

# オンプレミスでのCSSMの設定とISEへのライセンスの登録

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [設定](#)

#### [ネットワーク図](#)

[CSSMをオンプレミスでVMWARE ESXiにインストールします。](#)

[CSSMのオンプレミスの初期設定\(CSSM On-Prem\)。](#)

#### [オンプレミスのCSSMとスマートアカウントの統合](#)

[オプション1: インターネット接続を使用してCSSMをオンプレミスで登録します。](#)

[オプション2: インターネット接続なしでCSSMをオンプレミスで登録します。](#)

### [CSSMをオンプレミスでISEと統合します。](#)

[Windows CAから証明書を作成します。](#)

[Windows ServerでDNSレコードを追加します。](#)

### [トラブルシューティング](#)

[ホスト/IPアドレスに到達できません。\(ISEのエラー\)](#)

[SSOサービス: シスコにアクセスできません。\(CSSMオンプレミスのエラー\)](#)

[CSRの共通名がDNSで解決可能なホスト名またはIPアドレスではありません。もう一度やり直してください。\(CSSMオンプレミスのエラー\)](#)

---

## はじめに

このドキュメントでは、CSSM On-PremとCisco Identity Service Engine(ISE)およびCisco Smart Accountの統合によるシームレスなセットアップについて説明します。

## 前提条件

### 要件

ISE 3.X

Cisco Smart Software Manager(CSSM)バージョン8リリース202304 +

### 使用するコンポーネント

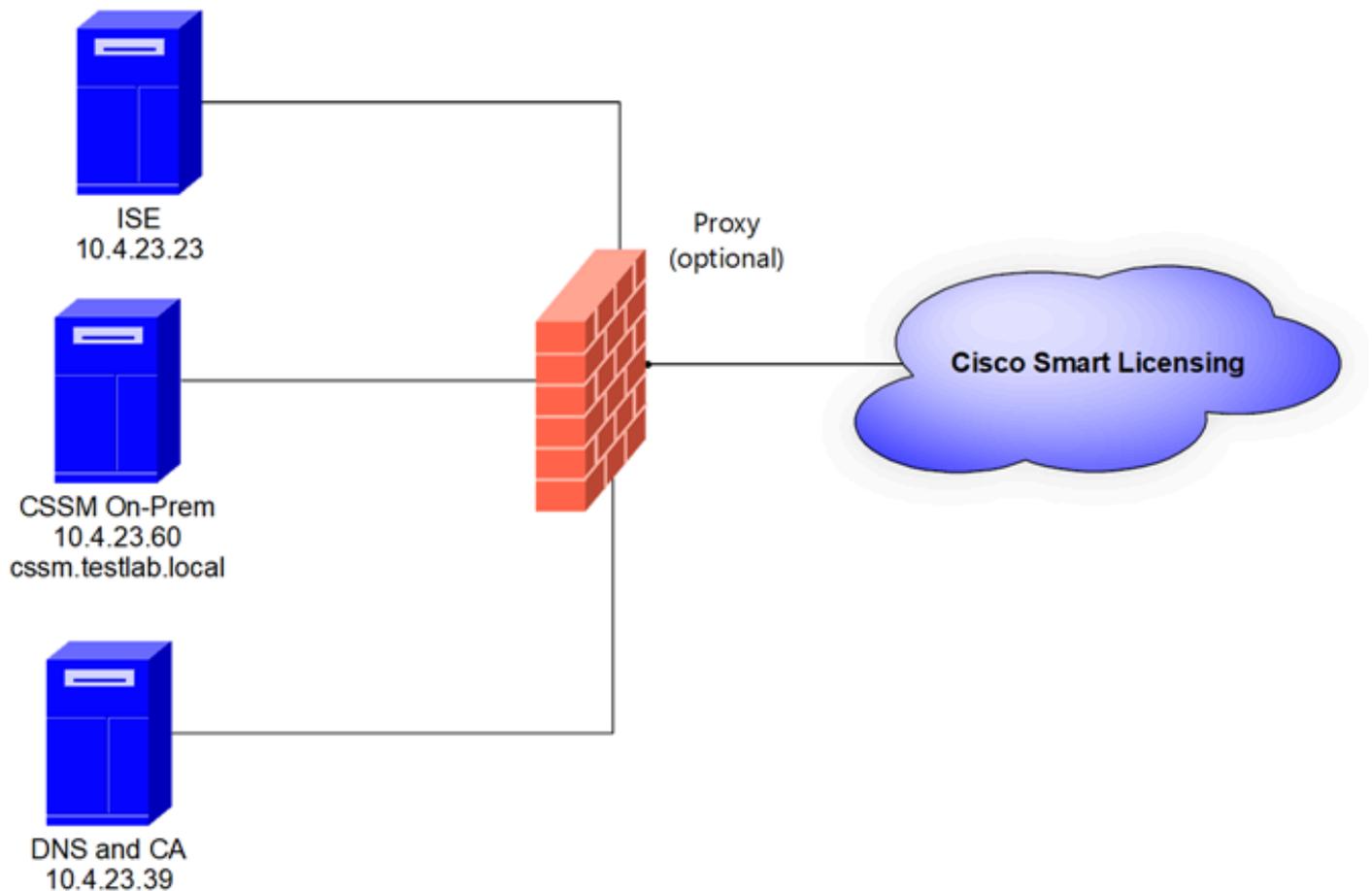
- Identity Service Engine(ISE)3.2パッチ2
- Prem 8.20234のSSM

- Windows Active Directory 2016(DNSおよび認証局サービス)
- VMWare ESXiバージョン7

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していません。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

### ネットワーク図



一般的なトポロジ

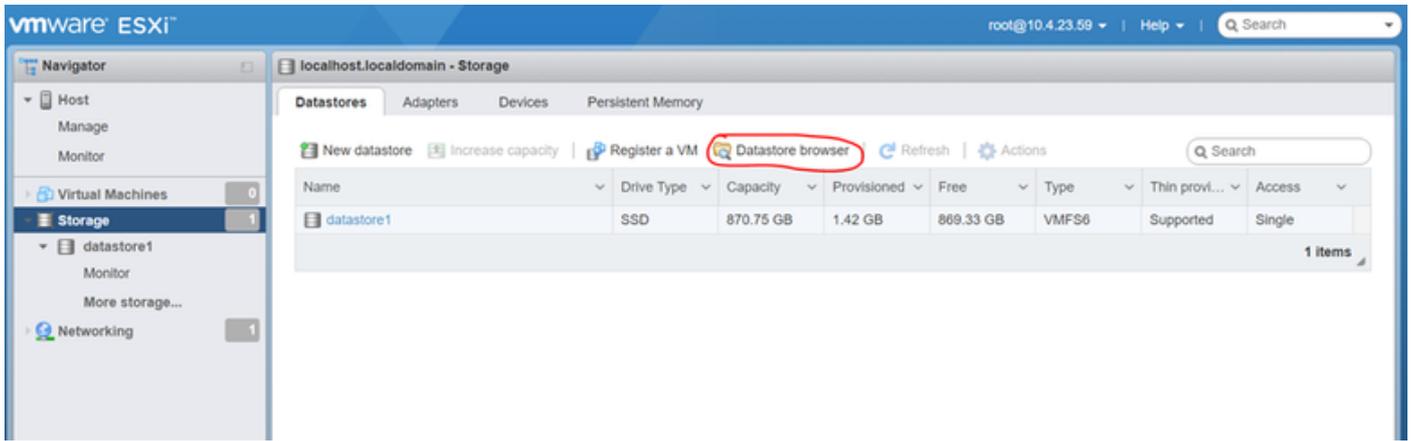
CSSMをオンプレミスでVMWARE ESXiにインストールします。

1. Cisco IOS®をダウンロードします。次のリンクを使用できます。

<https://software.cisco.com/download/home/286285506/type/286326948/release/8-202304>

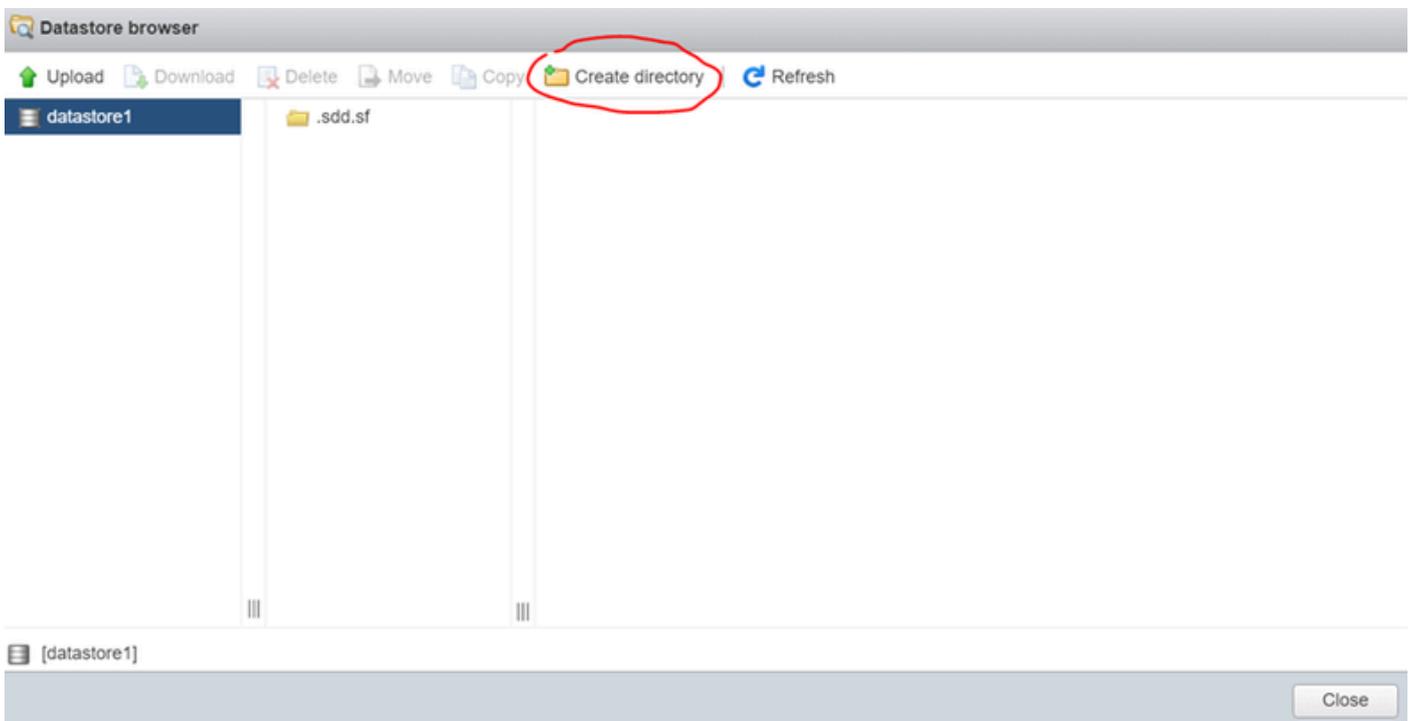
2. ISOをVMWARE ESXiにアップロードします。

Storage > Datastore Browserの順に移動します。



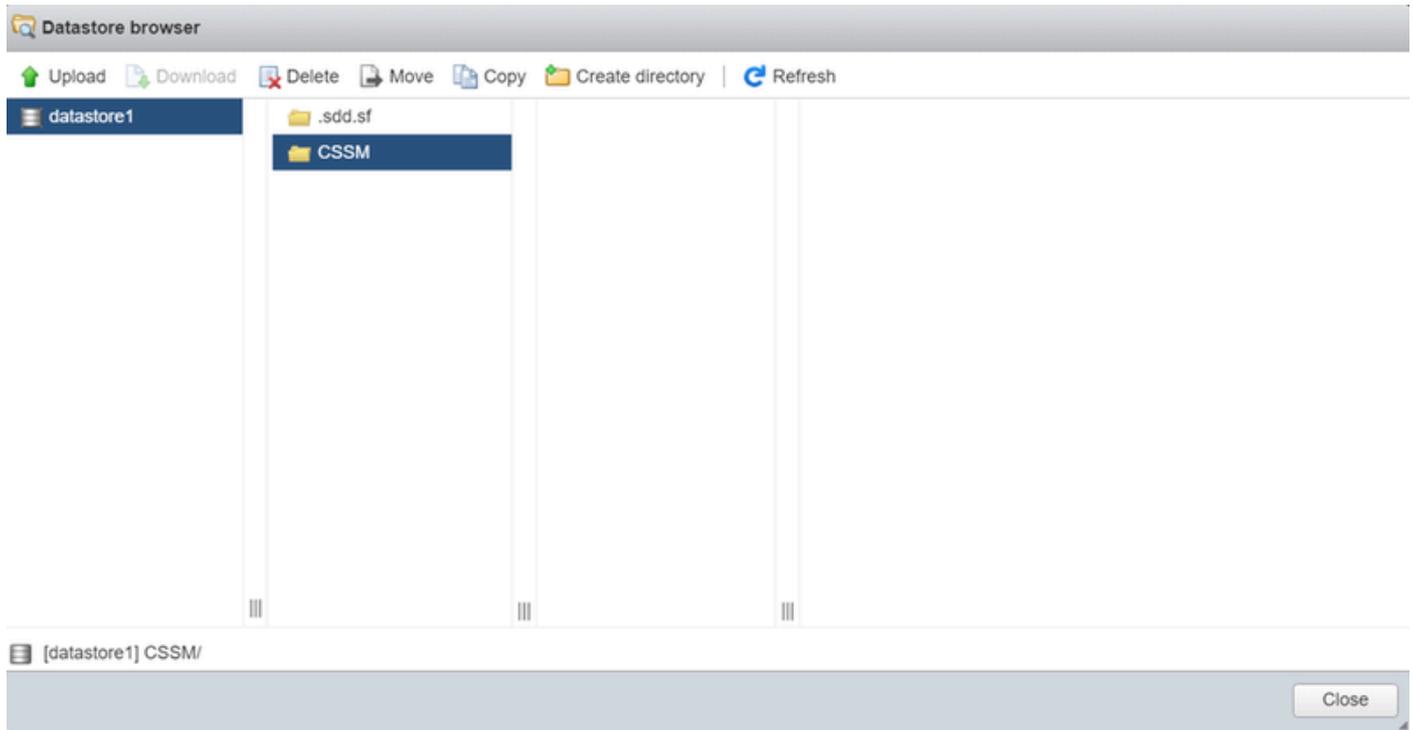
Data Browserセクション

3. Create Directoryをクリックして新しいフォルダを作成します（オプション）。



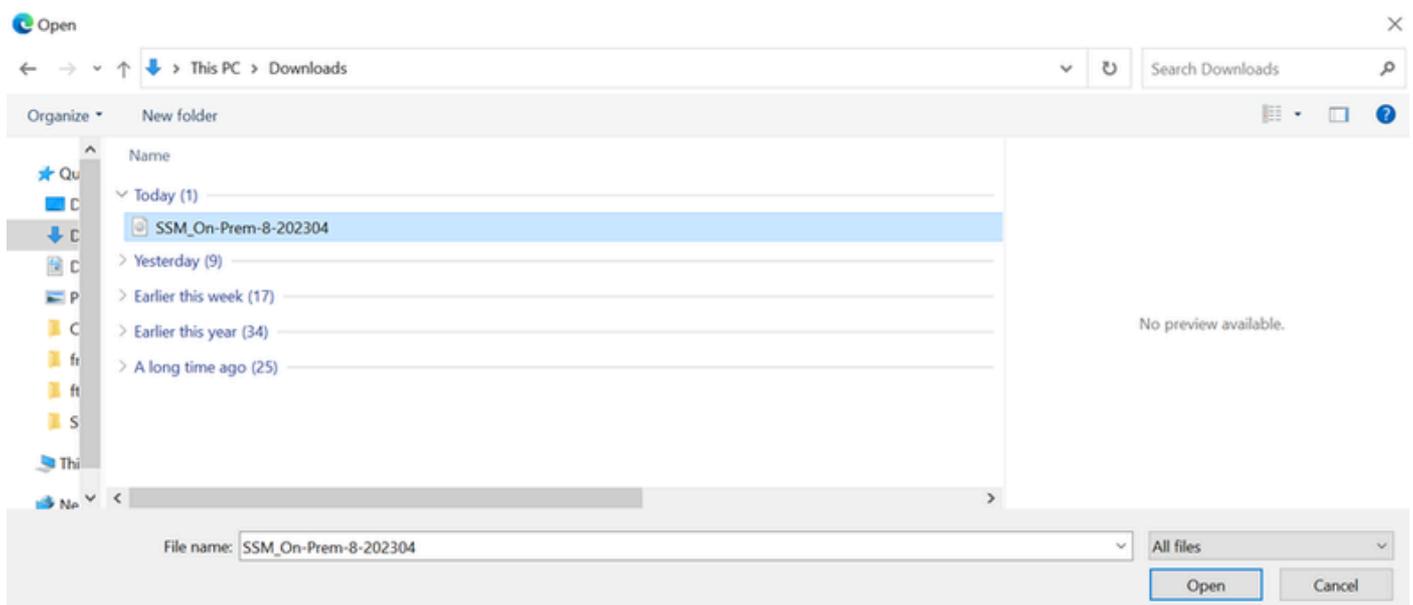
ディレクトリの作成

次の例では、CSSMフォルダが作成されています。



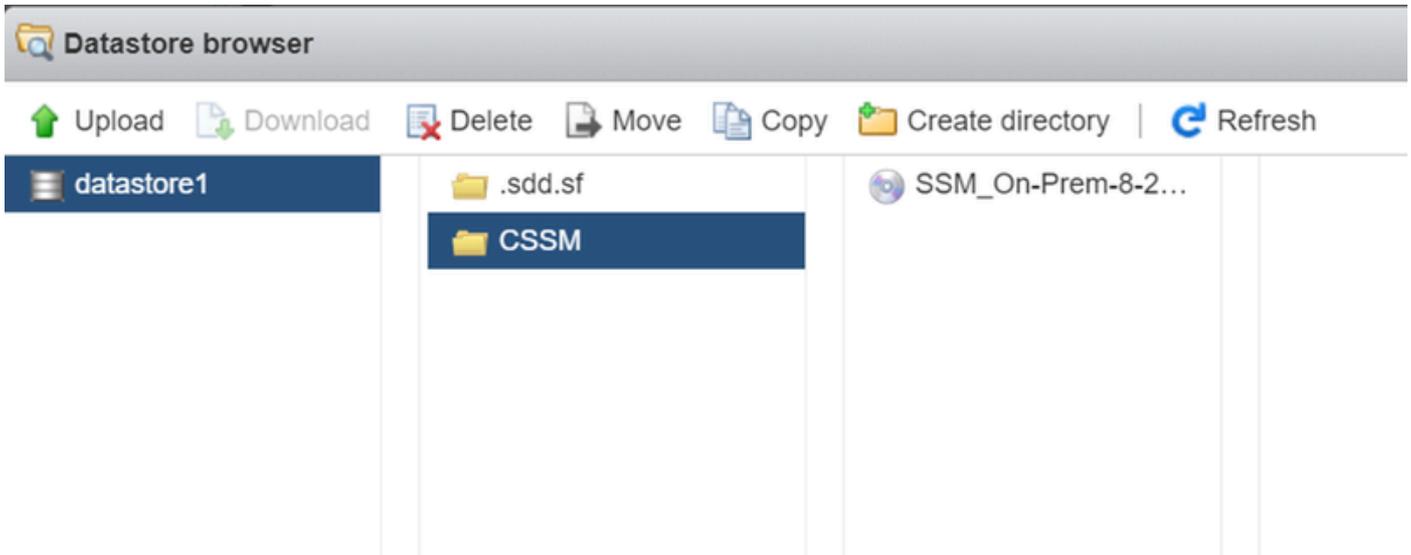
フォルダの作成

4. Uploadをクリックし、ISOファイルを選択します。



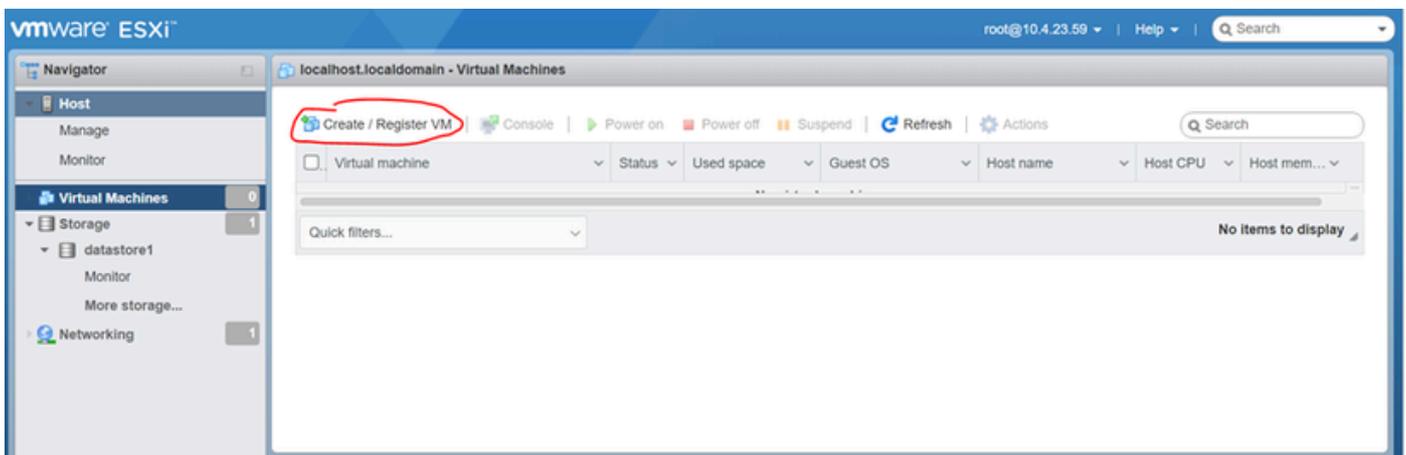
ISOのアップロード

これで、ISOファイルがCSSMフォルダ内に作成されました。



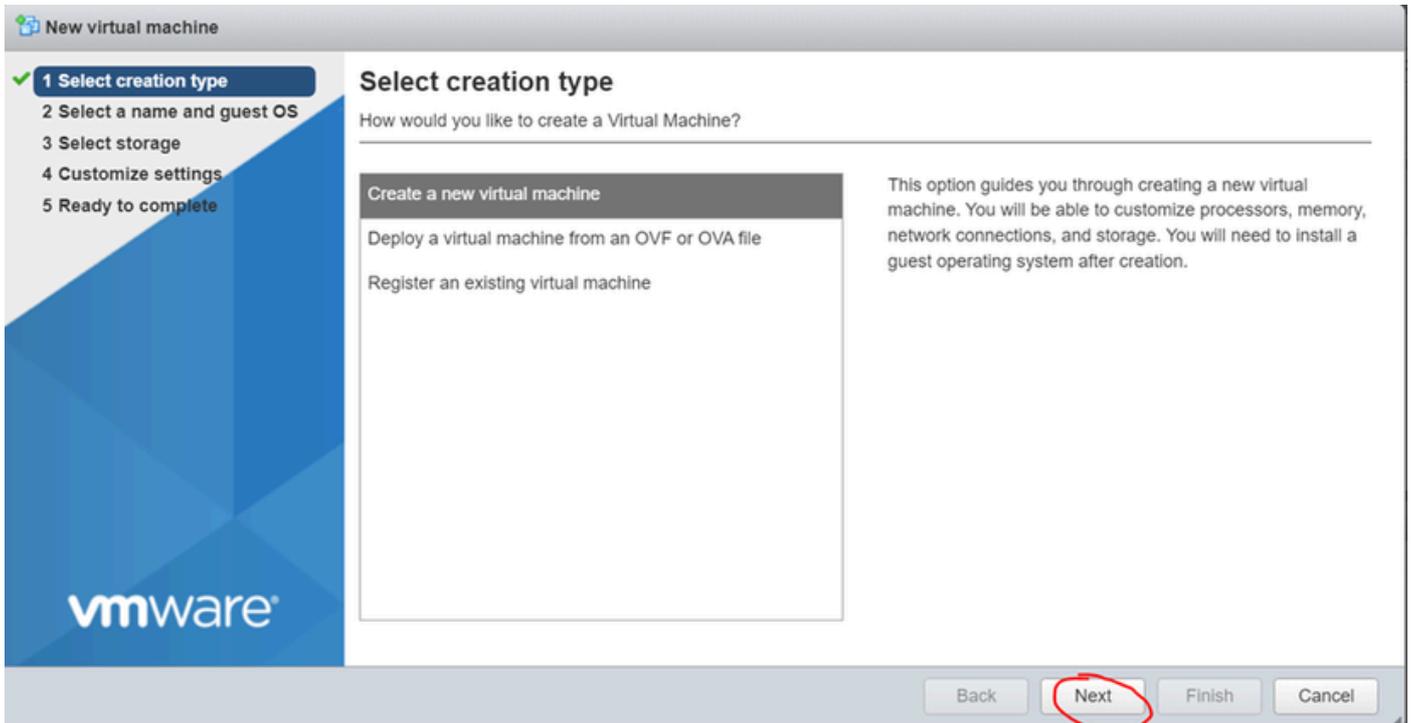
ISOのアップロードが完了します

5. 仮想マシンを作成します。仮想マシン> VMの作成/登録に移動します。



新しいVMの作成の手順01

6. Create a new virtual machineを選択し、nextをクリックします。

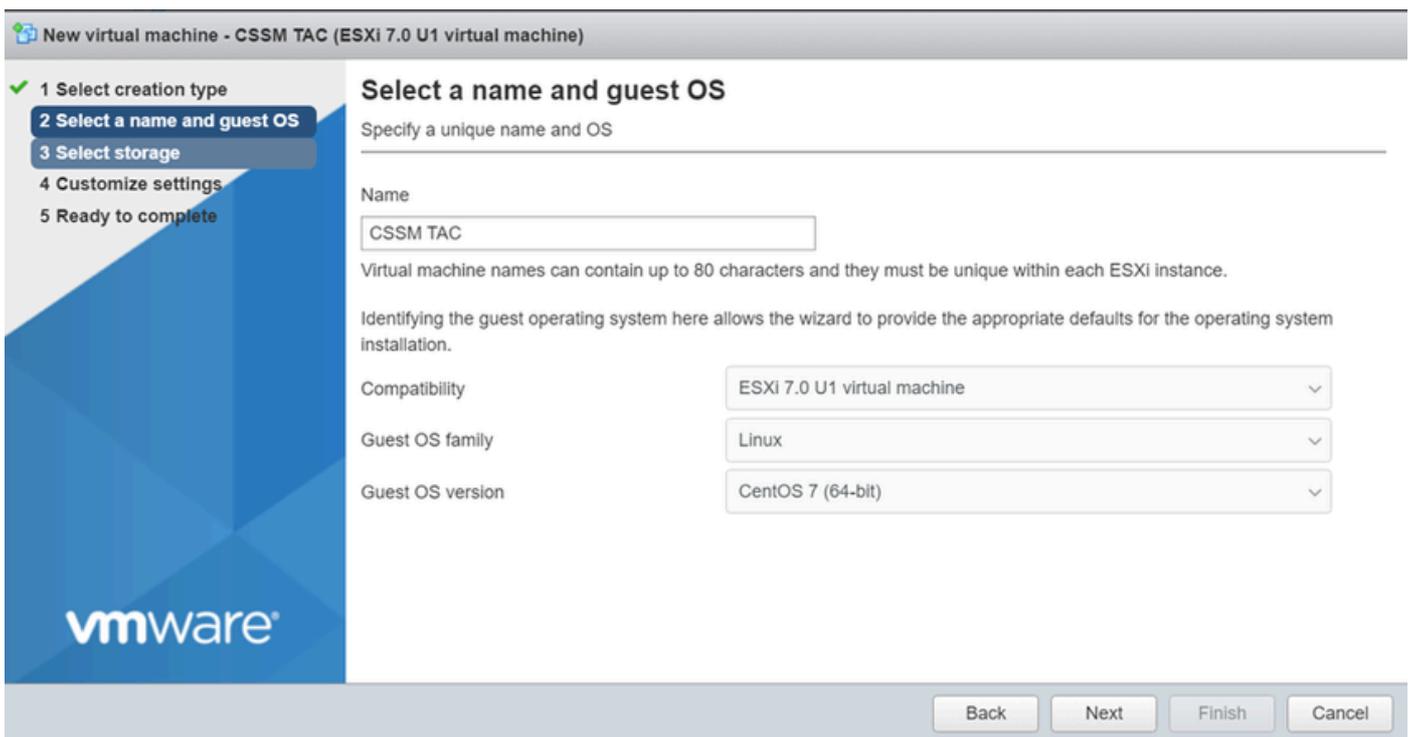


新しいVMの作成の手順02

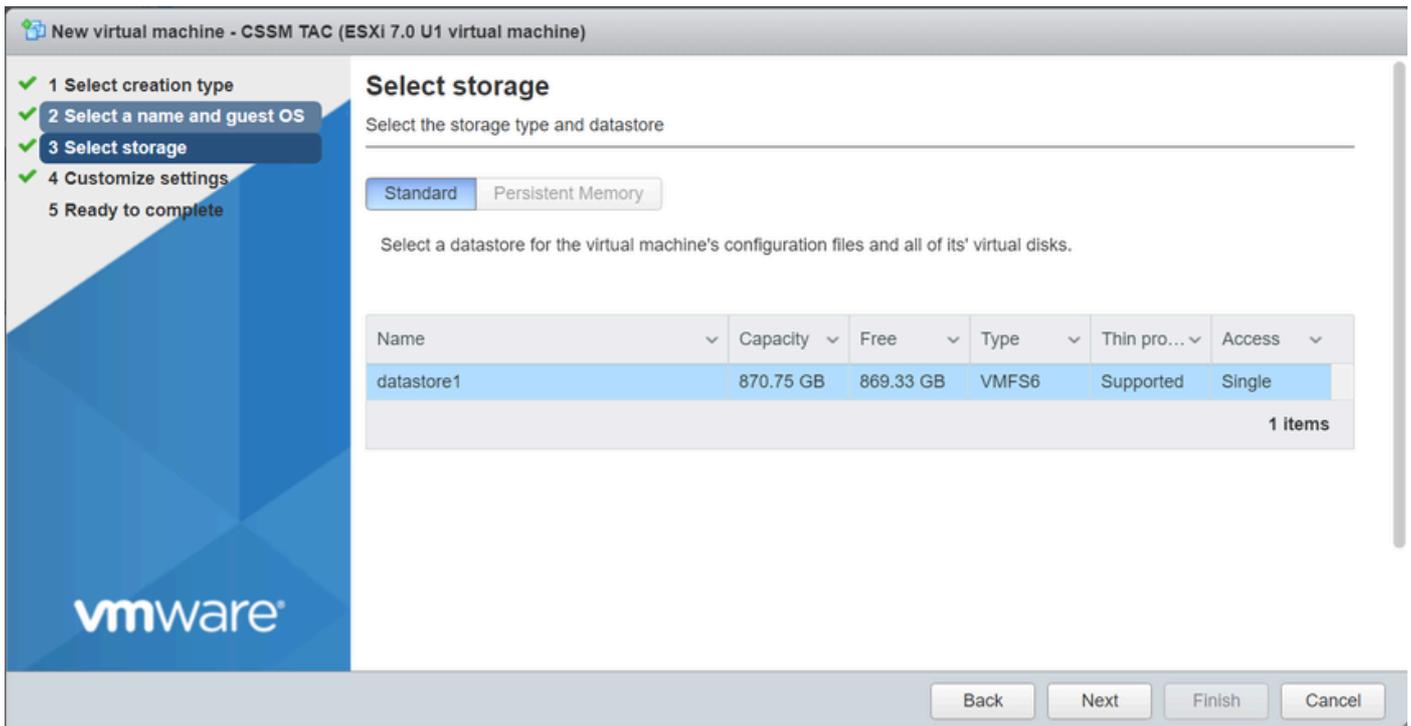
## 7. 次のパラメータを設定します。

- 名前：仮想マシンの名前を入力します。
- 互換性: ESXi 6.0以降またはESXi 6.5以降のいずれかを選択します。
- ゲストOSファミリ:Linux
- ゲストOSバージョン:CentOS 7 ( 64ビット ) または他の2.6x Linux ( 64ビット ) のいずれかを選択します。

[next] をクリックします。



8. storageを選択し、nextをクリックします。



記憶域リスト

9. 次のパラメータを構成します。

- CPU:4以上。実際のvCPU設定は、スケール要件によって異なります



注：選択した仮想ソケットの数に関係なく、ソケットあたりのコア数を1に設定する必要があります。たとえば、4つのvCPU構成は、4つのソケットおよびソケットごとに1つのコアとして設定する必要があります。

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

コアの構成

- メモリ:8 GB
- ハードディスク : 200 GB。プロビジョニングがシンプロビジョニングに設定されていることを確認。

▼  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		

ディスク構成

- ネットワークアダプタ: E1000アダプタのタイプを選択し、電源オン時に接続します。

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

ネットワーク設定の構成

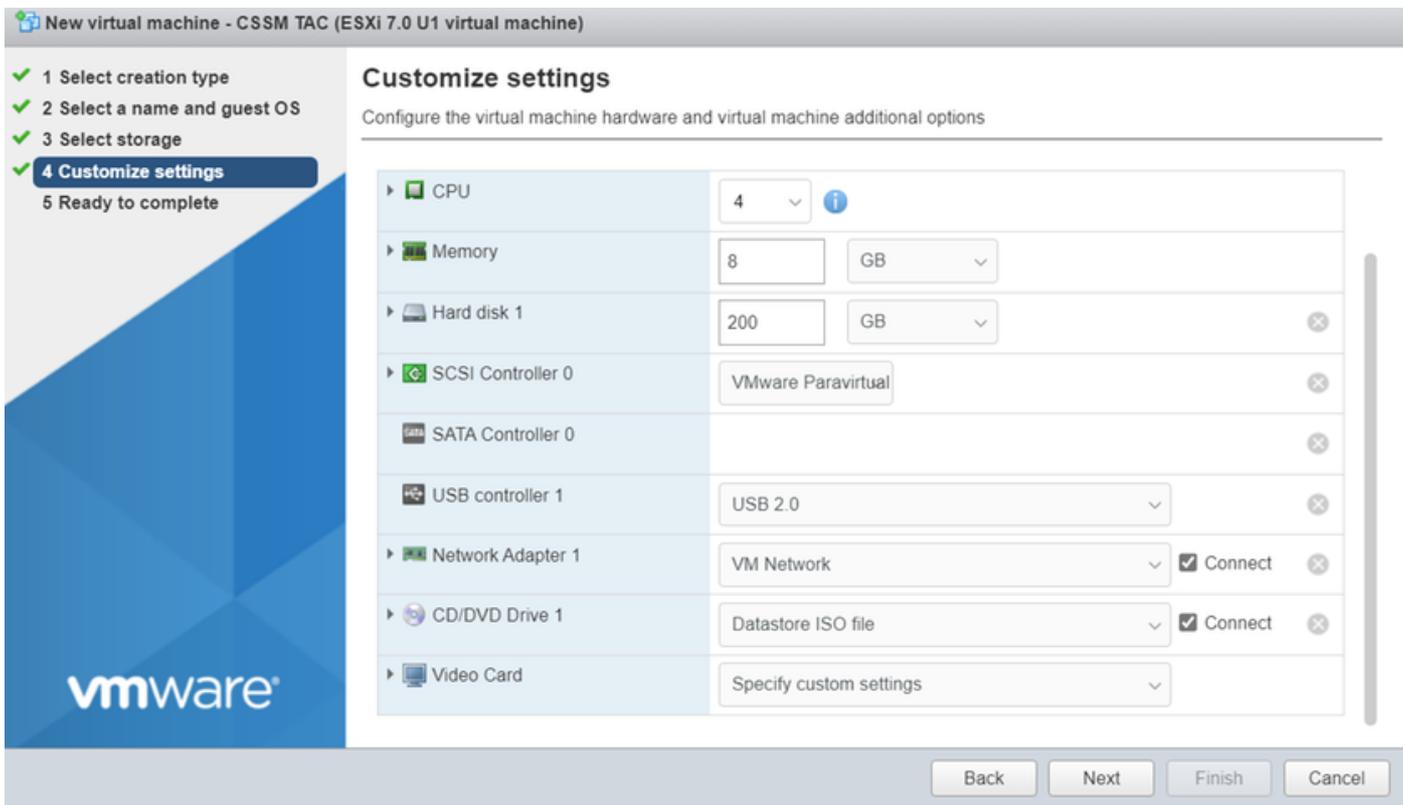
- CD / DVDドライブ: 「データISOファイル」を選択し、ISOファイルを選択します。

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イメージ

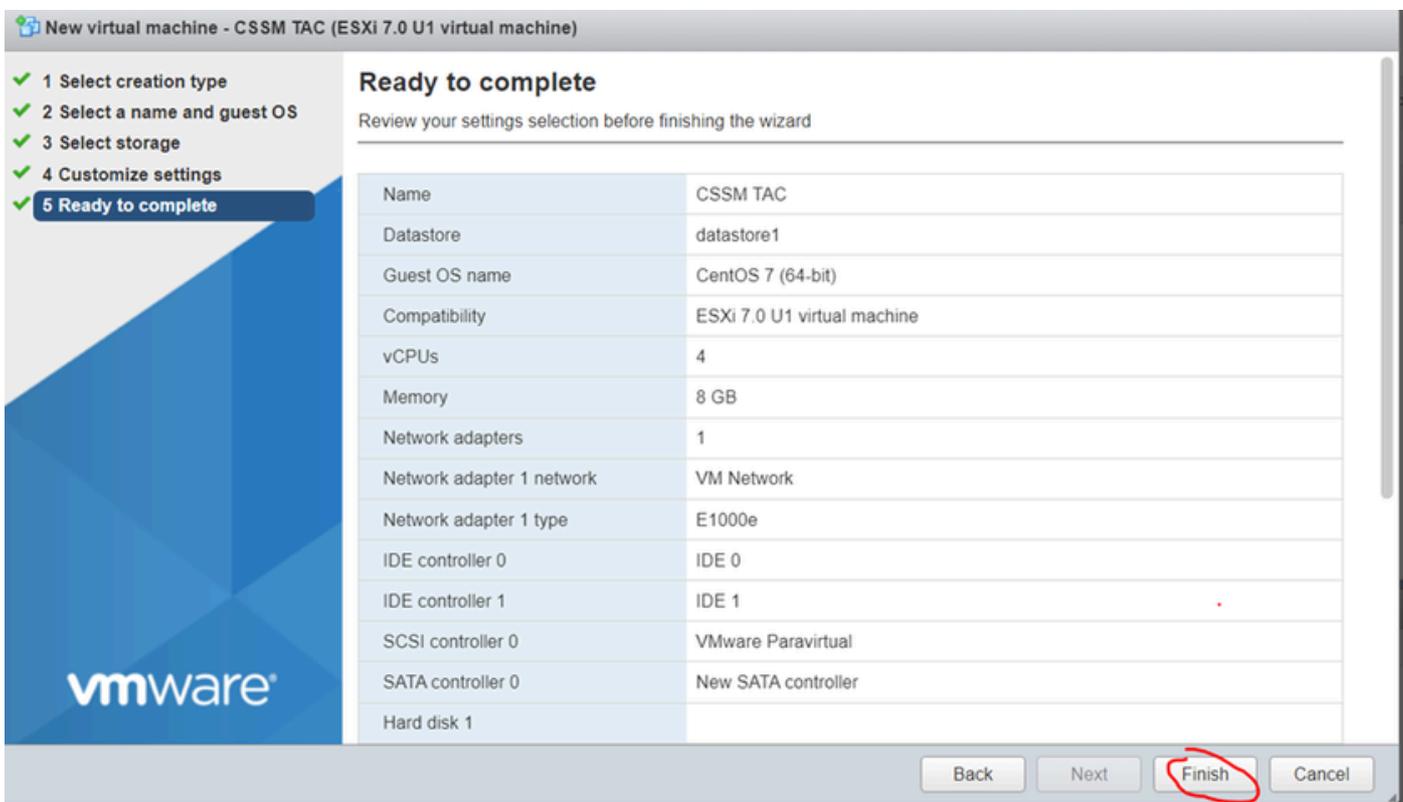
前の手順を完了したら、設定の概要を確認できます。



VM設定の概要01

[next] をクリックします。

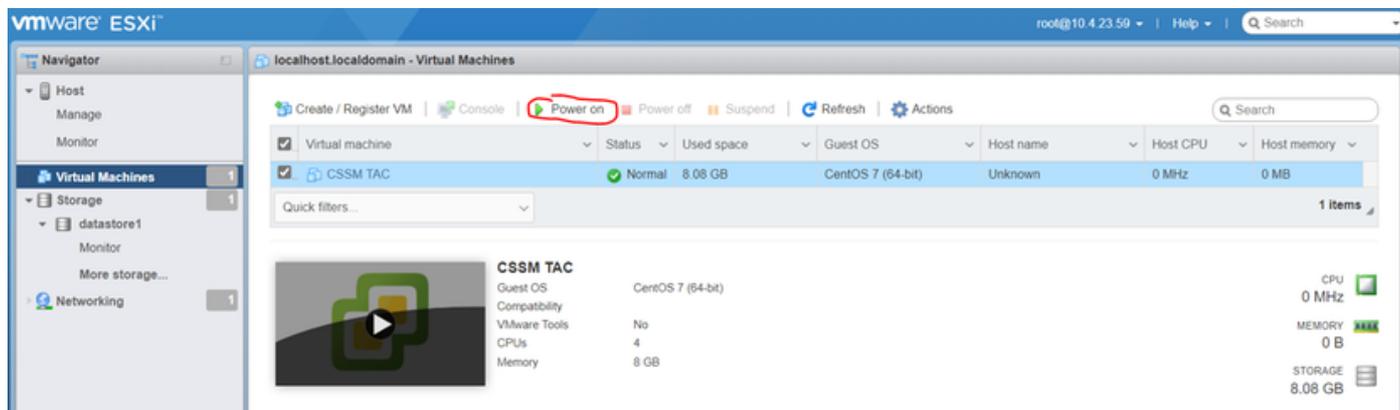
10. Finishをクリックします。



VM設定の概要02

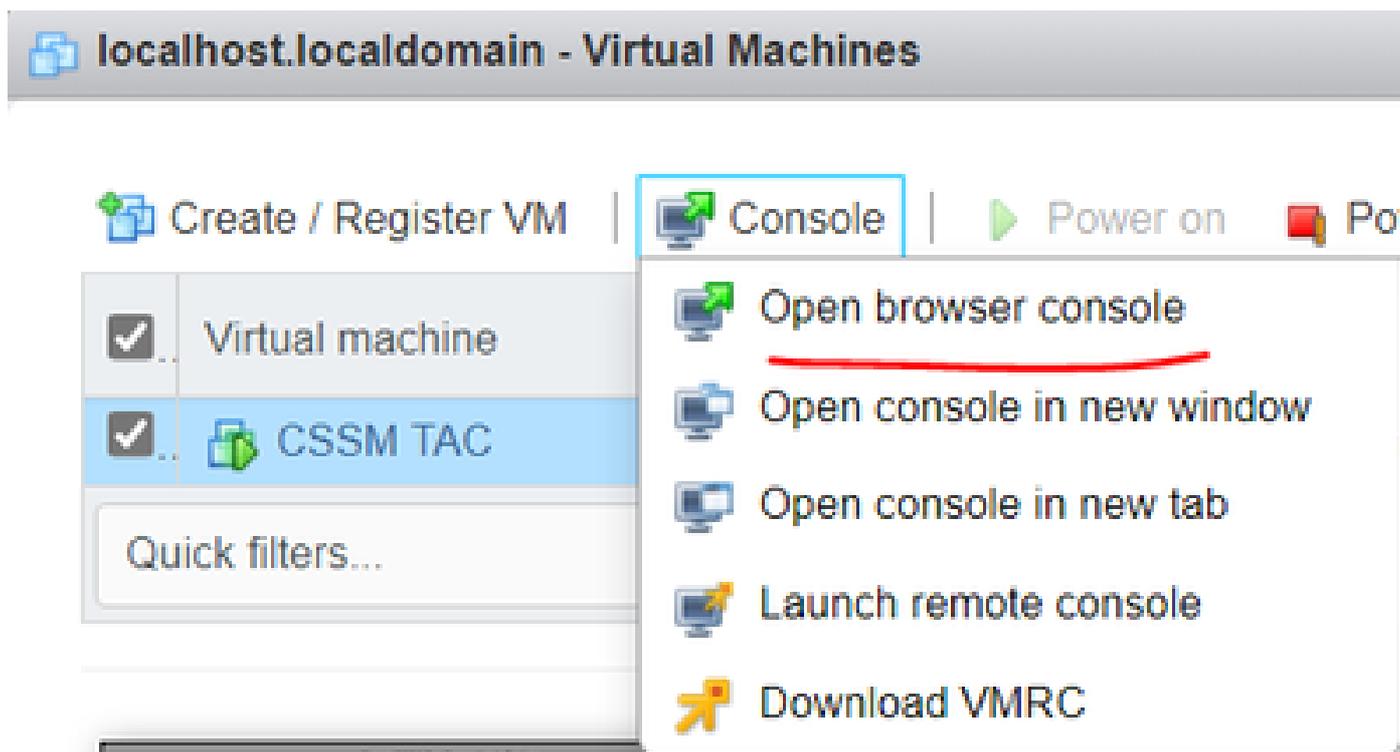
## CSSMオンプレミス(Cisco IOS)の初期設定。

1. VMWARE ESXiで、Virtual Machinesに移動し、使用しているVMを選択して、Power Onをクリックします。



電源オンオプション

2. VMコンソールを管理するには、複数のオプションがあります。Console > Open browser consoleの順に選択します。



VMを管理するためのオプション

3. ネットワーク設定を構成します。



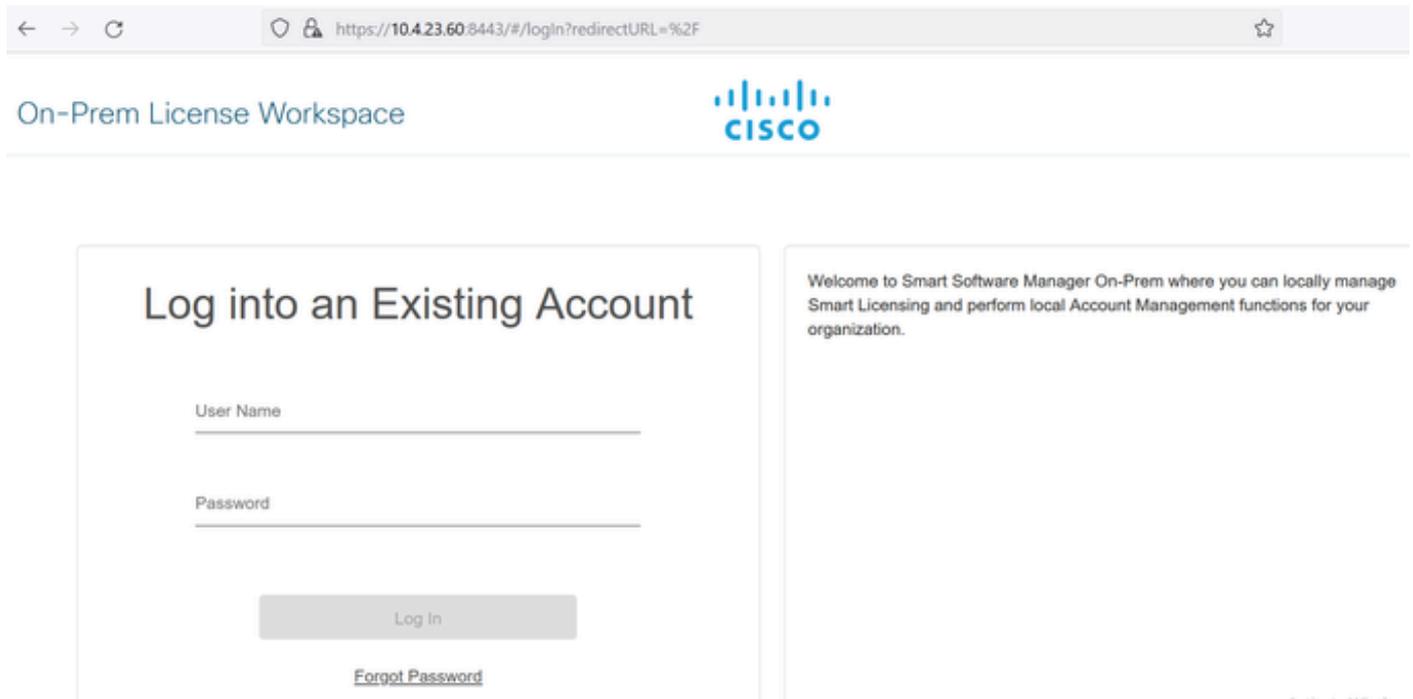
注:CSSM FQDNを解決するDNSサーバのIPアドレスを設定することが重要です。

---



CSSM初期設定が完了しました

5. ブラウザを開き、[https://<ip\\_address\\_CSSM>](https://<ip_address_CSSM>)と入力します。



On-Prem License Workspace

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.

CSSMログインページ

デフォルトのクレデンシャルを使用します。

ユーザ名 : admin

パスワード : CiscoAdmin!2345

6. 言語を選択します。
7. 新しいGUIパスワードを作成します。
8. ホストの共通名を設定します。(例 : hostname.yourdomain)。

この例では、`cssm.testlab.local`はHost Common Nameとして設定されています。

# 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

ホストの共通名設定

## 9. 設定を検証し、Applyをクリックします。

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の初期設定が完了しました。

## オンプレミスのCSSMとスマートアカウントの統合

スマートアカウントをPrem ServerのCSSMに関連付ける必要があります。

1. 次のリンクを使用してシスコスマートアカウントを開きます。

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

2. 次に、Smart Software ManagerセクションでManage Licensesを選択します。

--	--

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

ライセンスの管理オプション

3. Inventoryに移動し、スマートアカウント名と仮想アカウントの名前をコピーします。このガイドでは、これはInternalTestDemoAccount67およびAAA MEX TESTです。

The screenshot shows the Cisco Software Central interface. At the top, there is a navigation bar with the Cisco logo and search, OT, and globe icons. Below the navigation bar is a yellow banner for "Scheduled Downtime Notification". 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 active, and a dropdown menu shows "Virtual Account: AAA MEX TEST". Below this, there are tabs for "General", "Licenses", "Product Instances", and "Event Log". The "General" tab is selected, showing the "Virtual Account" details: "Description: Only for tests" and "Default Virtual Account: No".

ソフトウェアのCiscoページ

4. CSSM GUIを開き、Admin Workspaceオプションを選択します。

## 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.

メインCSSMメニュー

5. 次に、Accountsを選択します。

# On-Prem Admin Workspace

---

## Smart Software Manager On-Prem



Access  
Management



Settings



Accounts



Support  
Center



API Toolkit



Synchronization



Network



Users



Security

## 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>

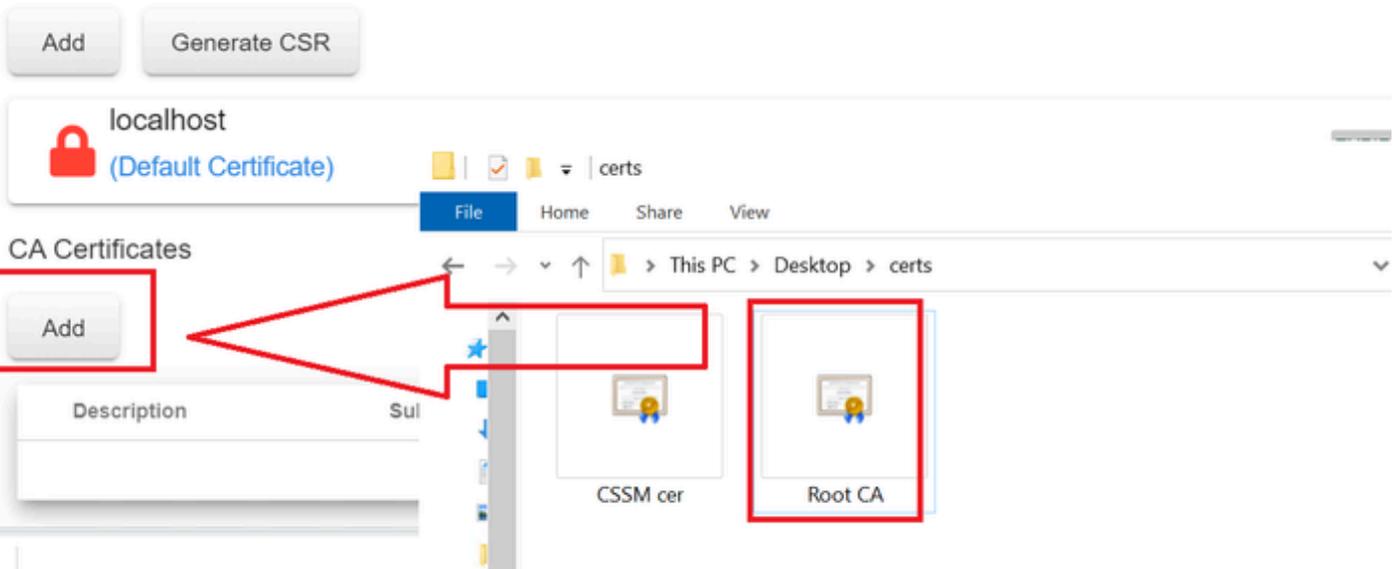
**Generate**

Cancel

CSR詳細。

4. 詳細については、このドキュメントの「Windows CAからの証明書の作成」を参照してください。
5. ルートCA証明書をアップロードします。

## Browser Certificate



ルートCAをアップロードしています。

[続行 ( Proceed ) ] をクリックします。



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

6. 説明を入力し、ルート証明書を選択して、OKをクリックします。

## Upload Certificate

• Description:

• Certificate:

説明ルートCA。

7. CAによって署名されたCSR(CSSM ID証明書)をアップロードします。

The screenshot shows the 'Browser Certificate' management interface. The 'Add' button is highlighted with a red box. A red arrow points from this button to the 'CSSM cer' file in a file explorer window. The file explorer shows two files: 'CSSM cer' and 'Root CA'. Below the file explorer, a table lists the certificates:

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

CSSM ID証明書のアップロード

注：この場合、中間証明書はCAに存在しません。ただし、アーキテクチャで中間証明書を使用する場合は、中間証明書が必須です。

8. 次に、両方の証明書がインストールされていることを確認します。

#### 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

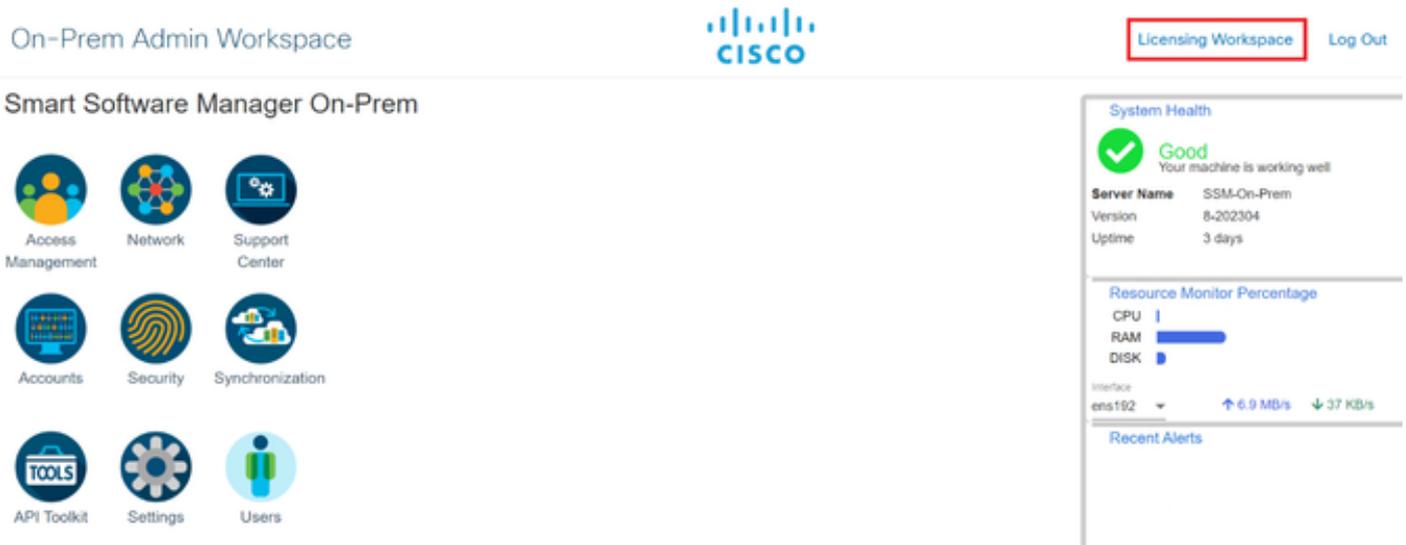
/DC=local/DC=testlab/CN=tes 2027-Apr-14 22:51:26

2024-Jul-16 21:18:52

[Actions](#)

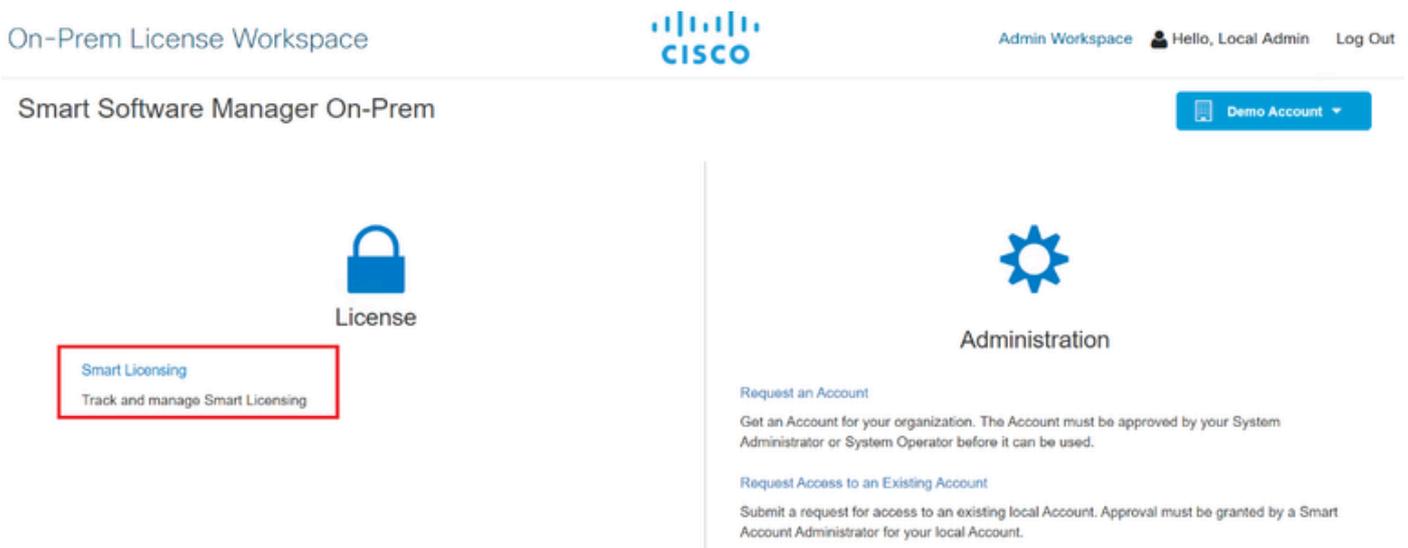
証明書の検証。

## 9. SSM On-Prem: Select licensing Workspaceでトークンを作成します。



ワークスペースページ。

## 10. Smart Licensingに移動します。



CSSMスマートライセンスページ

## 11. ローカル仮想アカウントを探し、New TokenをクリックしてProceedをクリックします。

# 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...**

新しいトークンオプション。

## 12. Create Tokenを選択してコピーします。

### 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

Cancel

新しいトークンの作成。



## 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](#).

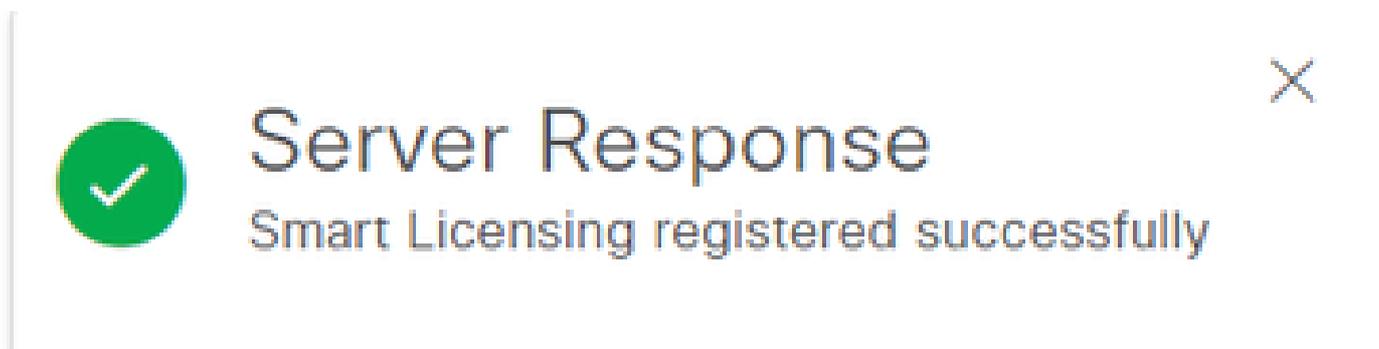
Cancel Register

### CSSMとISEの設定

注:ISEはCSSMとの接続を確立するためにこのパラメータを使用するため、ホスト名+ドメインをホストの共通名(CN)に設定することが重要です。ホスト名+ドメインの代わりに

IPアドレスを使用できますが、ホスト名+ドメインを使用することを推奨します

15. そして最後に、登録が完了しました。

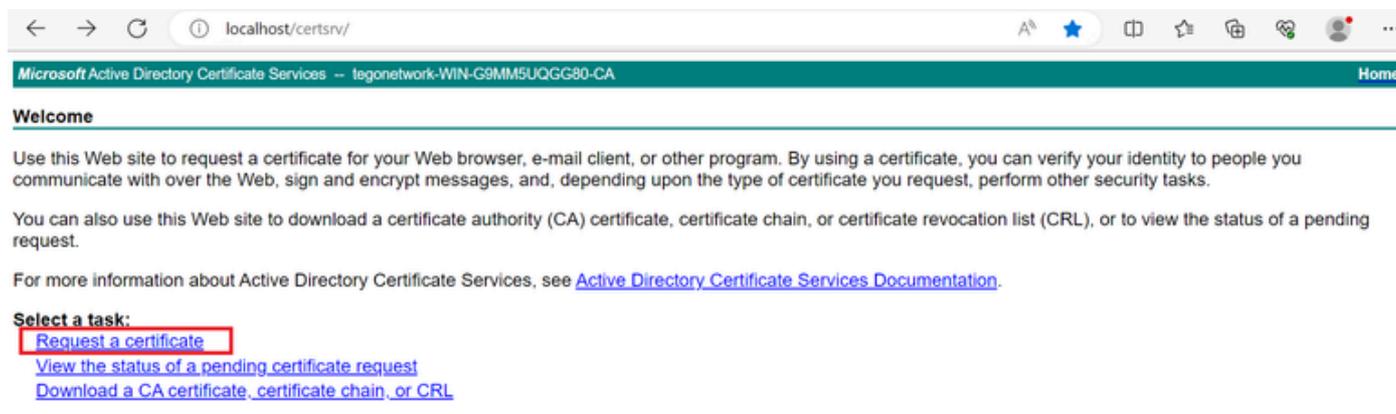


登録が完了しました。

Windows CAから証明書を作成します。

認証局の管理者は、次の手順を実行する必要があります。

1. Webブラウザを開き、<http://localhost/certsrv/>に移動します。
2. Request a certificateをクリックします。



証明書を要求します。

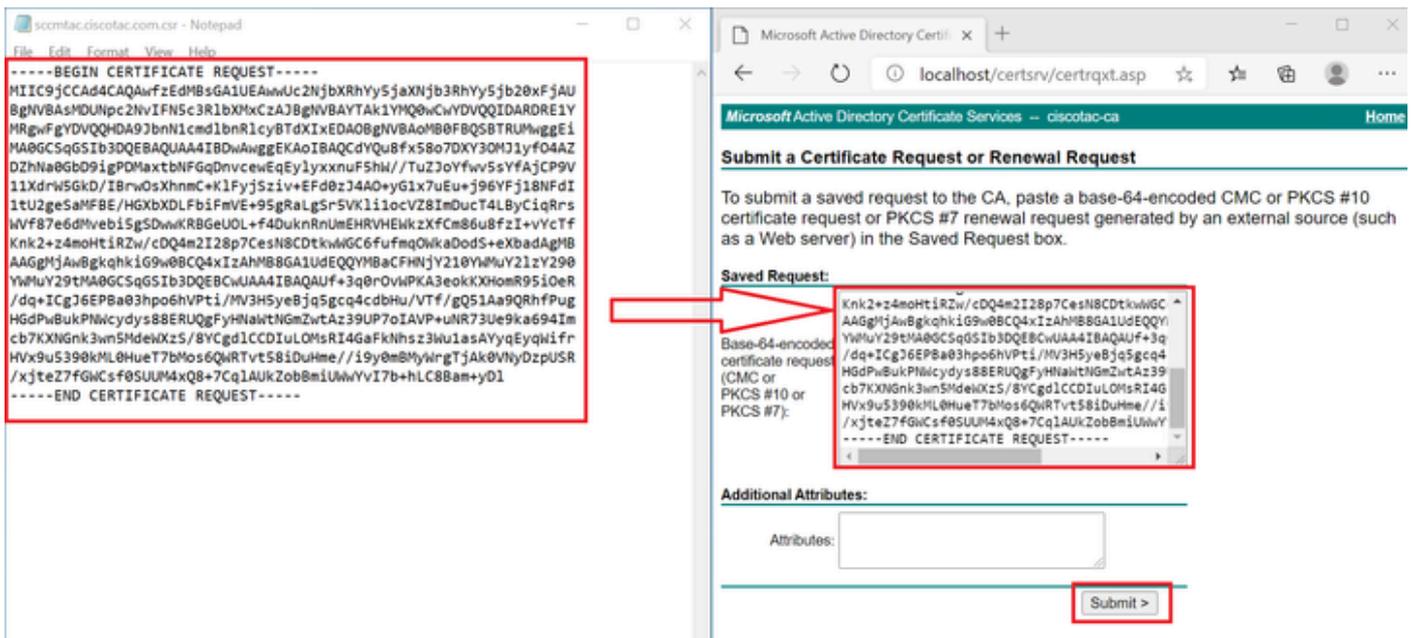
3. [advanced certificate request] をクリックします。



証明書の要求の詳細設定

4. 前に生成したCSRを開きます。 次に、情報をコピーして、Saved requestに貼り付けます

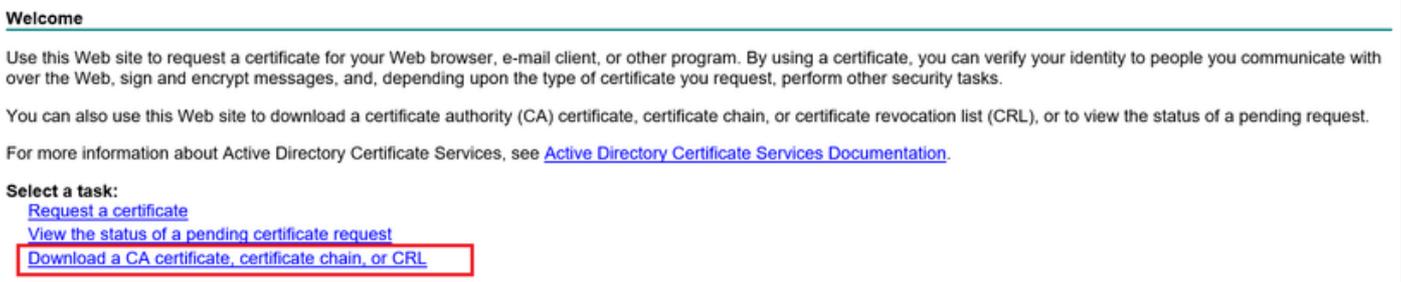
。



証明書を送信します。

Submitをクリックすると、証明書が自動的にダウンロードされます。

5. 次に、CA証明書ルートダウンロードします。 <http://localhost/certsrv/>に戻り、 [Download a CA Certificate, Certificate Chain, or CRL](#)を選択します。



ルートCAをダウンロードします。

6. エンコード方式としてBase64を使用して、CA証明書をダウンロードします。

## 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.

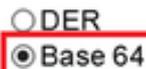
CA certificate:

Current [ciscotac-ca]



Encoding method:

DER  
 Base 64



[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

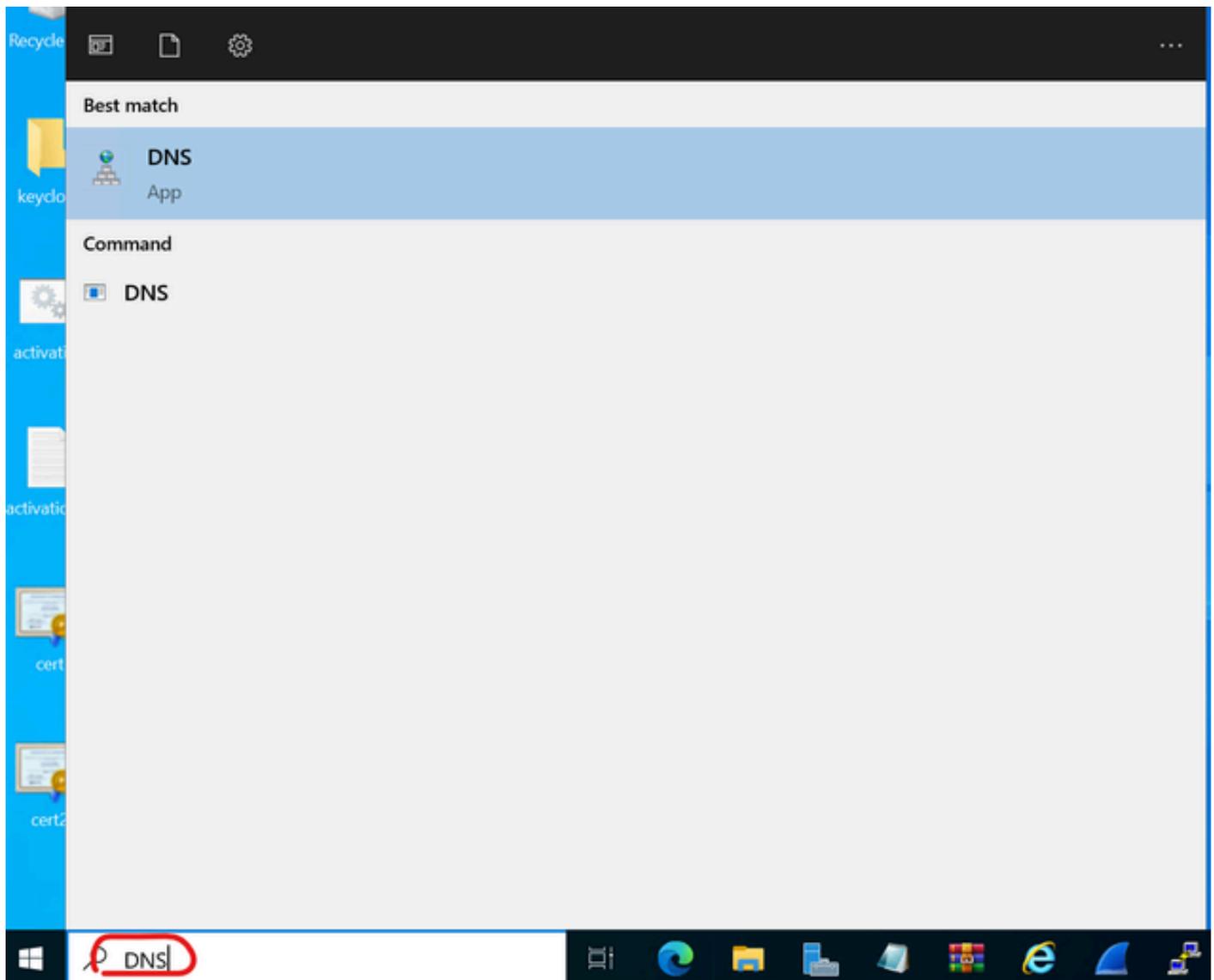
---

Base 64オプション

Windows ServerでDNSレコードを追加します。

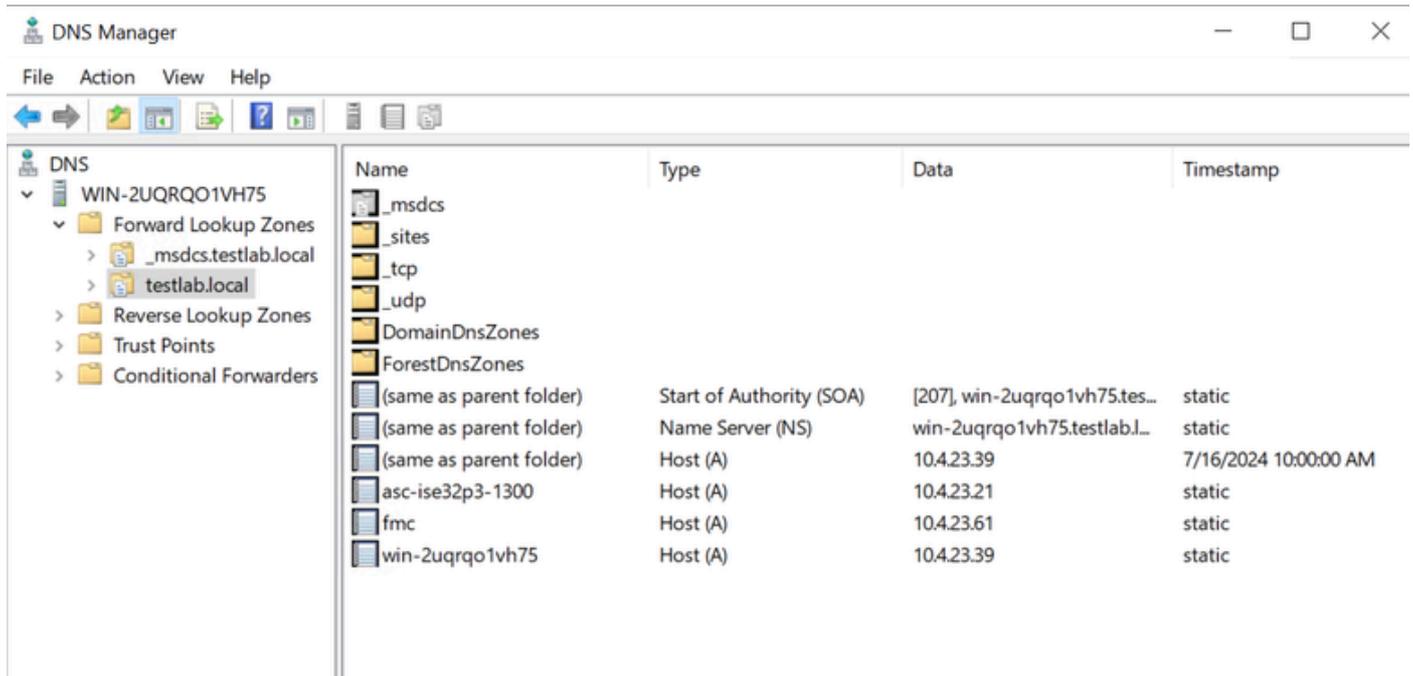
管理者の場合は、ISEおよびCSSM FQDNを追加します。

1. DNS Managerを開きます。Windowsのファインダで「DNS」と入力し、DNSアプリを開きます。



DNSオプション。

2. Forward Lookup Zonesに移動し、ドメインを選択します。



DNSマネージャ。

3. 画面上の黒いスペースを右クリックし、「New Host (A or AAAA)(新しいホスト ( Aまたは AAAA ) )」(新しいホスト ( AまたはAAAA ) )を選択します。

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



## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。