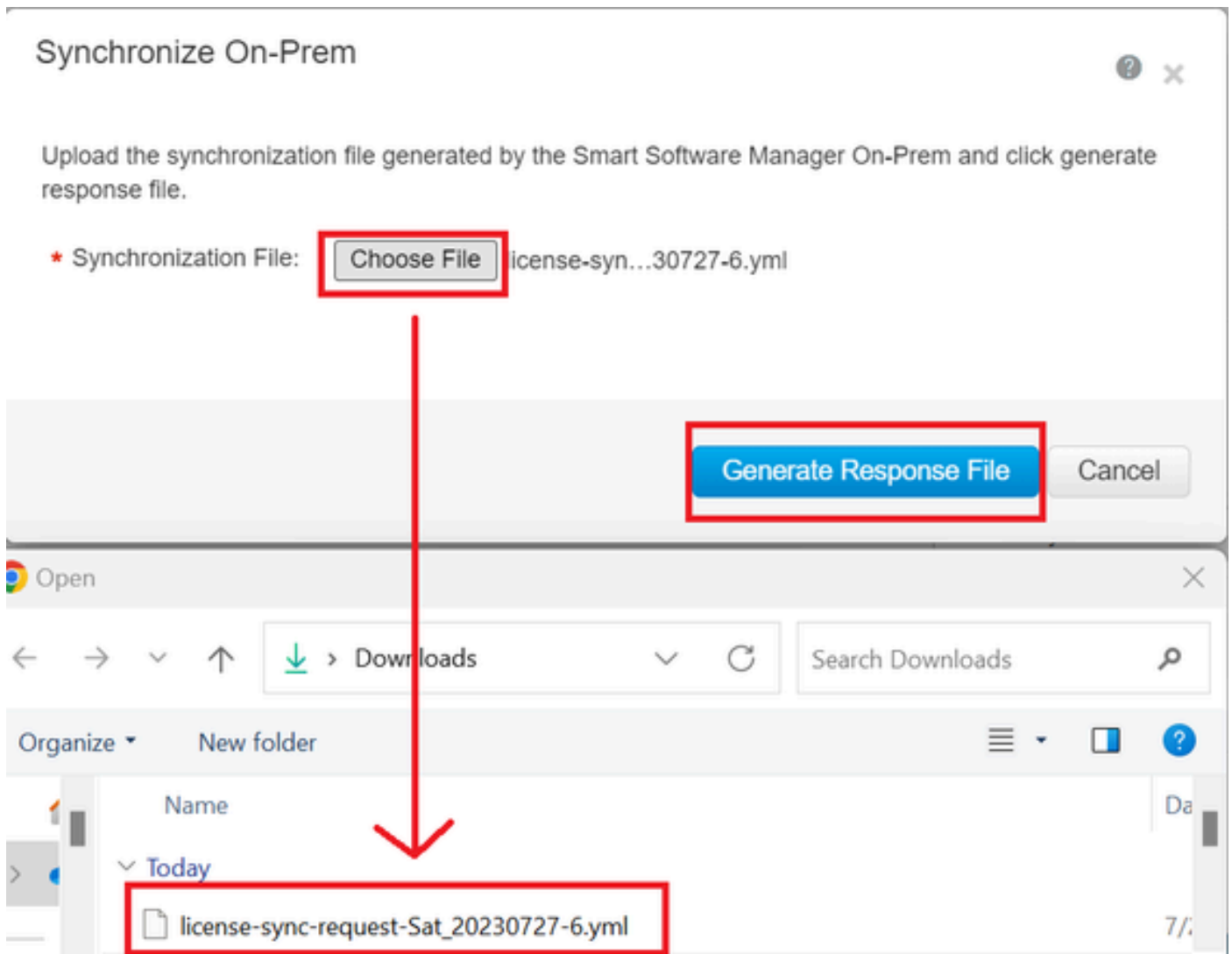
Téléchargement du fichier Sync.

Ouvrez votre compte Smart et sélectionnez Compte On-Prem, puis recherchez votre nom On-Prem CSSM dans la liste et cliquez sur Actions > File Sync



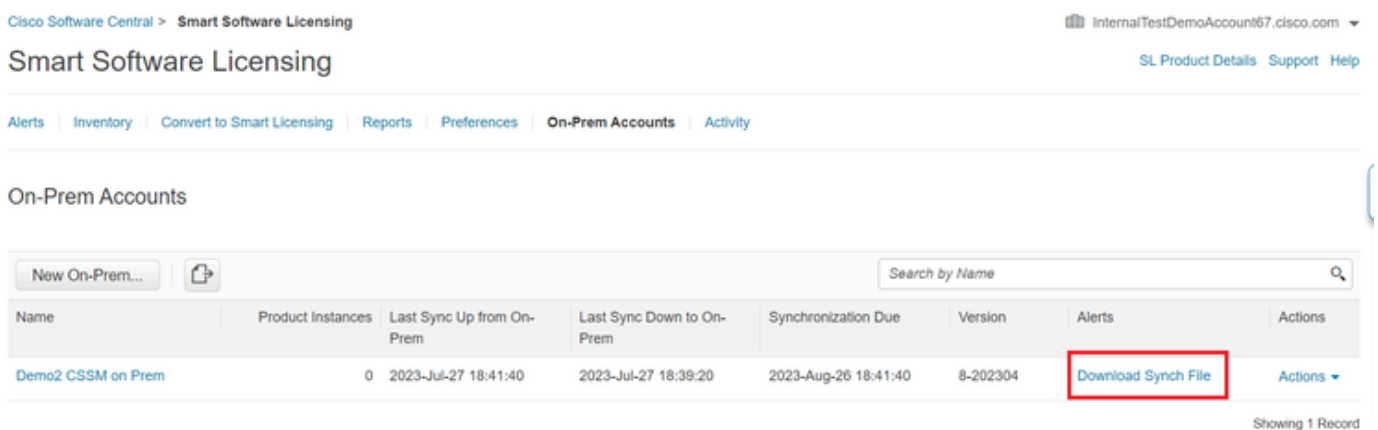
Téléchargement du fichier Sync.

Téléchargez ensuite le fichier de demande de synchronisation, et cliquez sur Generate Response File.



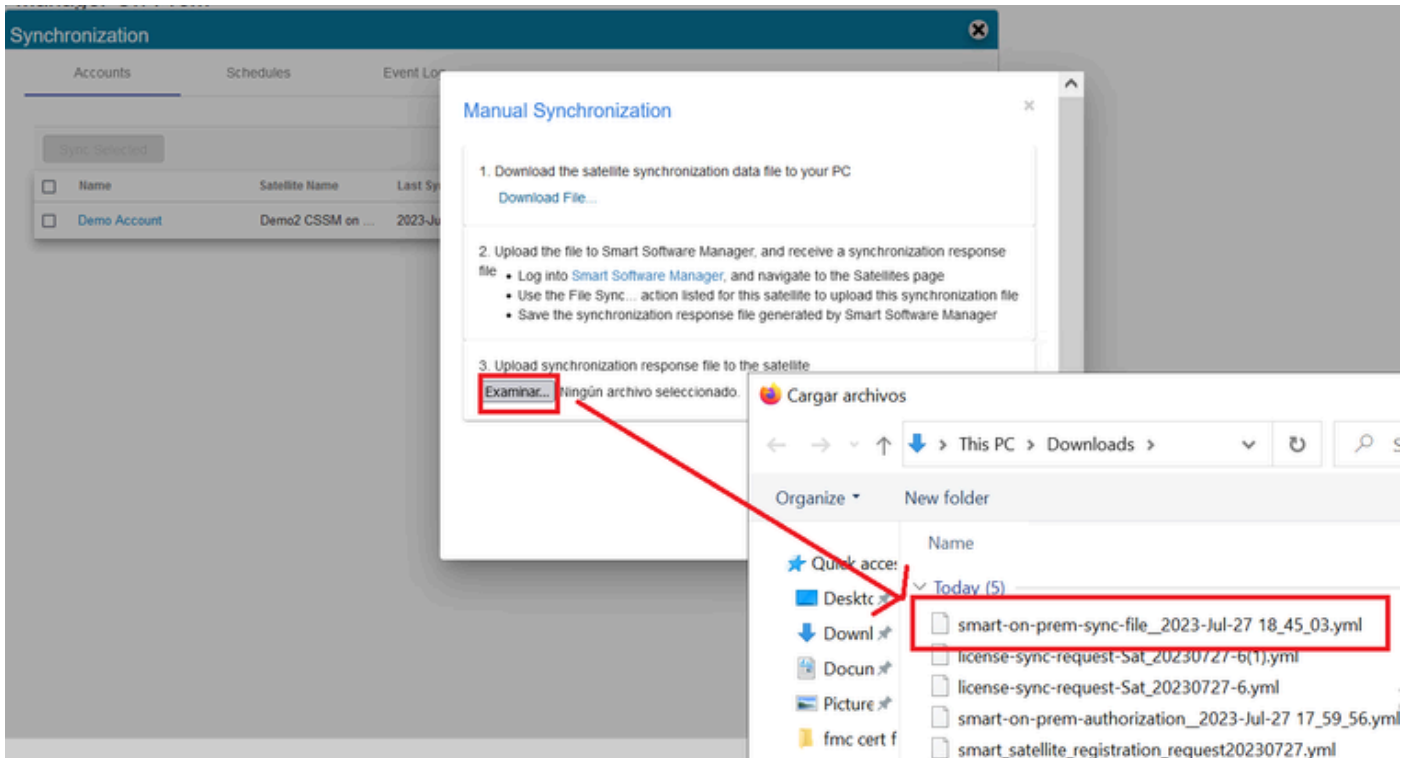
Générez un fichier de réponse.

Cliquez ensuite sur Télécharger le fichier de réponse de synchronisation



Fichier de synchronisation.

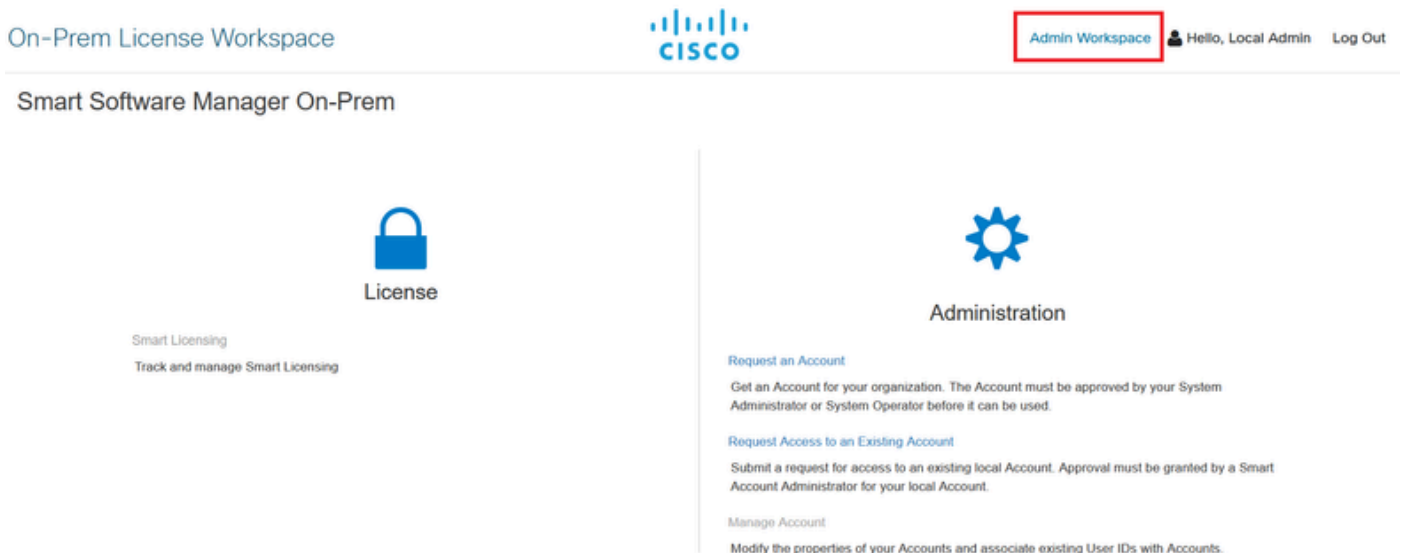
Et enfin, téléchargez le fichier de réponse de synchronisation dans le CSSM sur site.



Synchronisation terminée.

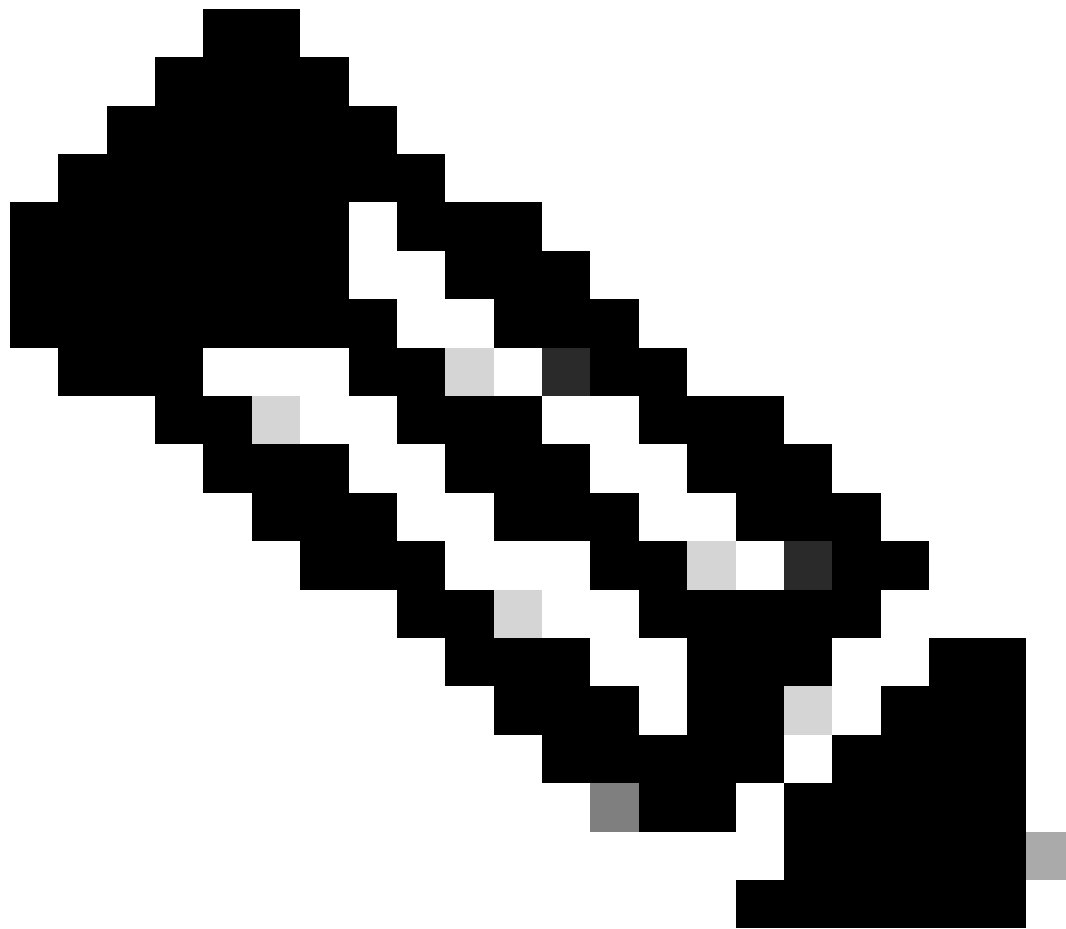
Intégration de CSSM On-Prem avec ISE.

1. Ouvrez l'interface graphique utilisateur de CSSM et sélectionnez Admin Workspace.



Menu principal CSSM.

2. Accédez à Security > Certificates > Generate CSR



Remarque : il est important que le nom d'hôte + domaine soit configuré sur le nom commun d'hôte car ISE utilise ce paramètre afin d'établir une connexion avec le CSSM. Vous pouvez utiliser une adresse IP au lieu du nom d'hôte + domaine, mais la recommandation est d'utiliser le nom d'hôte + domaine



Remarque : les étapes suivantes décrivent la procédure d'installation du certificat de l'interface utilisateur graphique dans le CSSM. Si vous souhaitez protéger la connexion de gestion à votre CSSM GUI à l'aide d'un certificat signé par votre autorité de certification personnelle, vous devez vérifier les étapes suivantes. Sinon, vérifiez directement l'étape 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				

Option CSR.

3. Saisissez ensuite vos informations personnelles. N'oubliez pas que le nom alternatif de l'objet est créé automatiquement en utilisant la même valeur que le nom commun. Le CSR est téléchargé automatiquement après avoir cliqué sur Générer.

Generate CSR

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

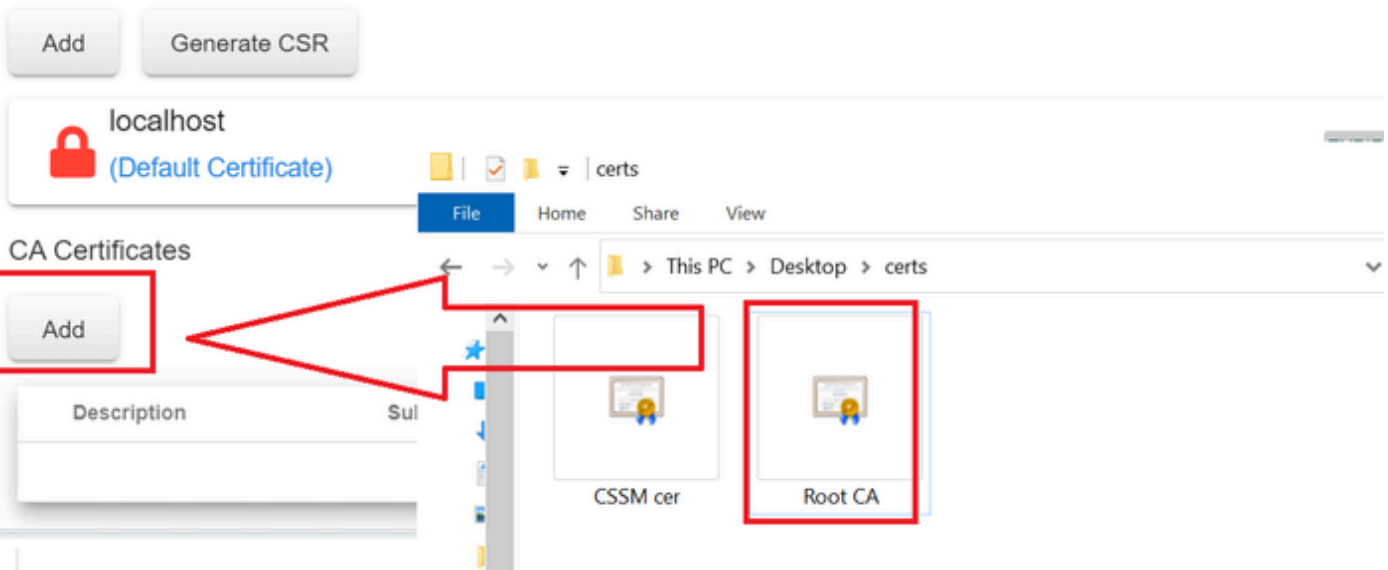
Generate

Cancel

Détails CSR.

4. Signez le CSR : pour plus d'informations, consultez la section « [Créer des certificats à partir de l'autorité de certification Windows](#). » de ce document.
5. Téléchargez le certificat CA racine.

Browser Certificate



Téléchargement de l'autorité de certification racine

Cliquez sur Continuer.



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

Option Continuer.

6. Entrez une description et choisissez le certificat racine et cliquez sur Ok.

Upload Certificate

* Description:

* Certificate:

Description de l'autorité de certification racine

7. Téléchargez le CSR signé par l'AC (certificat d'identité CSSM).

Browser Certificate

localhost
(Default Certificate)

CA Certificates

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

Téléchargement du certificat d'identité CSSM.



Remarque : REMARQUE : dans notre cas, le certificat intermédiaire n'existe pas dans notre CA. Toutefois, si vous utilisez un certificat intermédiaire dans votre architecture, le certificat intermédiaire est obligatoire.

8. Vérifiez ensuite que les deux certificats ont été installés.

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

Validation des certificats.

9. Créez un jeton sur le SSM On-Prem : Select licensing Workspace.

On-Prem Admin Workspace  **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

Page Workspace.


10. accédez à Licences Smart.

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.

11. Recherchez votre compte virtuel local, puis cliquez sur New Token et cliquez sur 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 csli as transport, you must configure the "license smart transport csli" 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...

Nouvelle option de jeton.

12. Sélectionnez Create Token et copiez-le.

Create Registration Token

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

Local Virtual Account: Default

Description:

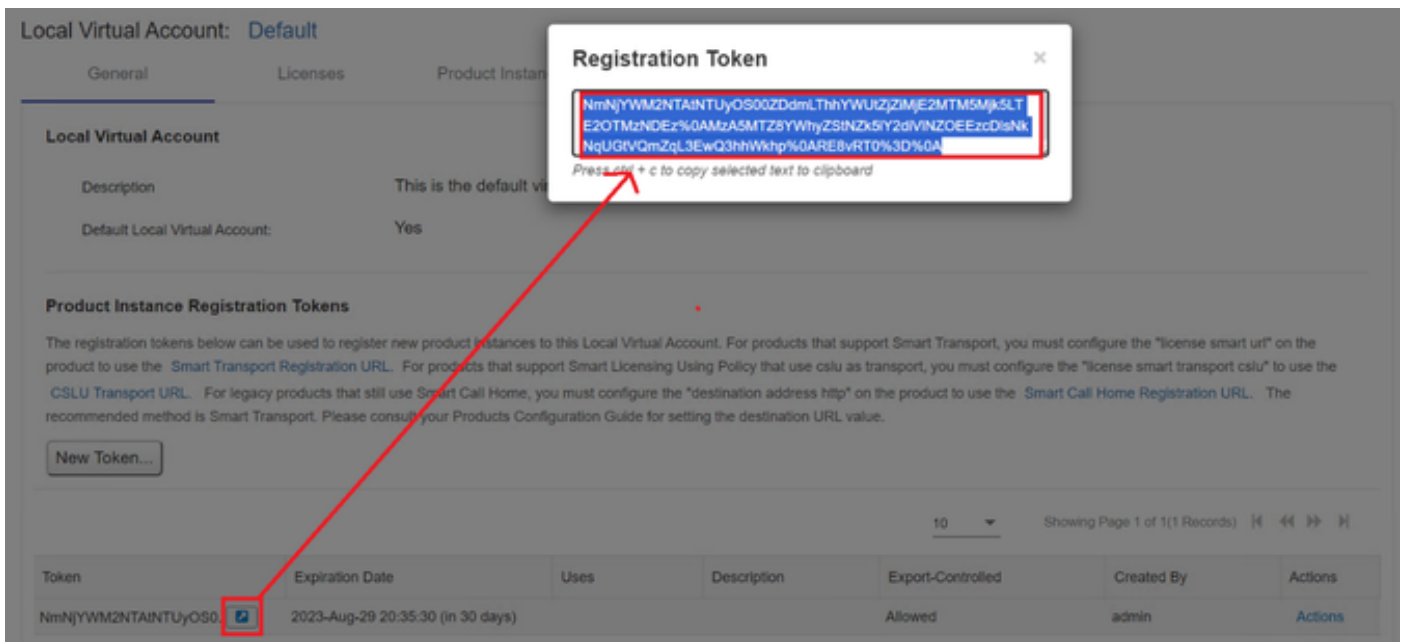
Expire After: Days
Enter a value between 1 and 9999, but Cisco recommends a maximum of 30 days

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 **i**

Create Token **Cancel**

Création du nouveau jeton.



Détails du jeton.

- Ouvrez l'interface utilisateur graphique d'ISE et accédez à Administration > Systems > Licensing, puis cliquez sur Registration details, sélectionnez la méthode hôte du serveur sur site SSM, et collez le jeton.

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

Enregistrement des licences.

- Entrez le nom de domaine complet SSM On-Prem FQDN sur l'hôte du serveur SSM On-Prem et cliquez sur 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](#).

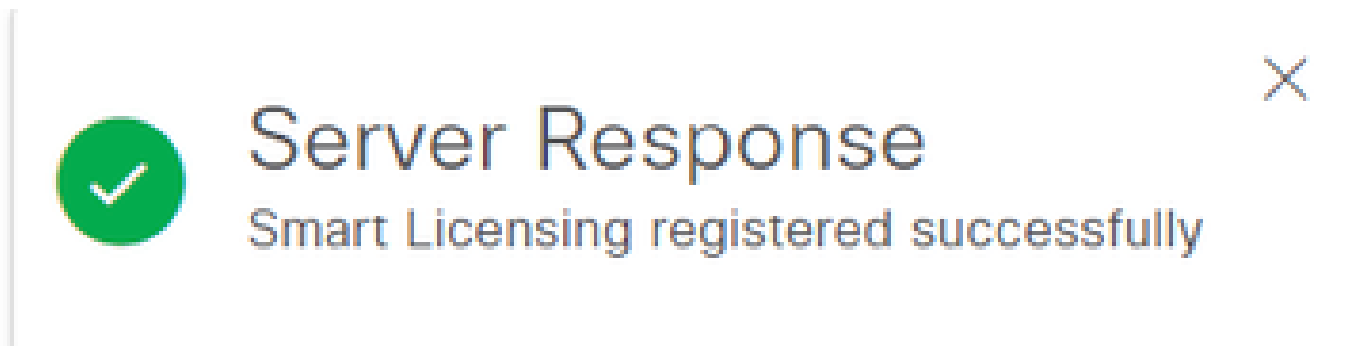
Cancel Register

Paramètres CSSM et ISE.

Remarque : il est important de configurer le nom d'hôte + le domaine sur le nom commun d'hôte car ISE utilise ce paramètre afin d'établir une connexion avec le CSSM. Vous

pouvez utiliser une adresse IP au lieu du nom d'hôte + domaine, cependant la recommandation est d'utiliser le nom d'hôte + domaine

15. Et enfin, l'enregistrement est terminé.

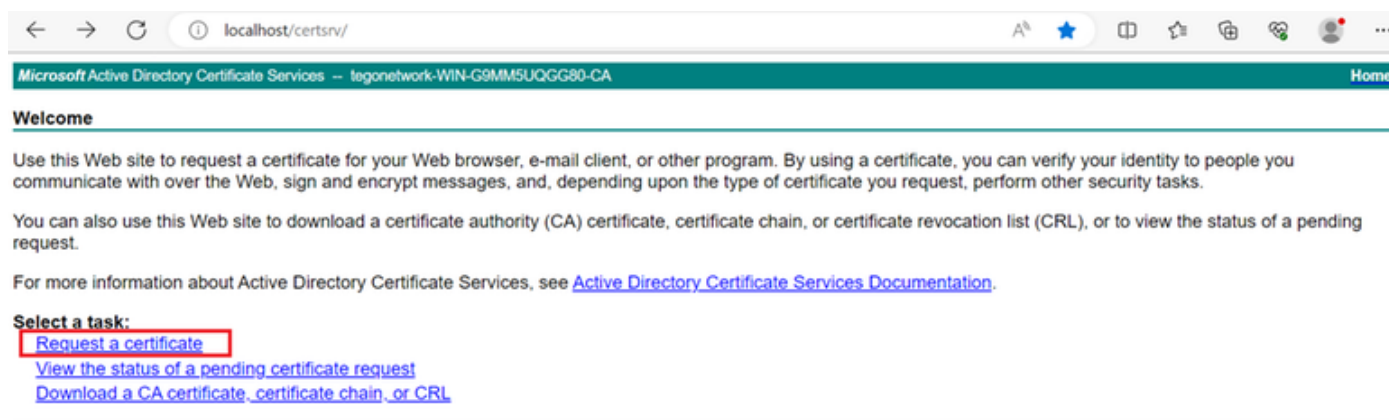


Inscription terminée.

Créer des certificats à partir de Windows CA.

Si vous êtes l'administrateur de l'autorité de certification, vous devez procéder comme suit :

1. Ouvrez un navigateur Web et accédez à <http://localhost/certsrv/>
2. Cliquez sur Demander un certificat.



Demander un certificat.

3. Cliquez sur Advanced certificate request (requête de certificat avancée).



Demande de certificat avancée.

4. Ouvrez la CSR générée précédemment. Copiez ensuite les informations et collez-les sur la demande enregistrée.

The screenshot shows a Notepad window on the left with a CSR (Certificate Signing Request) text. The text is as follows:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC9jCCAd4CAQAwFzEdMBsGA1UEAwwUc2NjbXRhYy5jaXNjb3R5Yy5jb20xYjA4
BgNVBAsMDUNpc2NvIFN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1
MRgWFGYDQQA9JbnN1cmd1bnR1cyBTdXIxEDA0BGNVBA0MB0FBQSBTRUMjggE1
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCdYQ8fX58o7DXY30HJ1yF04AZ
DZHN80B091gPDMaxtbNFGqDnvcwEqEy1yxnuF5hm//TuZ3oYfvv5sYfAjCP9V
11Xdrw5Gkd/IBrW0sXhnmC+K1FyJsziv+EFd0zJ4A0+yG1x7uEu+j96Yfj18NFdI
1tU2geSaMFBE/HGXbXDLFbiFmVE+95gRalG5r5VK1i1ocVZ8ImDucT4LByCiqRrs
WVf87e6dMvebi5gSDwkkRBGeUOL+f4DuknRnUmEHRVHEnkzXfcm86u8fzI+vYcTf
Knk2+z4moHTiRZw/cDQ4m2I28p7CesN8CDtkwGC6fufmqOwkadDdS+eXbadAgHB
AAGhJjAwBgkqhkiG9w0BCCQ4xIzAHMB8GA1UdEQYMBaCFHnjY210YmUy21zY290
YmUy29tMA0GCSqGSIb3DQEBCwUAA4IBAQAUF+3q0rOvHKA3eokKXHomR9510eR
/dq+ICgJ6EPBa03hpo6hVPTi/MV3H5ye8j5gcq4cDbHu/VTf/gQ51Aa9QRhfPug
HdPwBukPNwcydys88ERUQgFyHnaltNGmZwtAz39UP7oIAPV+uNR73Ue9ka694Im
cb7XNgnk3w5HdeIXzS/8YCGd1CCDIuLQMsRI46aFKHnsz3Wu1asAYyEyqhiFr
HvX9u5390kML0HueT7bMos6QwRTvt581DuHme//19y0m8MyWrgTjAk0VnyDzPUSR
/xjTeZ7fGwCsF0SUUM4xQ8+7Cq1AUkZob8m1UwVYvI7b+hLC8Bam+yD1
-----END CERTIFICATE REQUEST-----
```

The browser window on the right shows the Microsoft Active Directory Certificate Services interface. The 'Saved Request' field is highlighted in red, and the 'Submit >' button is also highlighted in red.

Envoyer le certificat.

Après avoir cliqué sur Submit, le certificat est téléchargé automatiquement.

5. Téléchargez maintenant la racine du certificat CA. Revenez à <http://localhost/certsrv/> et sélectionnez Télécharger un certificat CA, une chaîne de certificats ou une liste de révocation de certificats.

The screenshot shows the 'Welcome' page of the Microsoft Active Directory Certificate Services. The page contains the following text:

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Téléchargez l'autorité de certification racine.

6. Téléchargez le certificat CA en utilisant la méthode de codage 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](#)

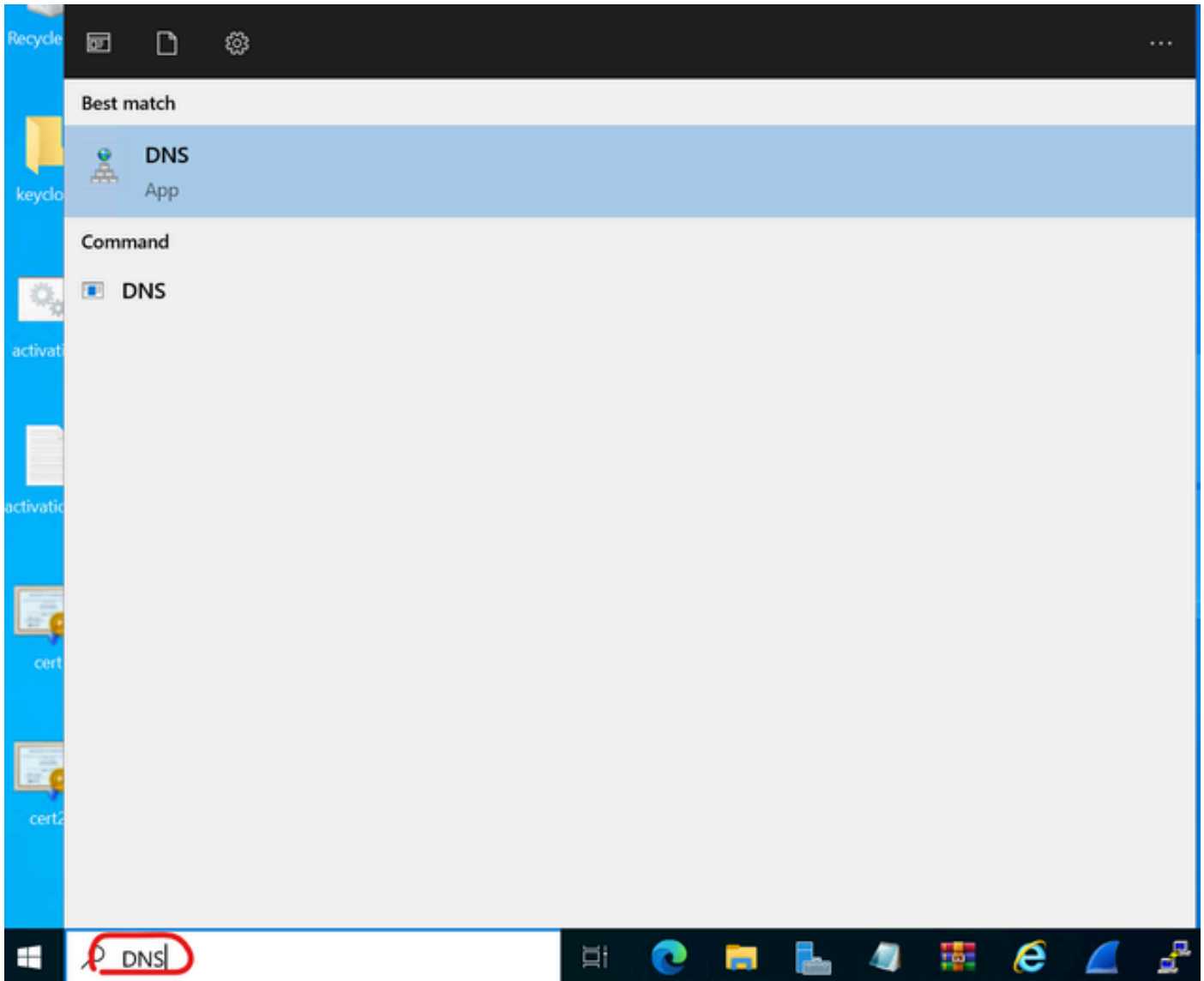
[Download latest base CRL](#)

Option Base 64.

Ajoutez des enregistrements DNS sur Windows Server.

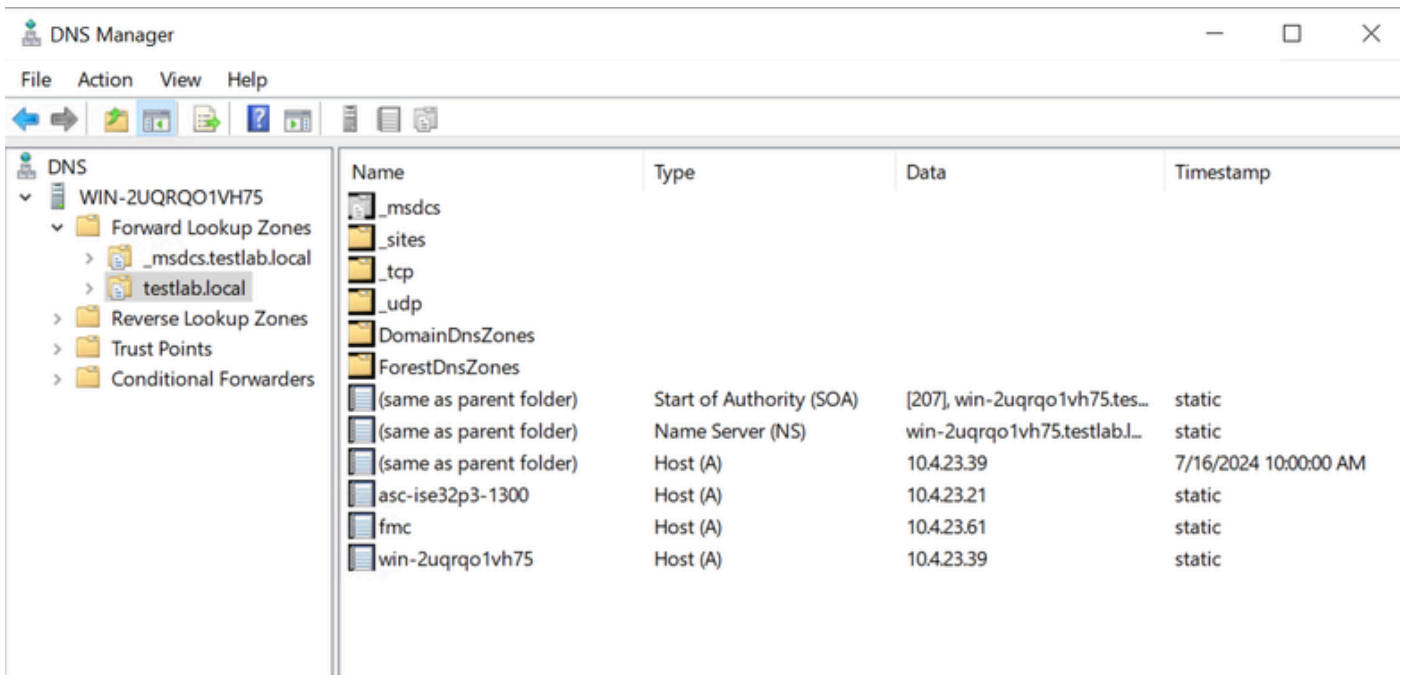
Si vous êtes l'administrateur, ajoutez les noms de domaine complets ISE et CSSM.

1. Ouvrez le Gestionnaire DNS : Tapez « DNS » dans le chercheur Windows et ouvrez l'application DNS.



Option DNS.

2. Naviguez jusqu'à Forward Lookup Zones > Et choisissez votre domaine.



Gestionnaire DNS.

3. Cliquez avec le bouton droit de la souris sur un espace noir de l'écran et sélectionnez «
Nouvel hôte (A ou 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



À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.