Cài đặt Microsoft ADFS

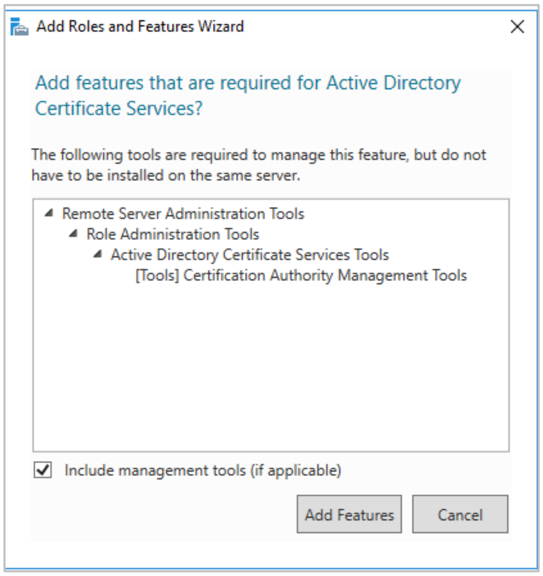
Table of Contents

Lưu ý khi cài đặt trên EC2

1/ Sau khi cài đặt AD thành công. Cấu hình DHCP option-set với DNS trỏ về AD vừa tạo. Sau đó cấu hình VPC sử dụng DHCP option-set mới

2/ Tạo mới ADFS. EC2 VM sẽ tự động lấy IP/DNS theo cấu hình mới. Security Group có thể mất nên phải tạo lại RDP rule để truy cập lại.

Cài đặt một Active Directory Certificate Service (ADCS)



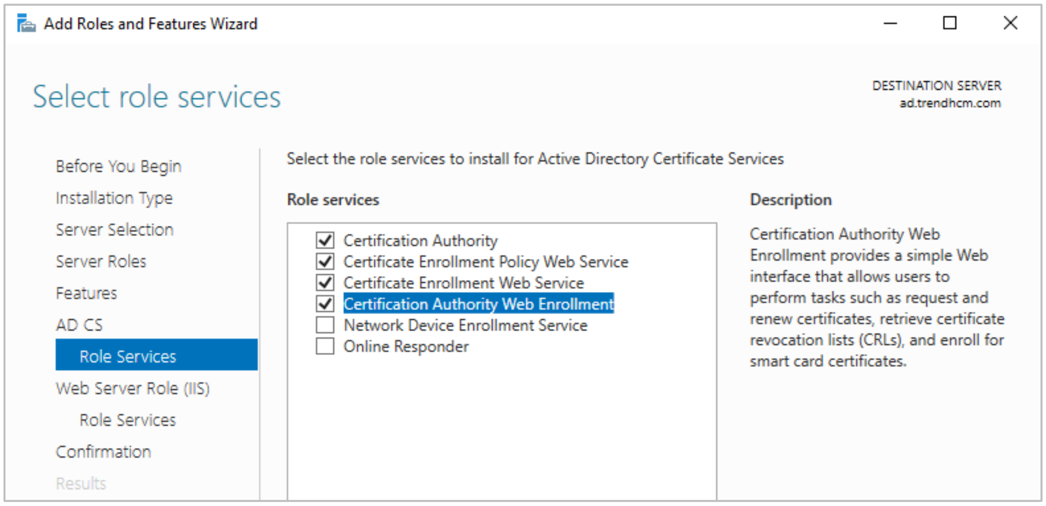
Add Roles and Features Wizard

Add features that are required for Active Directory Certificate Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - Active Directory Certificate Services Tools
      - [Tools] Certification Authority Management Tools

☑ Include management tools (if applicable)



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
ad.trendhcm.com

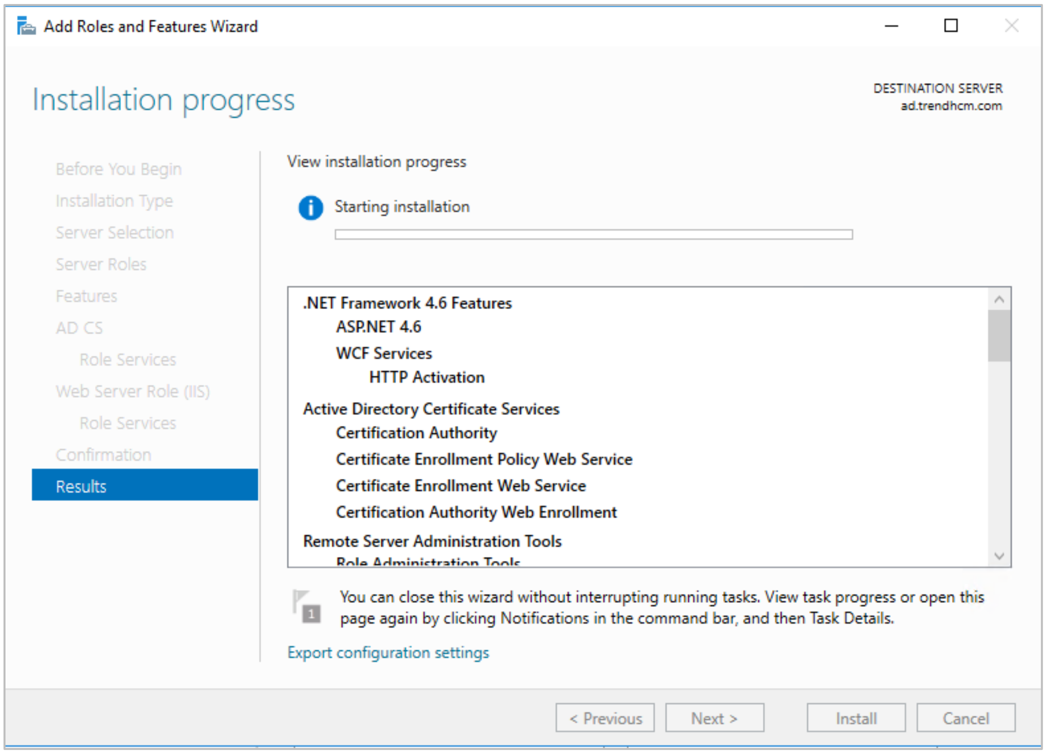
Select the role services to install for Active Directory Certificate Services

Role services

☑ Certification Authority
☑ Certificate Enrollment Policy Web Service
☑ Certificate Enrollment Web Service
☑ Certification Authority Web Enrollment
□ Network Device Enrollment Service
□ Online Responder

Description

Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.



View installation progress

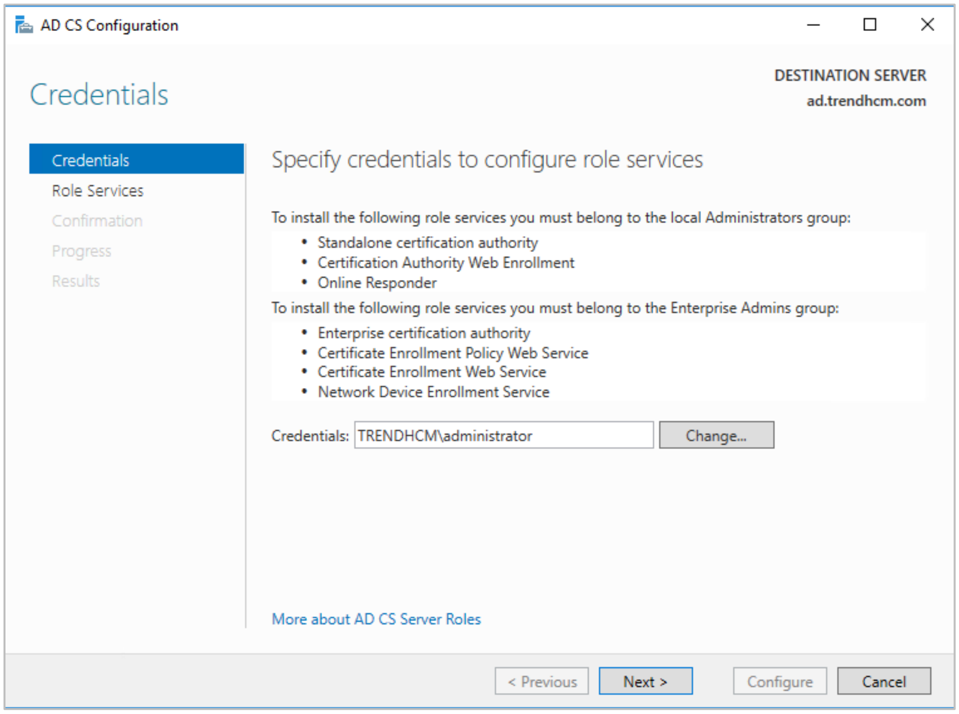
Starting installation

.NET Framework 4.6 Features
ASP.NET 4.6
WCF Services
HTTP Activation
Active Directory Certificate Services
Certification Authority
Certificate Enrollment Policy Web Service
Certificate Enrollment Web Service
Certification Authority Web Enrollment
Remote Server Administration Tools
Role Administration Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Cấu hình ADCS – cấu hình role CA



Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

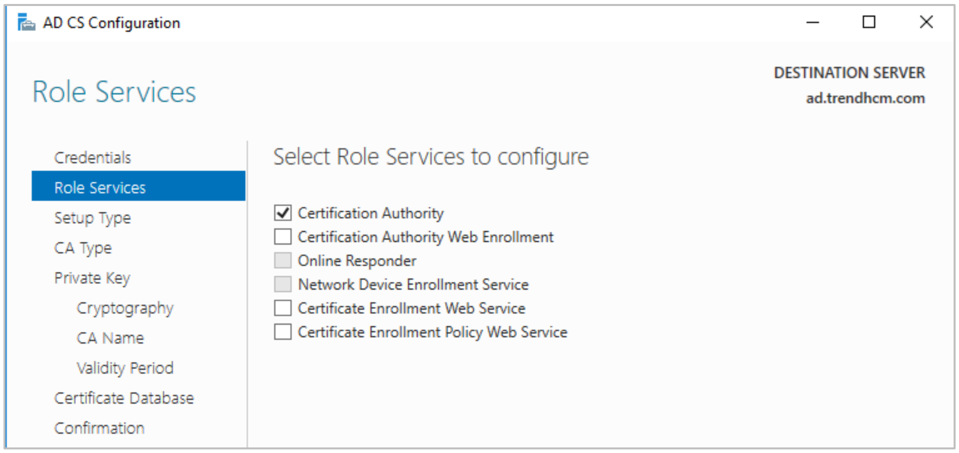
- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: TRENDHCM\administrator

More about AD CS Server Roles



AD CS Configuration

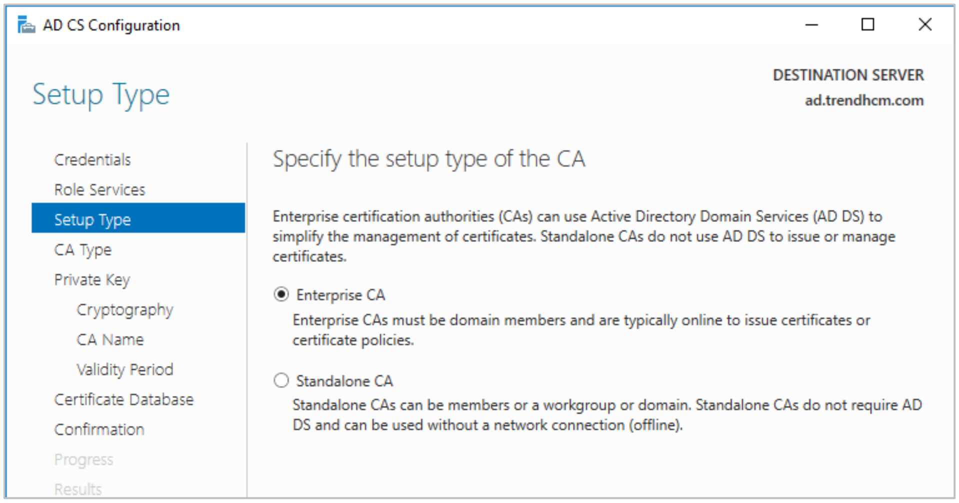
DESTINATION SERVER
ad.trendhcm.com

Role Services

- Credentials
- **Role Services**
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation

Select Role Services to configure

☑ Certification Authority
☐ Certification Authority Web Enrollment
☐ Online Responder
☐ Network Device Enrollment Service
☐ Certificate Enrollment Web Service
☐ Certificate Enrollment Policy Web Service



AD CS Configuration

DESTINATION SERVER
ad.trendhcm.com

Setup Type

- Credentials
- Role Services
- **Setup Type**
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the setup type of the CA

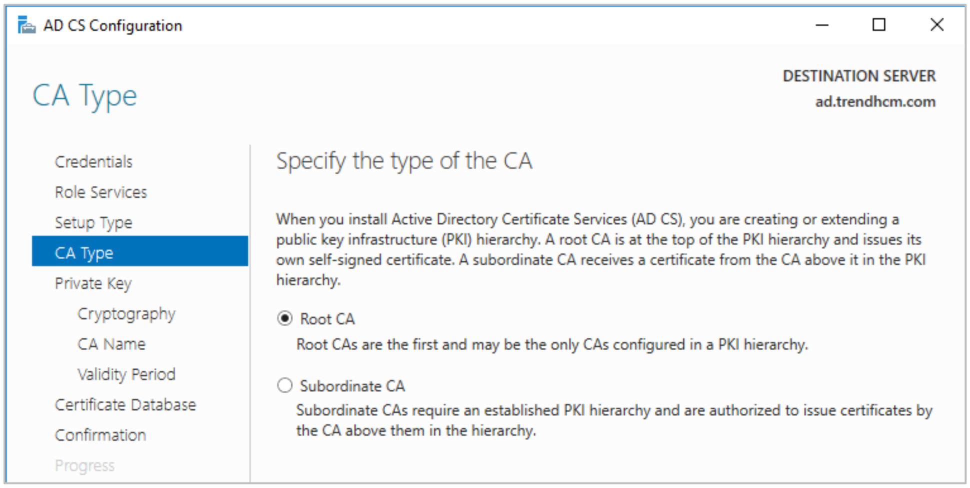
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

● Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

○ Standalone CA

Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).



AD CS Configuration

DESTINATION SERVER
ad.trendhcm.com

CA Type

- Credentials
- Role Services
- Setup Type
- **CA Type**
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation
- Progress

Specify the type of the CA

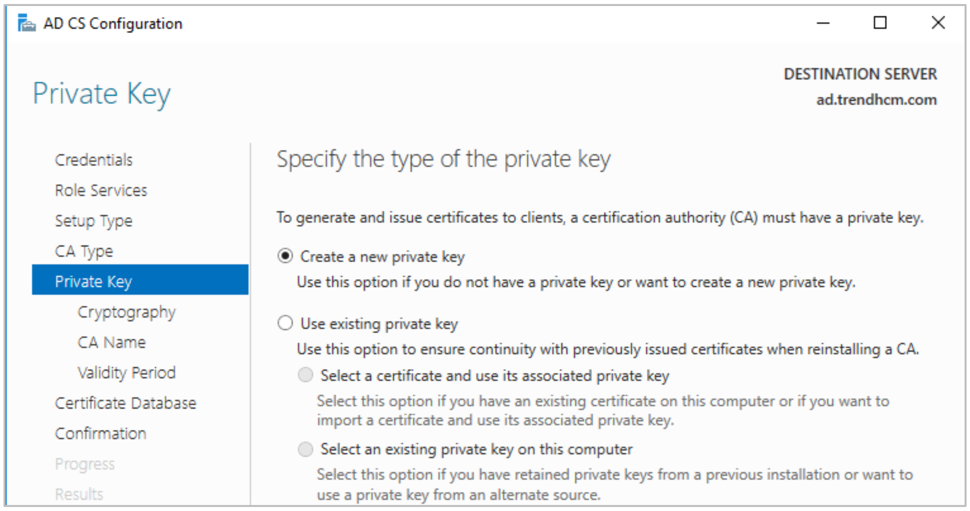
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

● Root CA

Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

○ Subordinate CA

Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.



Private Key

DESTINATION SERVER
ad.trendhcm.com

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

● Create a new private key

Use this option if you do not have a private key or want to create a new private key.

○ Use existing private key

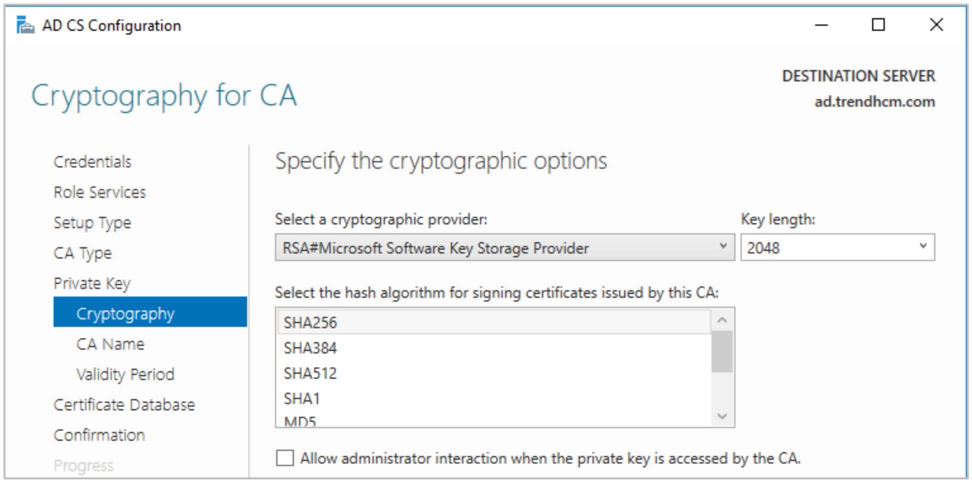
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

○ Select a certificate and use its associated private key

Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer

Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.



Cryptography for CA

DESTINATION SERVER
ad.trendhcm.com

Specify the cryptographic options

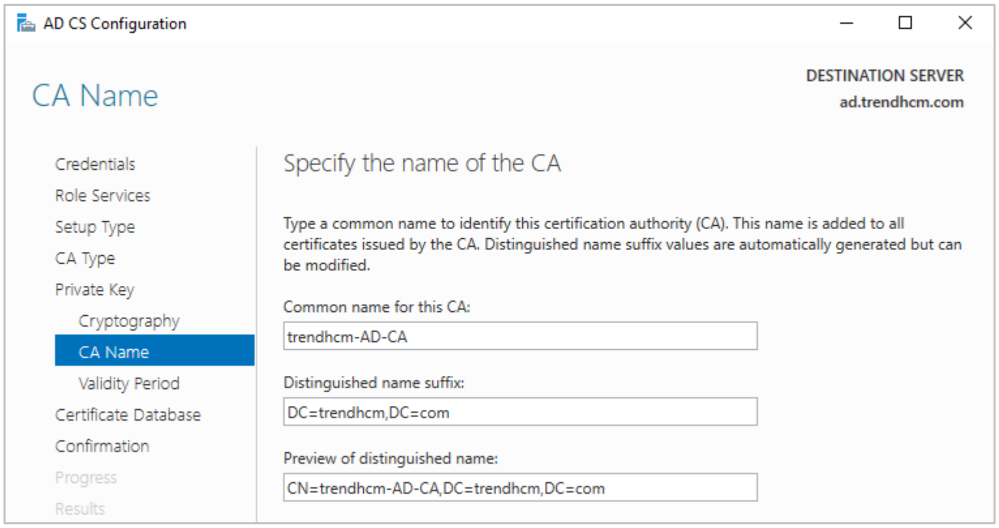
Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

□ Allow administrator interaction when the private key is accessed by the CA.



CA Name

DESTINATION SERVER
ad.trendhcm.com

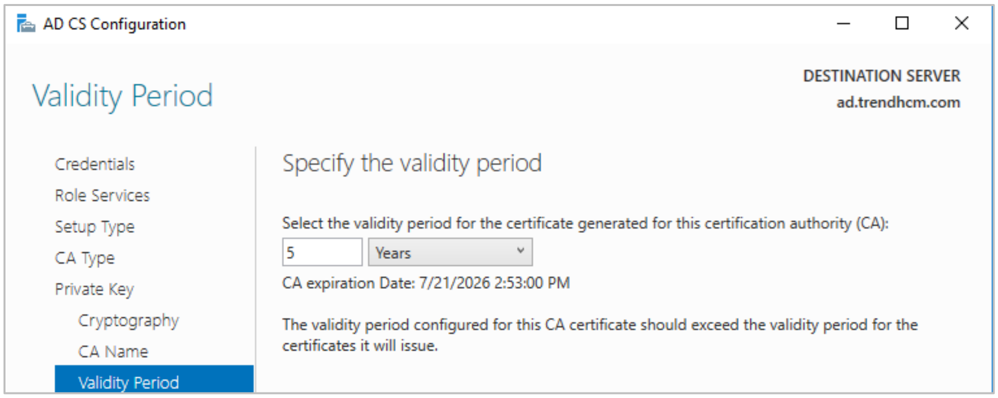
Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA: trendhcm-AD-CA

Distinguished name suffix: DC=trendhcm,DC=com

Preview of distinguished name: CN=trendhcm-AD-CA,DC=trendhcm,DC=com



Validity Period

DESTINATION SERVER
ad.trendhcm.com

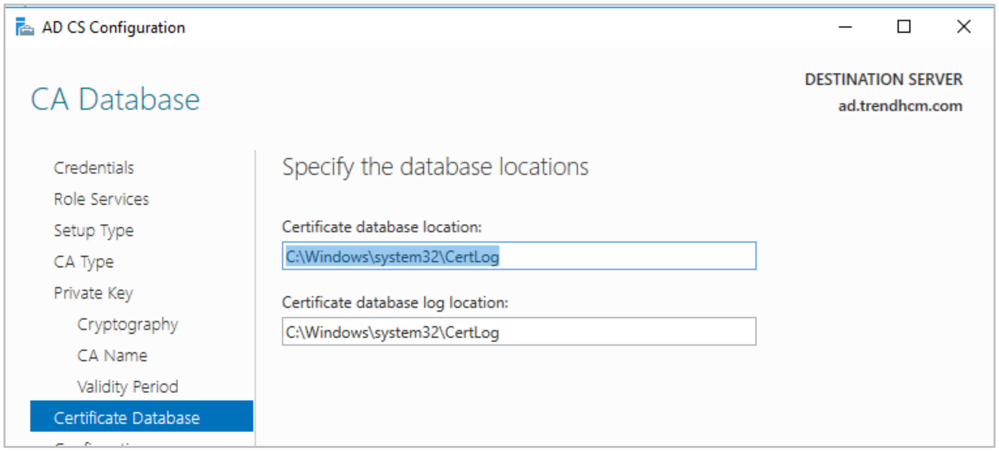
Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

5 Years

CA expiration Date: 7/21/2026 2:53:00 PM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.



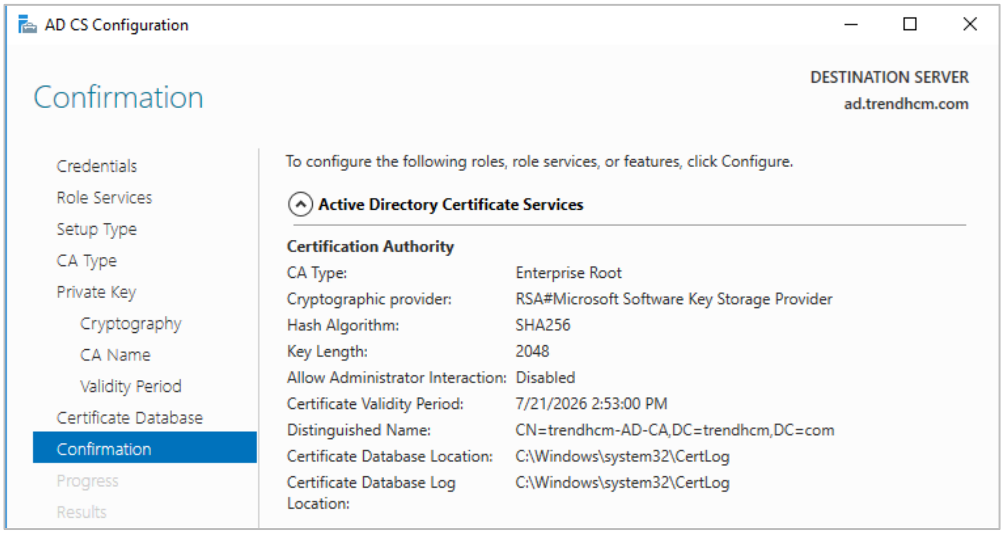
CA Database

DESTINATION SERVER
ad.trendhcm.com

Specify the database locations

Certificate database location:
C:\Windows\system32\CertLog

Certificate database log location:
C:\Windows\system32\CertLog



Confirmation

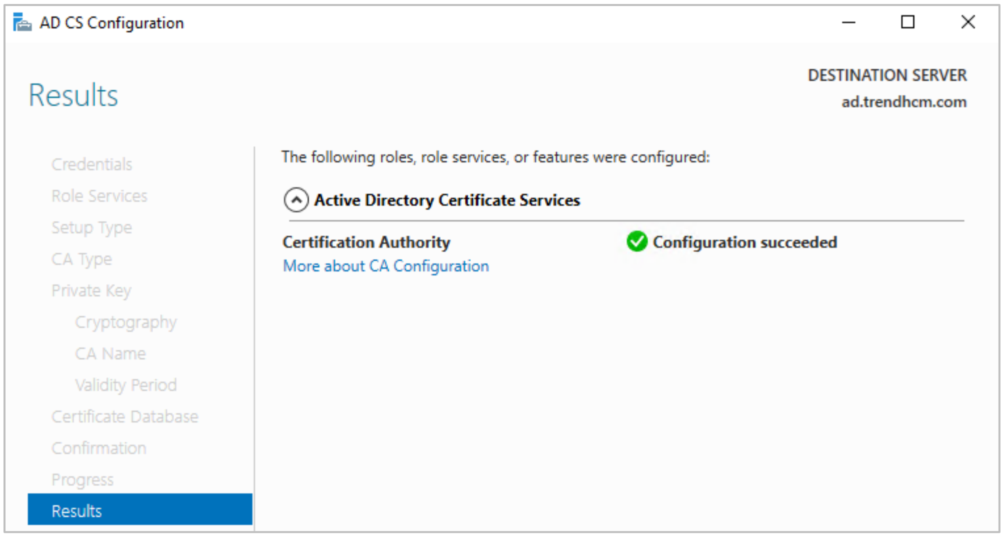
DESTINATION SERVER
ad.trendhcm.com

To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	7/21/2026 2:53:00 PM
Distinguished Name:	CN=trendhcm-AD-CA,DC=trendhcm,DC=com
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog



AD CS Configuration

Results

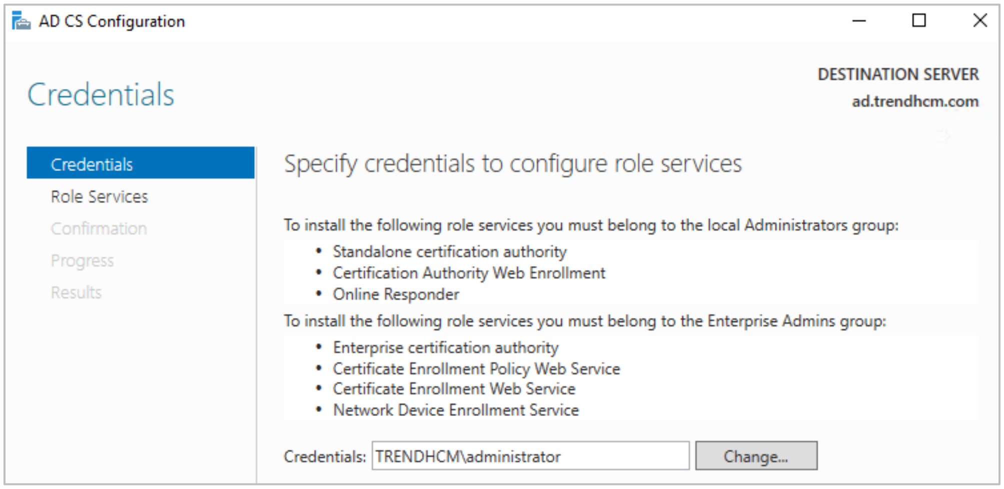
DESTINATION SERVER
ad.trendhcm.com

The following roles, role services, or features were configured:

Active Directory Certificate Services

Certification Authority More about CA Configuration	✓ Configuration succeeded

Cấu hình ADCS role service khác



AD CS Configuration

Credentials

DESTINATION SERVER
ad.trendhcm.com

Specify credentials to configure role services

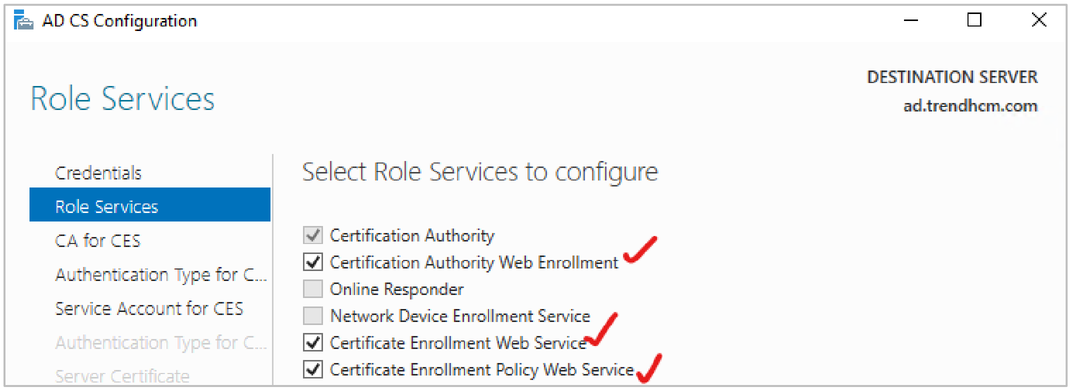
To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: TRENDHCM\administrator



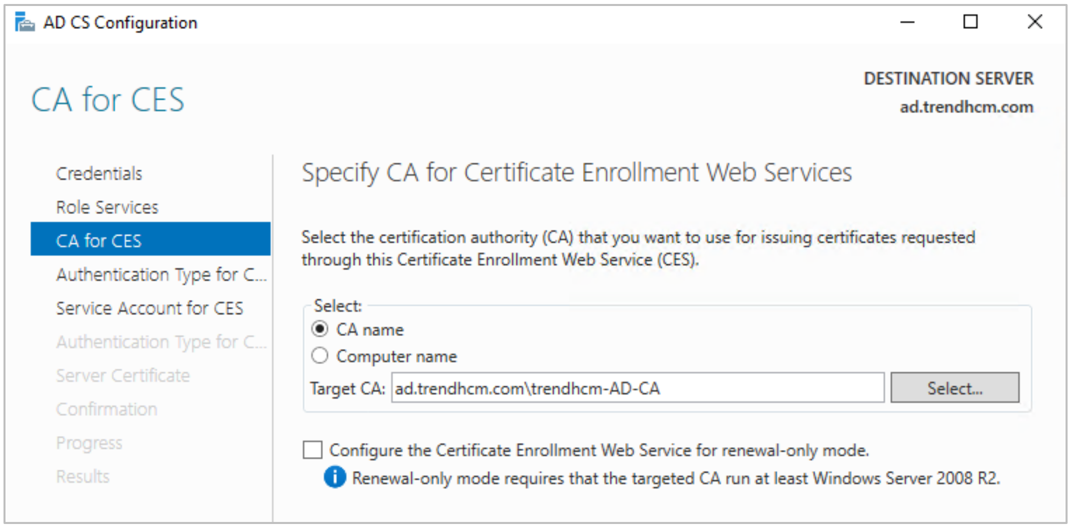
AD CS Configuration

Role Services

DESTINATION SERVER
ad.trendhcm.com

Select Role Services to configure

☑ Certification Authority
☑ Certification Authority Web Enrollment ✓
□ Online Responder
□ Network Device Enrollment Service ✓
☑ Certificate Enrollment Web Service
☑ Certificate Enrollment Policy Web Service ✓


AD CS Configuration

DESTINATION SERVER
ad.trendhcm.com

CA for CES

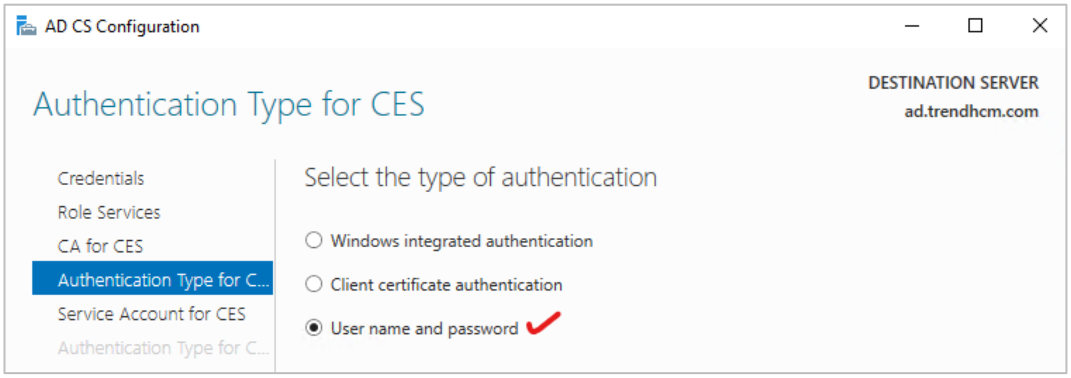
Specify CA for Certificate Enrollment Web Services

Select the certification authority (CA) that you want to use for issuing certificates requested through this Certificate Enrollment Web Service (CES).

Select:
● CA name
○ Computer name
Target CA: ad.trendhcm.com\trendhcm-AD-CA

□ Configure the Certificate Enrollment Web Service for renewal-only mode.

Renewal-only mode requires that the targeted CA run at least Windows Server 2008 R2.

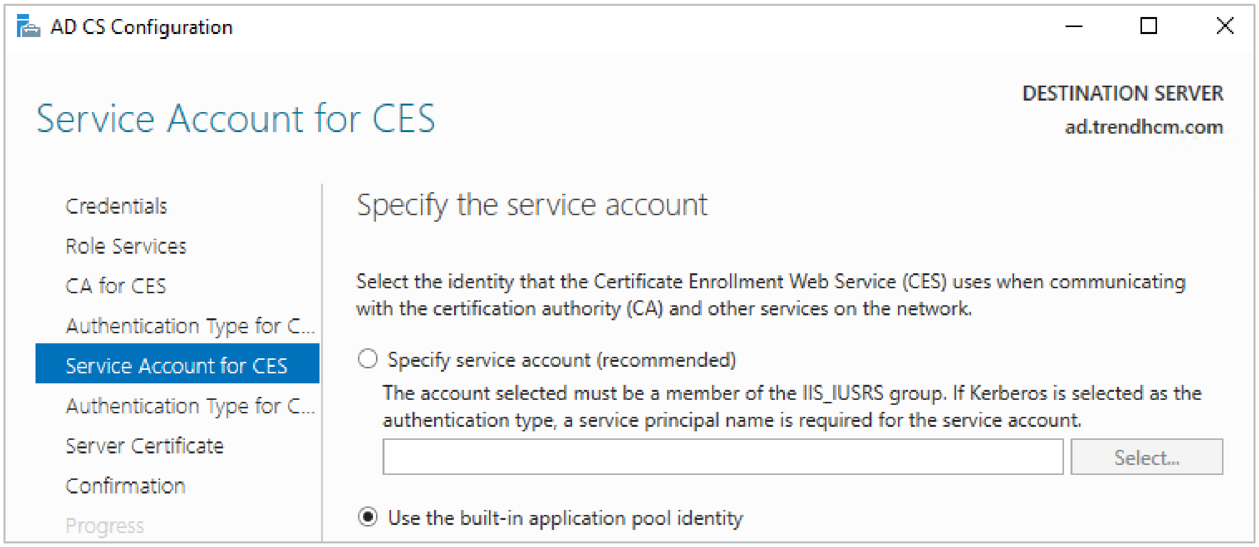

AD CS Configuration

DESTINATION SERVER
ad.trendhcm.com

Authentication Type for CES

Select the type of authentication

○ Windows integrated authentication
○ Client certificate authentication
● User name and password ✓


AD CS Configuration

DESTINATION SERVER
ad.trendhcm.com

Service Account for CES

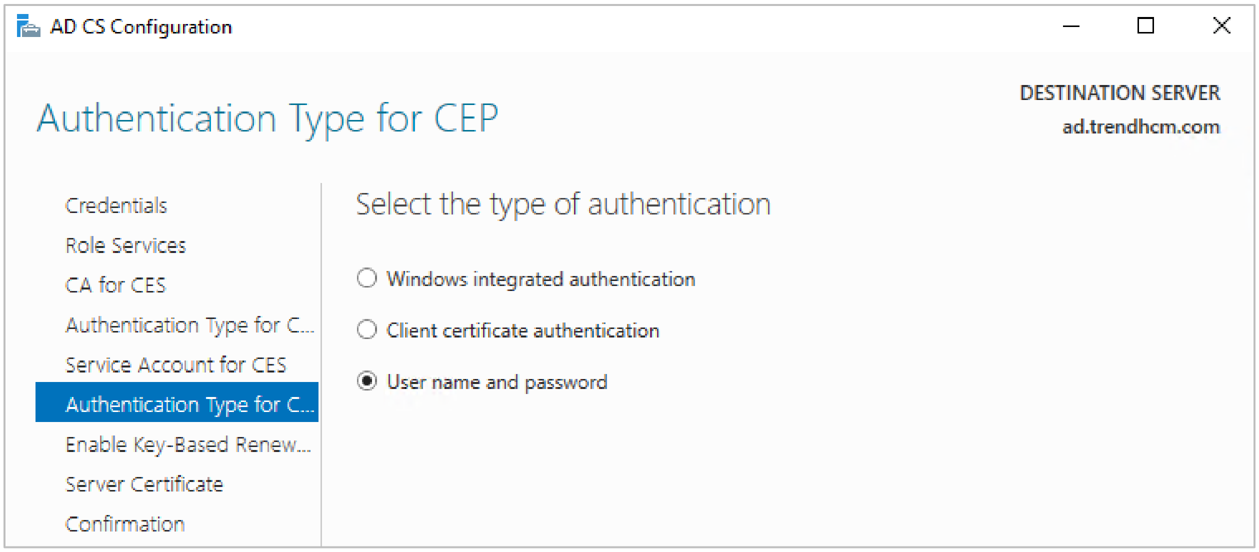
Specify the service account

Select the identity that the Certificate Enrollment Web Service (CES) uses when communicating with the certification authority (CA) and other services on the network.

○ Specify service account (recommended)

The account selected must be a member of the IIS_IUSRS group. If Kerberos is selected as the authentication type, a service principal name is required for the service account.

● Use the built-in application pool identity



AD CS Configuration

Authentication Type for CEP

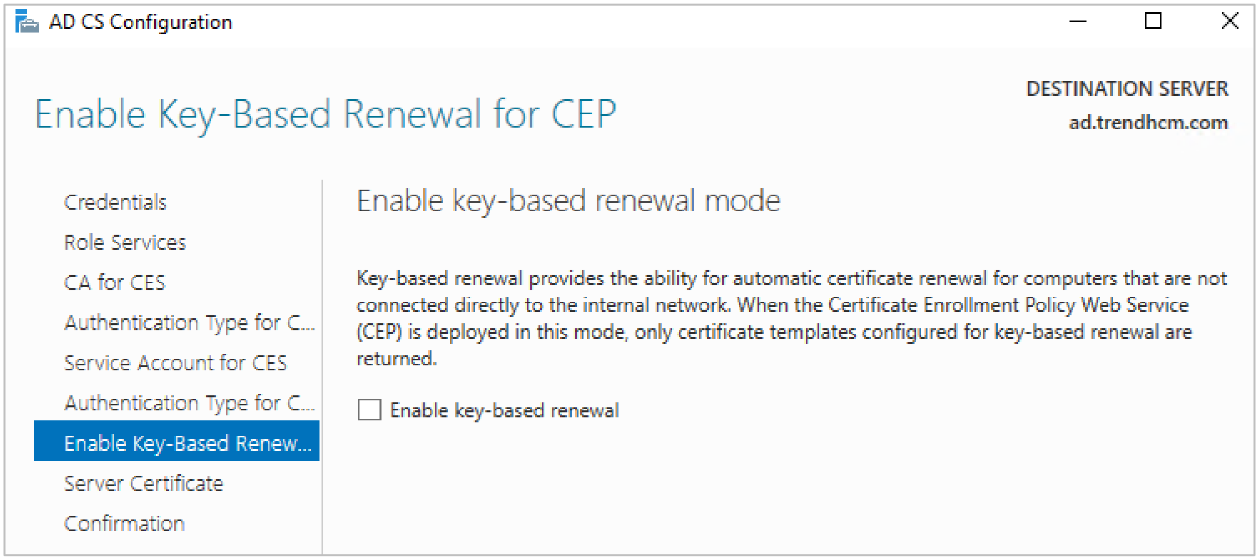
DESTINATION SERVER
ad.trendhcm.com

Select the type of authentication

○ Windows integrated authentication

○ Client certificate authentication

● User name and password



AD CS Configuration

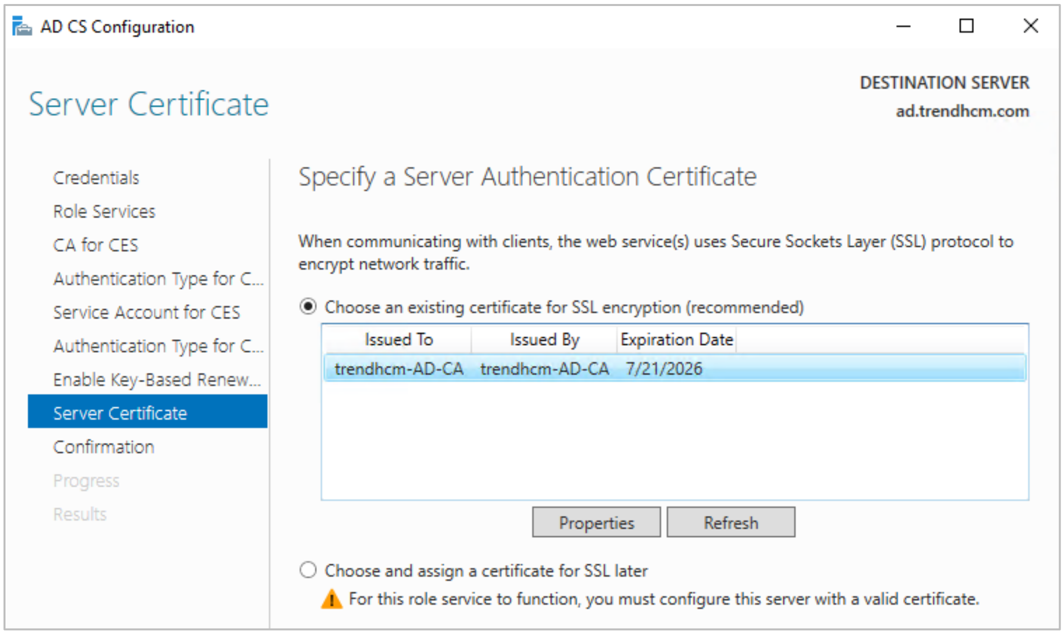
Enable Key-Based Renewal for CEP

DESTINATION SERVER
ad.trendhcm.com

Enable key-based renewal mode

Key-based renewal provides the ability for automatic certificate renewal for computers that are not connected directly to the internal network. When the Certificate Enrollment Policy Web Service (CEP) is deployed in this mode, only certificate templates configured for key-based renewal are returned.

□ Enable key-based renewal



Server Certificate

DESTINATION SERVER
ad.trendhcm.com

Specify a Server Authentication Certificate

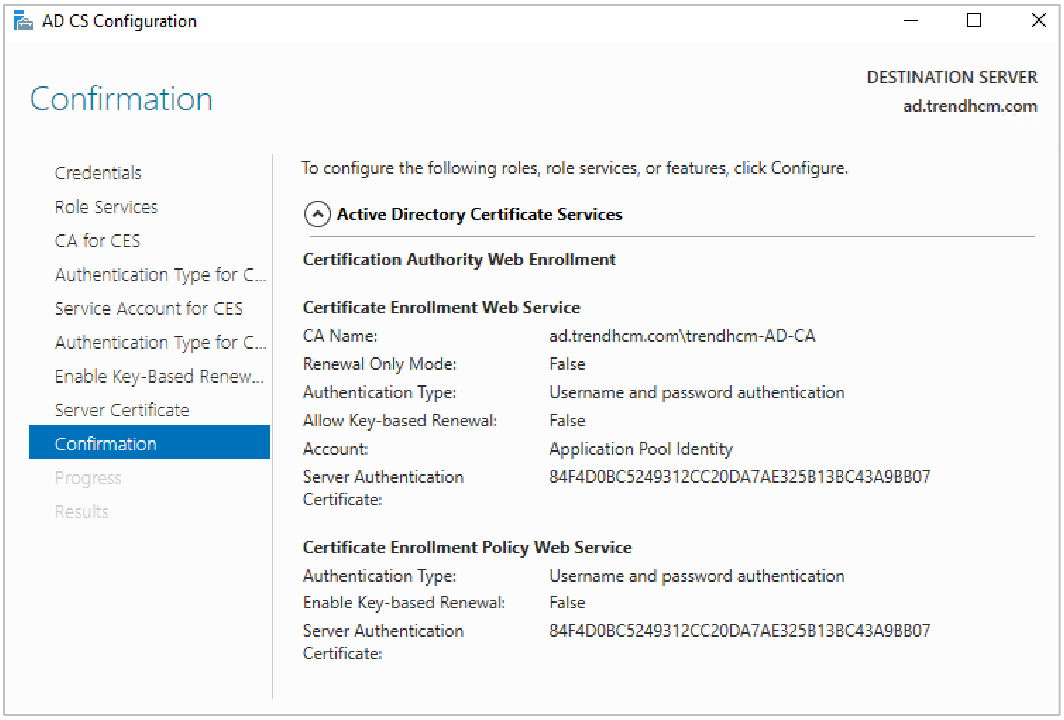
When communicating with clients, the web service(s) uses Secure Sockets Layer (SSL) protocol to encrypt network traffic.

● Choose an existing certificate for SSL encryption (recommended)

Issued To	Issued By	Expiration Date
trendhcm-AD-CA	trendhcm-AD-CA	7/21/2026

○ Choose and assign a certificate for SSL later

⚠ For this role service to function, you must configure this server with a valid certificate.



Confirmation

DESTINATION SERVER
ad.trendhcm.com

To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

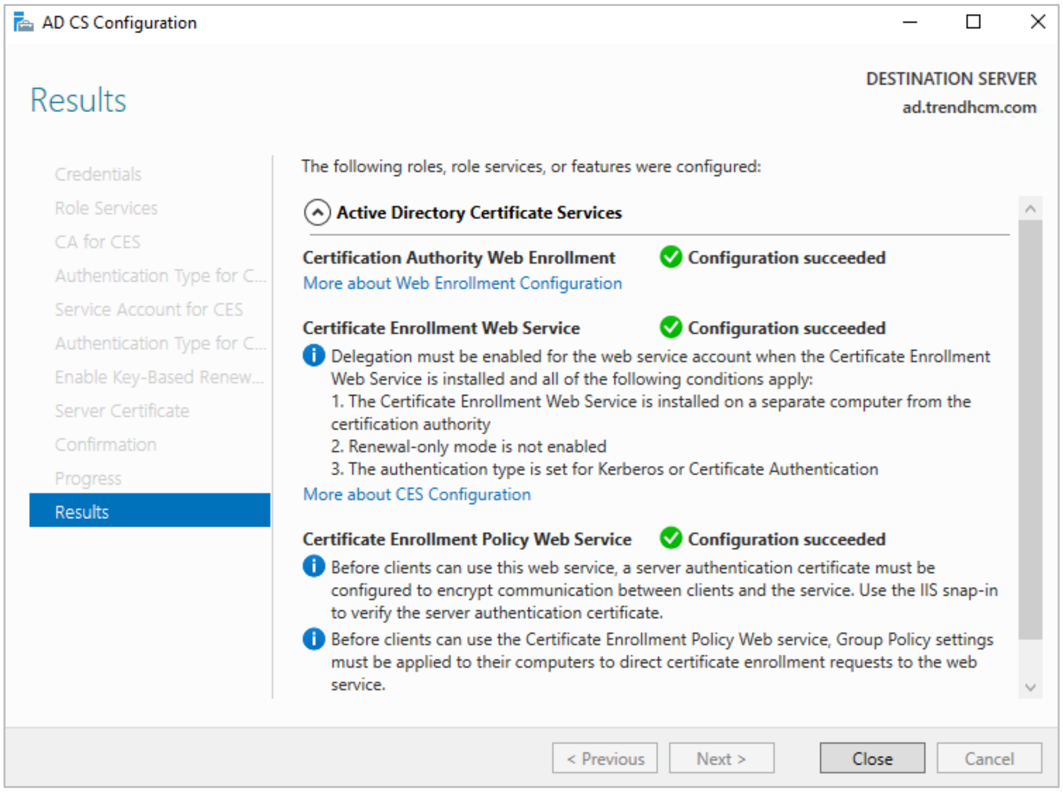
Certification Authority Web Enrollment

Certificate Enrollment Web Service

CA Name:	ad.trendhcm.com\trendhcm-AD-CA
Renewal Only Mode:	False
Authentication Type:	Username and password authentication
Allow Key-based Renewal:	False
Account:	Application Pool Identity
Server Authentication Certificate:	84F4D0BC5249312CC20DA7AE325B13BC43A9BB07

Certificate Enrollment Policy Web Service

Authentication Type:	Username and password authentication
Enable Key-based Renewal:	False
Server Authentication Certificate:	84F4D0BC5249312CC20DA7AE325B13BC43A9BB07



The following roles, role services, or features were configured:

Active Directory Certificate Services

Certification Authority Web Enrollment ✓ **Configuration succeeded**
More about Web Enrollment Configuration

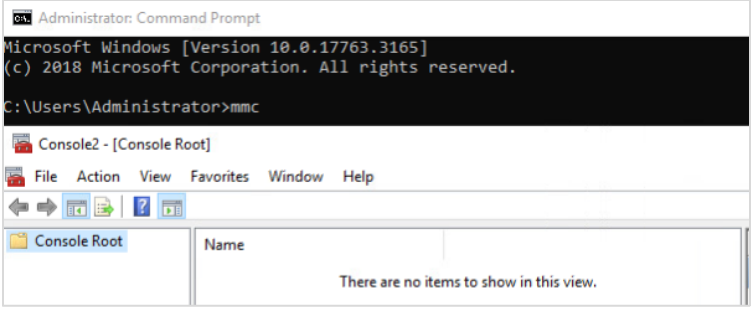
Certificate Enrollment Web Service ✓ **Configuration succeeded**
Delegation must be enabled for the web service account when the Certificate Enrollment Web Service is installed and all of the following conditions apply:
1. The Certificate Enrollment Web Service is installed on a separate computer from the certification authority
2. Renewal-only mode is not enabled
3. The authentication type is set for Kerberos or Certificate Authentication
More about CES Configuration

Certificate Enrollment Policy Web Service ✓ **Configuration succeeded**
Before clients can use this web service, a server authentication certificate must be configured to encrypt communication between clients and the service. Use the IIS snap-in to verify the server authentication certificate.
Before clients can use the Certificate Enrollment Policy Web service, Group Policy settings must be applied to their computers to direct certificate enrollment requests to the web service.

Cấu hình certificate service cho máy chủ AD

Cấu hình trên AD server

Access vào MMC trên máy ADCS: https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-view-certificates-with-the-mmc-snap-in

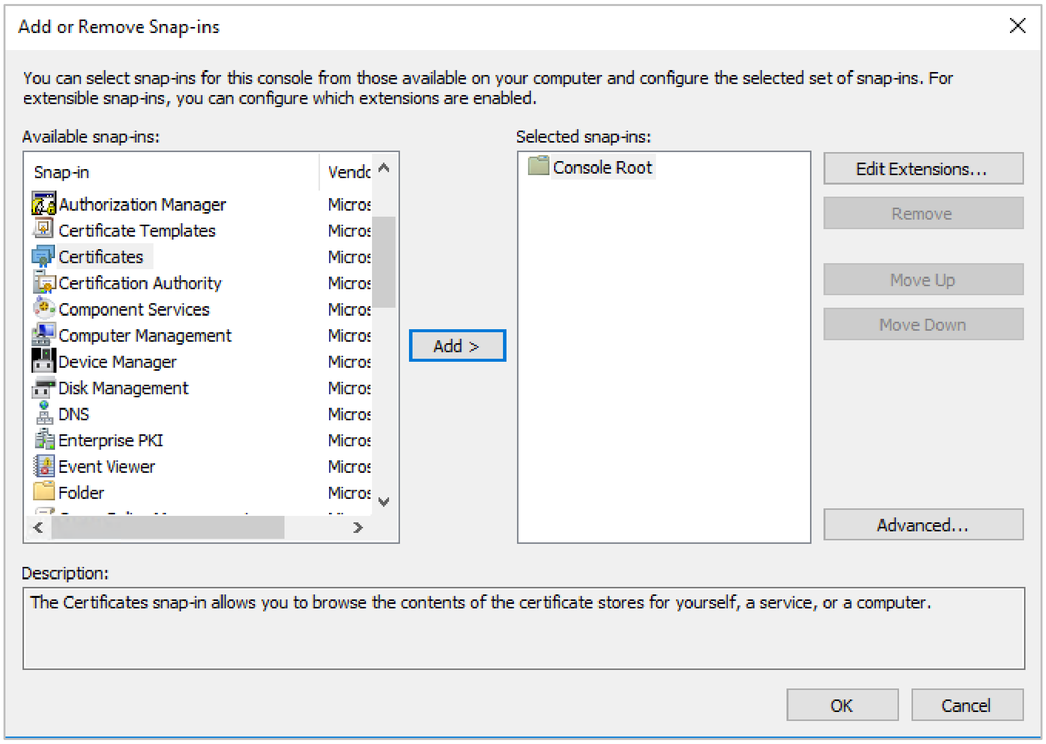


```
Microsoft Windows [Version 10.0.17763.3165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>mmc
```

There are no items to show in this view.

File >> Add/Remove Snap In



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

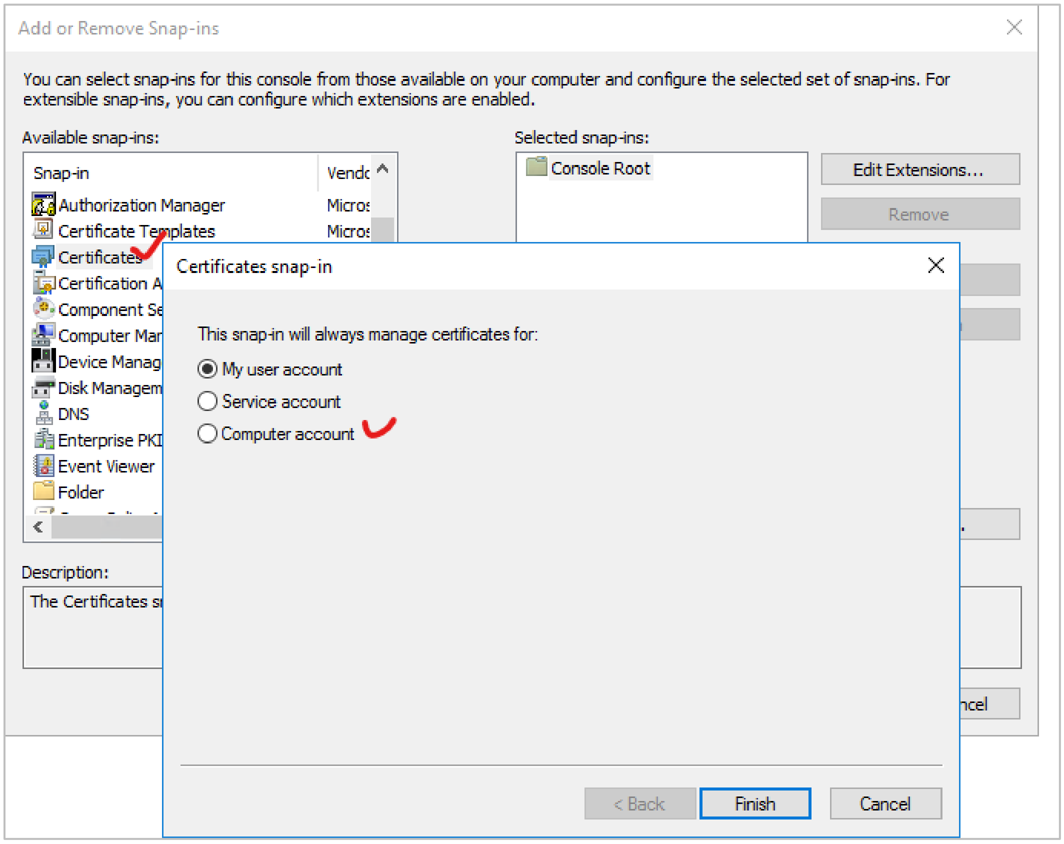
Snap-in	Vendc
Authorization Manager	Micros
Certificate Templates	Micros
Certificates	Micros
Certification Authority	Micros
Component Services	Micros
Computer Management	Micros
Device Manager	Micros
Disk Management	Micros
DNS	Micros
Enterprise PKI	Micros
Event Viewer	Micros
Folder	Micros

Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.



Certificates snap-in

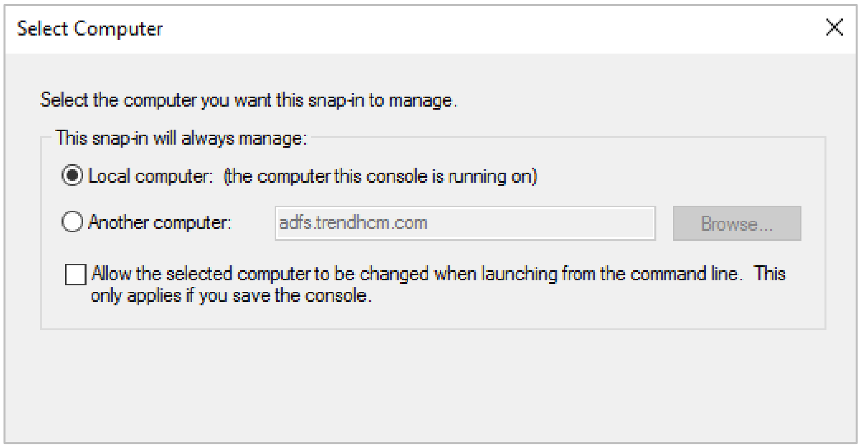
This snap-in will always manage certificates for:

● My user account

○ Service account

○ Computer account

Note: chọn Computer account



Select Computer

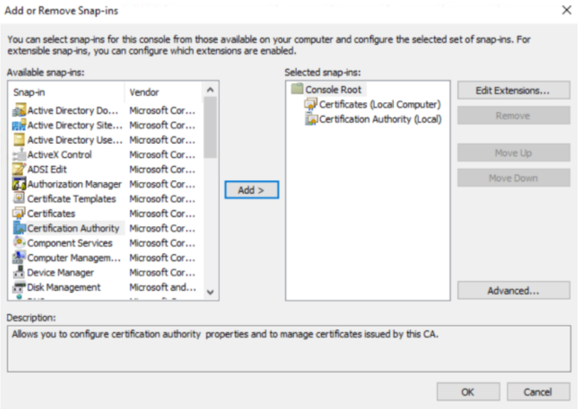
Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer: adfs.trendhcm.com

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

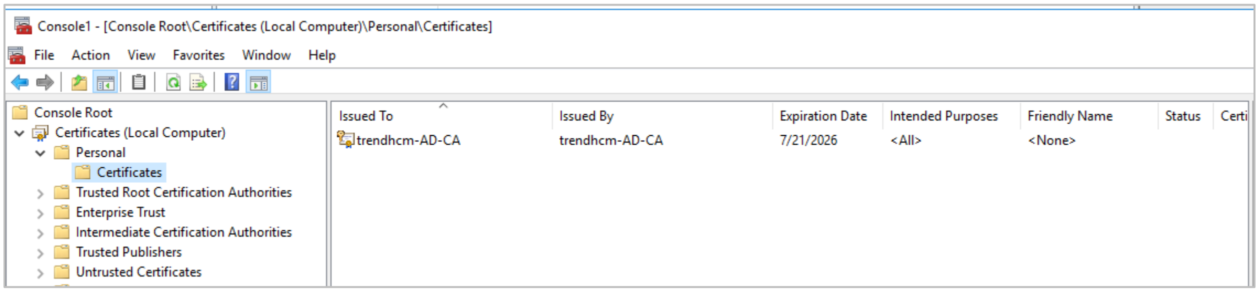
Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...

Selected snap-ins:

- Console Root
  - Certificates (Local Computer)
  - Certification Authority (Local)

Description:

Allows you to configure certification authority properties and to manage certificates issued by this CA.

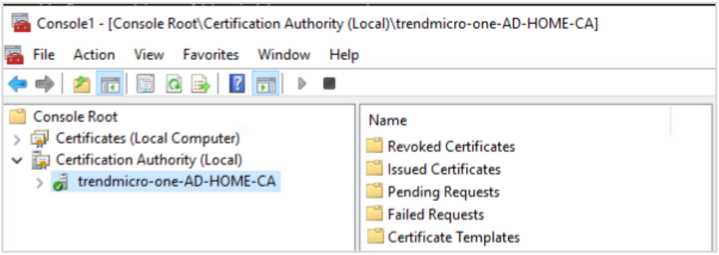


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

- Console Root
  - Certificates (Local Computer)
    - Personal
      - Certificates
    - Trusted Root Certification Authorities
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certi
trendhcm-AD-CA	trendhcm-AD-CA	7/21/2026	<All>	<None>		

Config a template

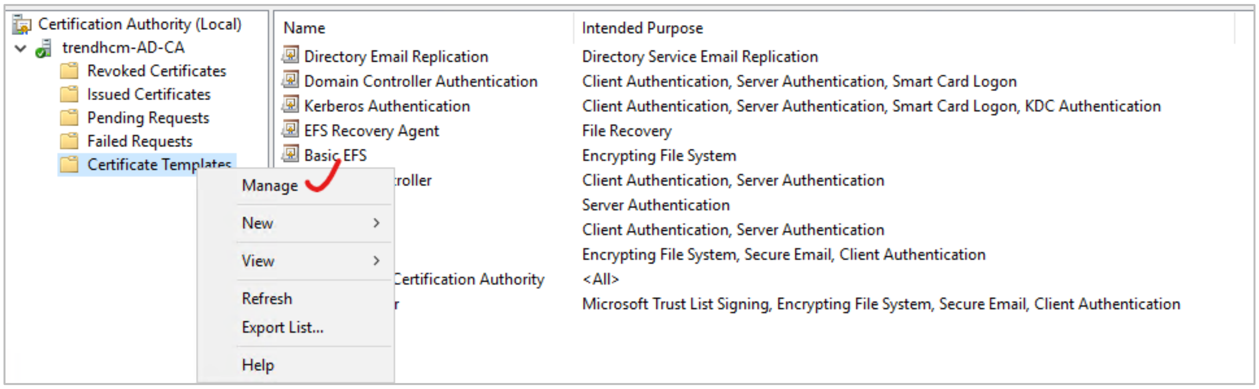


Console1 - [Console Root\Certification Authority (Local)\trendmicro-one-AD-HOME-CA]

- Console Root
  - Certificates (Local Computer)
  - Certification Authority (Local)
    - trendmicro-one-AD-HOME-CA

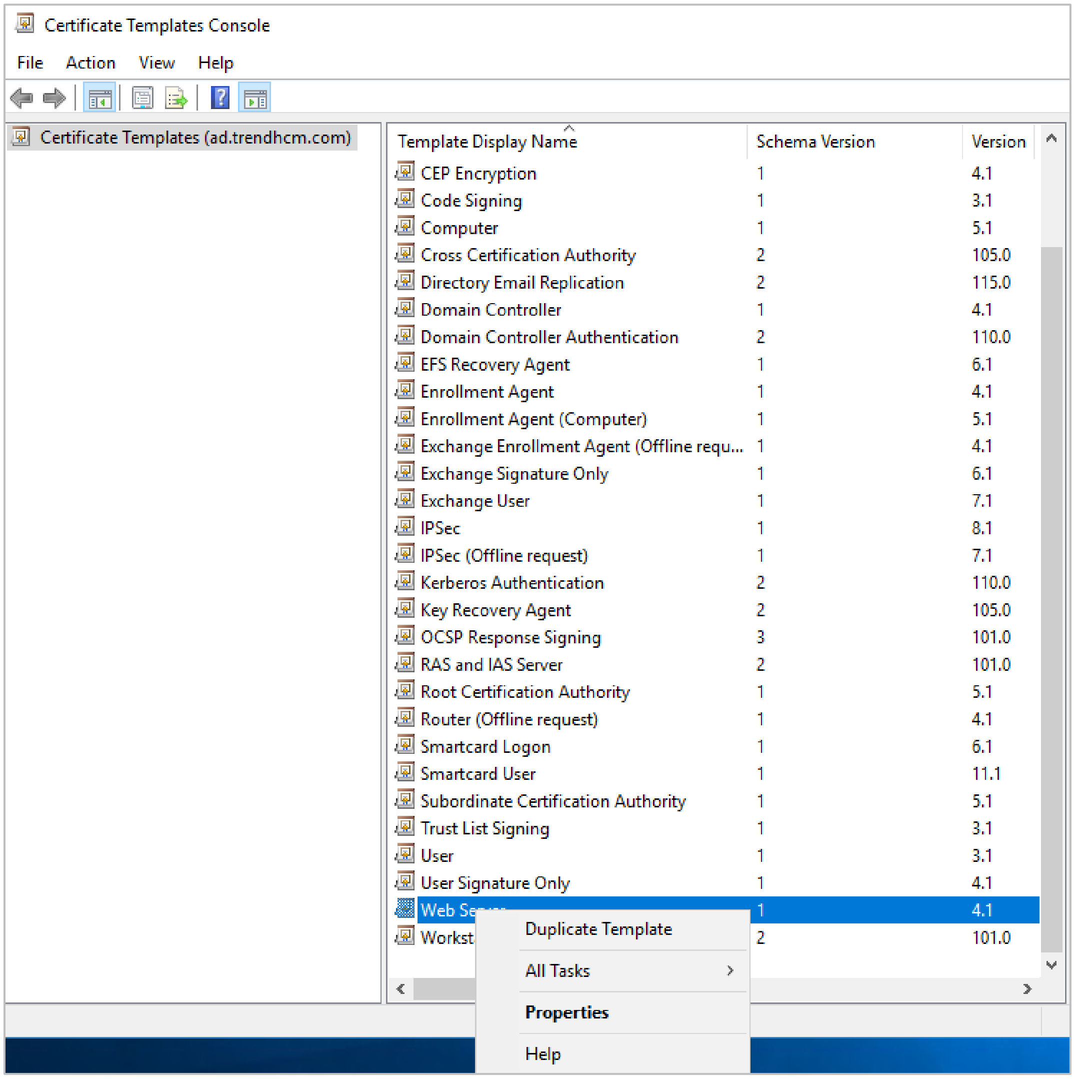
Name

- Revoked Certificates
- Issued Certificates
- Pending Requests
- Failed Requests
- Certificate Templates



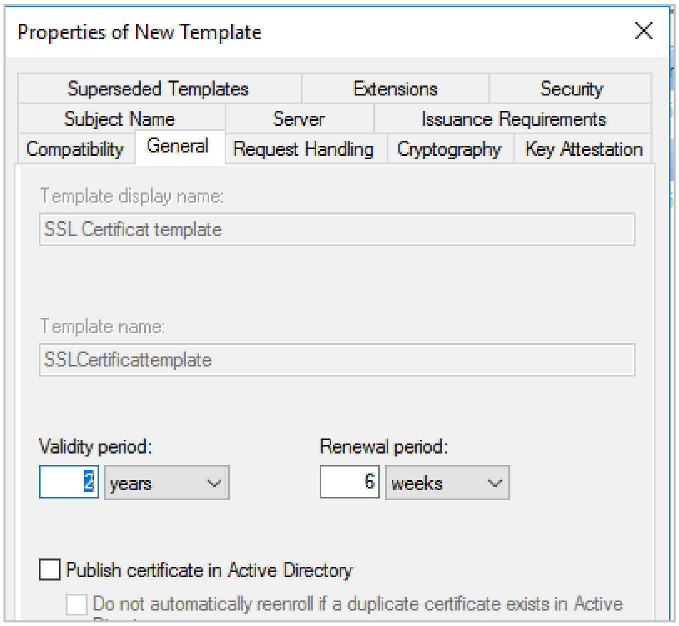
Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentication, Smart Card Logon
Kerberos Authentication	Client Authentication, Server Authentication, Smart Card Logon, KDC Authentication
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
troller	Client Authentication, Server Authentication
	Server Authentication
	Client Authentication, Server Authentication
	Encrypting File System, Secure Email, Client Authentication
Certification Authority	<All>
r	Microsoft Trust List Signing, Encrypting File System, Secure Email, Client Authentication

In the Certificate Templates snap-in, right-click the Web Server template and select Duplicate.


Certificate Templates Console
File
Action
View
Help
Certificate Templates (ad.trendhcm.com)
Duplicate Template
All Tasks
Properties
Help

Template Display Name	Schema Version	Version
CEP Encryption	1	4.1
Code Signing	1	3.1
Computer	1	5.1
Cross Certification Authority	2	105.0
Directory Email Replication	2	115.0
Domain Controller	1	4.1
Domain Controller Authentication	2	110.0
EFS Recovery Agent	1	6.1
Enrollment Agent	1	4.1
Enrollment Agent (Computer)	1	5.1
Exchange Enrollment Agent (Offline requ...	1	4.1
Exchange Signature Only	1	6.1
Exchange User	1	7.1
IPSec	1	8.1
IPSec (Offline request)	1	7.1
Kerberos Authentication	2	110.0
Key Recovery Agent	2	105.0
OCSP Response Signing	3	101.0
RAS and IAS Server	2	101.0
Root Certification Authority	1	5.1
Router (Offline request)	1	4.1
Smartcard Logon	1	6.1
Smartcard User	1	11.1
Subordinate Certification Authority	1	5.1
Trust List Signing	1	3.1
User	1	3.1
User Signature Only	1	4.1
Web Se	1	4.1
Workst	2	101.0

>> Click Duplicate Template



Template display name:
SSL Certificat template

Template name:
SSLCertificattemplate

Validity period: 2 years

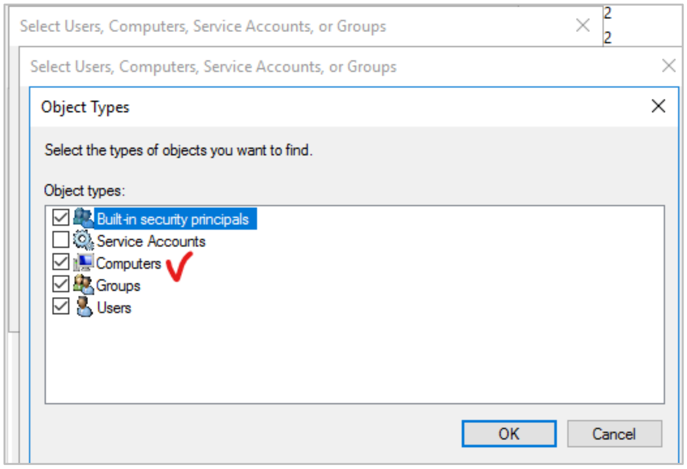
Renewal period: 6 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active

On the Security tab, click Add.

Click Object Types, check Computers, and then click Ok.



Select Users, Computers, Service Accounts, or Groups
Select Users, Computers, Service Accounts, or Groups
Object Types
OK
Cancel

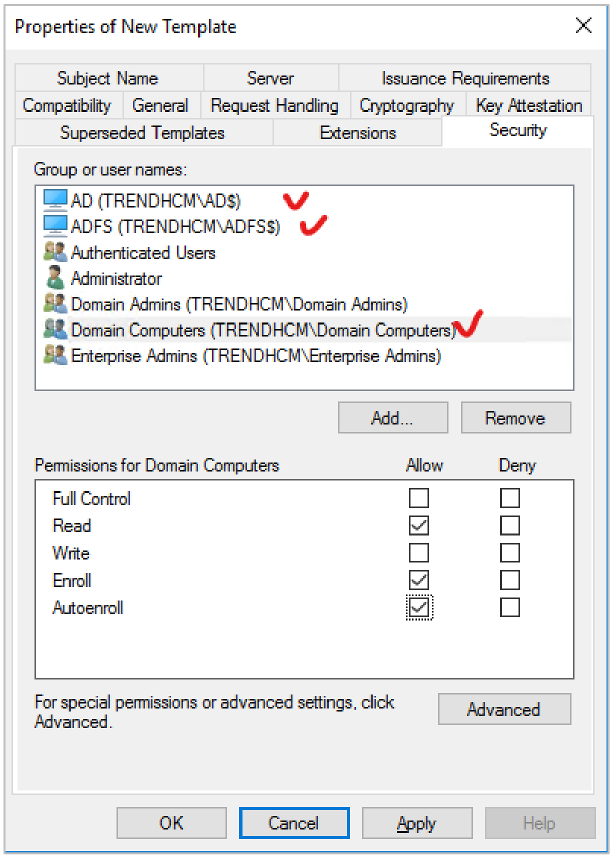
Select the types of objects you want to find.

Object types:

☑ Built-in security principals
□ Service Accounts
☑ Computers ✓
☑ Groups
☑ Users

Click Check Names and then lick OK.

With Domain Computers selected, check read, enroll, and auto-enroll permissions.



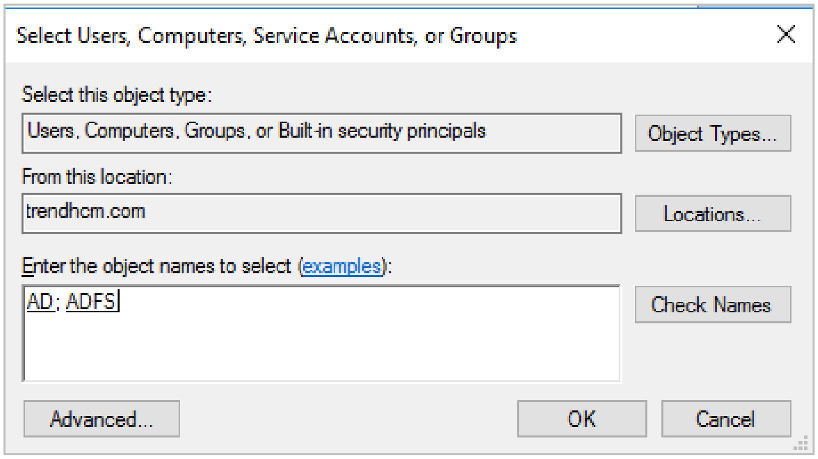
Properties of New Template

Group or user names:

- AD (TRENDHCM\AD$) ✓
- ADFS (TRENDHCM\ADFS$) ✓
- Authenticated Users
- Administrator
- Domain Admins (TRENDHCM\Domain Admins)
- Domain Computers (TRENDHCM\Domain Computers) ✓
- Enterprise Admins (TRENDHCM\Enterprise Admins)

Permissions for Domain Computers	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	☑	□

For special permissions or advanced settings, click Advanced.



Select Users, Computers, Service Accounts, or Groups

Select this object type:

Users, Computers, Groups, or Built-in security principals

From this location:

trendhcm.com

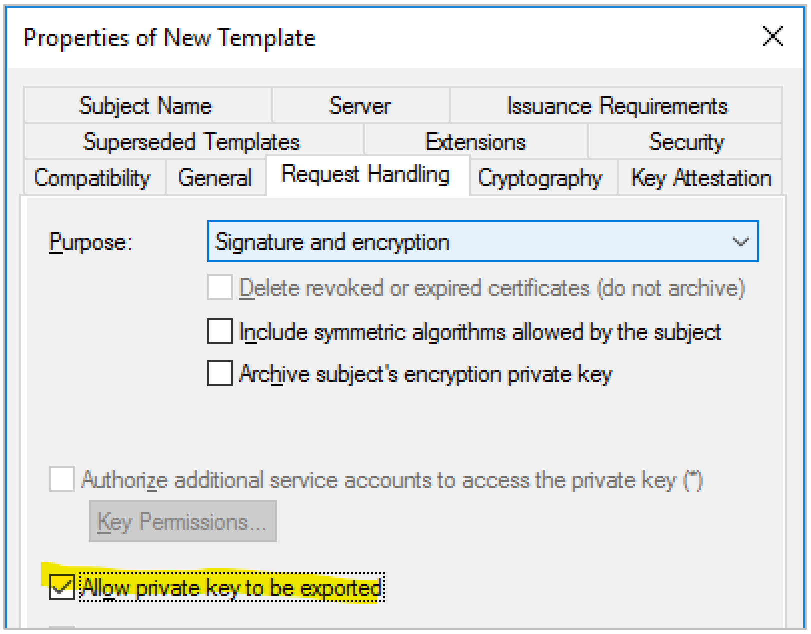
Enter the object names to select (examples):

AD; ADFS

On the Request Handling tab, check the Allow private key to be exported box.

On the General tab, update the template display name to SSL Certificate Template or similar.

Click OK to save the new template.



Purpose: Signature and encryption

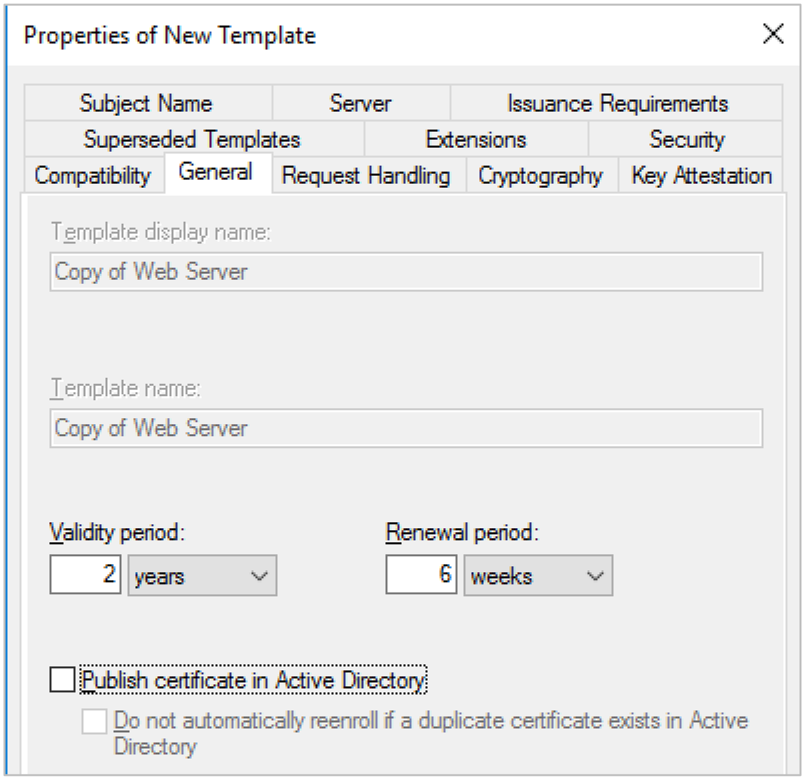
□ Delete revoked or expired certificates (do not archive)

□ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

□ Authorize additional service accounts to access the private key (*)

☑ Allow private key to be exported



Template display name: Copy of Web Server

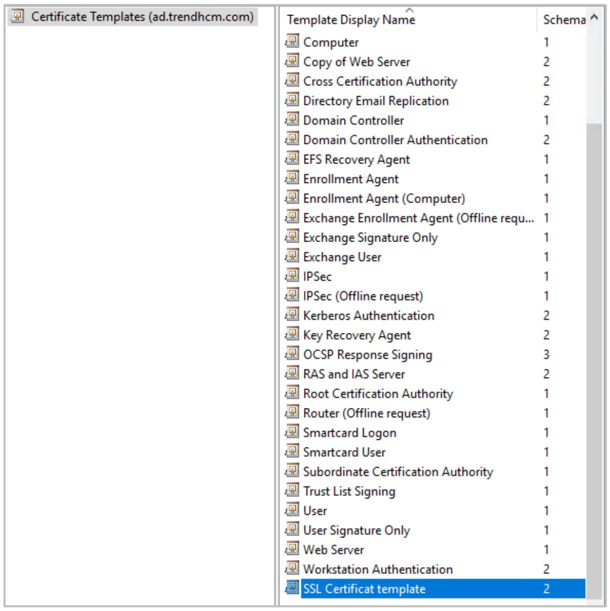
Template name: Copy of Web Server

Validity period: 2 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

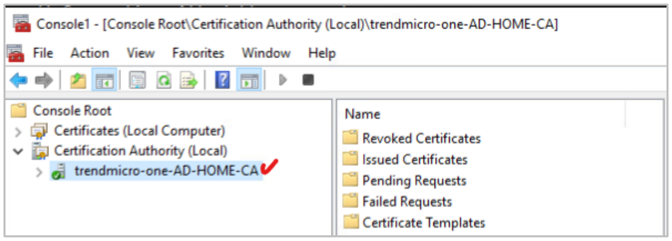
□ Do not automatically reenroll if a duplicate certificate exists in Active Directory



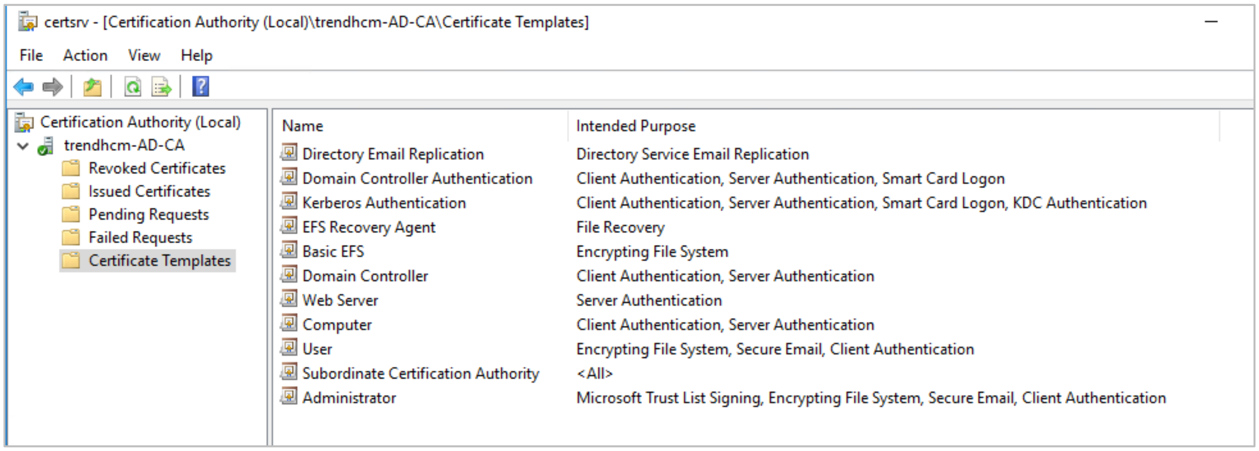
Template Display Name	Schema
Computer	1
Copy of Web Server	2
Cross Certification Authority	2
Directory Email Replication	2
Domain Controller	1
Domain Controller Authentication	2
EFS Recovery Agent	1
Enrollment Agent	1
Enrollment Agent (Computer)	1
Exchange Enrollment Agent (Offline requ...	1
Exchange Signature Only	1
Exchange User	1
IPSec	1
IPSec (Offline request)	1
Kerberos Authentication	2
Key Recovery Agent	2
OCSP Response Signing	3
RAS and IAS Server	2
Root Certification Authority	1
Router (Offline request)	1
Smartcard Logon	1
Smartcard User	1
Subordinate Certification Authority	1
Trust List Signing	1
User	1
User Signature Only	1
Web Server	1
Workstation Authentication	2
SSL Certificat template	2

Assign a template to a CA

Under Certification Authority (Local), expand the node with the CA name.


Console1 - [Console Root\Certification Authority (Local)\trendmicro-one-AD-HOME-CA]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Certification Authority (Local)
trendmicro-one-AD-HOME-CA
Name
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates

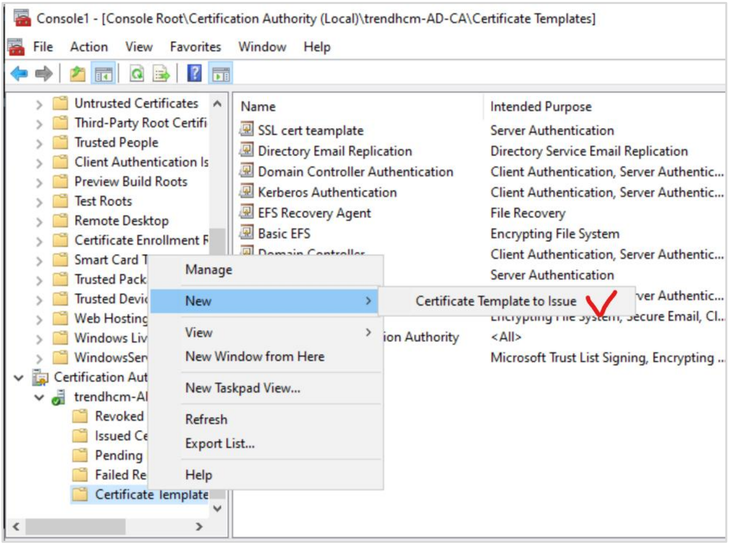
Click to select the Certificate Templates container (under the CA name, not the Certificate Templates snap-in).



Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentication, Smart Card Logon
Kerberos Authentication	Client Authentication, Server Authentication, Smart Card Logon, KDC Authentication
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentication
Web Server	Server Authentication
Computer	Client Authentication, Server Authentication
User	Encrypting File System, Secure Email, Client Authentication
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting File System, Secure Email, Client Authentication

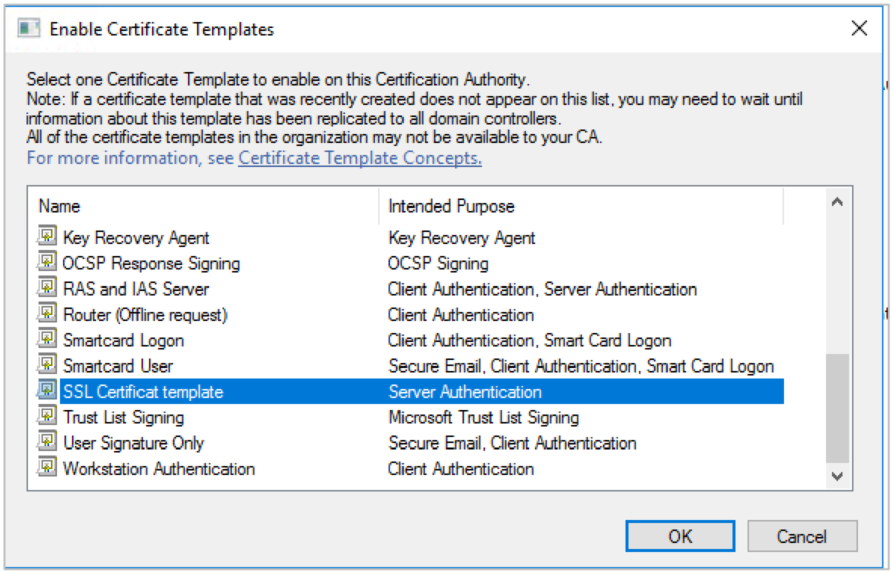
Right click the container and select New, and then **Certificate Template to Issue.**

Select SSL Certificate Template and click OK.



Console1 - [Console Root\Certification Authority (Local)\trendhcm-AD-CA\Certificate Templates]

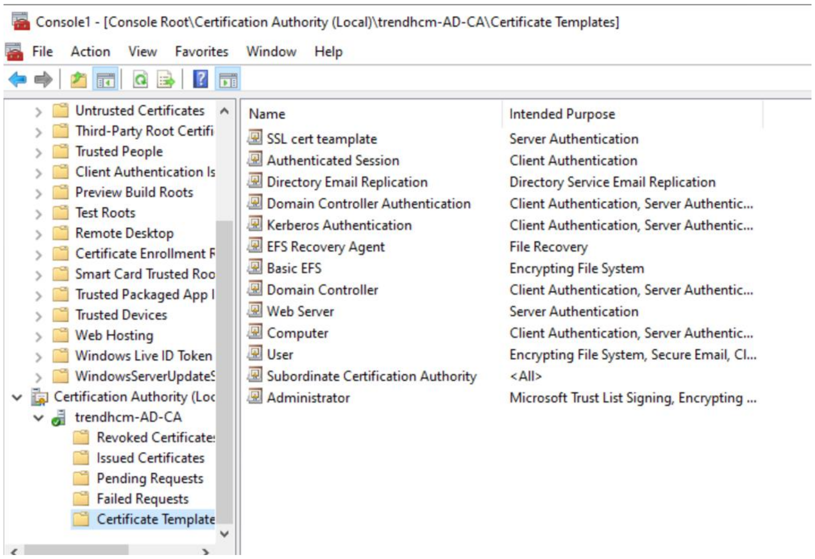
Name	Intended Purpose
SSL cert teamplate	Server Authentication
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
	Server Authentication
	ver Authentic...
	Encrypting File System, Secure Email, Cl...
ion Authority	<All>
	Microsoft Trust List Signing, Encrypting ...



Enable Certificate Templates

Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon
SSL Certificat template	Server Authentication
Trust List Signing	Microsoft Trust List Signing
User Signature Only	Secure Email, Client Authentication
Workstation Authentication	Client Authentication



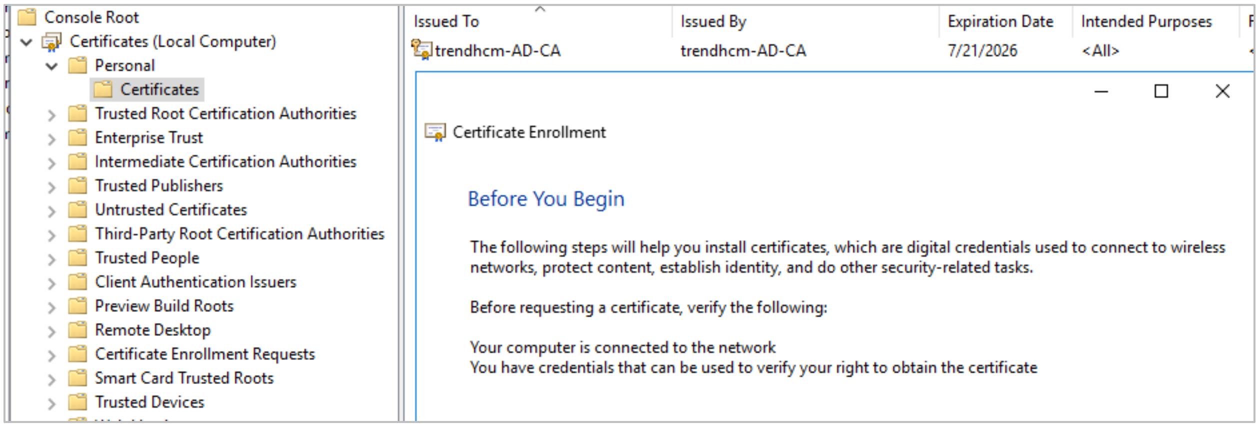
Console1 - [Console Root\Certification Authority (Local)\trendhcm-AD-CA\Certificate Templates]

Name	Intended Purpose
SSL cert teamplate	Server Authentication
Authenticated Session	Client Authentication
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting ...

Request and enroll a new SSL certificate for AD FS (still configure on AD server)

Open the MMC window and add the Certificates snap-in for the local Computer account.

Right-click the [Personal] node and choose [All Tasks] -> [Request New Certificate]



Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

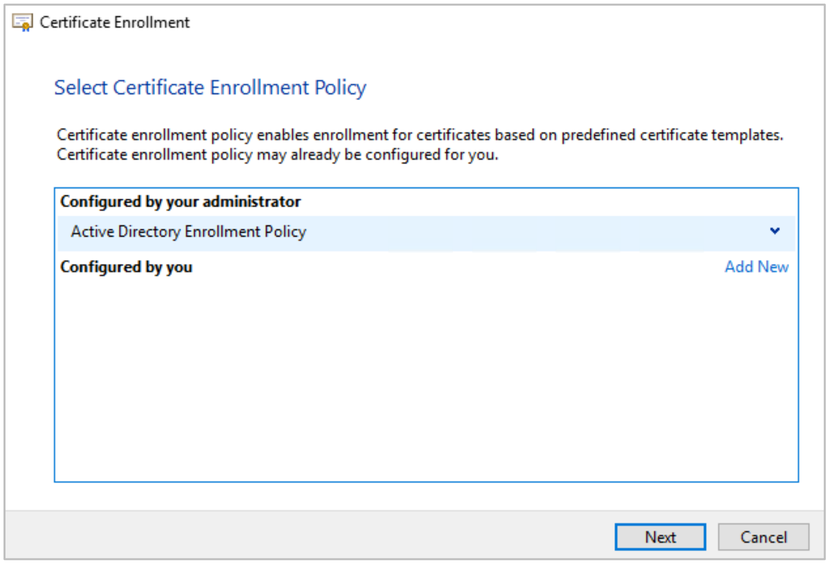
Before requesting a certificate, verify the following:

Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate

Click Next twice to get to the Request certificates page. Your can see the template you created in the previous step.

Click the More information is required... link.

Under Subject name, under Type, select Common name.

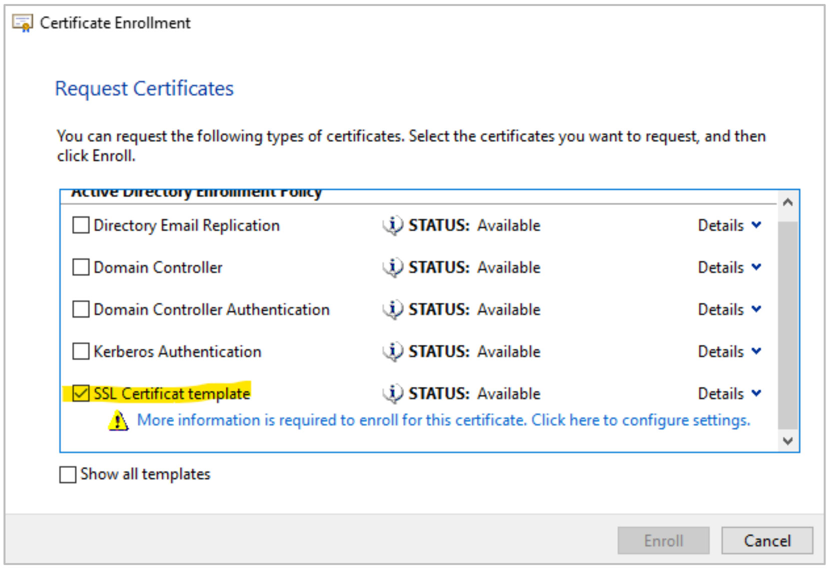


Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator
Active Directory Enrollment Policy

Configured by you



Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

□ Directory Email Replication	STATUS: Available	Details
□ Domain Controller	STATUS: Available	Details
□ Domain Controller Authentication	STATUS: Available	Details
□ Kerberos Authentication	STATUS: Available	Details
☑ SSL Certificat template	STATUS: Available	Details

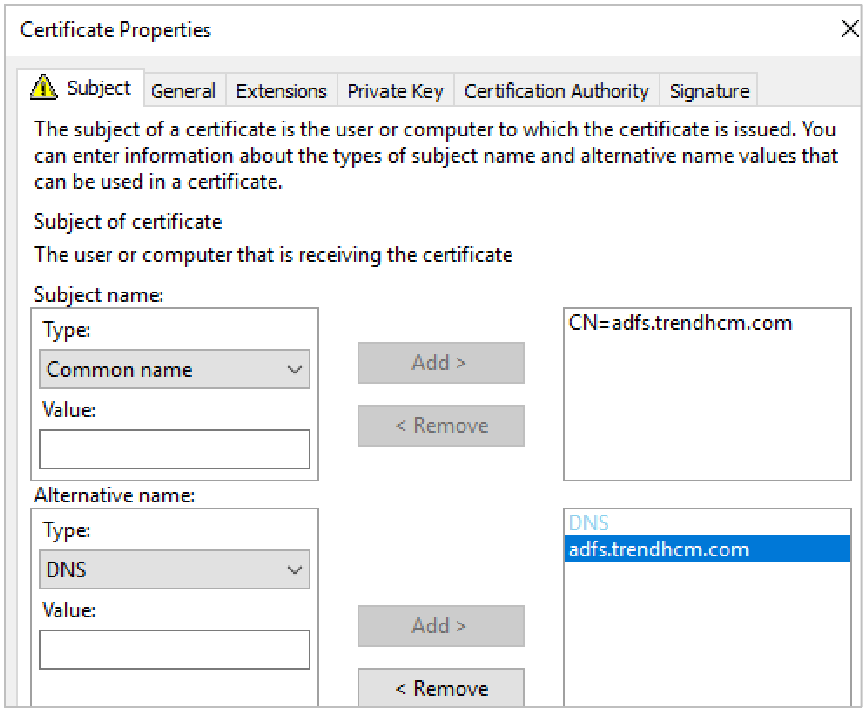
⚠ More information is required to enroll for this certificate. Click here to configure settings.

□ Show all templates

Enter your federation service name, for example "fs.contoso.com" and then click Add.

Under Alternative name, under Type, select DNS.

Using the same process, add a subject alternative name of type DNS for your federation service name, for example, “fs.contoso.com” (the same name you added above).



Certificate Properties

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Common name

Value:

CN=adfs.trendhcm.com

Alternative name:

Type: DNS

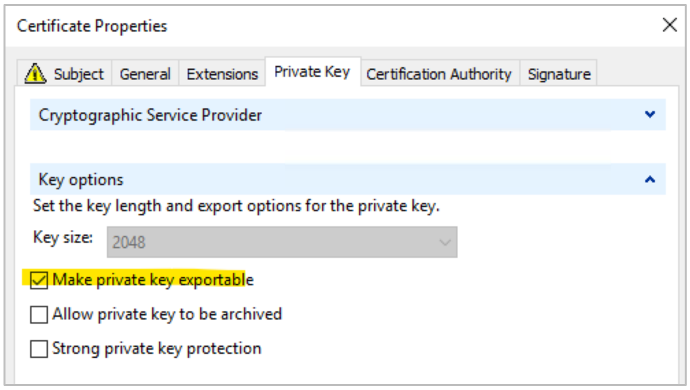
Value:

DNS
adfs.trendhcm.com

If you are using AD FS with DRS, add an additional SAN of type DNS for each UPN suffix in use in your environment, for example “enterpriseregistration.contoso.com”.

Click the Private Key tab.

Under Key options, ensure the Make private key exportable option is checked and click OK.



Key options

Set the key length and export options for the private key.

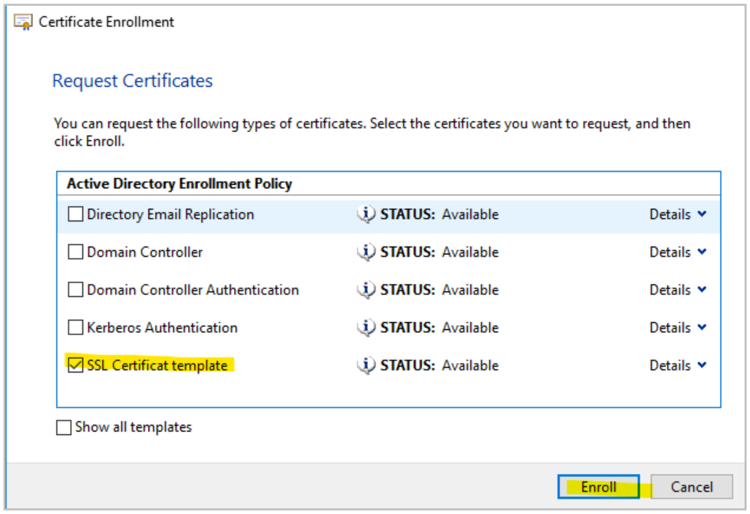
Key size: 2048

☑ Make private key exportable

☐ Allow private key to be archived

☐ Strong private key protection

Back on the Request Certificates wizard page, ensure the checkbox for the template is checked and click Enroll.



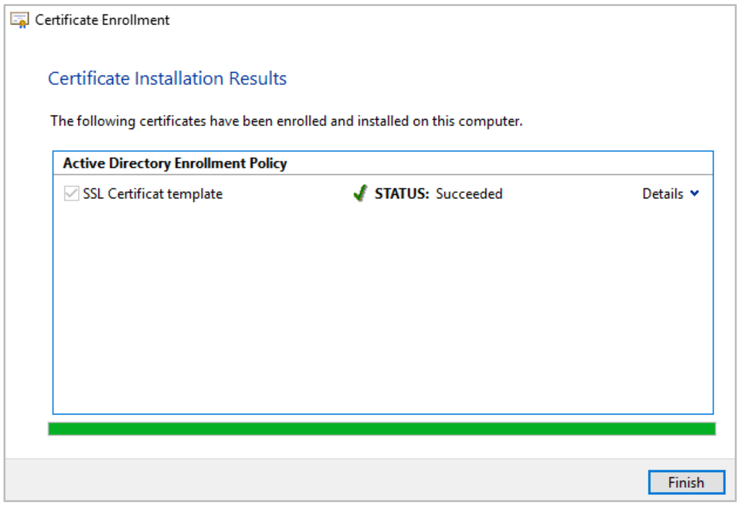
Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy		
☐ Directory Email Replication	STATUS: Available	Details
☐ Domain Controller	STATUS: Available	Details
☐ Domain Controller Authentication	STATUS: Available	Details
☐ Kerberos Authentication	STATUS: Available	Details
☑ SSL Certificat template	STATUS: Available	Details

☐ Show all templates

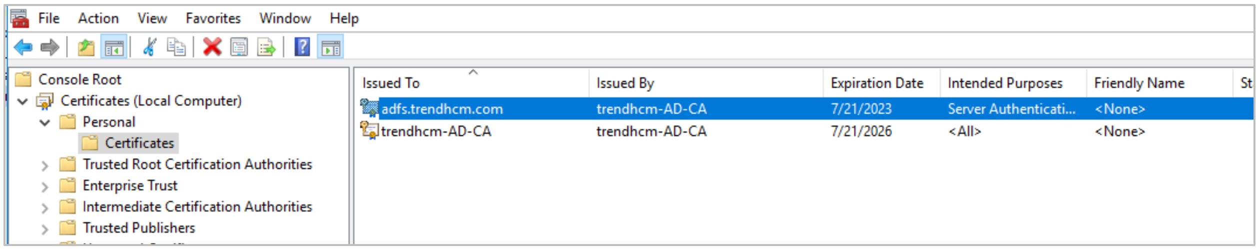
You can now see the certificate you requested and enrolled in the Personal store in the Certificates snap-in.



Certificate Installation Results

The following certificates have been enrolled and installed on this computer.

Active Directory Enrollment Policy		
☑ SSL Certificat template	✓ STATUS: Succeeded	Details


File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers

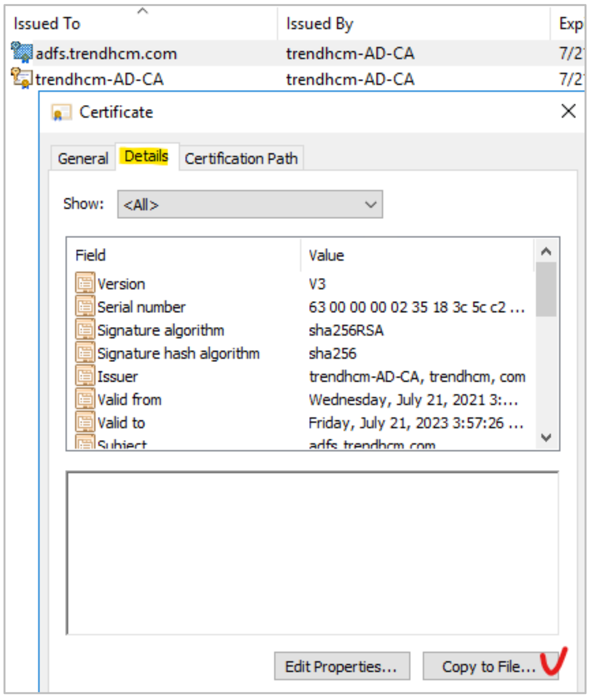
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	St
adfs.trendhcm.com	trendhcm-AD-CA	7/21/2023	Server Authenticati...	<None>	
trendhcm-AD-CA	trendhcm-AD-CA	7/21/2026	<All>	<None>	

Export the SSL certificate to a .PFX file

In the Certificates snap-in for the Local Machine, click the Personal store.

Double-click the SSL certificate you used for your federation service.

On the Details tab, click Copy to file and then click Next in the wizard.



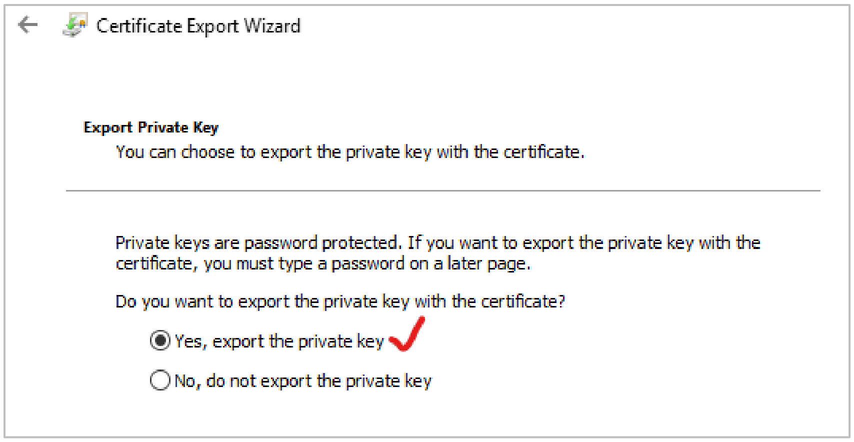
Issued To	Issued By	Exp
adfs.trendhcm.com	trendhcm-AD-CA	7/2
trendhcm-AD-CA	trendhcm-AD-CA	7/2

Show: <All>

Field	Value
Version	V3
Serial number	63 00 00 00 02 35 18 3c 5c c2 ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	trendhcm-AD-CA, trendhcm, com
Valid from	Wednesday, July 21, 2021 3:...
Valid to	Friday, July 21, 2023 3:57:26 ...
Subject	adfs.trendhcm.com

Ensure .pfx is selected, Include all certificates in the certification path if possible and Export all extended properties are checked and then click Next.

Select Password, enter a password, and then click Next.



Certificate Export Wizard

Export Private Key

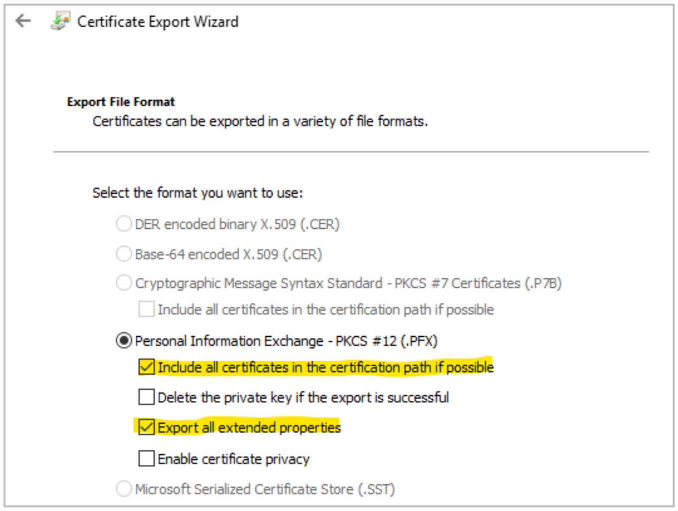
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key ✓

○ No, do not export the private key



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

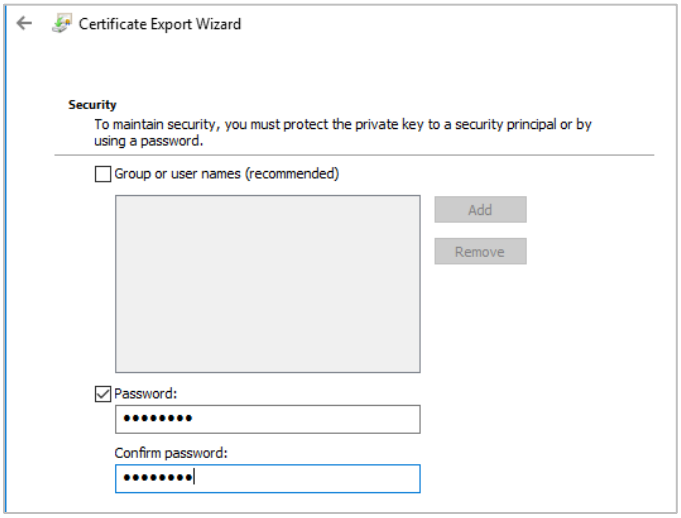
☑ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

☑ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)



Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

□ Group or user names (recommended)

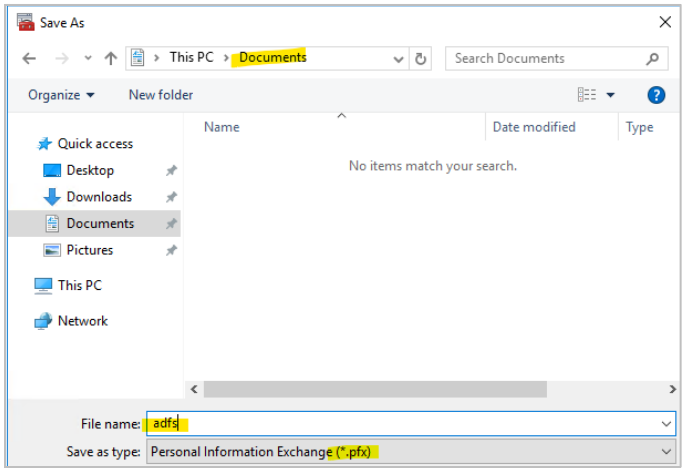
☑ Password:

••••••••

Confirm password:

••••••••

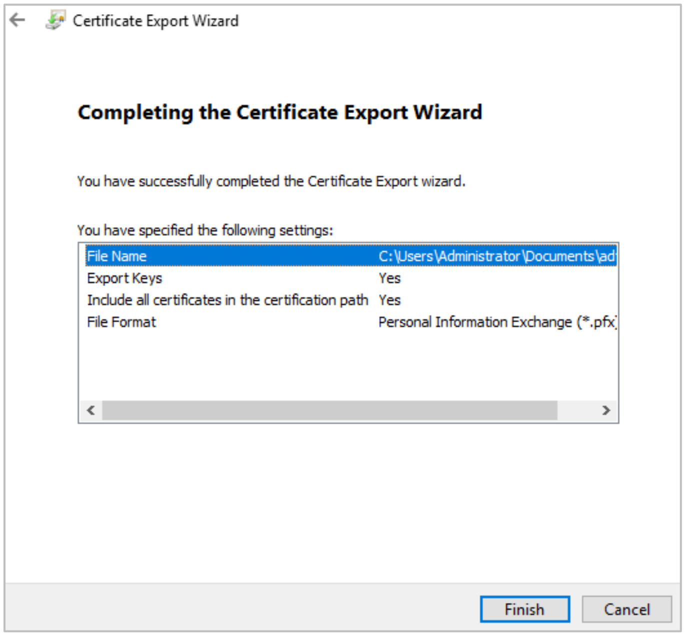
Select a file location and name, click Next, and then click Finish.



No items match your search.

File name: adfs

Save as type: Personal Information Exchange (*.pfx)



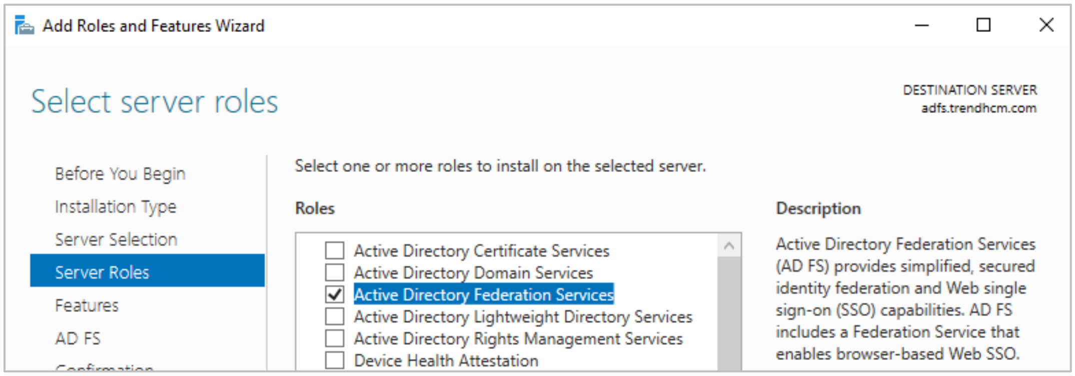
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\Administrator\Documents\ad
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Personal Information Exchange (*.pfx

Cài đặt một máy chủ ADFS (Tại DMZ) và cấu hình ADFS



Select server roles

DESTINATION SERVER
adfs.trendhcm.com

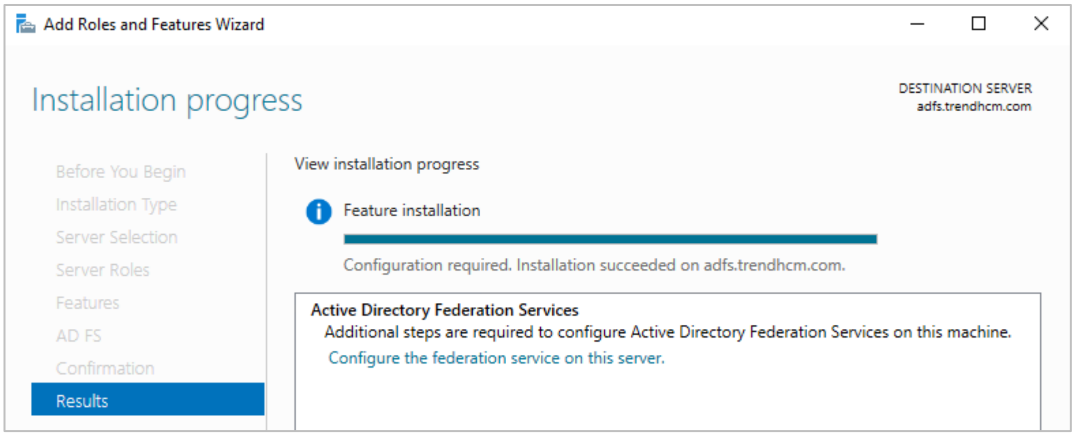
Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☑ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation

Description

Active Directory Federation Services (AD FS) provides simplified, secured identity federation and Web single sign-on (SSO) capabilities. AD FS includes a Federation Service that enables browser-based Web SSO.



Installation progress

DESTINATION SERVER
adfs.trendhcm.com

View installation progress

Feature installation

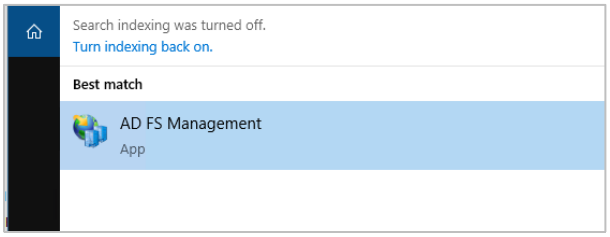
Configuration required. Installation succeeded on adfs.trendhcm.com.

Active Directory Federation Services

Additional steps are required to configure Active Directory Federation Services on this machine.

Configure the federation service on this server.

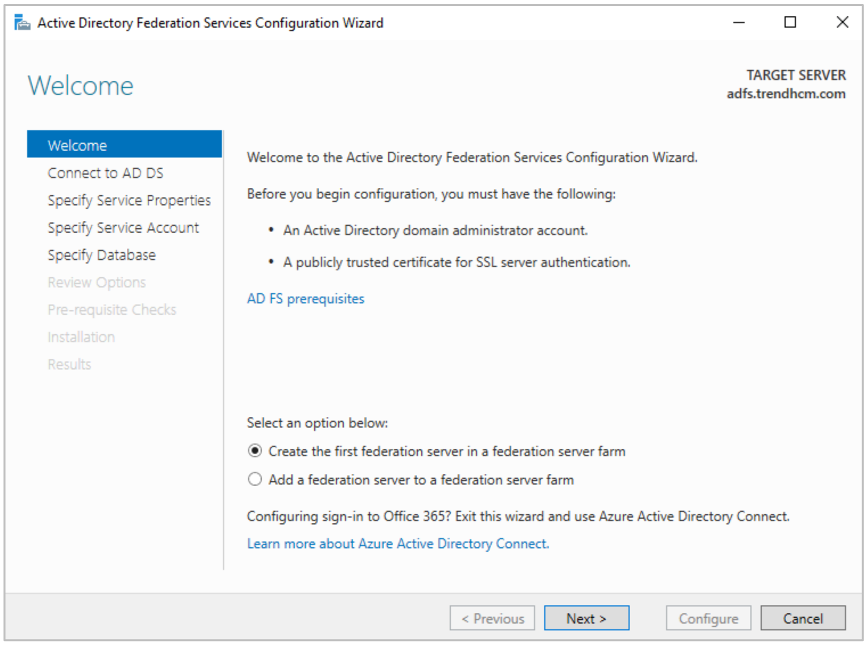
Open ADFS management



Search indexing was turned off.
Turn indexing back on.

Best match

AD FS Management
App



Welcome

TARGET SERVER
adfs.trendhcm.com

Welcome to the Active Directory Federation Services Configuration Wizard.

Before you begin configuration, you must have the following:

- An Active Directory domain administrator account.
- A publicly trusted certificate for SSL server authentication.

AD FS prerequisites

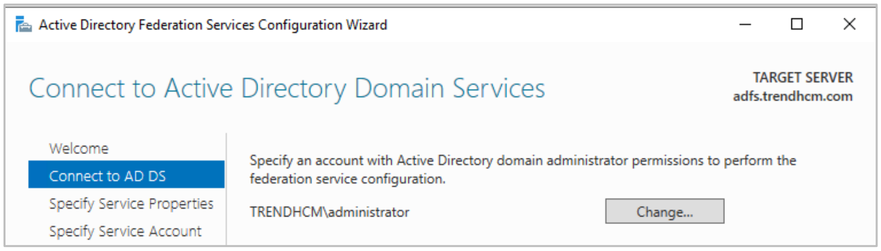
Select an option below:

● Create the first federation server in a federation server farm

○ Add a federation server to a federation server farm

Configuring sign-in to Office 365? Exit this wizard and use Azure Active Directory Connect.

Learn more about Azure Active Directory Connect.

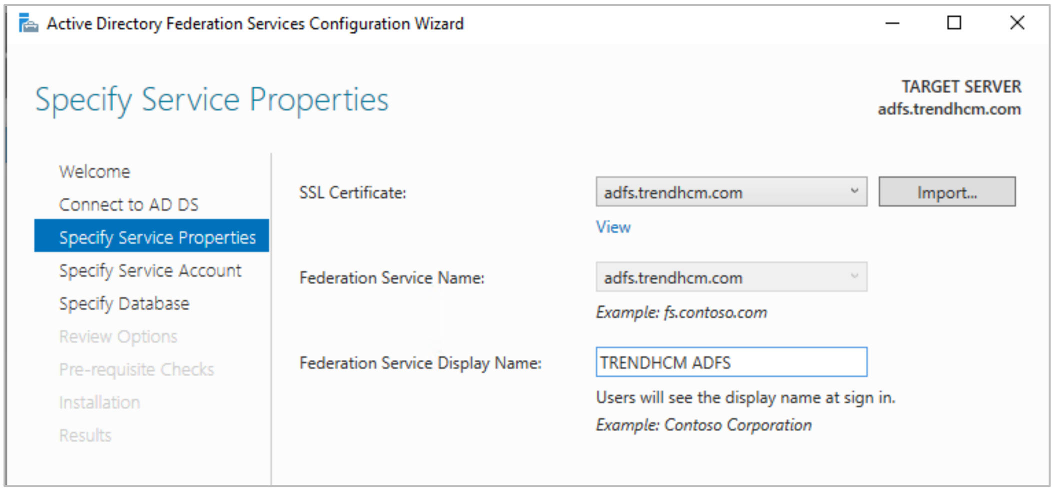

Active Directory Federation Services Configuration Wizard
Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Change...

Connect to Active Directory Domain Services

TARGET SERVER
adfs.trendhcm.com

Specify an account with Active Directory domain administrator permissions to perform the federation service configuration.

TRENDHCM\administrator



Active Directory Federation Services Configuration Wizard

Specify Service Properties

TARGET SERVER
adfs.trendhcm.com

SSL Certificate: adfs.trendhcm.com

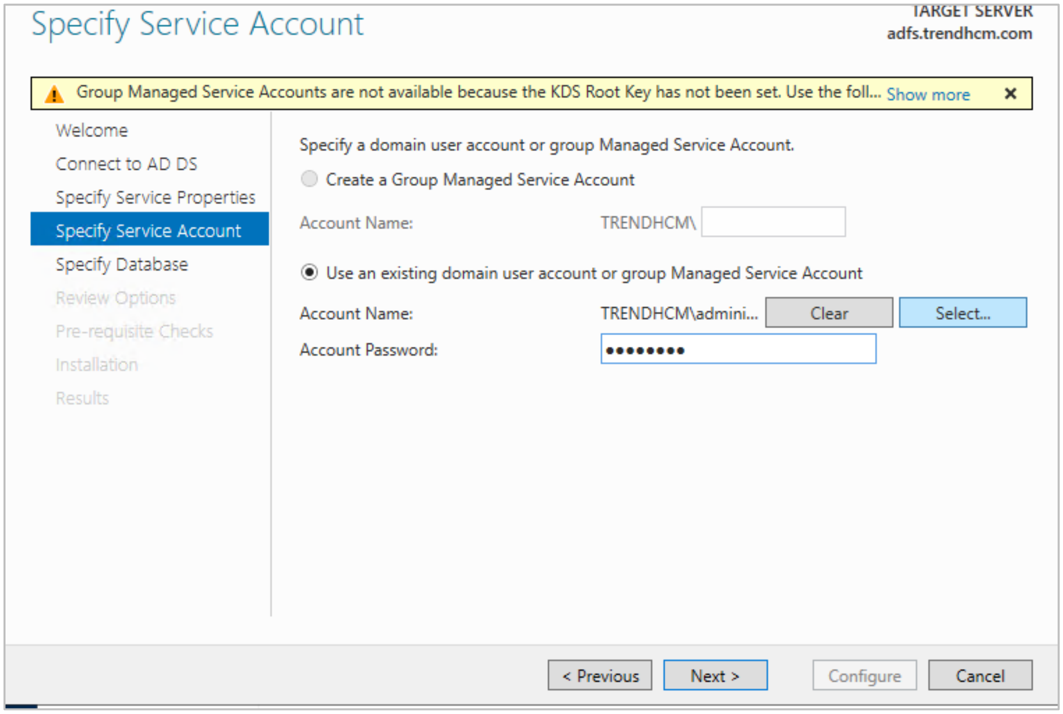
Federation Service Name: adfs.trendhcm.com

Example: fs.contoso.com

Federation Service Display Name: TRENDHCM ADFS

Users will see the display name at sign in.

Example: Contoso Corporation



Specify Service Account

TARGET SERVER
adfs.trendhcm.com

⚠ Group Managed Service Accounts are not available because the KDS Root Key has not been set. Use the foll... Show more ✕

Specify a domain user account or group Managed Service Account.

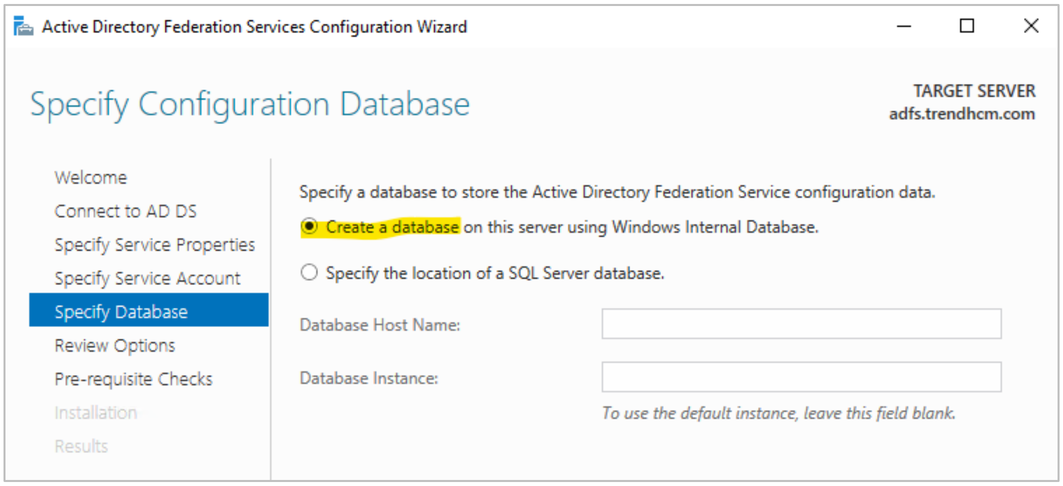
○ Create a Group Managed Service Account

Account Name: TRENDHCM\

● Use an existing domain user account or group Managed Service Account

Account Name: TRENDHCM\admini...

Account Password: ●●●●●●●●●



Active Directory Federation Services Configuration Wizard

Specify Configuration Database

TARGET SERVER
adfs.trendhcm.com

Specify a database to store the Active Directory Federation Service configuration data.

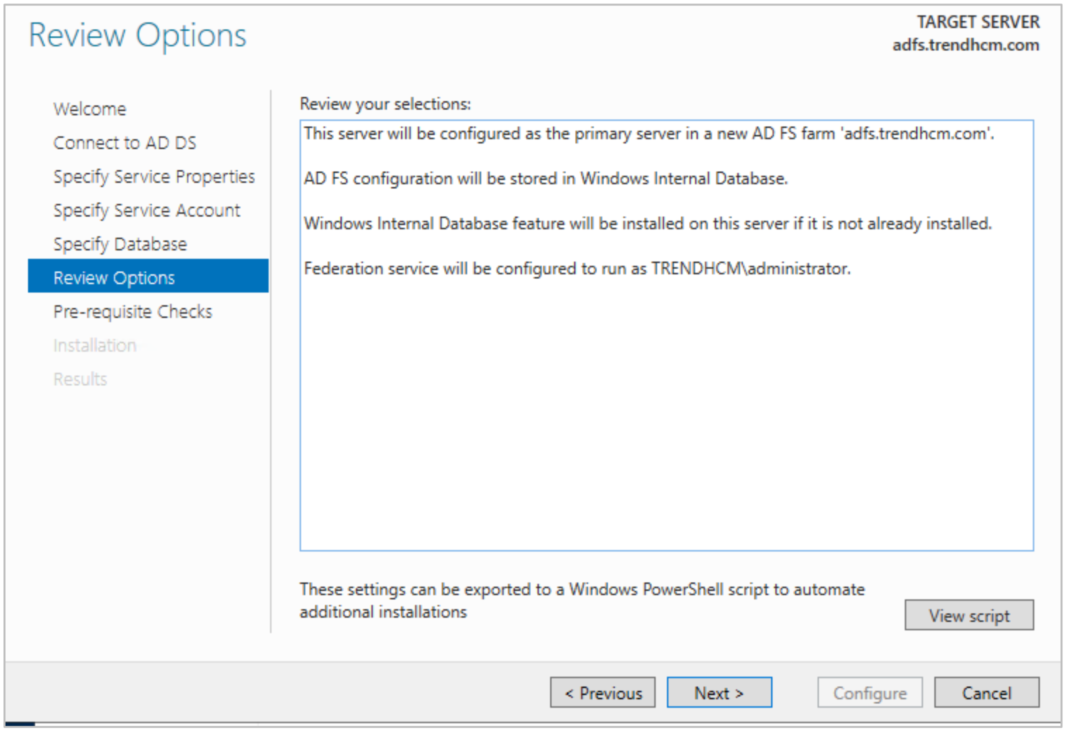
● Create a database on this server using Windows Internal Database.

○ Specify the location of a SQL Server database.

Database Host Name:

Database Instance:

To use the default instance, leave this field blank.



Review Options

TARGET SERVER
adfs.trendhcm.com

Review your selections:

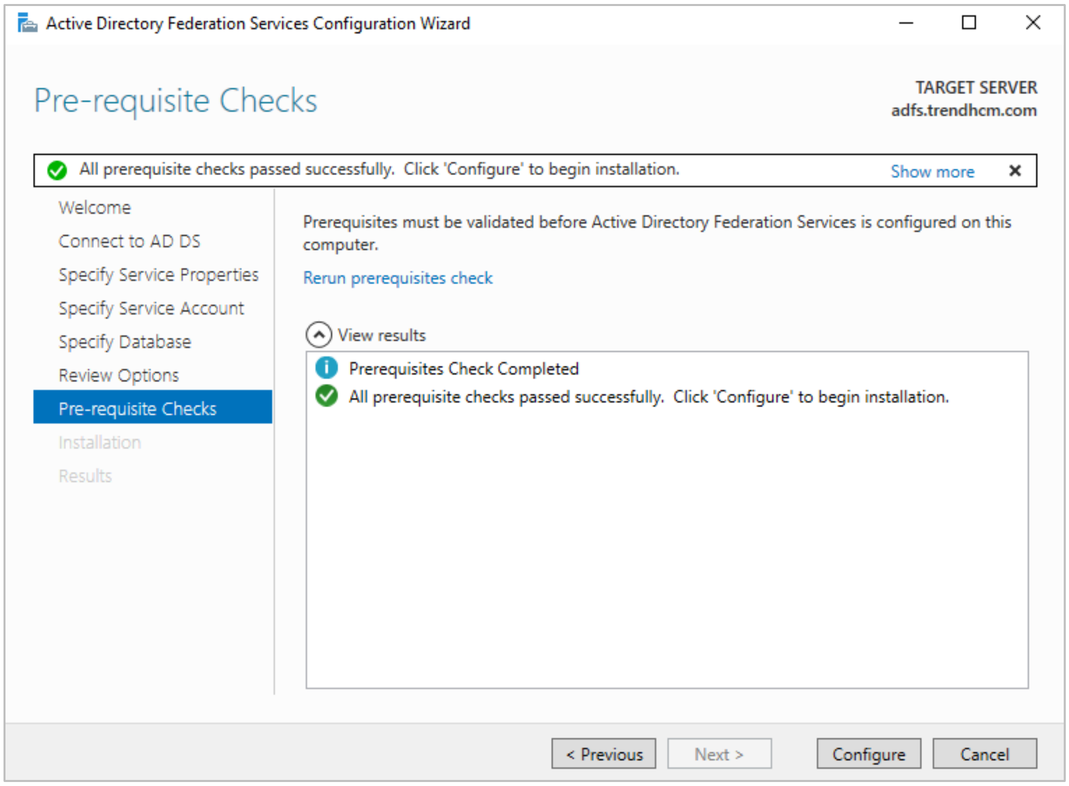
This server will be configured as the primary server in a new AD FS farm 'adfs.trendhcm.com'.

AD FS configuration will be stored in Windows Internal Database.

Windows Internal Database feature will be installed on this server if it is not already installed.

Federation service will be configured to run as TRENDHCM\administrator.

These settings can be exported to a Windows PowerShell script to automate additional installations

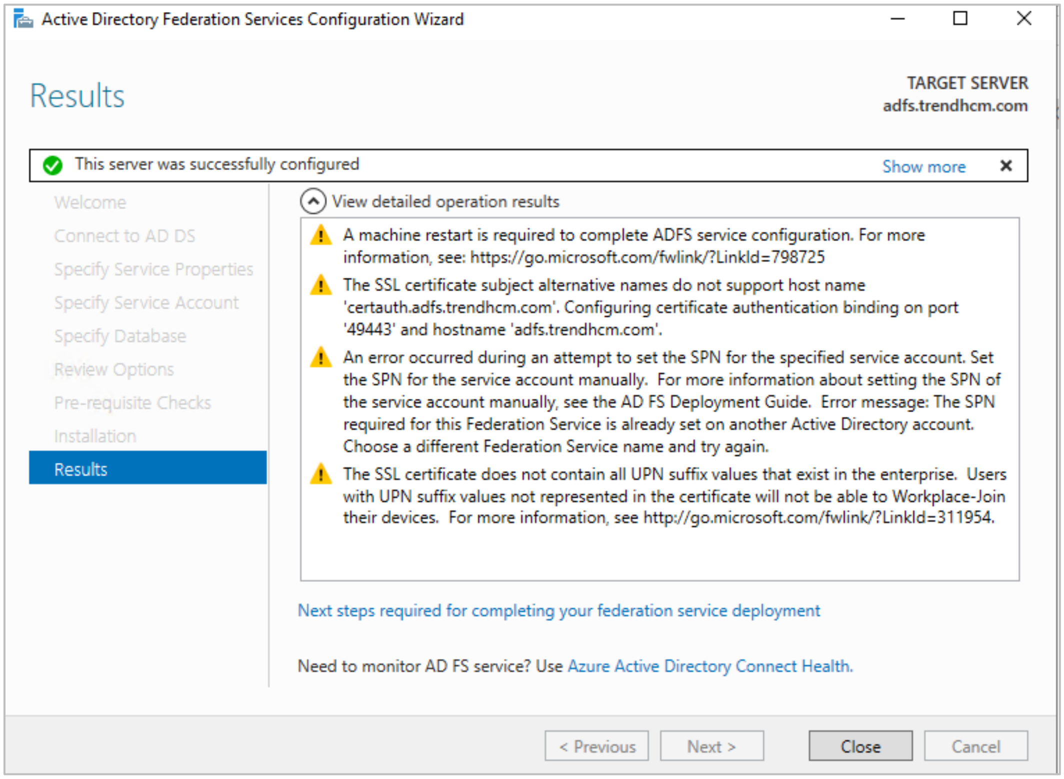


All prerequisite checks passed successfully. Click 'Configure' to begin installation.

Prerequisites must be validated before Active Directory Federation Services is configured on this computer.

Prerequisites Check Completed

All prerequisite checks passed successfully. Click 'Configure' to begin installation.



This server was successfully configured

A machine restart is required to complete ADFS service configuration. For more information, see: https://go.microsoft.com/fwlink/?LinkId=798725

The SSL certificate subject alternative names do not support host name 'certauth.adfs.trendhcm.com'. Configuring certificate authentication binding on port '49443' and hostname 'adfs.trendhcm.com'.

An error occurred during an attempt to set the SPN for the specified service account. Set the SPN for the service account manually. For more information about setting the SPN of the service account manually, see the AD FS Deployment Guide. Error message: The SPN required for this Federation Service is already set on another Active Directory account. Choose a different Federation Service name and try again.

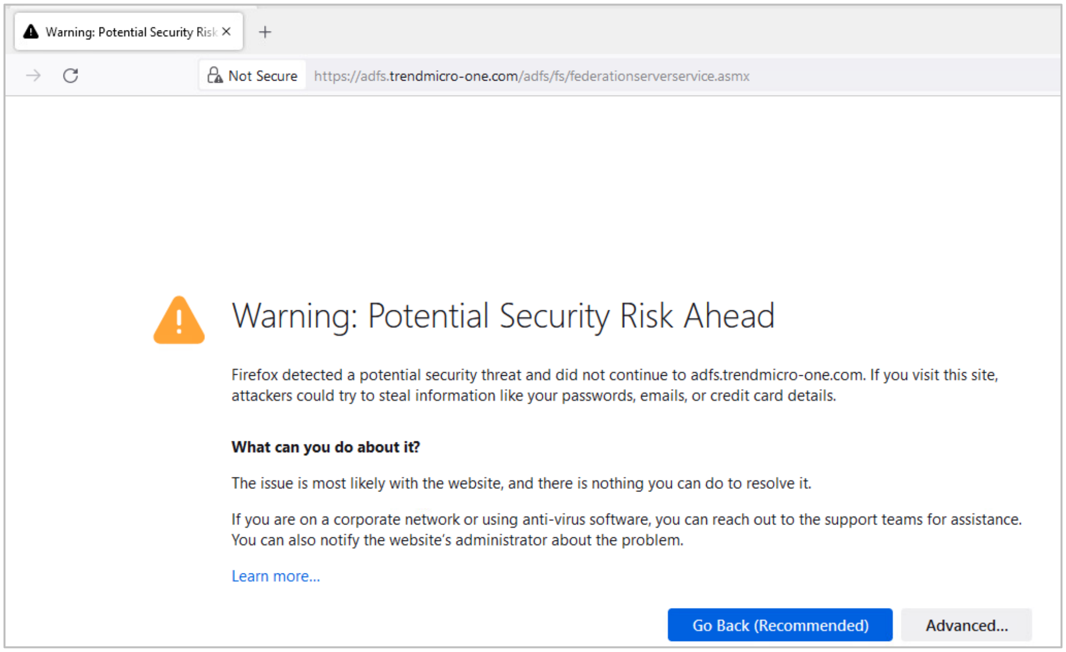
The SSL certificate does not contain all UPN suffix values that exist in the enterprise. Users with UPN suffix values not represented in the certificate will not be able to Workplace-Join their devices. For more information, see http://go.microsoft.com/fwlink/?LinkId=311954.

Need to monitor AD FS service? Use Azure Active Directory Connect Health.

Completed install ADFS

Test

https://adfs.trendmicro-one.com/adfs/fs/federationserverservice.asmx


Warning: Potential Security Risk
Not Secure
https://adfs.trendmicro-one.com/adfs/fs/federationserverservice.asmx

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to adfs.trendmicro-one.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

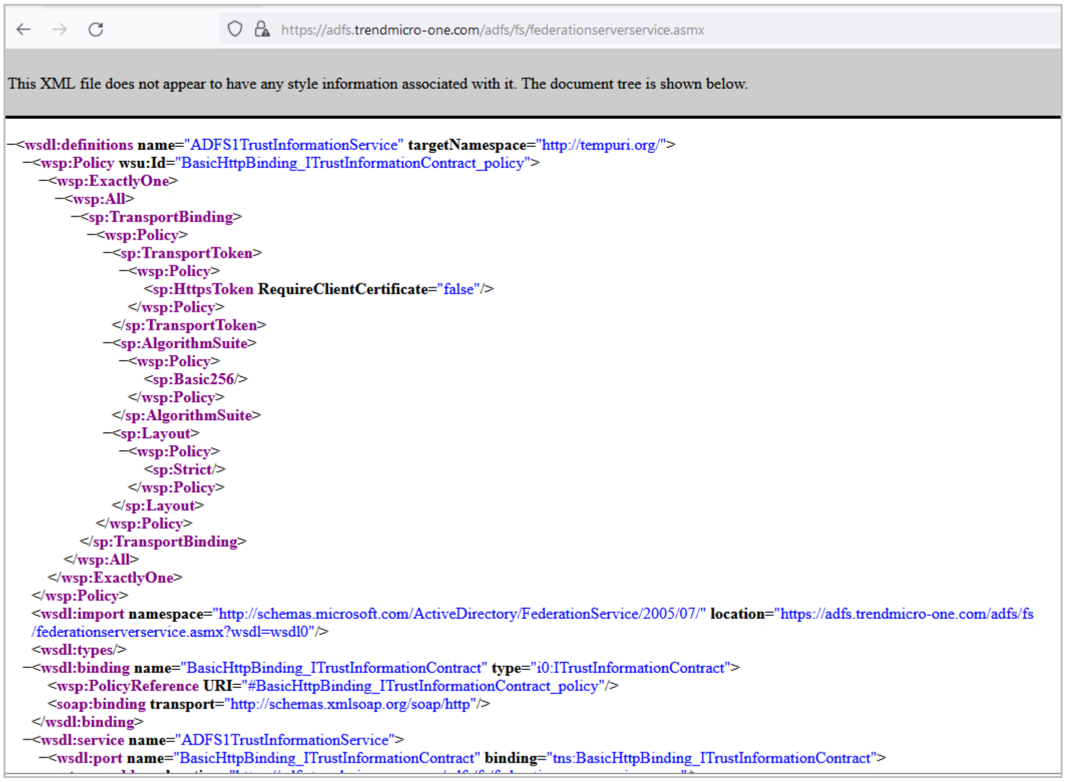
What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more...

Go Back (Recommended)
Advanced...



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
−<wsdl:definitions name="ADFS1TrustInformationService" targetNamespace="http://tempuri.org/">
  −<wsp:Policy wsu:Id="BasicHttpBinding_ITrustInformationContract_policy">
    −<wsp:ExactlyOne>
      −<wsp:All>
        −<sp:TransportBinding>
          −<wsp:Policy>
            −<sp:TransportToken>
              −<wsp:Policy>
                  <sp:HttpsToken RequireClientCertificate="false"/>
                </wsp:Policy>
              </sp:TransportToken>
            −<sp:AlgorithmSuite>
              −<wsp:Policy>
                  <sp:Basic256/>
                </wsp:Policy>
              </sp:AlgorithmSuite>
            −<sp:Layout>
              −<wsp:Policy>
                  <sp:Strict/>
                </wsp:Policy>
              </sp:Layout>
            </wsp:Policy>
          </sp:TransportBinding>
        </wsp:All>
      </wsp:ExactlyOne>
    </wsp:Policy>
    <wsdl:import namespace="http://schemas.microsoft.com/ActiveDirectory/FederationService/2005/07/" location="https://adfs.trendmicro-one.com/adfs/fs
    /federationserverservice.asmx?wsdl=wsdl0"/>
    <wsdl:types/>
  −<wsdl:binding name="BasicHttpBinding_ITrustInformationContract" type="i0:ITrustInformationContract">
      <wsp:PolicyReference URI="#BasicHttpBinding_ITrustInformationContract_policy"/>
      <soap:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    </wsdl:binding>
  −<wsdl:service name="ADFS1TrustInformationService">
    −<wsdl:port name="BasicHttpBinding_ITrustInformationContract" binding="tns:BasicHttpBinding_ITrustInformationContract">
```