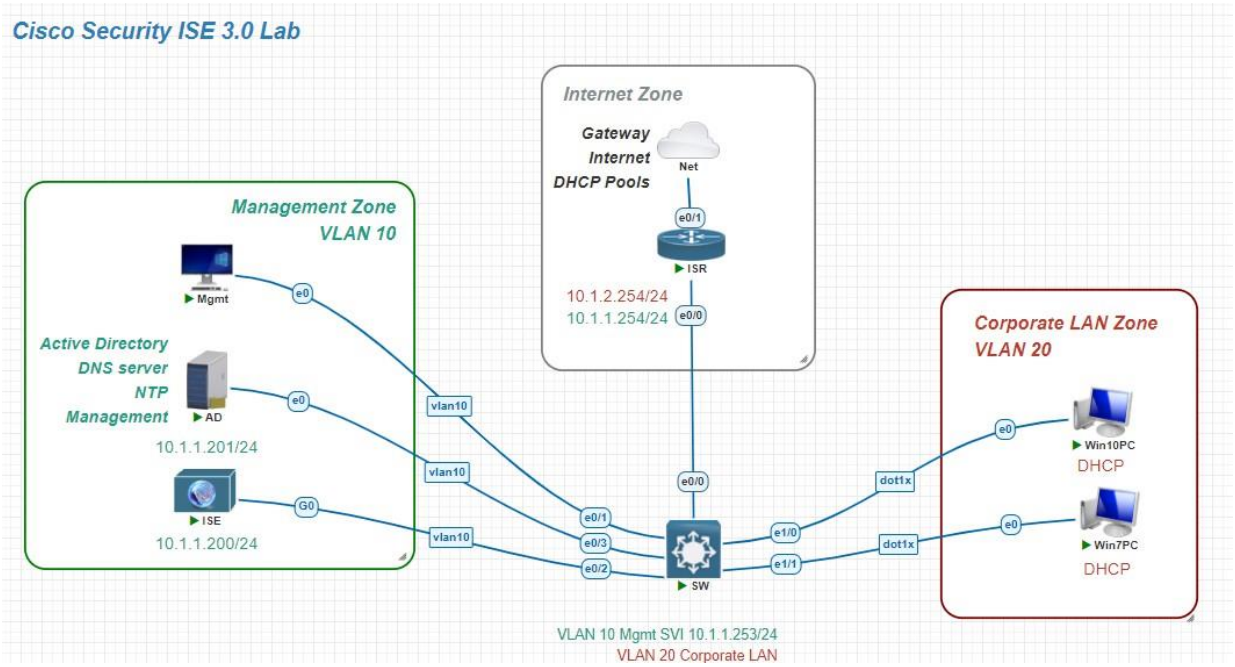
LAB : CÀI ĐẶT CA WINDOWS SERVER

I. Sơ đồ:



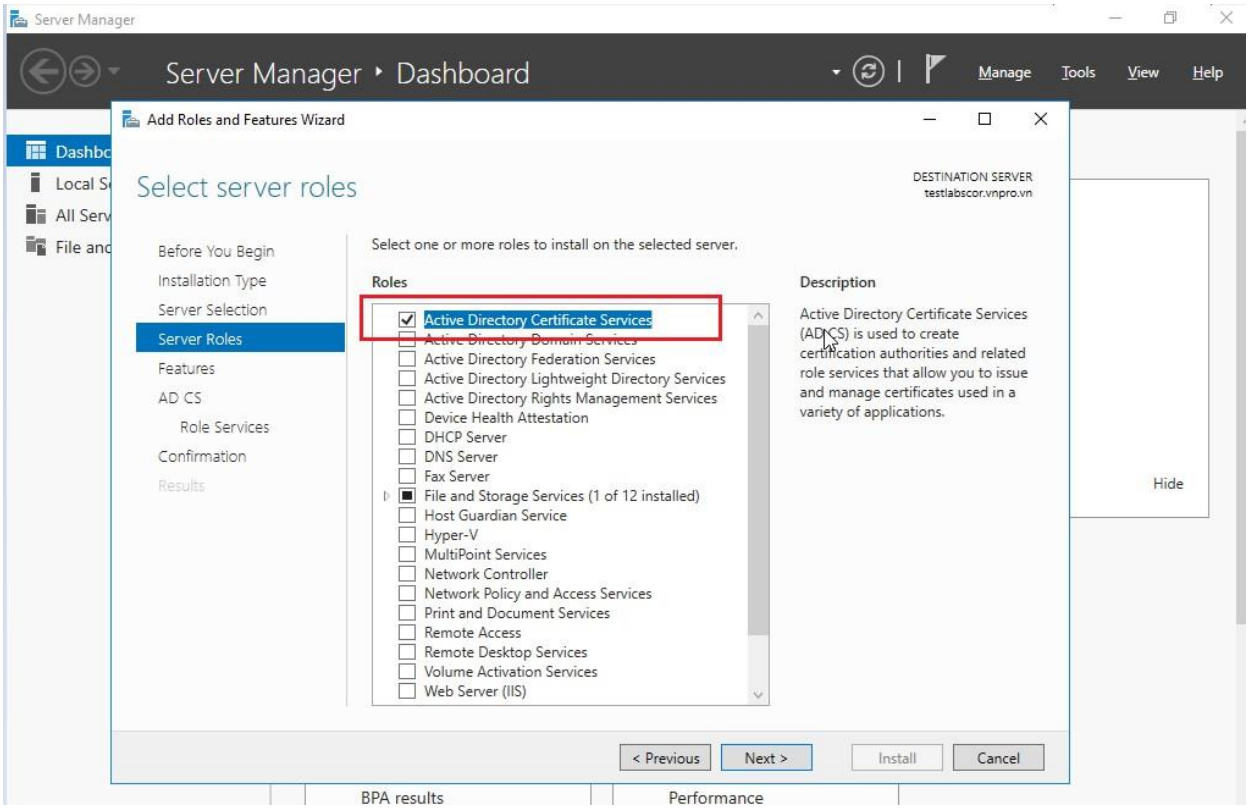
II. Mục đích thực hiện:

Ở bài trước ISE của bạn đã được tích hợp với Active Directory (AD), tiếp theo cung cấp chứng chỉ CA để tiến hành xác nhận kỹ càng về tổ chức yêu cầu chứng chỉ. Quá trình xác thực này hoàn toàn phụ thuộc vào loại chứng chỉ SSL. Thủ tục kiểm tra chứng chỉ số được cho là phần quan trọng nhất theo quan điểm an ninh mạng. Certificate Authority phải đảm bảo các chứng chỉ SSL chỉ được cấp cho các thực thể hợp pháp. Vì vậy, các cơ quan cấp chứng chỉ phải được thực thi tốt theo một quy trình xác thực nghiêm ngặt và chính xác để đảm bảo không cung cấp nhầm hoặc sai cho một tổ chức nào cả

III. Thực hiện:

1. Cài đặt Active Directory Certificate Service:

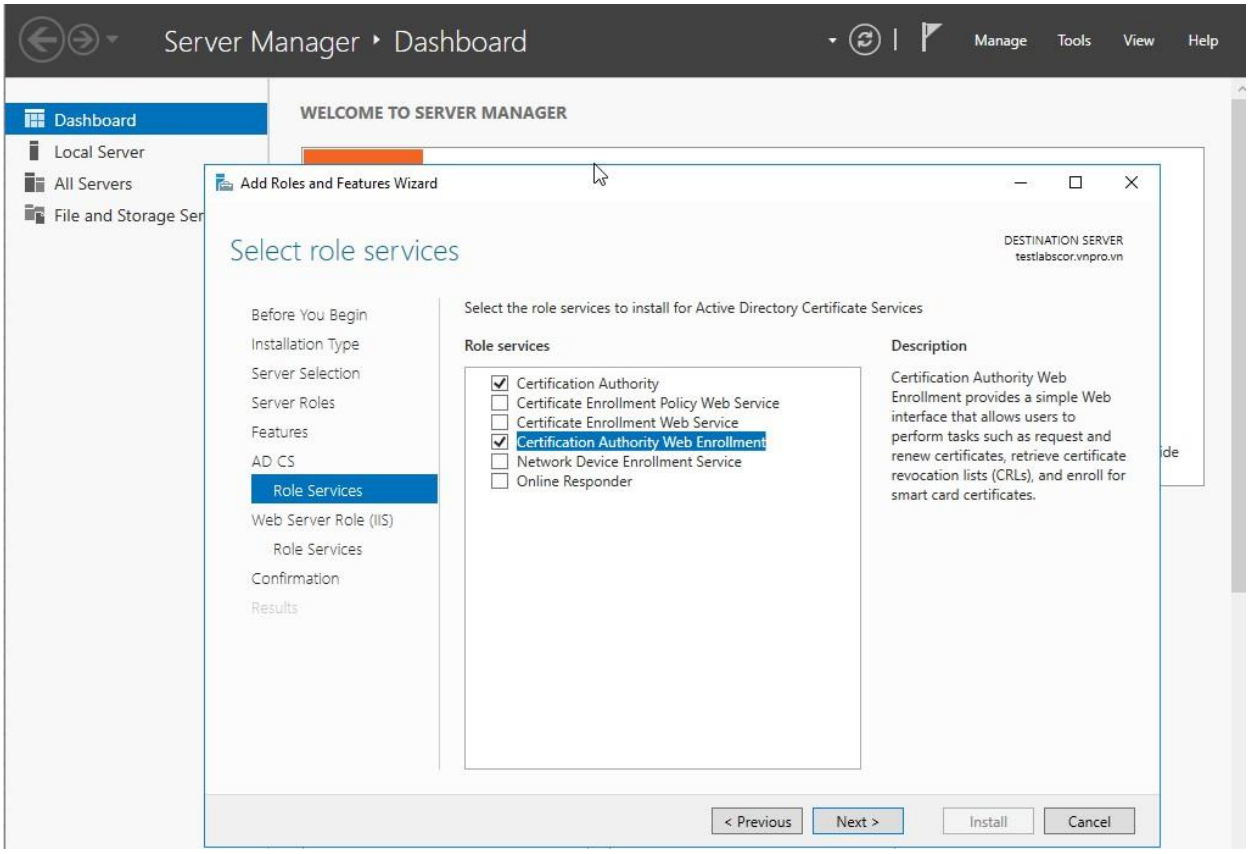
✓ Đầu tiên mở **Server Manager** trên CA. Sau đó chọn **Add Roles and Feature**



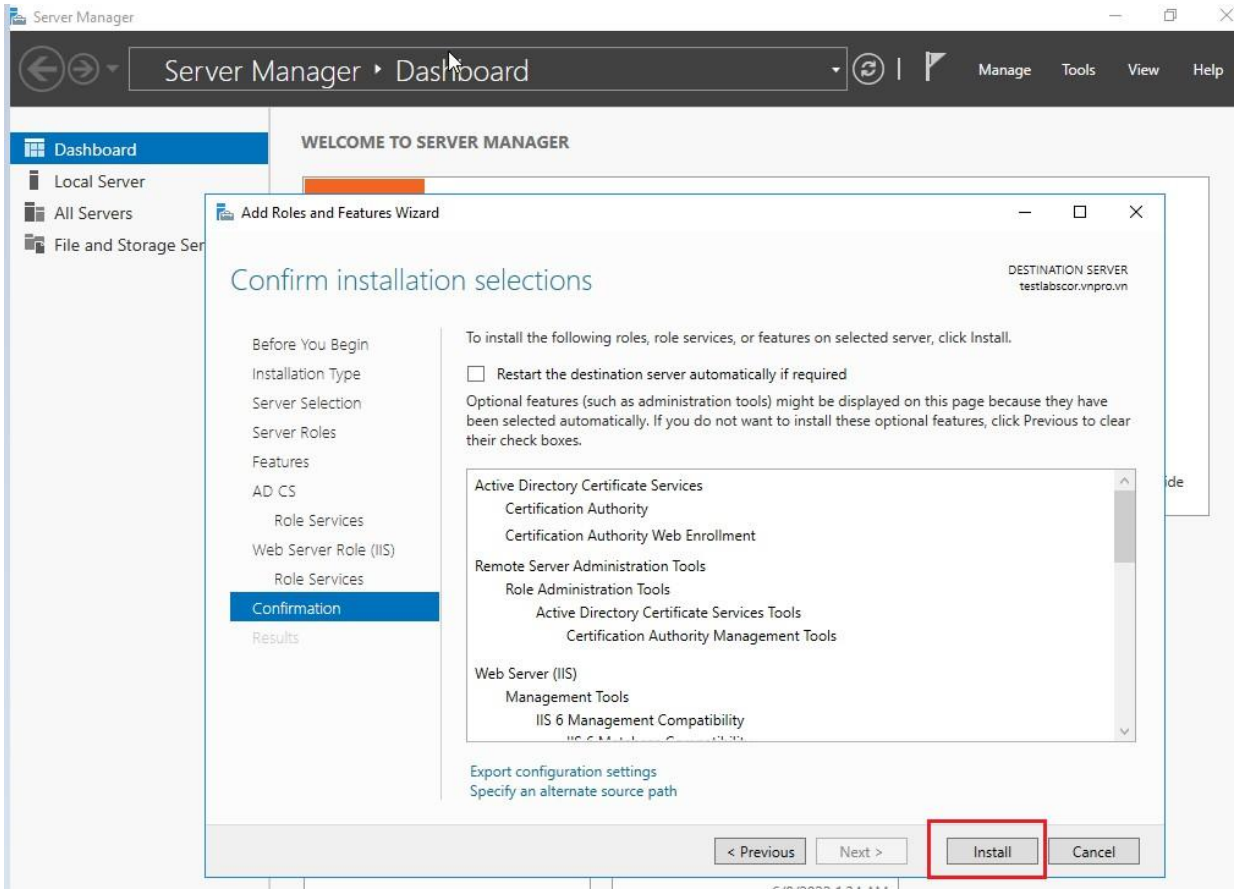
✓ Tiếp tục nhấn **Next** cho đến mục **AD CS - Role Service**

✓ Tích chọn **Certification Authority** và **Certification Authority Web Environment**

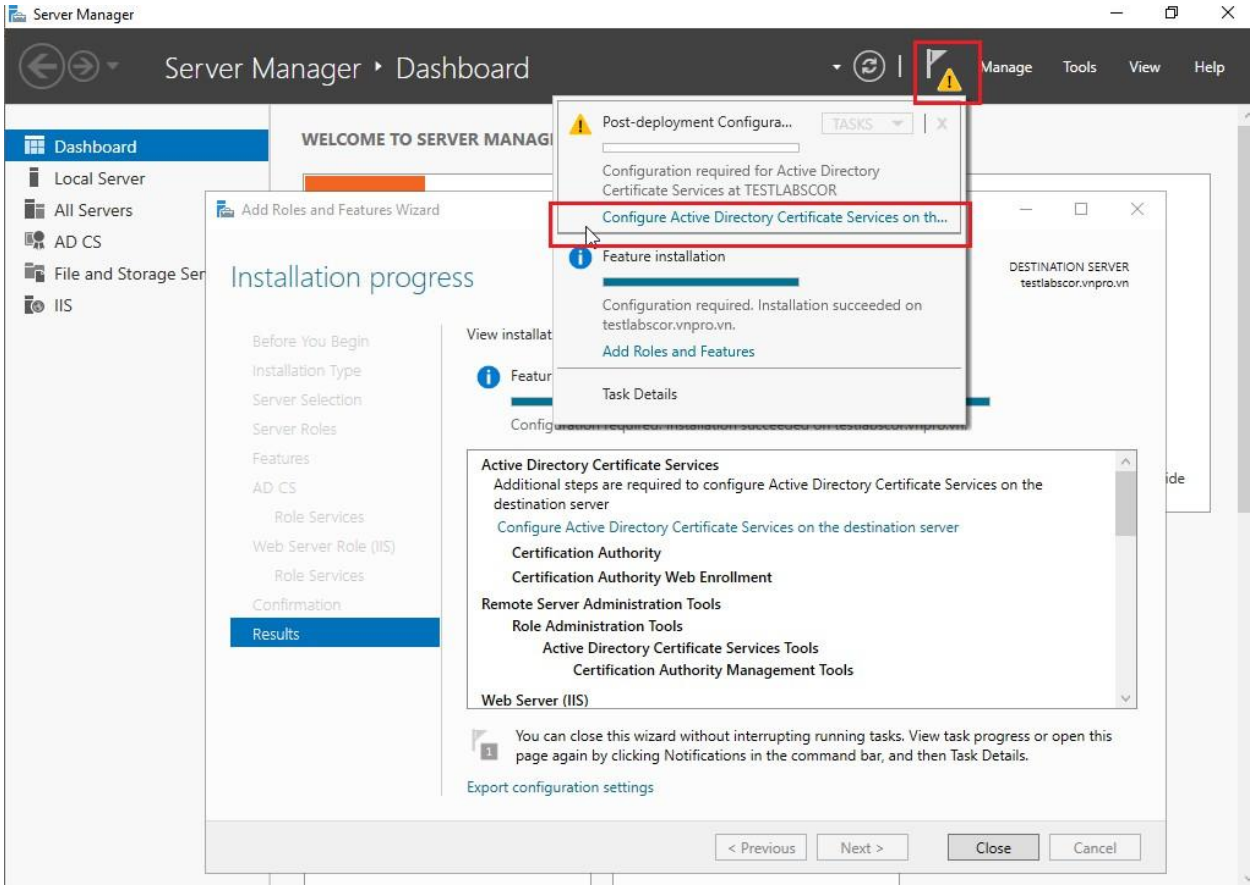
✓ Sau đó nhất **Next**



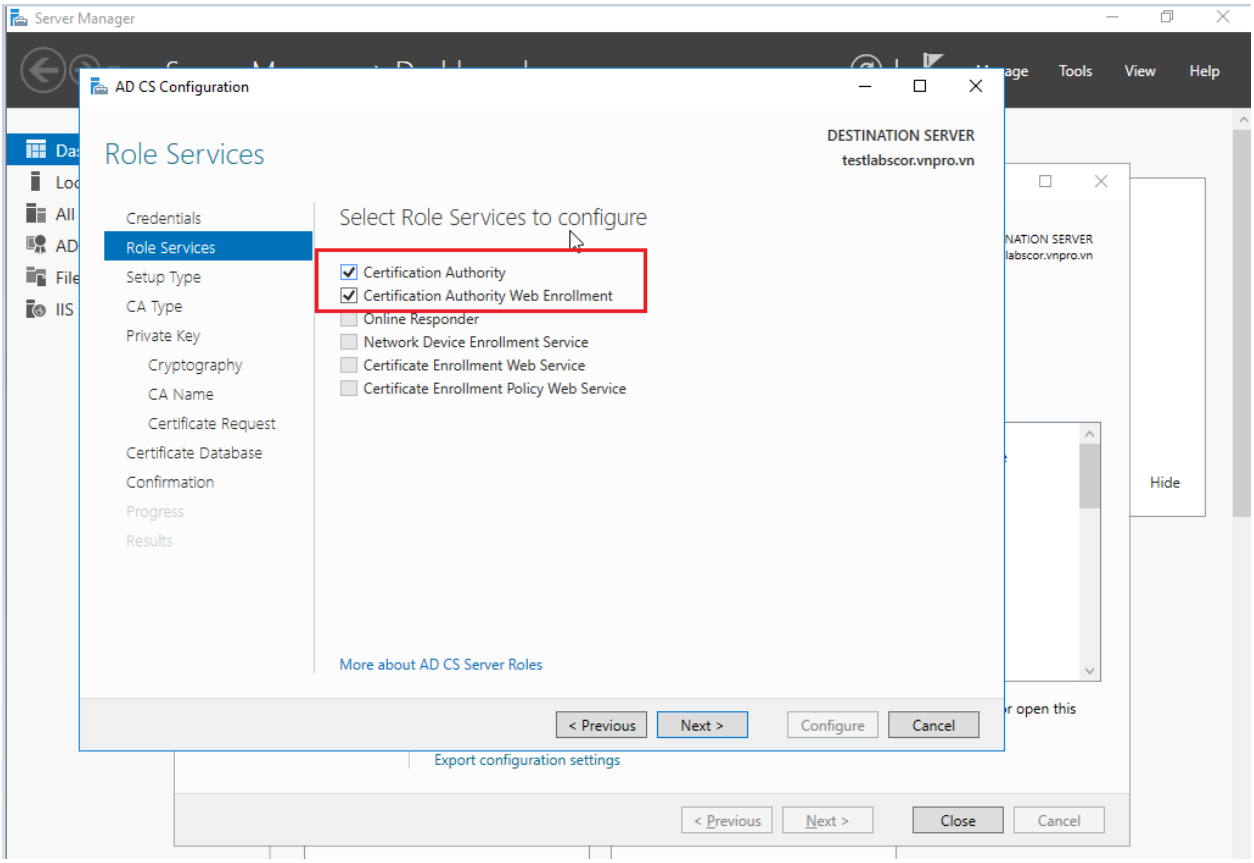
Nhấn **Install**



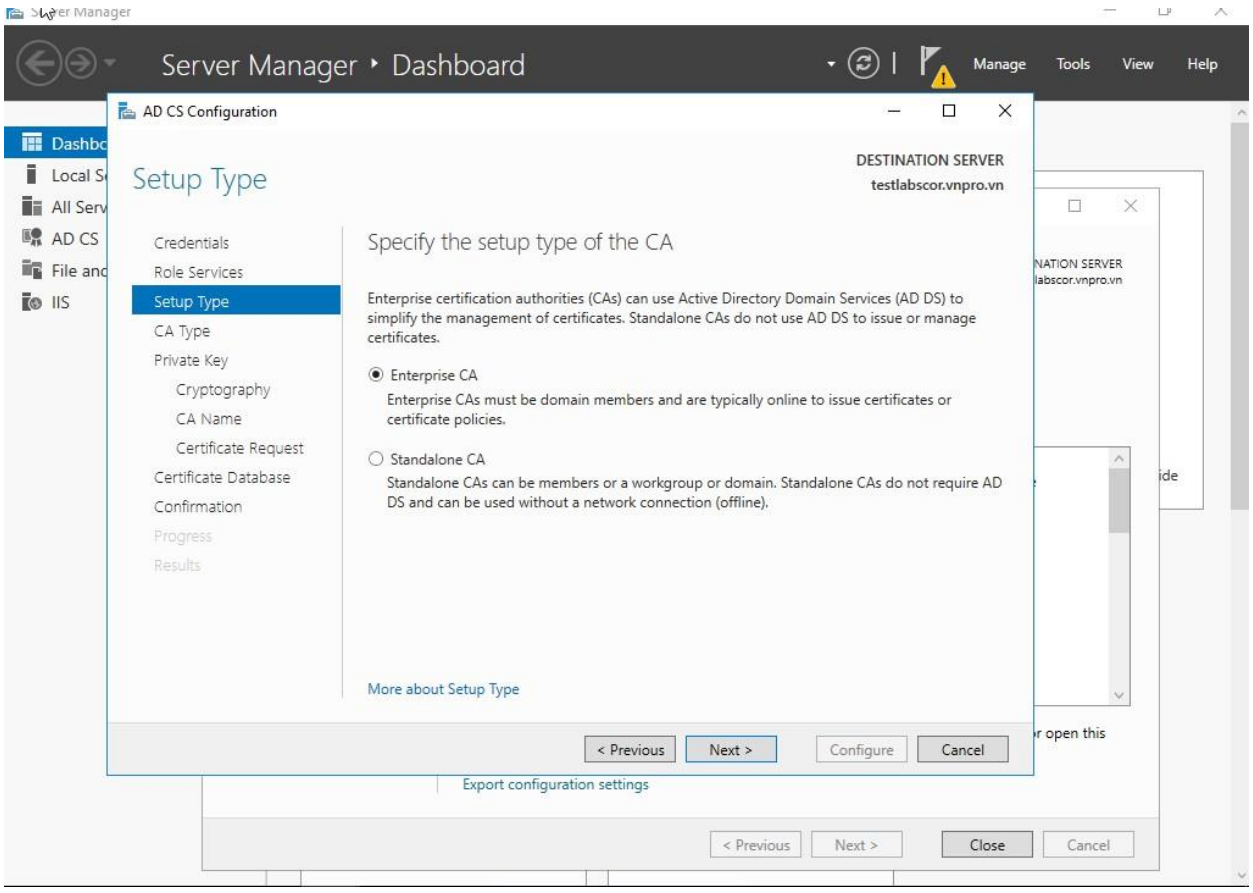
✓ Sau khi cài đặt thành công, chọn mục **Notification** > **Configure Active Directory Certificates on this server**



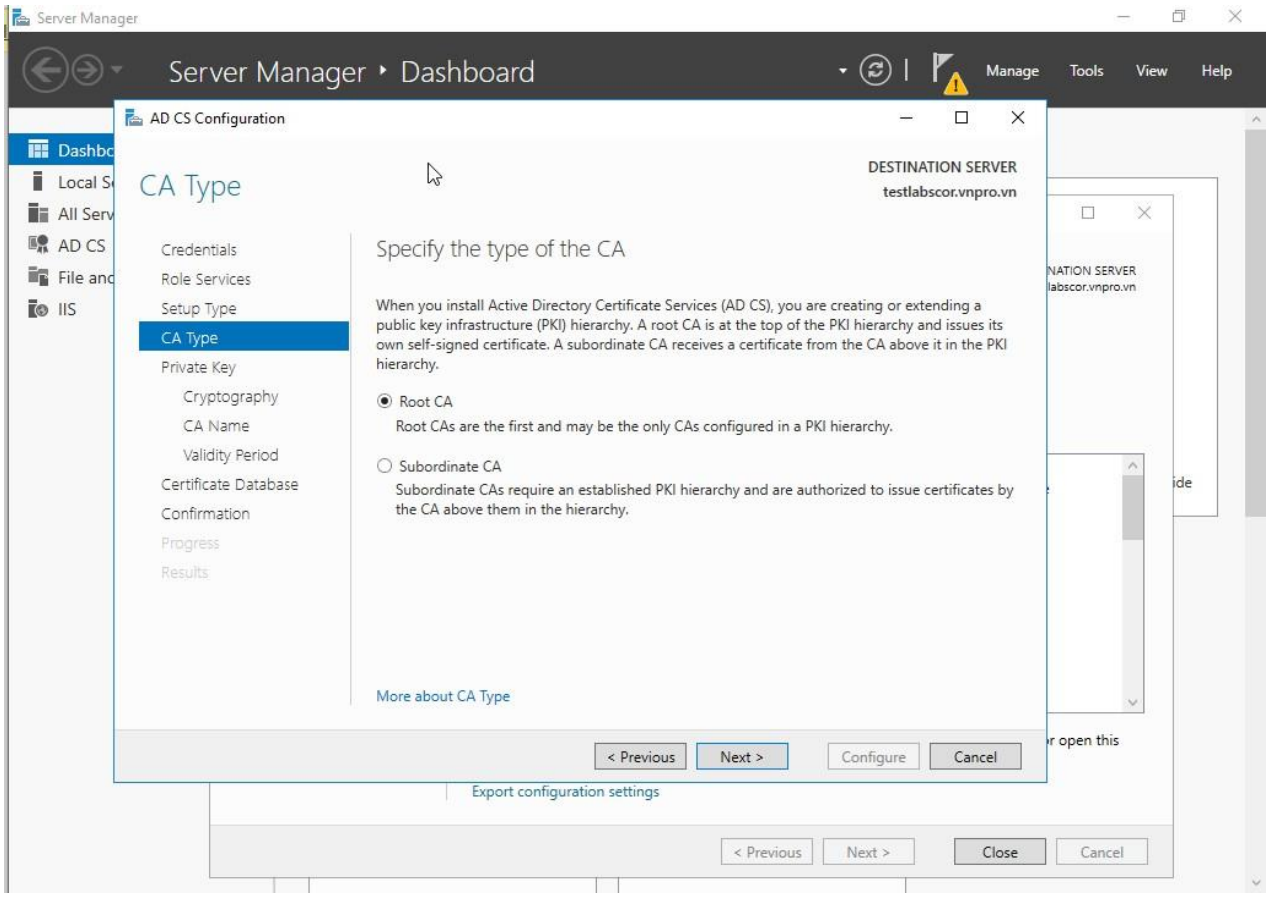
✓ Tích chọn như hình dưới và nhấn **Next**



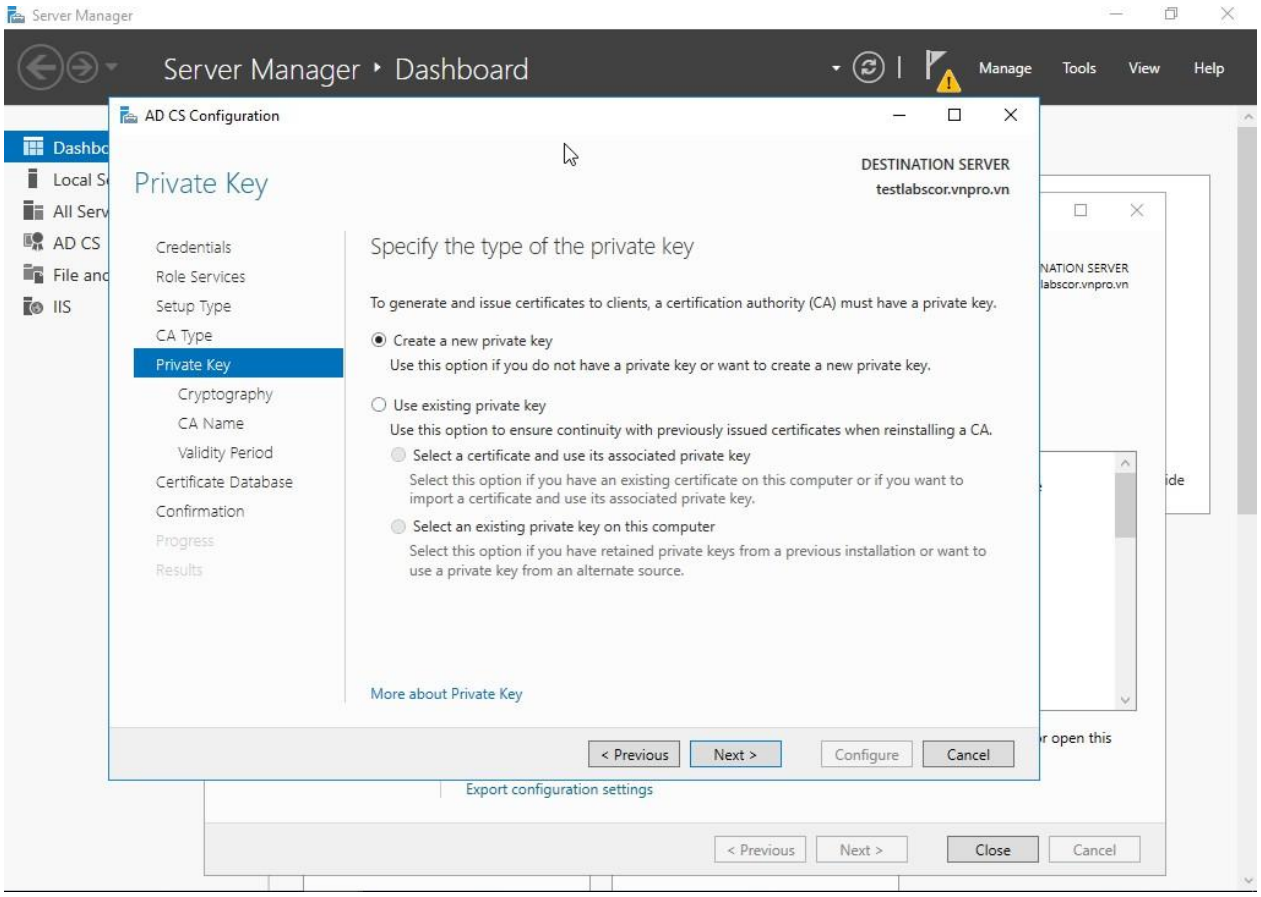
✓ Chọn **Enterprise CA** và nhấn **Next**



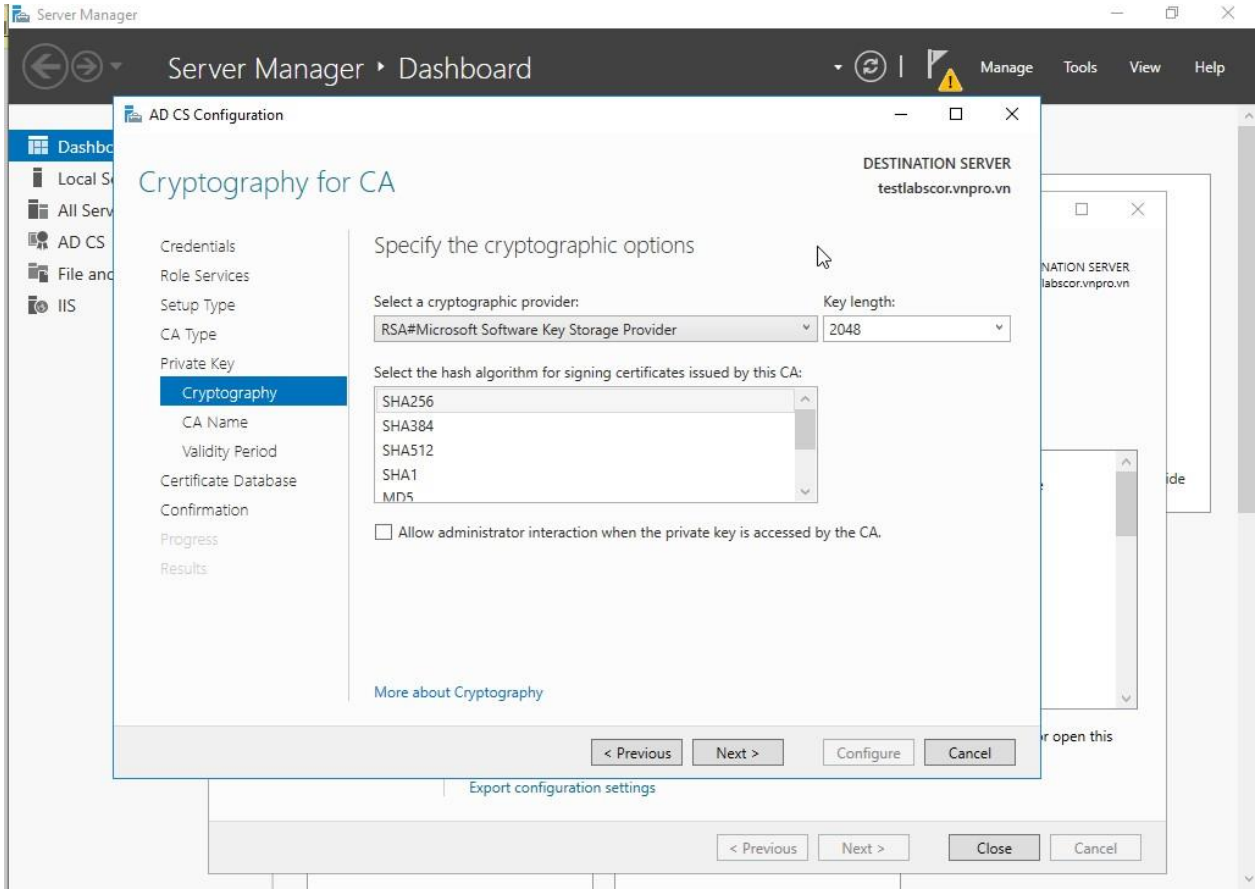
✓ Chọn **Root CA** và nhấn **Next**



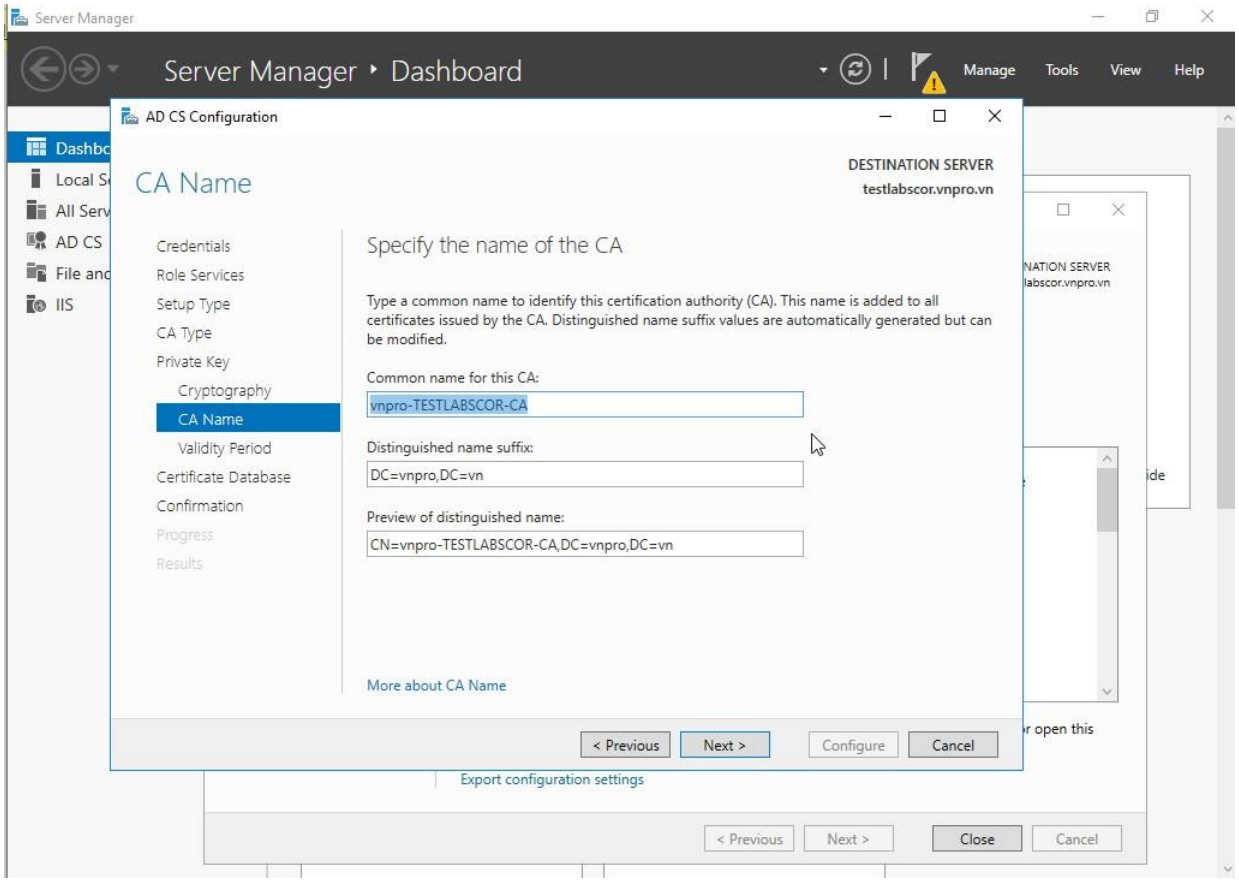
✓ Chọn **Create a new private key** và nhấn **Next**



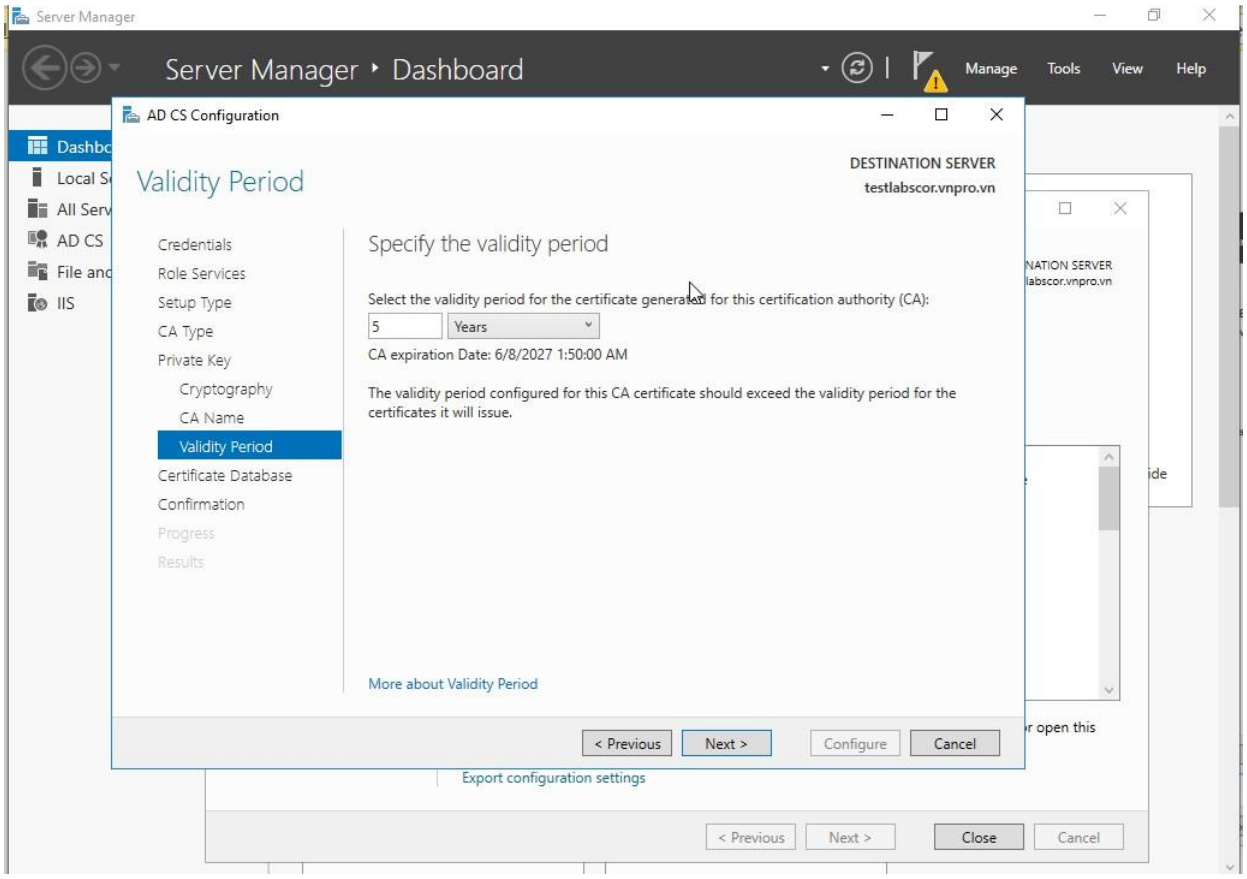
✓ Chọn **cryptographic provider**, **key length**, thuật toán **hash** hoặc có thể để mặc định và nhấn **Next**


Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
AD CS Configuration
Cryptography for CA
DESTINATION SERVER
testlabscor.vnpro.vn
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
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.
More about Cryptography
< Previous
Next >
Configure
Cancel
Export configuration settings
Close

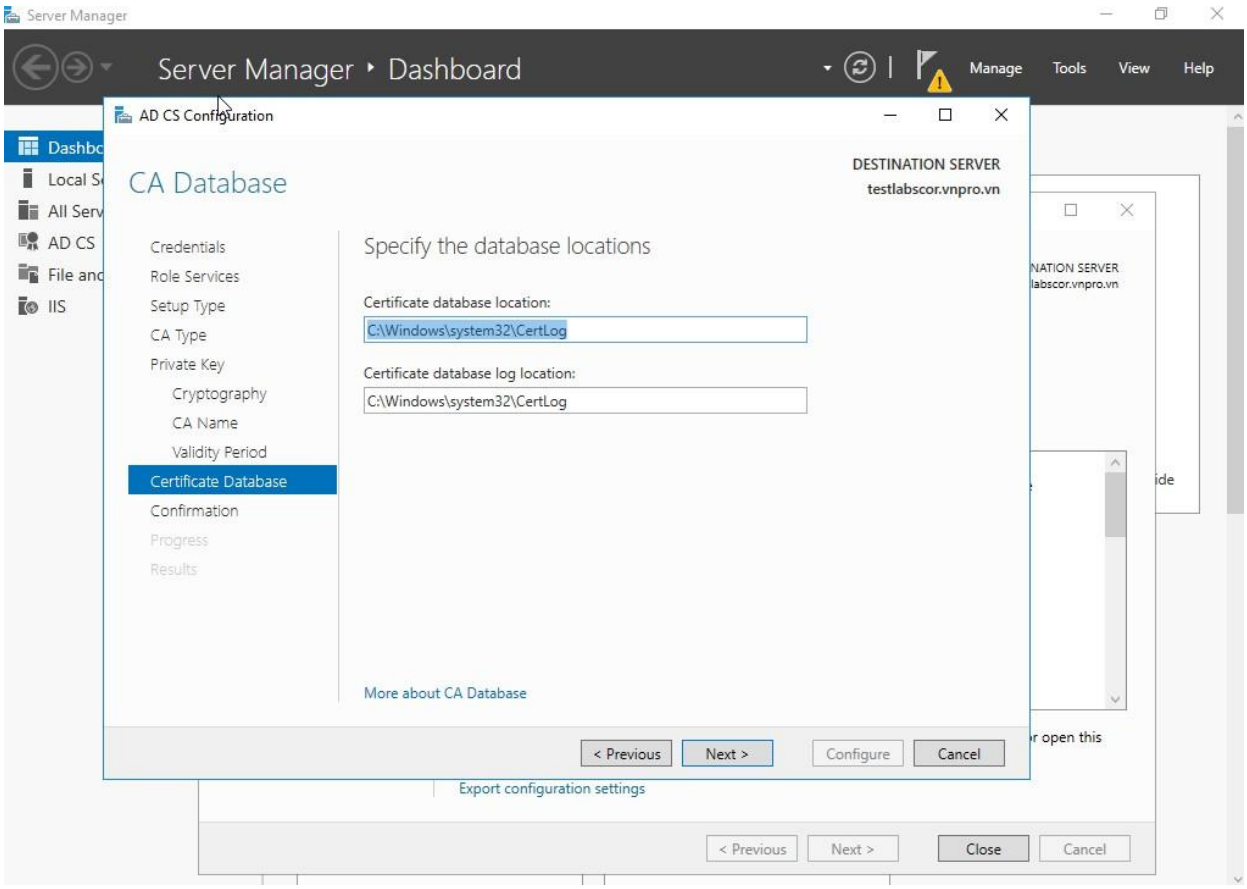
✓ Nhấn **Next**


Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
AD CS Configuration
CA Name
DESTINATION SERVER
testlabscor.vnpro.vn
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
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:
vnpro-TESTLABSCOR-CA
Distinguished name suffix:
DC=vnpro,DC=vn
Preview of distinguished name:
CN=vnpro-TESTLABSCOR-CA,DC=vnpro,DC=vn
More about CA Name
< Previous
Next >
Configure
Cancel
Export configuration settings
Close

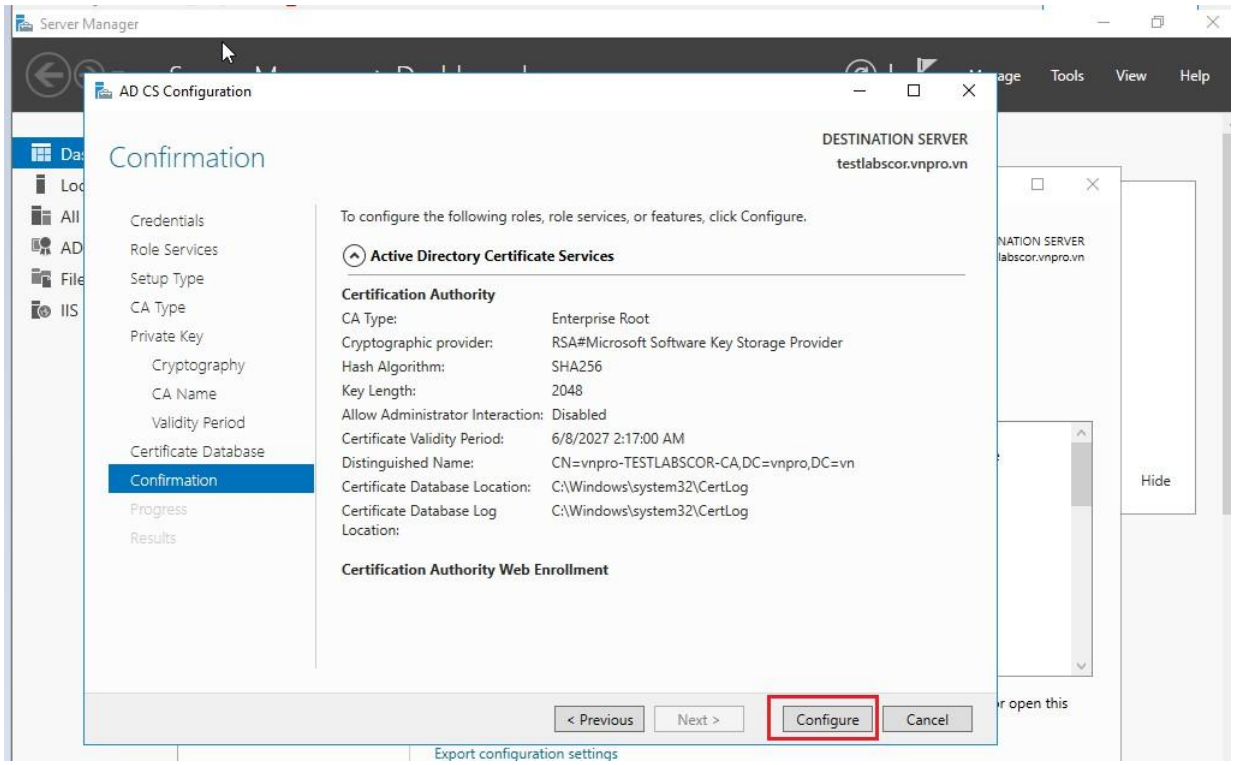
✓ Chọn thời gian hiệu lực của certificates và nhấn **Next**



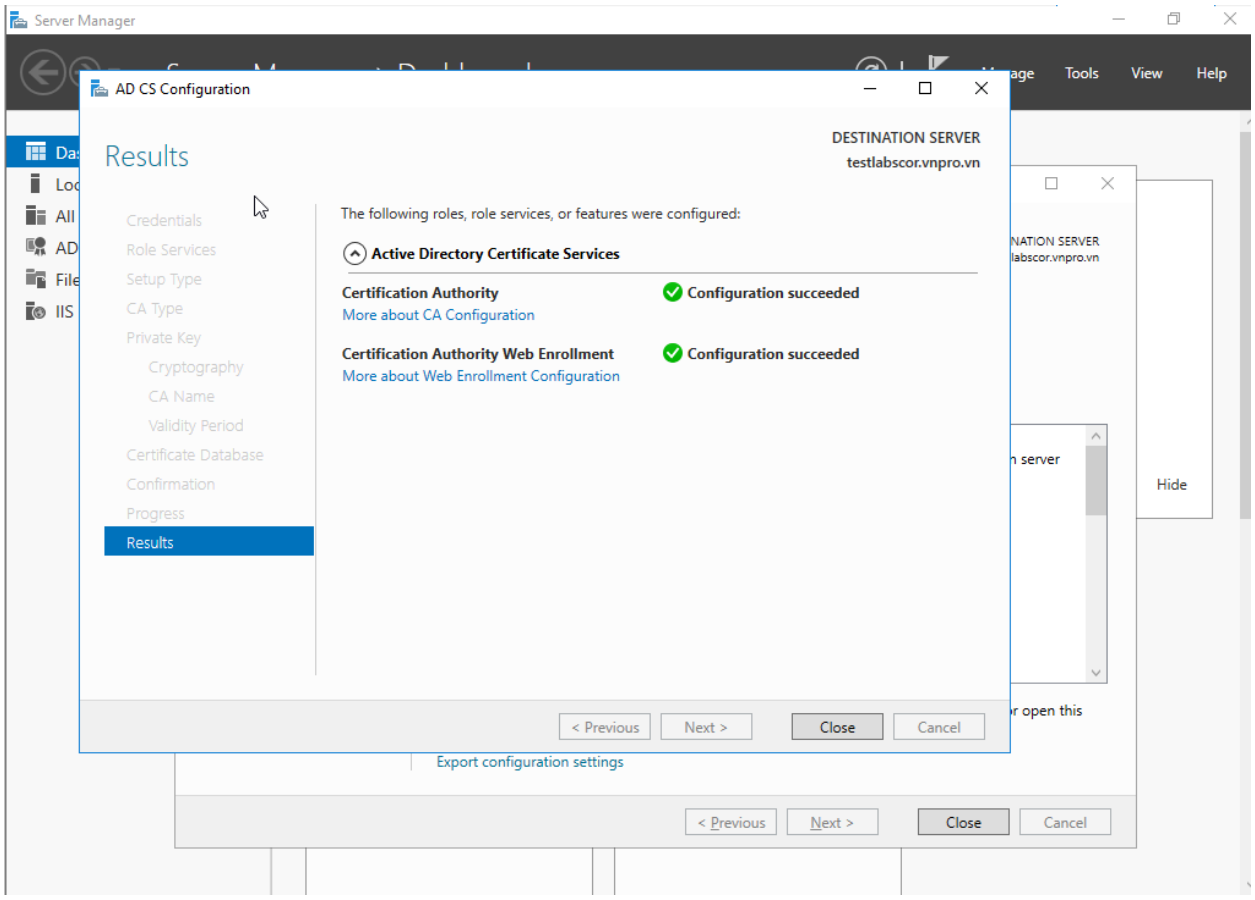
✓ Nhấn **Next**



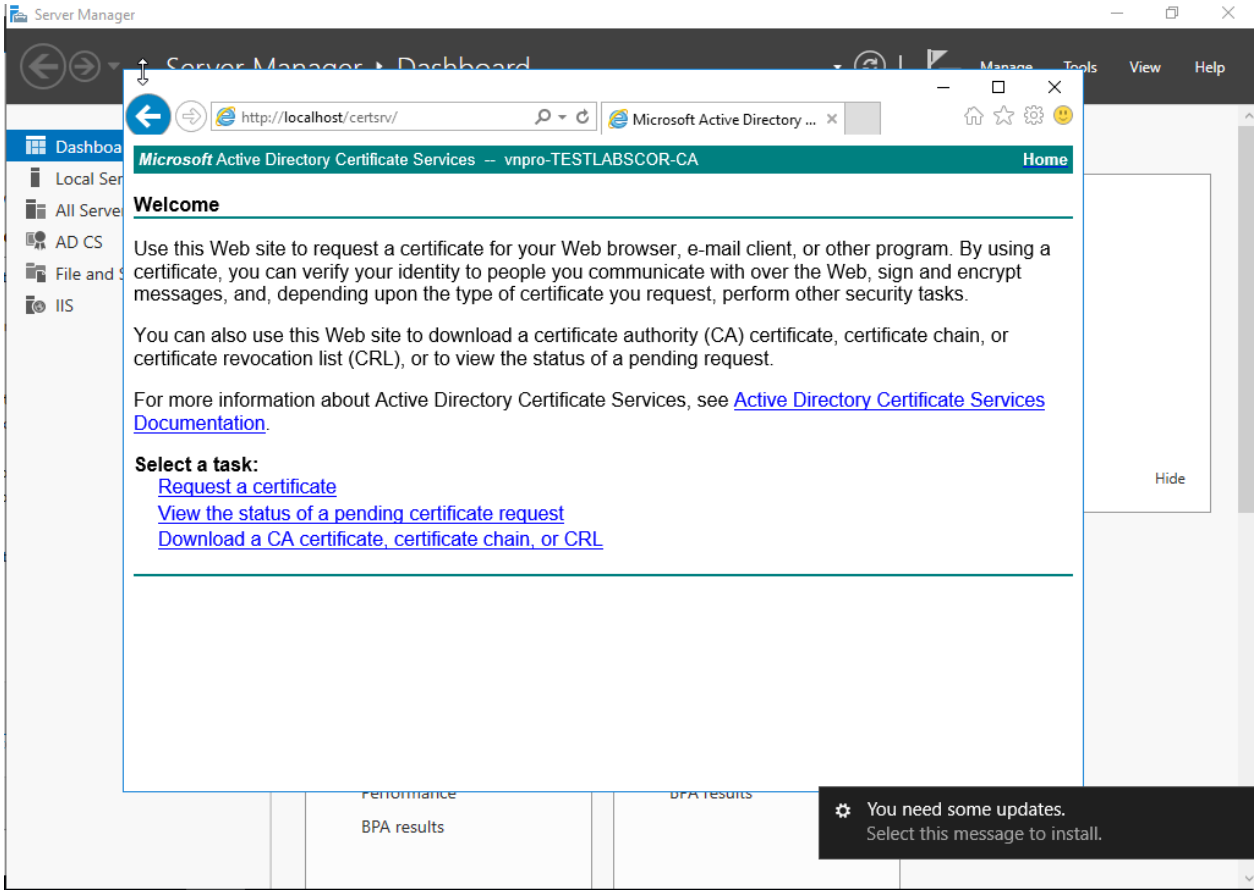
✓ Nhấn **Configure**



✓ Thông báo như hình dưới là thành công



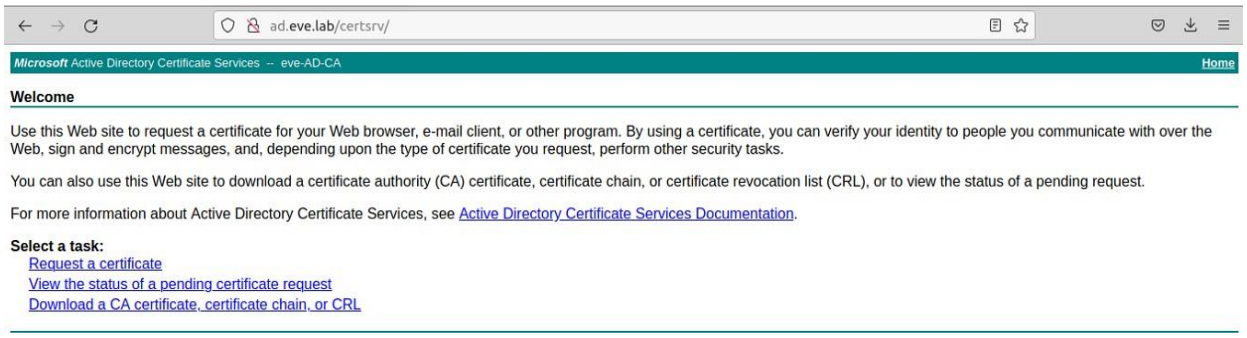
Mở trình duyệt và truy cập vào địa chỉ *http://localhost/certsrv*, AD CS



2. Tải xuống chứng chỉ CA:

Bước 1 trong trình duyệt web trên PC quản trị viên, mở một tab mới và điều hướng đến

http://ad.eve.lab/certsrv.



Bước 2 Khi được nhắc Sử dụng Administrator / Test123.

Bước 3 Nhấp vào liên kết **Download a CA certificate, certificate chain, or CRL**

Bước 4 Nhấp vào **Download CA certificate**

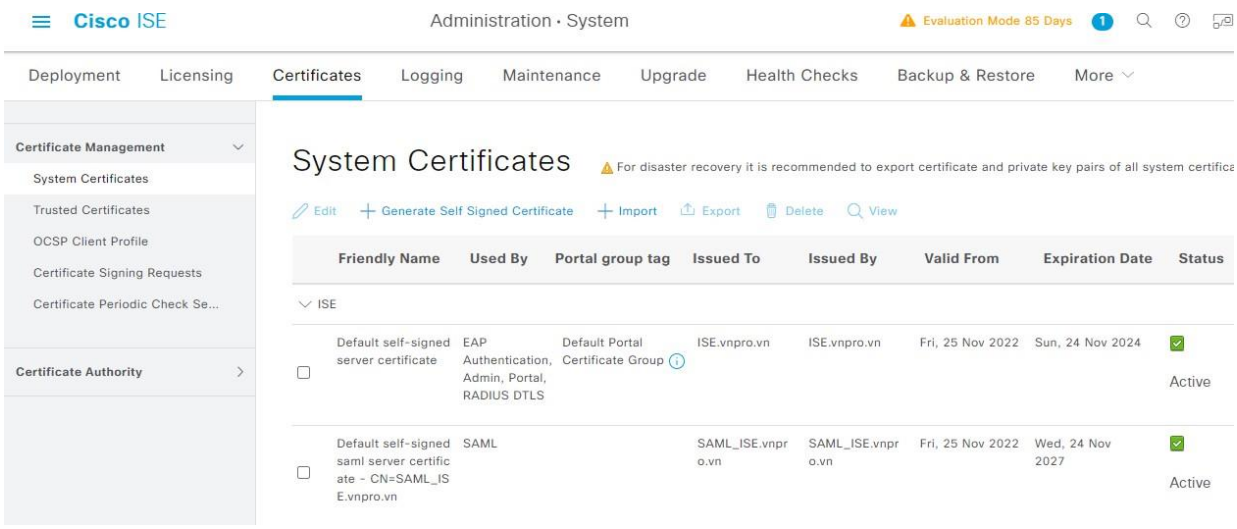
Bước 5 Nhấp OK để lưu .

Lưu ý nếu sử dụng Firefox, bạn có thể phải nhấp vào liên kết **install** this **CA certificate** này ở đầu để cài đặt chứng chỉ CA trong trình duyệt. Điều này phải được thực hiện do thực tế là Firefox

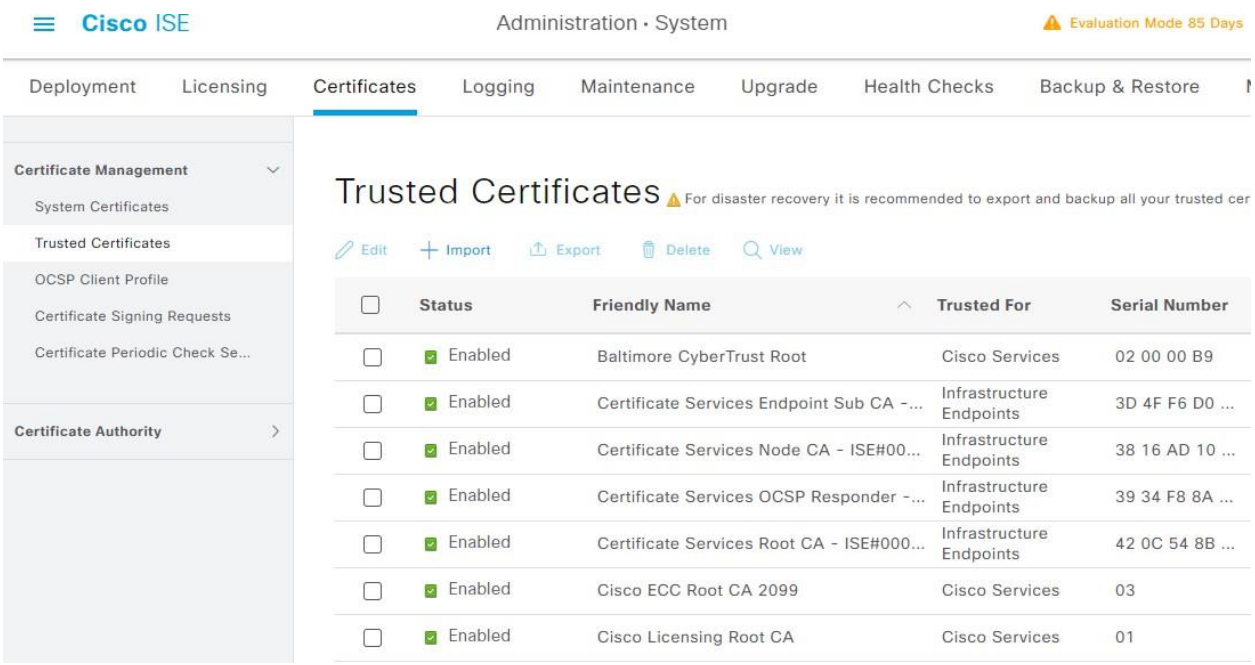
Sử dụng một chứng chỉ riêng biệt từ hệ điều hành. Chọn tin tưởng CA này để xác định trang web và bấm OK

3. Cài đặt chứng chỉ CA:

Bước 6 Trong tab Cisco ISE admin portal , điều hướng đến **Administrator > System > Certificates.**



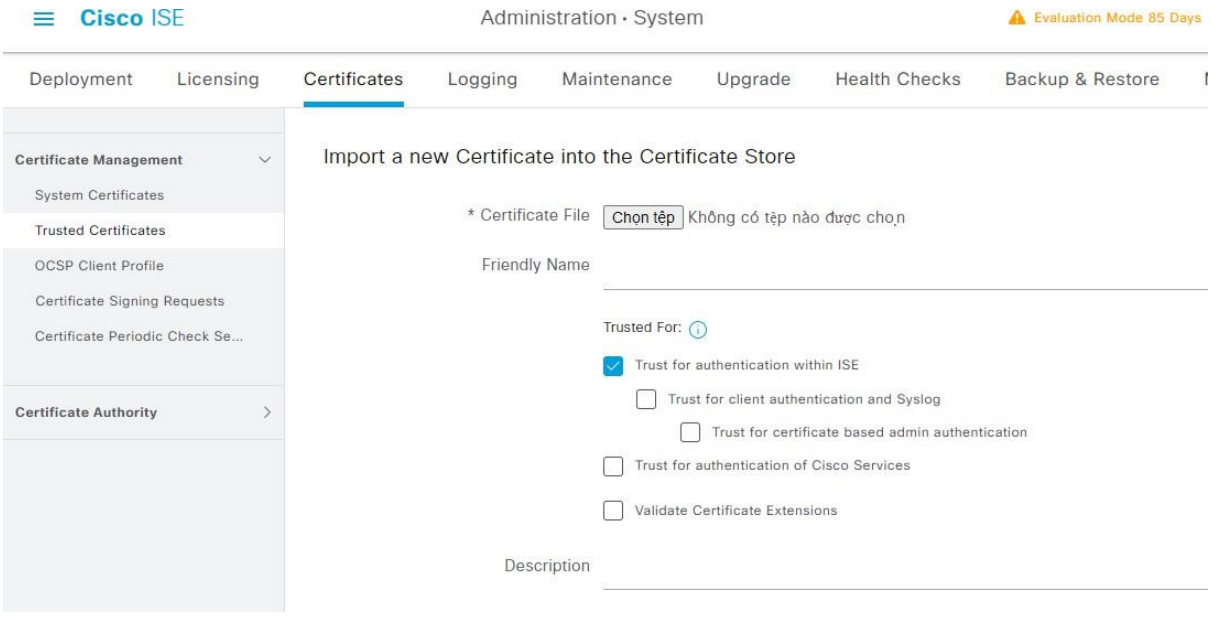
Bước 7 Sau đó chọn **Trusted Certificates** dưới **Certificate Management**.



Bước 8 Nhấp vào nút **Import** vào ngăn bên phải.

Bước 9 Nhấp vào **Browse** …và điều hướng đến thư mục tải xuống của bạn.

(C:\Users\Administrator\Downloads).

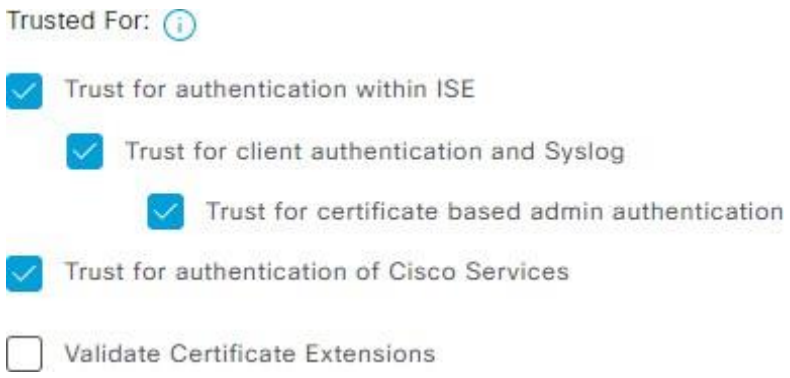


Bước 10 Chọn tệp **certnew.cer** và sau đó chọn nút **Open**.

Lưu ý rằng bạn có thể hoặc không thể thấy tiện ích mở rộng.cer tùy thuộc vào Windows Explorer của bạn

Bước 11 Trong trường Friendly Name Nhập **demo.local CA Certificate**.

Bước 12 Chọn ba tùy chọn sau như được chỉ ra trong ảnh chụp màn hình.

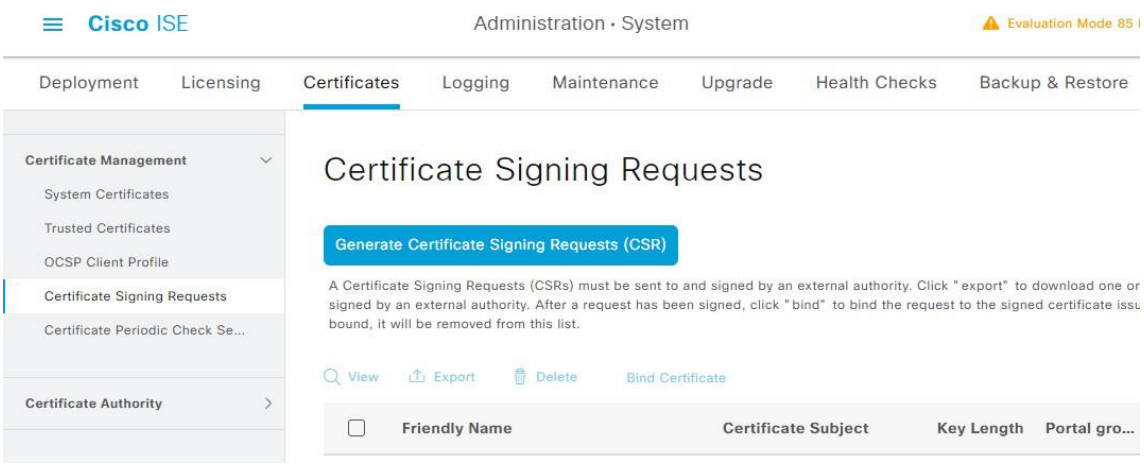


Bước 13: Trong trường Description , **CA cert from ad1.demo.local.**

Bước 14: Nhấp vào Gửi ở phía dưới.

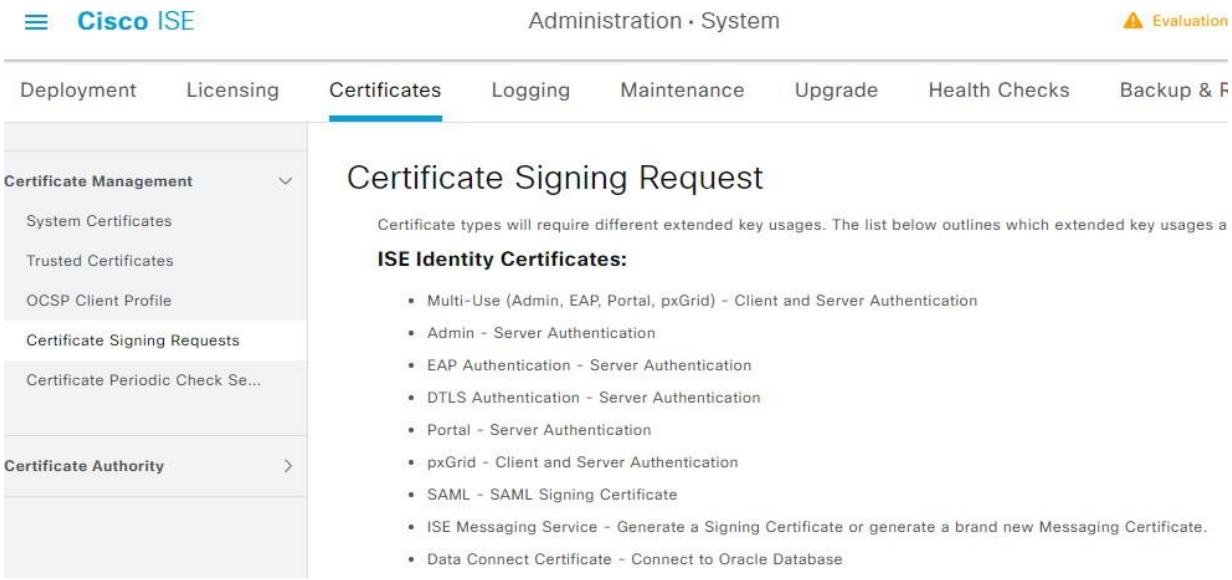
4. Tạo yêu cầu ký chứng chỉ

Bước 15: ở khung bên trái, chọn **Certificate Signing Request**



Bước 16: Nhấp vào nút ở đầu ngăn bên phải, **Generate Certificate Signing Request (CSR)**

Yêu cầu (CSR).



Bước 17: Thực hiện quy trình sau để tạo CSR của bạn.

Usage

Certificate(s) will be used for: Admin

Allow Wildcard Certificates

Subject

Common Name (CN): $FQDN$

Organizational Unit (OU): IT

Organization (O): ISE Lab

City (L): BT

City (L): BT

State (ST): HCM

Country (C): VN

Subject Alternative Name (SAN)

DNS Name	*.eve.lab
IP Address	10.1.1.200

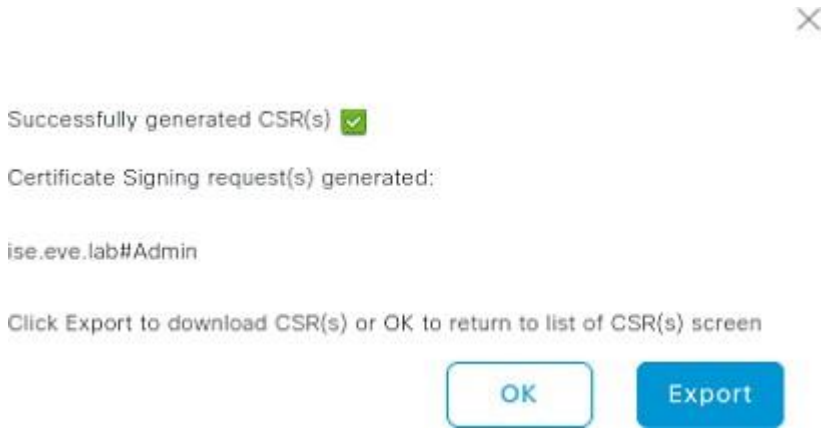
* Key type: RSA

* Key Length: 4096

* Digest to Sign With: SHA-384

Certificate Policies

Bước 18: bạn sẽ nhận được một cửa sổ bật lên xác nhận thông báo cho bạn mà bạn đã tạo thành công CSR của bạn.

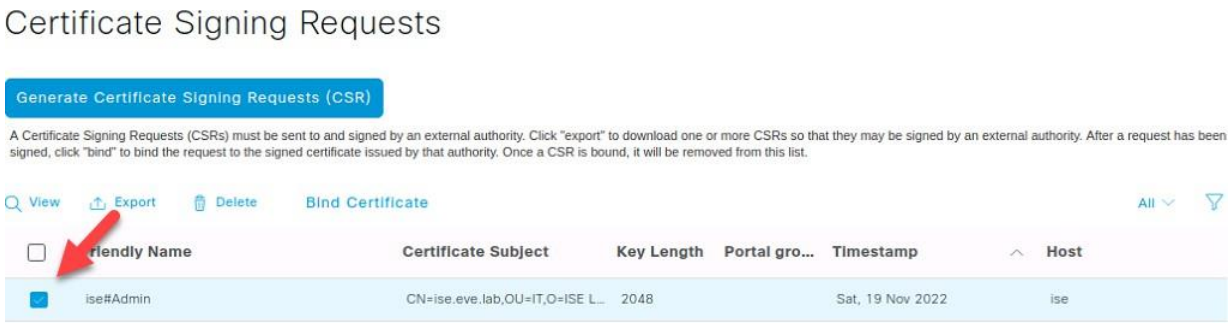


Bước 19: Click **Export**

Bước 20: Save the file

Bước 21: Ở khung bên trái, nhấp vào **Certificate Signing Request** một lần nữa.

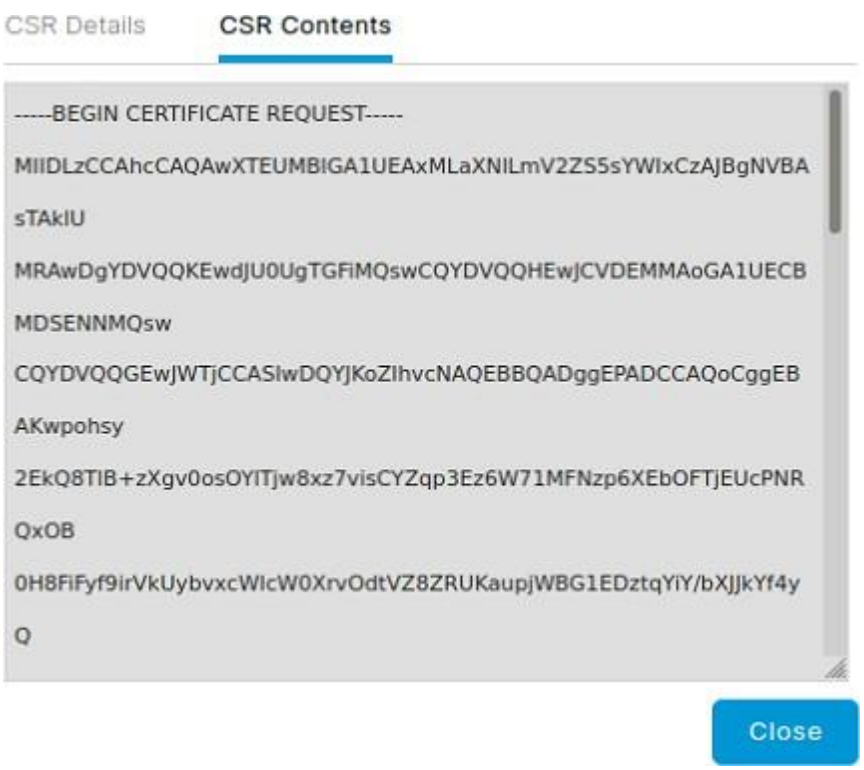
Bước 22: Trong khung bên phải Chọn hộp kiểm ở bên trái của CSR đã xử lý trước đó.



Bước 23: Nhấp vào nút Xem trong thanh công cụ.

Bước 24: Quan sát các chi tiết CSR.

Bước 25: Nhấp vào Tab CSR Nội dung và quan sát văn bản của yêu cầu chứng chỉ.



Bước 26: Highlight (Ctrl-A) và sao chép các nội dung hoàn chỉnh vào bảng tạm (nhấp chuột phải vào và chọn sao chép hoặc nhấn Ctrl-C sẽ hoạt động).

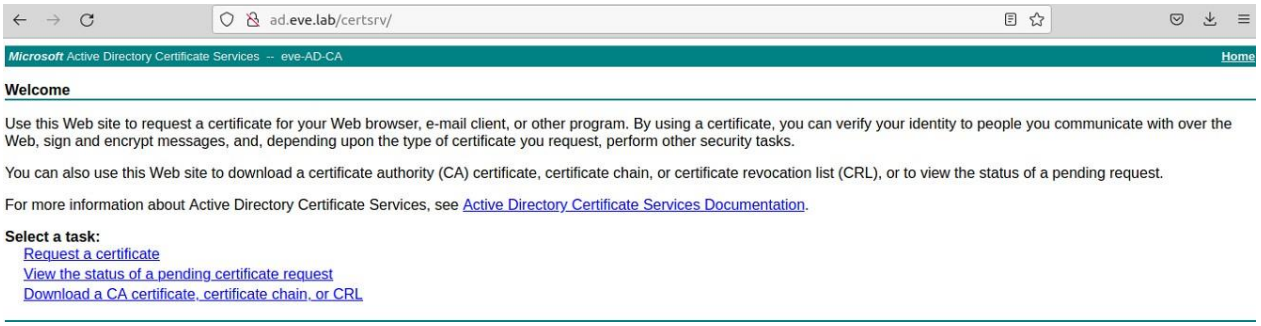
Bước 27: Nhấp **Close.**

Bước 28: Quay trở lại Tab cho trang Microsoft Active Directory.

(http://ad.eve.lab/certsrv với username **administrator**, password: **Test123**)

Bước 29: Nhấp vào liên kết **Home** ở góc trên bên phải.

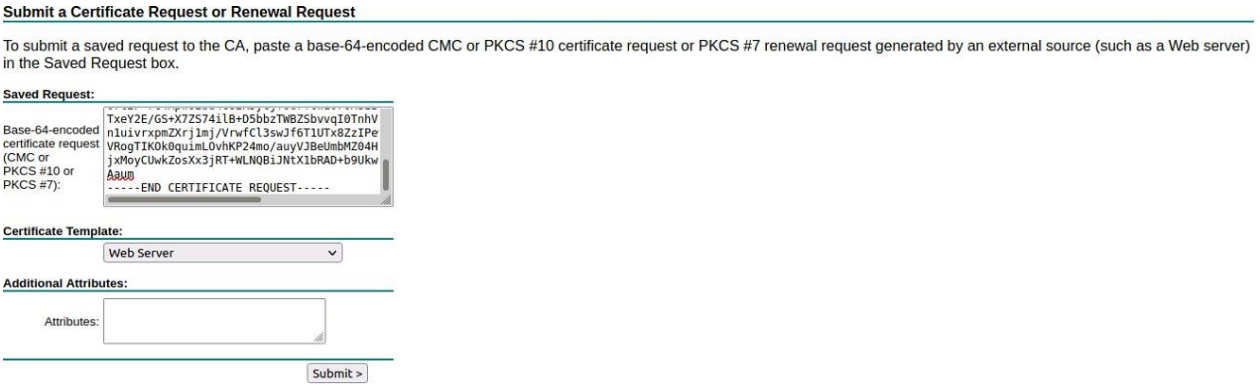
Bước 30: Nhấp vào **Request a certificate.**



Bước 31: Nhấp vào liên kết **advanced certificate request link.**

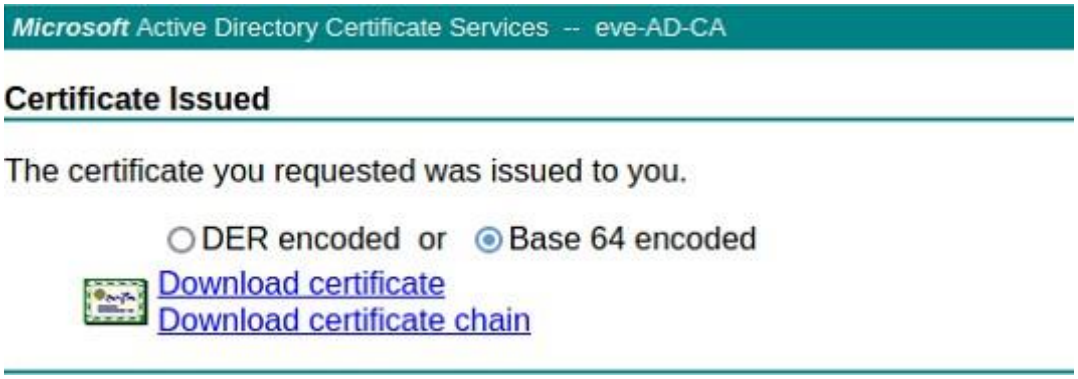
Bước 32: Nhấp chuột phải và dán nội dung vào trường và **Send Requests.**

Bước 33: Từ **Certificate Template** thả xuống và chọn **Web server**

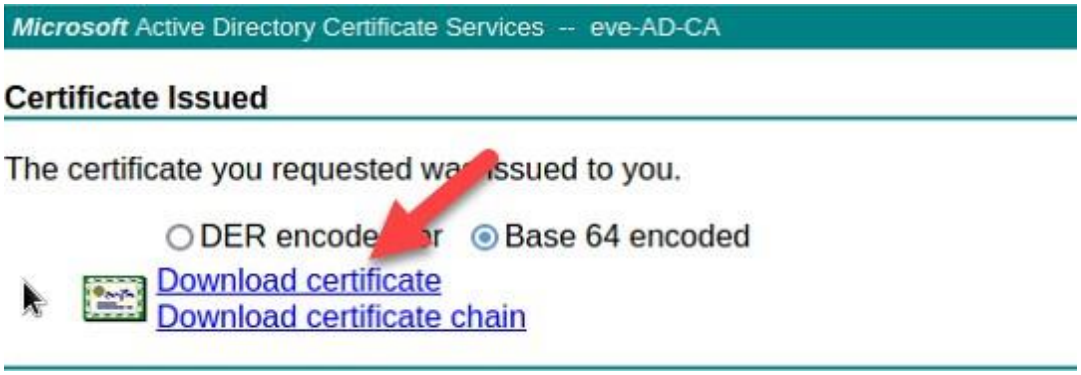


Bước 34: Nhấp vào **Submit > button**

Bước 35: Chọn **Base 64 encoded**



Bước 36: Nhấp vào **Download certificate**



Bước 37: Nhấp vào **OK** để lưu tệp.

Bước 38: Mở thư mục Download và đổi tên **certnew (1).cer** mới thành chứng chỉ "**ise Admin Cert.cer"**

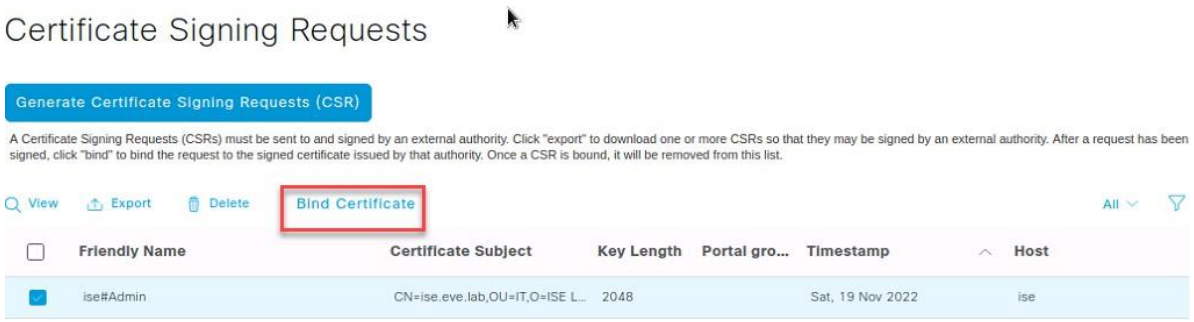
Cài đặt (Bind) CA signed certificate:

Bước 39: Quay trở lại tab Trình duyệt Cisco ISE.

Bước 40: trong trang Certificate Management > Certificate Signing Request ,

Hộp kiểm bên trái của CSR đã xử lý trước đó.

Bước 41: Thanh công cụ nhỏ ở trên, nhấp vào nút Chứng chỉ liên kết.



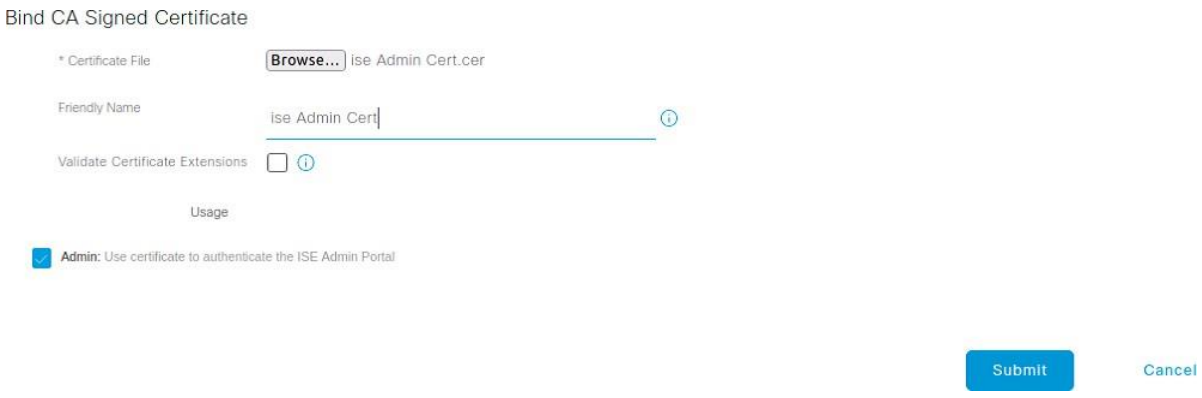
Bước 42: Nhấp vào Browse và điều hướng đến Downloads folder nếu cần.

Bước 43: Chọn tệp **ise Admin Cert.cer.**

Bước 44: Nhấp vào **Open**.

Bước 45: Trong trường Friendly Name Enter **ise-1 Admin Cert**.

Bước 46: Chọn **Admin**, để gán chứng chỉ cho vai trò quản trị viên.

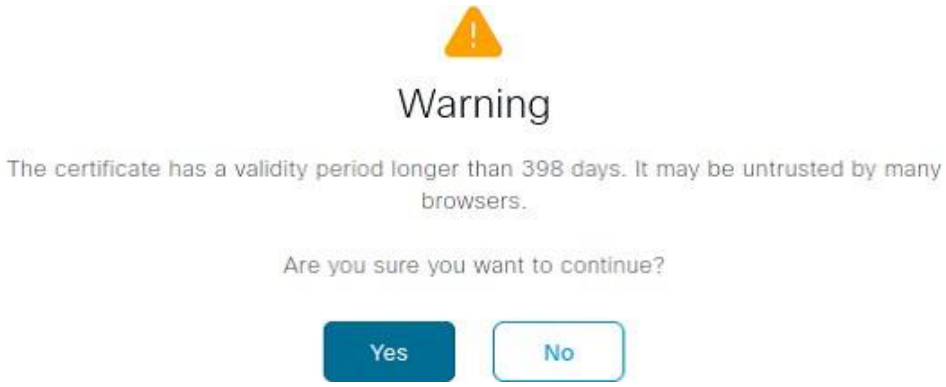


Bước 47: Nhấp vào **Submit**.

Bước 48: Hệ thống sẽ đăng nhập cho bạn và khởi động lại các dịch vụ.

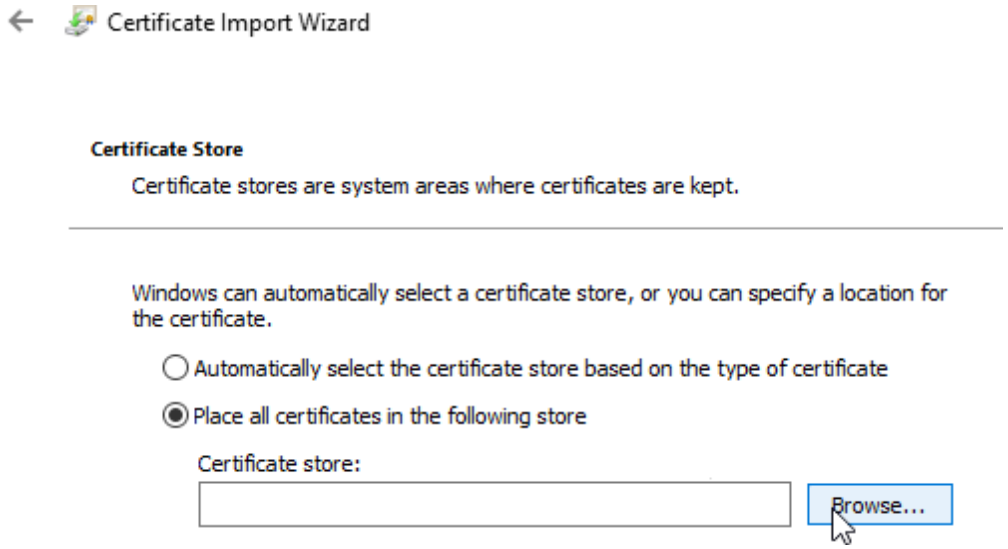
Bước 49: Đăng nhập lại sau vài phút.

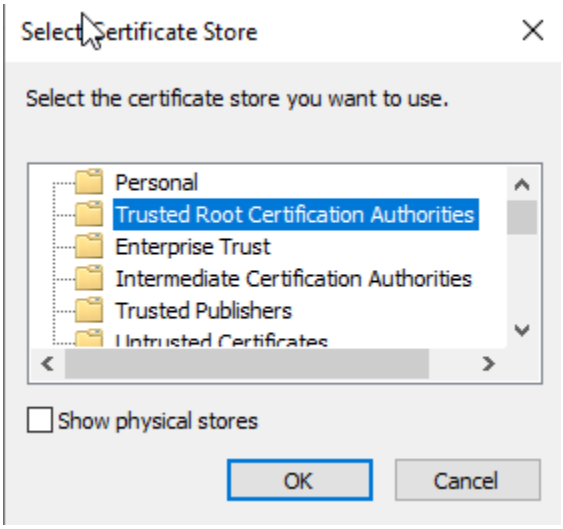
Lưu ý: Bạn có thể kiểm tra trạng thái của dịch vụ khởi động lại thông qua bảng điều khiển hoặc CLI bằng cách sử dụng lệnh **show application status ise**. Khi máy chủ ứng dụng đang chạy, bạn sẽ có thể đăng nhập.



Xác minh chứng chỉ

Bước 50: Trong thanh URL trình duyệt của bạn, nhấp vào biểu tượng khóa ở bên trái của https: //. Quan sát Lĩnh vực sau chỉ ra chứng chỉ CA đã ký đáng tin cậy.





Bước 51: Nhấp vào mũi tên bên phải và sau đó **More Information**.

Bước 52: Nhấp vào **View Certificate**.

Bước 53: Quan sát được phát hành bởi **Root-CA** cho nhóm của bạn.

Bước 54: Nhấp vào tab **Details** và cuộn xuống **Certificate** > **Extensions** > **Certificate Subject Alt Name** và quan sát cấu hình **Wildcard** của bạn.

Bước 55: Đóng tất cả các cửa sổ bật lên.

Xác minh kết quả:

Bạn đã hoàn thành nhiệm vụ này khi bạn đạt được kết quả này:

Bạn đã cài đặt thành công **CA certificate** trên **Cisco ISE**

Bạn đã xác minh chứng chỉ thông qua trình duyệt web của bạn

3. Cấu hình LDAP Integration

Trong nhiệm vụ này, bạn sẽ định cấu hình **Cisco ISE** để tích hợp với **LDAP**. Sau đó bạn sẽ định cấu hình nhóm **LDAP** và Thuộc tính người dùng để sử dụng trong Cisco ISE trong các phòng thí nghiệm sau này

Hoàn thành các bước sau:

Định cấu hình LDAP như một nguồn nhận dạng bên ngoài

Bước 1: Trong **ISE Admin Portal** , điều hướng đến **Administrator** > **Identity Management** > **External Identity Sources** và sau đó ở khung bên trái, chọn **LDAP**.

Bước 2: Trong khung bên phải, nhấp + **Add** vào thanh công cụ.

Bước 3: trong trường Tên Nhập **LDAP_eve_lab.**

Bước 4: Trong trường Mô tả Nhập **eve.lab LDAP configuration**.

Bước 5: Trong trình đơn thả xuống cho lược đồ, chọn **Active Directory**.

Bước 6: Nhấp vào tab **Connection**.

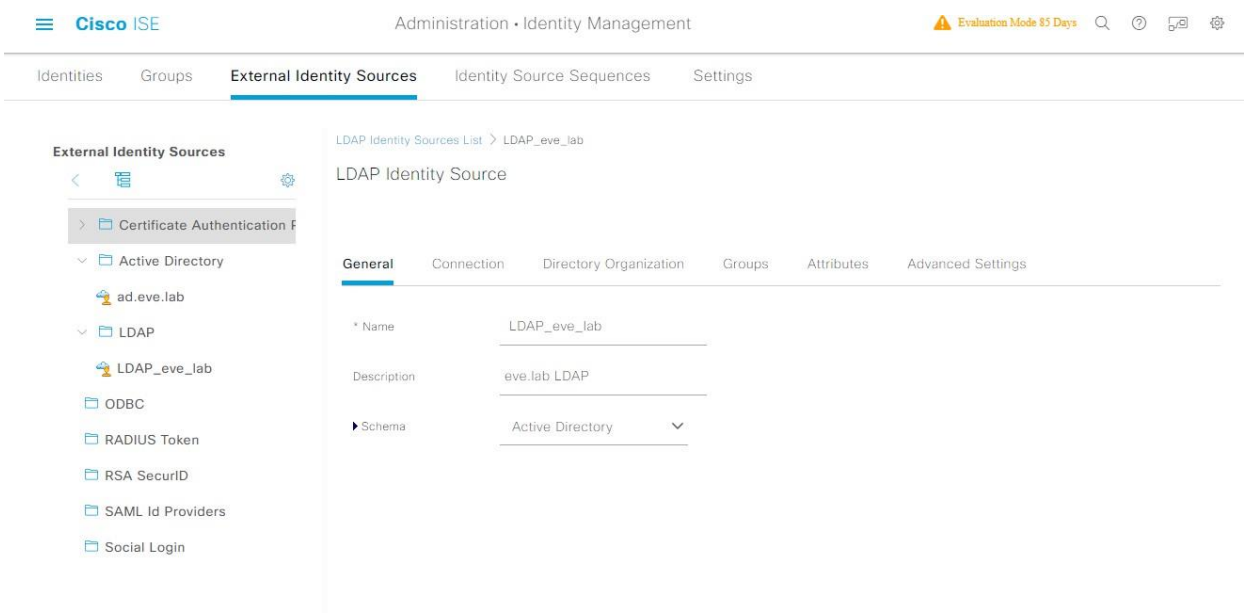
Bước 7: trong trường Hostname/IP nhập **ad.eve.lab**

Bước 8: Chọn **Authentication Access**

Bước 9: Trong AdminDN Enter cn=administrator,cn=user,dc=eve,dc=lab.

Bước 10: Trong trường password Nhập Test123

Bước 11: Xác minh cài đặt của bạn với ảnh chụp màn hình bên dưới.



Bước 12: Cuộn xuống và nhấp vào nút Kiểm tra liên kết với máy chủ. Điều này nên thành công.

Lưu ý: Quan sát thời gian phản hồi để so sánh trong tương lai. Ghi chú nó trong hướng dẫn phòng thí nghiệm này nếu cần thiết.

Bước 13: Bây giờ bạn đã xác minh thành công trong kết nối LDAP, sửa đổi

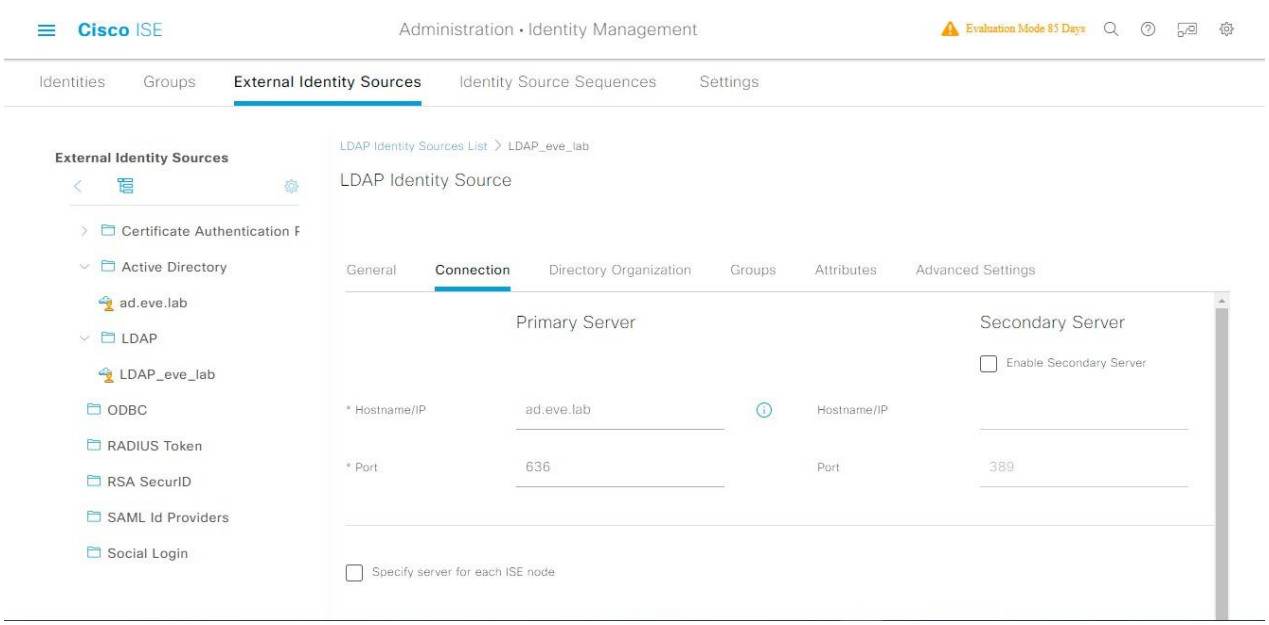
Cấu hình để thực hiện tra cứu LDAP an toàn (LDAPS). Thay đổi **Port** từ

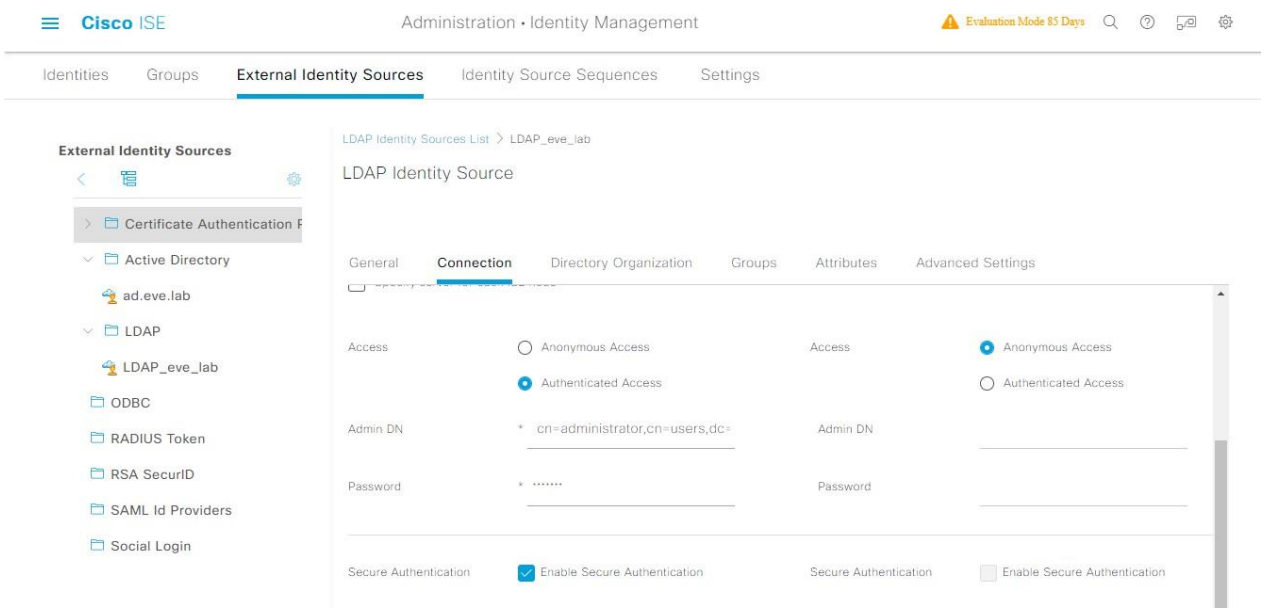
389 đến **636.**

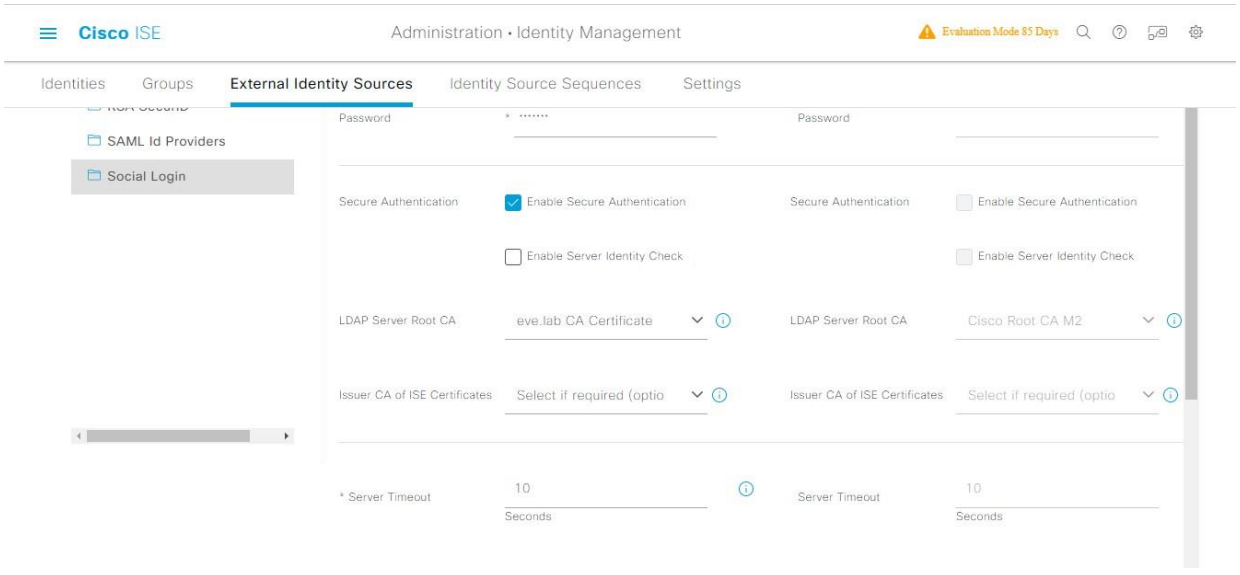
Bước 14: cho phép **Secure Authentication**.

Bước 15: Trong **LDAP Server Root CA**, chọn demo.local CA Certificate.

Bước 16: Xác minh cấu hình của bạn với ảnh chụp màn hình sau.


Cisco ISE
Administration · Identity Management
Evaluation Mode 85 Days
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
External Identity Sources
Certificate Authentication F
Active Directory
ad.eve.lab
LDAP
LDAP_eve_lab
ODBC
RADIUS Token
RSA SecurID
SAML Id Providers
Social Login
LDAP Identity Sources List > LDAP_eve_lab
LDAP Identity Source
General
Connection
Directory Organization
Groups
Attributes
Advanced Settings
Primary Server
Secondary Server
Enable Secondary Server
* Hostname/IP
ad.eve.lab
Hostname/IP
* Port
636
Port
389
Specify server for each ISE node


Cisco ISE
Administration · Identity Management
Evaluation Mode 85 Days
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
External Identity Sources
Certificate Authentication F
Active Directory
ad.eve.lab
LDAP
LDAP_eve_lab
ODBC
RADIUS Token
RSA SecurID
SAML Id Providers
Social Login
LDAP Identity Sources List > LDAP_eve_lab
LDAP Identity Source
General
Connection
Directory Organization
Groups
Attributes
Advanced Settings
Access
Anonymous Access
Authenticated Access
Admin DN
* cn=administrator,cn=users,dc=
Password
Secure Authentication
Enable Secure Authentication


Cisco ISE
Administration · Identity Management
Evaluation Mode 85 Days
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
SAML Id Providers
Social Login
Password
Secure Authentication
Enable Secure Authentication
Enable Server Identity Check
LDAP Server Root CA
eve.lab CA Certificate
Cisco Root CA M2
Issuer CA of ISE Certificates
Select if required (optio
* Server Timeout
10
Seconds

Bước 17: Nhấp vào nút liên kết thử nghiệm với máy chủ. Điều này nên thành công.

Lưu ý: Quan sát thời gian phản hồi giữa liên kết LDAP văn bản rõ ràng trước đó trong LDAPS trói buộc. Cần thêm thời gian để thiết lập và xác minh đường hầm SSL trước khi thực hiện của tra cứu LDAP. Hãy ghi nhớ điều này khi thiết kế và kiến trúc vị trí của Cisco ISE trong môi trường sản xuất.

Bước 18: Nhấp vào tab **Directory Organization**.

Bước 19: Trong trường Subject Search Base nhập dc=eve,dc=lab

Bước 20: Trong trường Group Search Base nhập dc=demo,dc=local.

Bước 21: Vì bạn sẽ không sử dụng LDAP cho tra cứu địa chỉ MAC,

Bước 22: Nhấp vào **Submit** ở phía dưới để lưu cấu hình này.

Thêm thuộc tính LDAP vào từ điển Cisco ISE

Bước 23: Chọn **Group** từ các tab ở trên cùng.

Bước 24: Nhấp vào nút **+Add** trên thanh công cụ và chọn chọn nhóm từ thư mục.

Bước 25: Chấp Retrieve Groups (*) và nhấp vào nút.

Bước 26: Chọn CN=Contractors,OU=Group,OU=HCC,DC=demo,dc=local từ danh sách.

Bước 27: Nhấp OK.

Bước 28: Chọn **Attributes** từ các tab ở trên cùng.

Bước 29: Nhấp vào nút **+Add** trên thanh công cụ và chọn **Select Attributes from Directory.**

Bước 30: Nhập **compartor2@demo.local** trong hộp văn bản chủ đề ví dụ và nhấp vào **Retrieve Attributes**

Bước 31: Từ danh sách các thuộc tính Chọn **userPrincipleName.**

Bước 32: Nhấp **OK**.

Bước 33: Cuộn xuống phía dưới và nhấp vào **Save**.

Xác minh kết quả:

Bạn đã hoàn thành nhiệm vụ này khi bạn đạt được kết quả này:

+ Bạn đã định cấu hình thành công và thử nghiệm Cisco ISE để lấy dữ liệu từ Active Directory của POD thông qua LDAP

+ Bạn đã sửa đổi thành công cấu hình của Cisco ISE để xác thực và lấy dữ liệu từ máy chủ Active Directory của POD của bạn thông qua LDAPS.