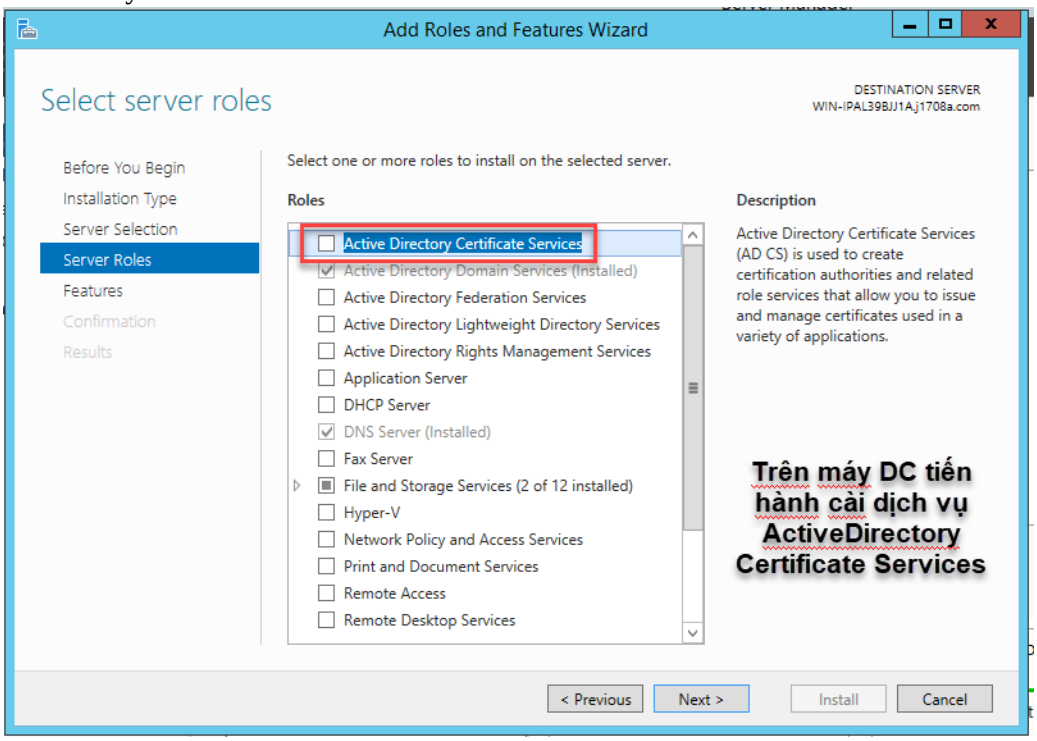
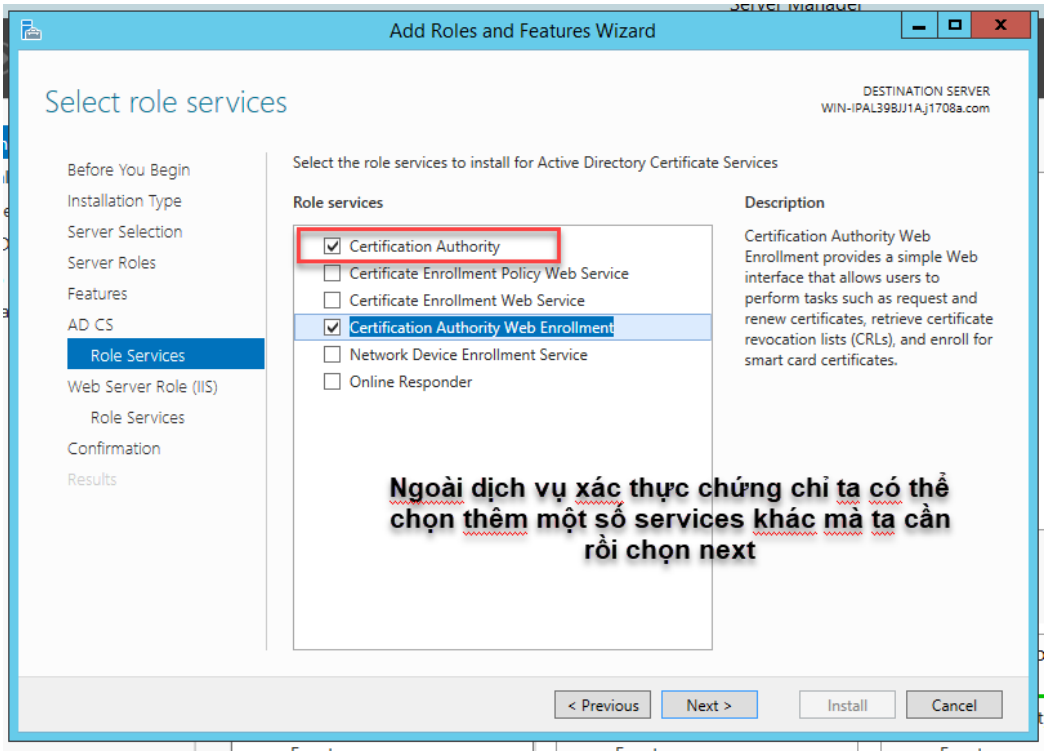
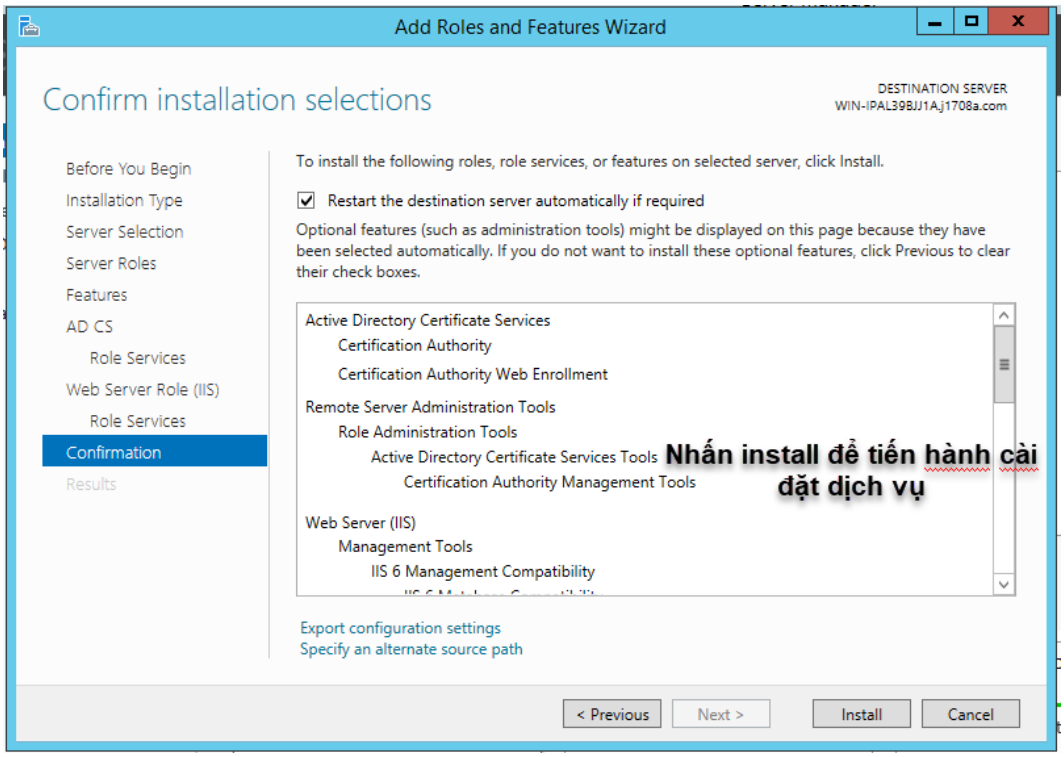
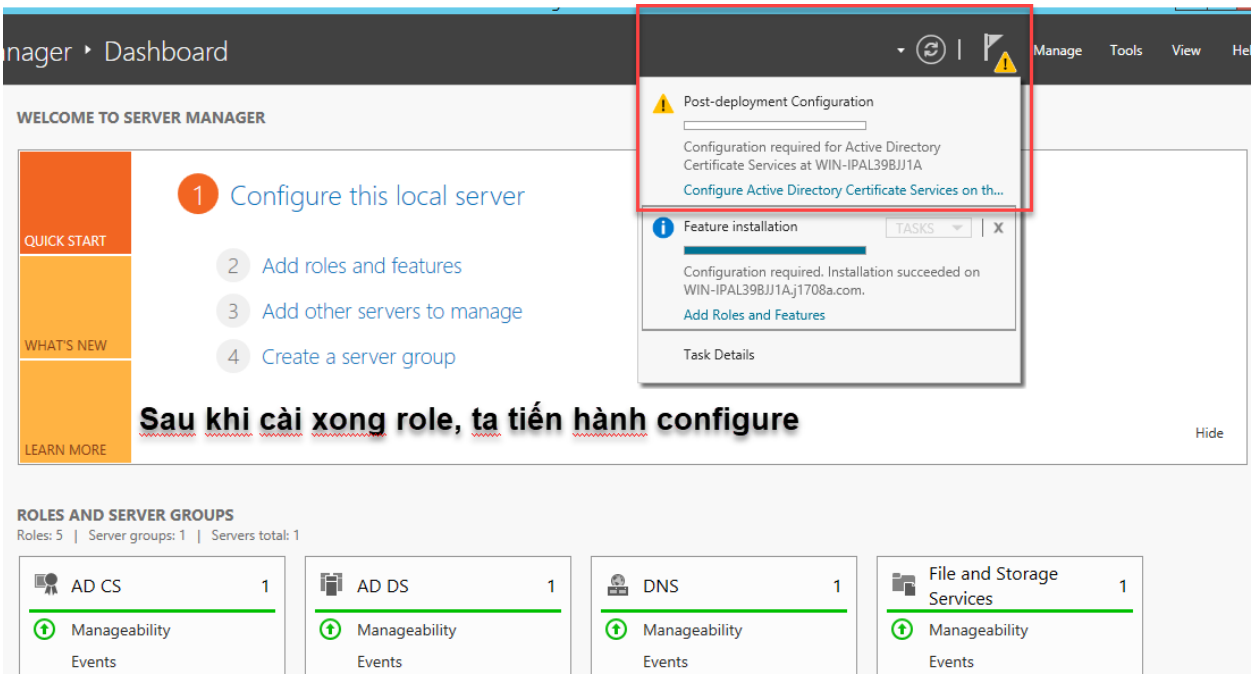
LAB 12 – RADIUS SERVER

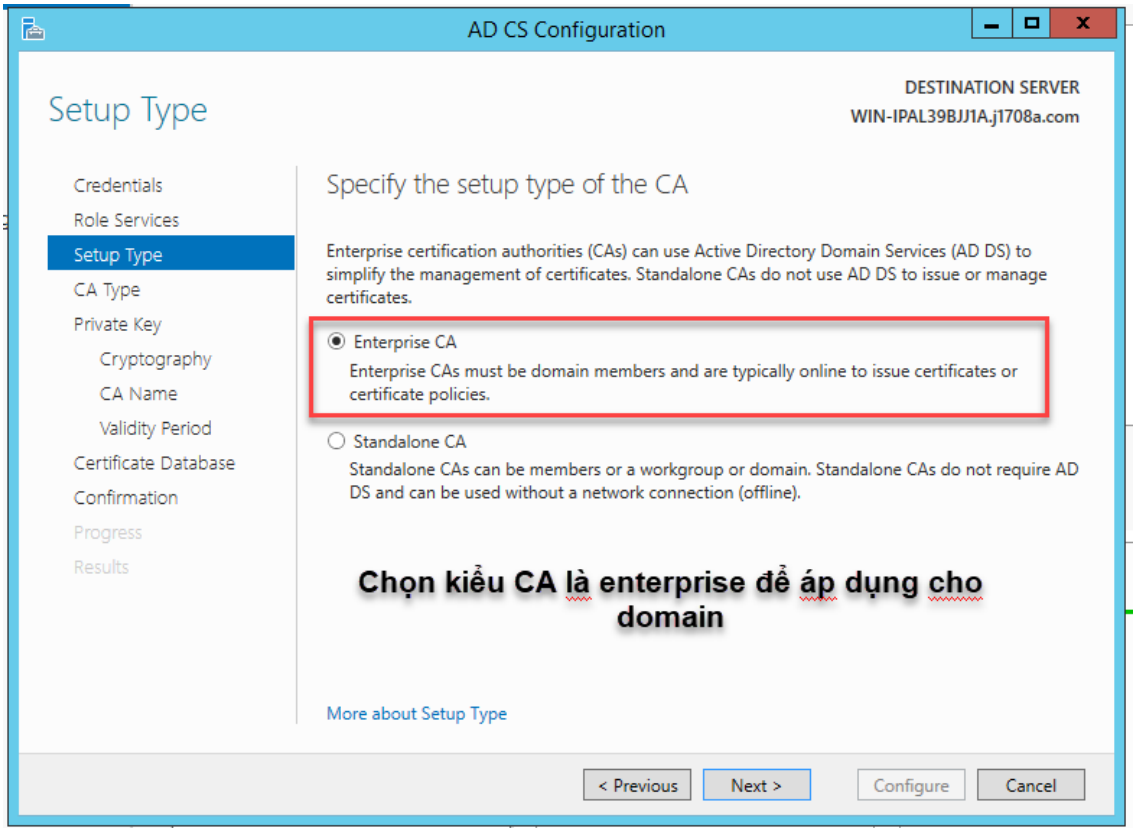
1. **Chuẩn bị**
   Chuẩn bị 2 máy một máy DC và một máy member
2. **Tạo máy radius server xác thực**
   + Trên máy DC

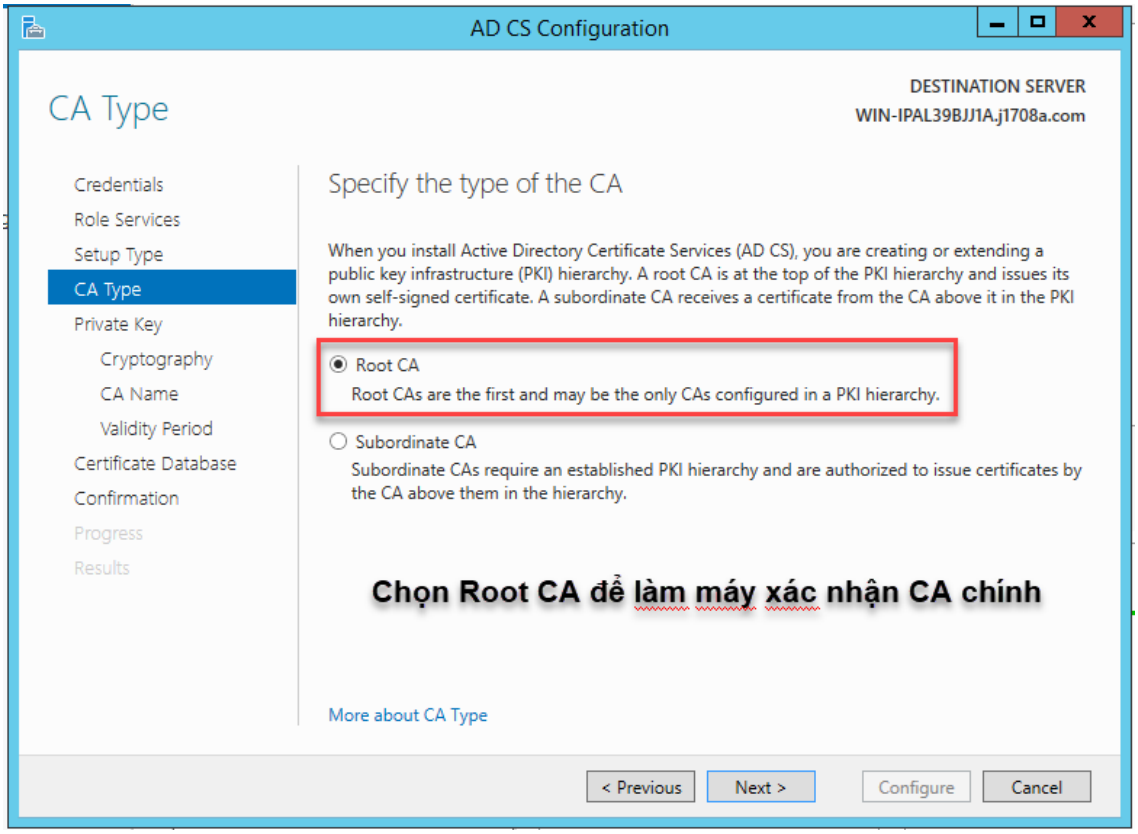


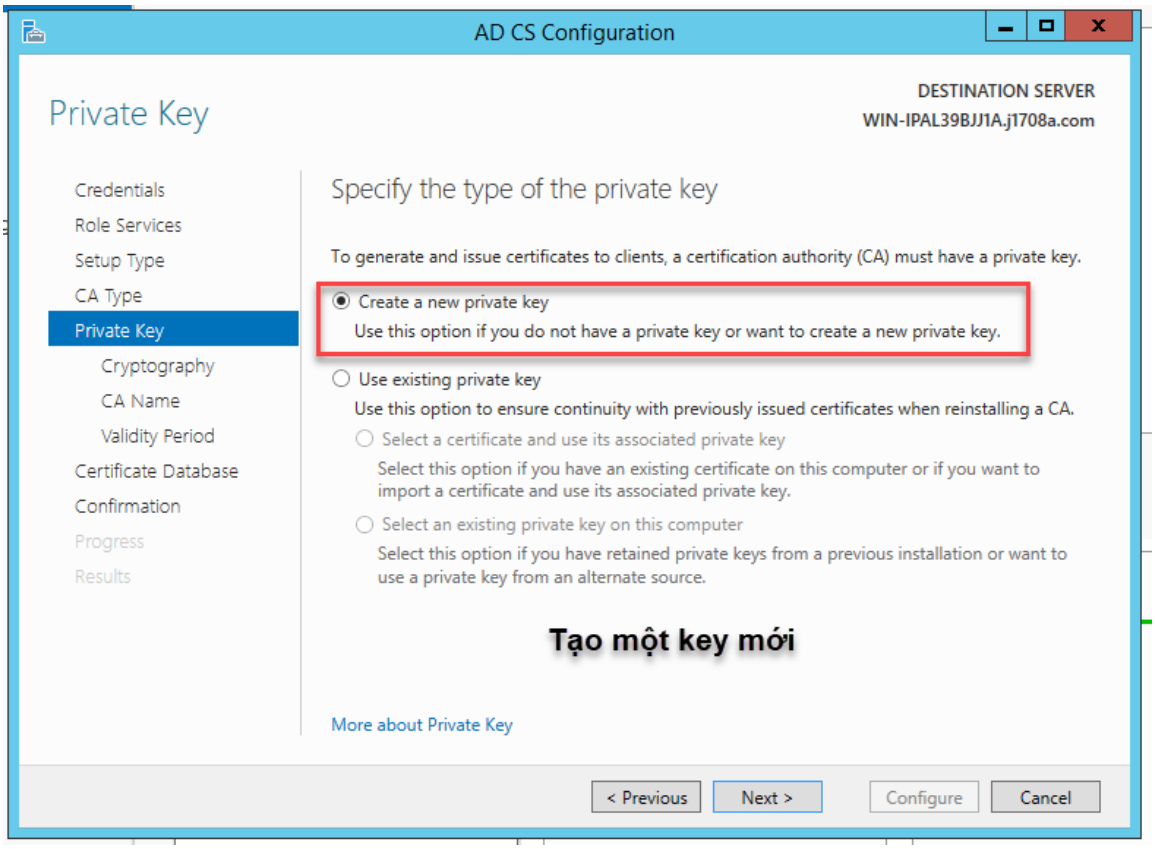


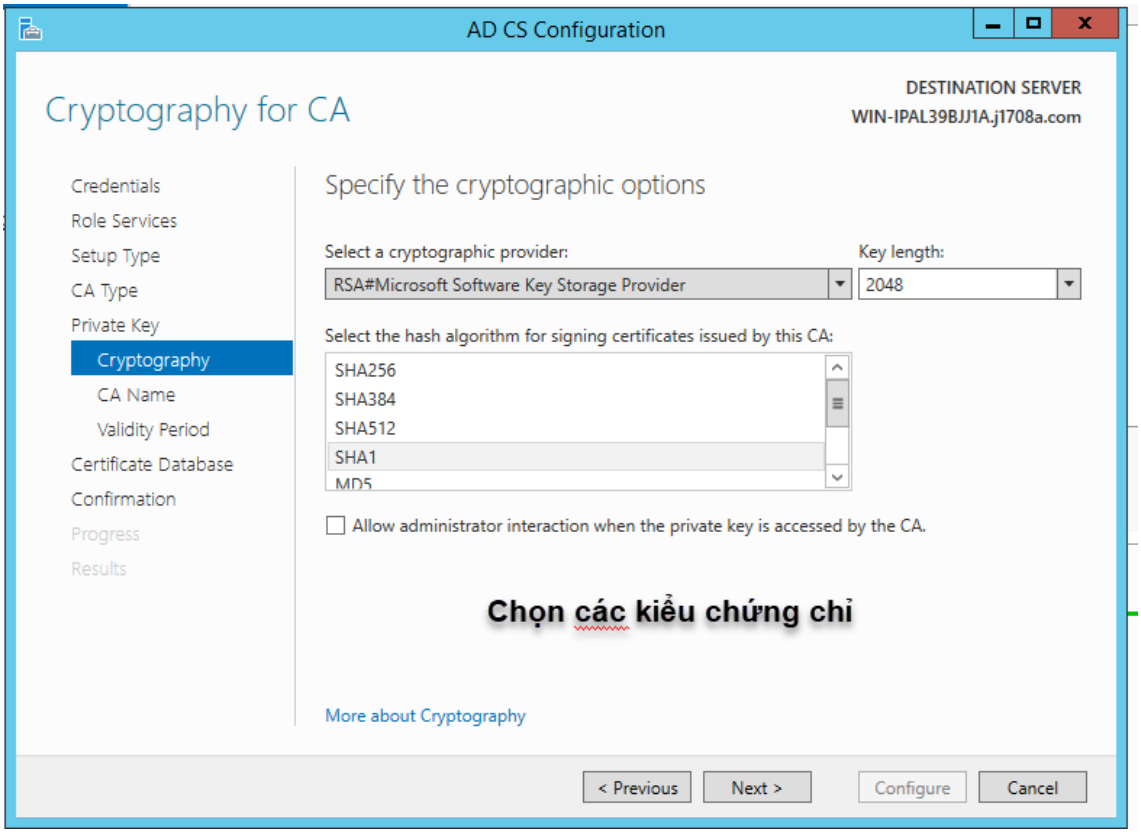

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
WIN-IPAL39BJJ1A.j1708a.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Active Directory Certificate Services
Certification Authority
Certification Authority Web Enrollment
Remote Server Administration Tools
Role Administration Tools
Active Directory Certificate Services Tools
Certification Authority Management Tools
Web Server (IIS)
Management Tools
IIS 6 Management Compatibility
Nhấn install để tiến hành cài đặt dịch vụ
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

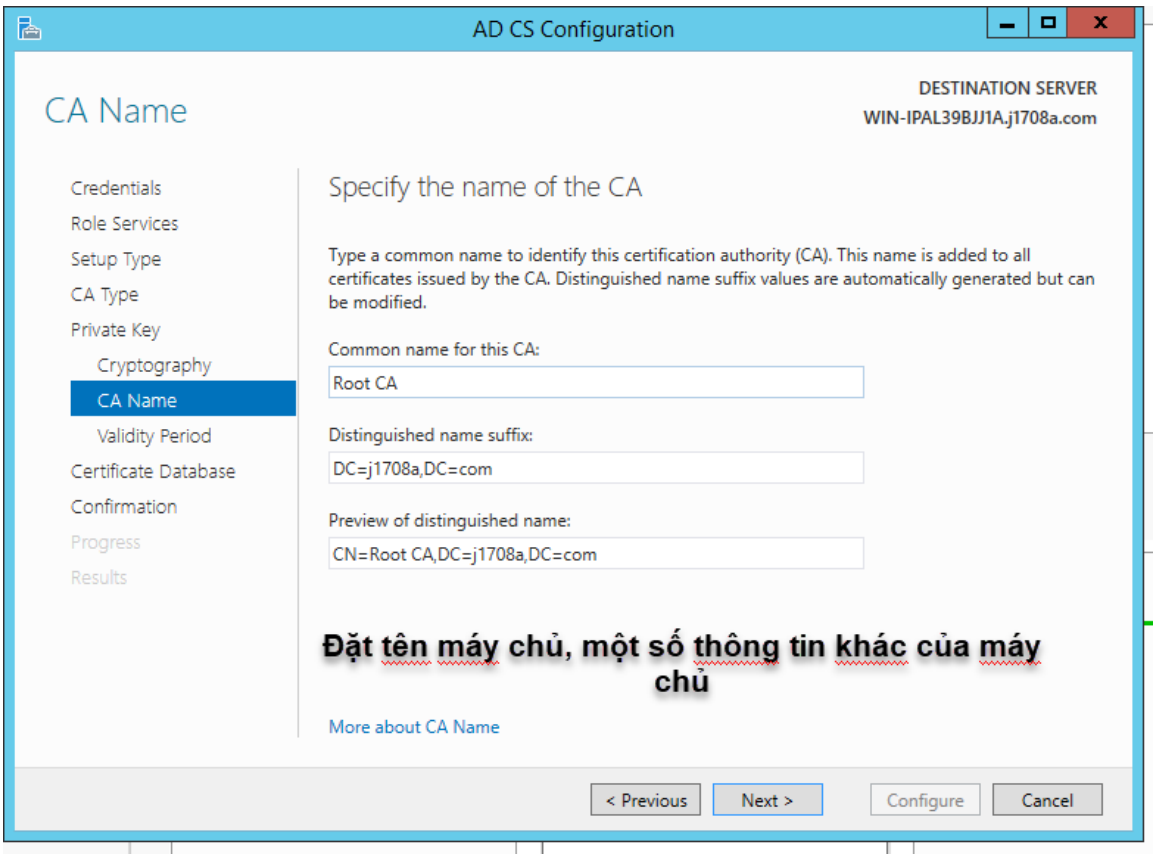

nager ‣ Dashboard
Manage
Tools
View
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
Post-deployment Configuration
Configuration required for Active Directory Certificate Services at WIN-IPAL39BJJ1A
Configure Active Directory Certificate Services on th...
Feature installation
TASKS
Configuration required. Installation succeeded on WIN-IPAL39BJJ1A.j1708a.com.
Add Roles and Features
Task Details
Sau khi cài xong role, ta tiến hành configure
Hide
ROLES AND SERVER GROUPS
Roles: 5 | Server groups: 1 | Servers total: 1
AD CS 1
AD DS 1
DNS 1
File and Storage Services 1
Manageability
Events

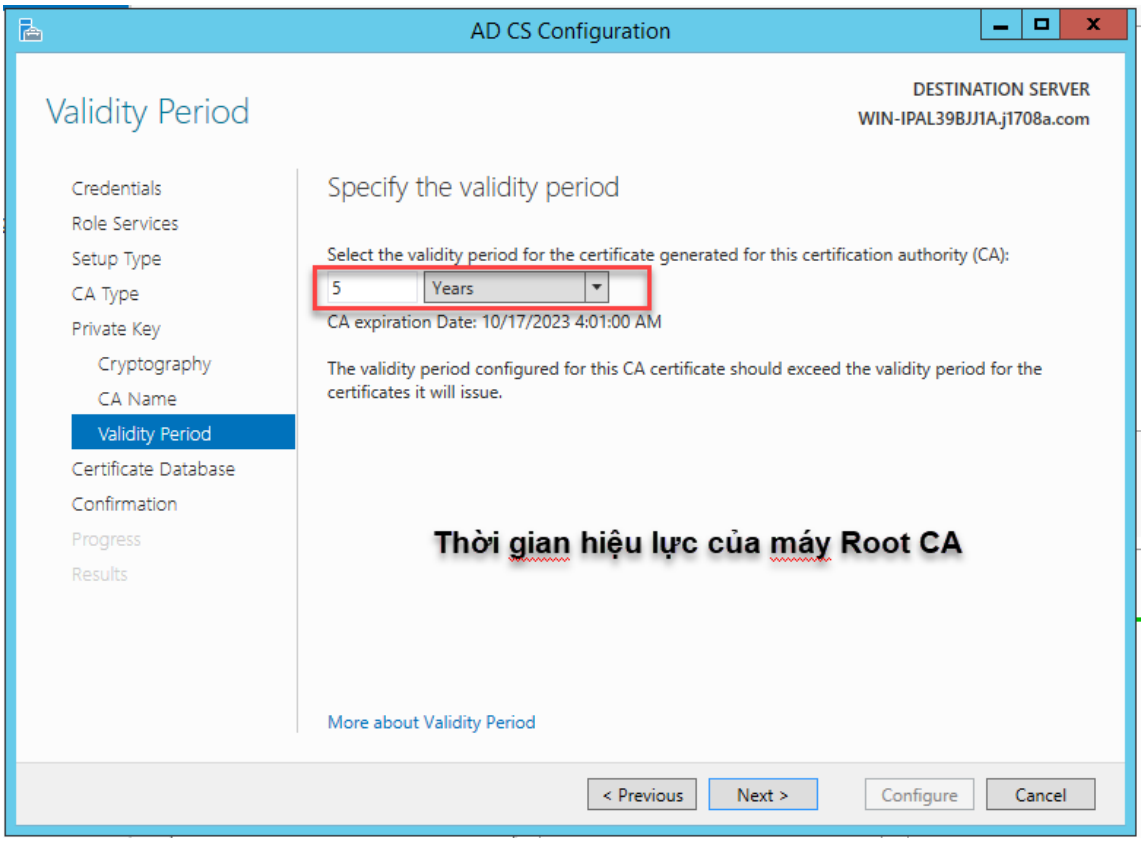

AD CS Configuration
Setup Type
DESTINATION SERVER
WIN-IPAL39BJJ1A.j1708a.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the setup type of the CA
Enterprise certification authorities (CAs) can 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).
Chọn kiểu CA là enterprise để áp dụng cho domain
More about Setup Type
< Previous
Next >
Configure
Cancel

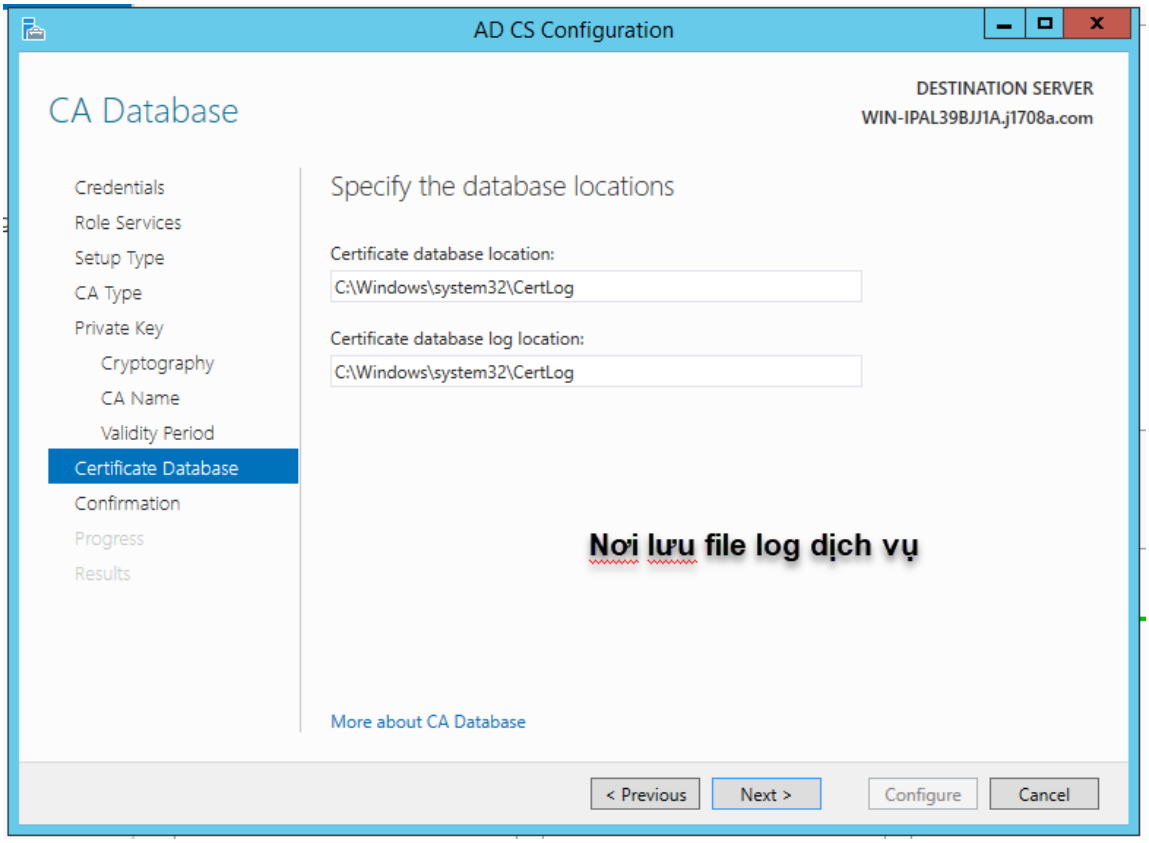

AD CS Configuration
CA Type
DESTINATION SERVER
WIN-IPAL39BJJ1A.j1708a.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the type of the CA
When you install Active Directory Certificate Services (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.
Chọn Root CA để làm máy xác nhận CA chính
More about CA Type
< Previous
Next >
Configure
Cancel

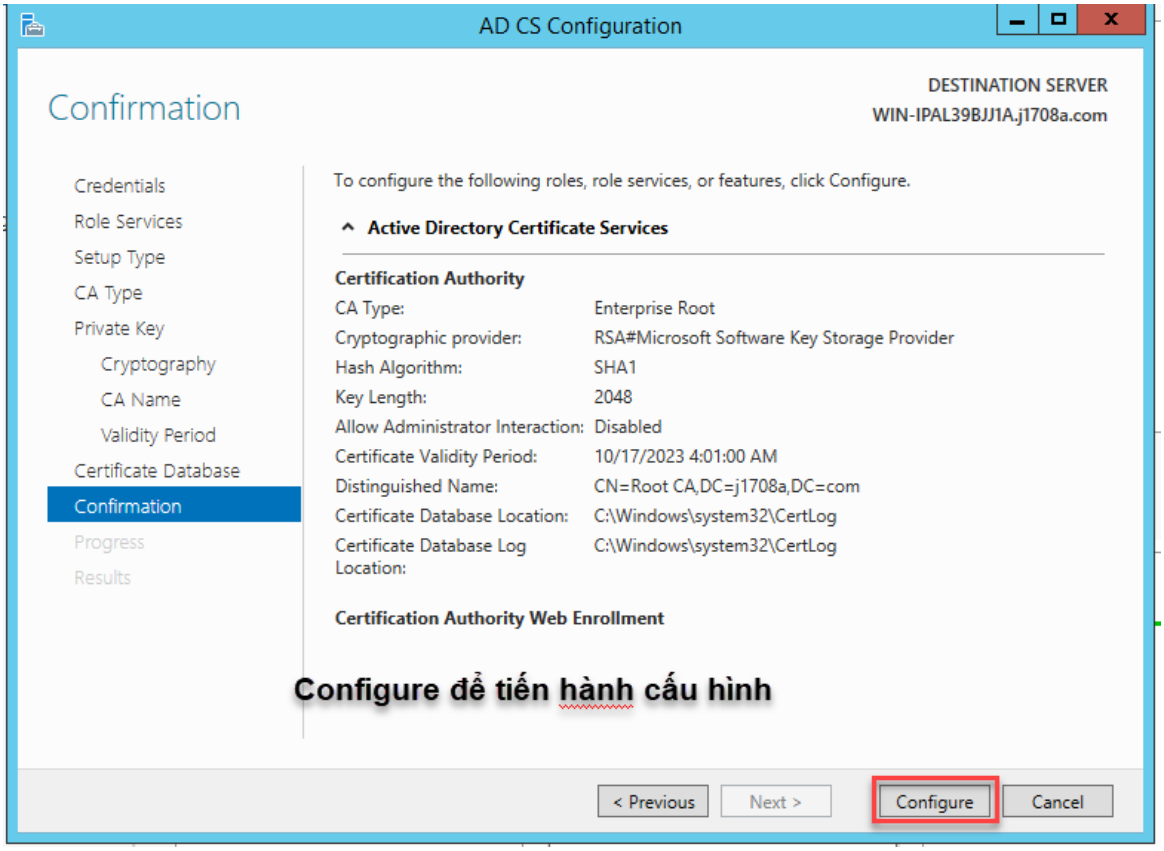

AD CS Configuration
Private Key
DESTINATION SERVER
WIN-IPAL39BJJ1A.j1708a.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the type of the private key
To generate and issue certificates to clients, 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.
Tạo một key mới
More about Private Key
< Previous
Next >
Configure
Cancel

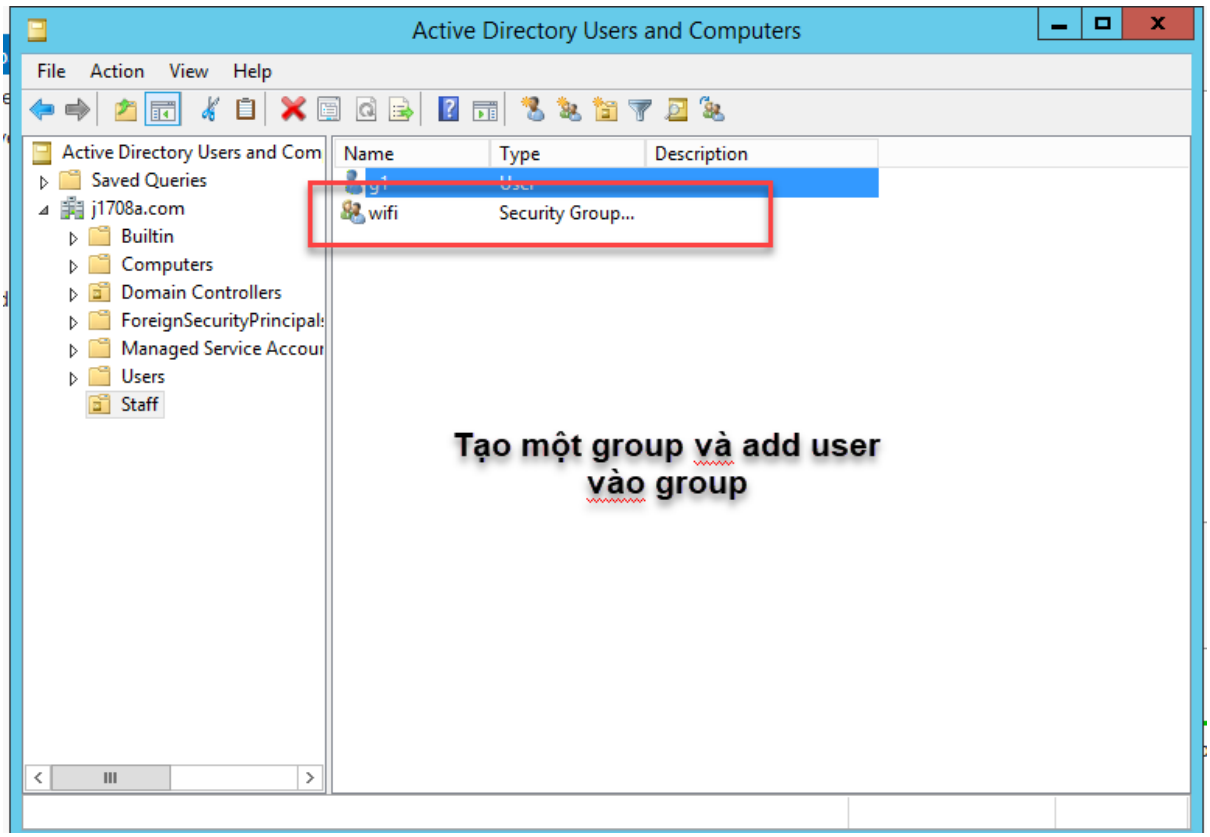

AD CS Configuration
Cryptography for CA
DESTINATION SERVER
WIN-IPAL39BJJ1A.j1708a.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the cryptographic options
Select a cryptographic provider:
RSA#Microsoft 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.
Chọn các kiểu chứng chỉ
More about Cryptography
< Previous
Next >
Configure
Cancel


AD CS Configuration
CA Name
DESTINATION SERVER
WIN-IPAL39BJJ1A.j1708a.com
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:
Root CA
Distinguished name suffix:
DC=j1708a,DC=com
Preview of distinguished name:
CN=Root CA,DC=j1708a,DC=com
Đặt tên máy chủ, một số thông tin khác của máy chủ
More about CA Name
< Previous
Next >
Configure
Cancel

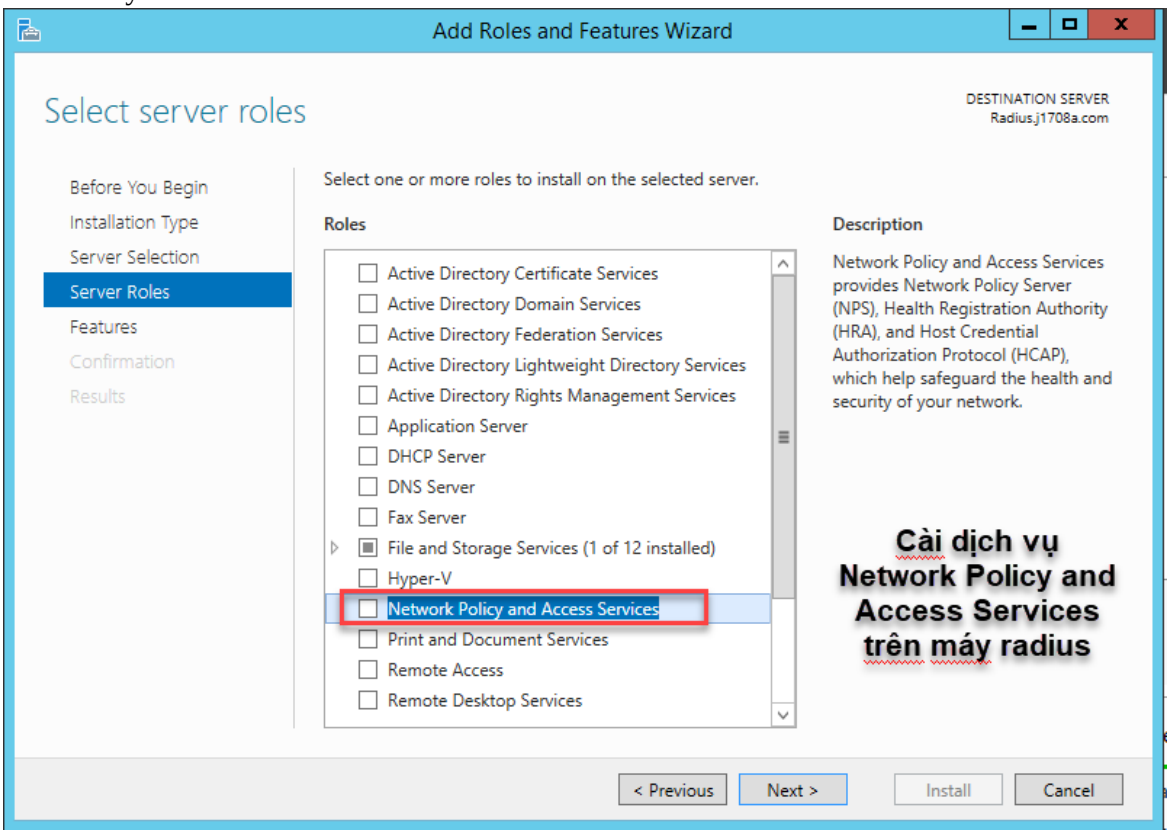

AD CS Configuration
Validity Period
DESTINATION SERVER
WIN-IPAL39BJJ1A.j1708a.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the validity period
Select the validity period for the certificate generated for this certification authority (CA):
5
Years
CA expiration Date: 10/17/2023 4:01:00 AM
The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.
Thời gian hiệu lực của máy Root CA
More about Validity Period
< Previous
Next >
Configure
Cancel

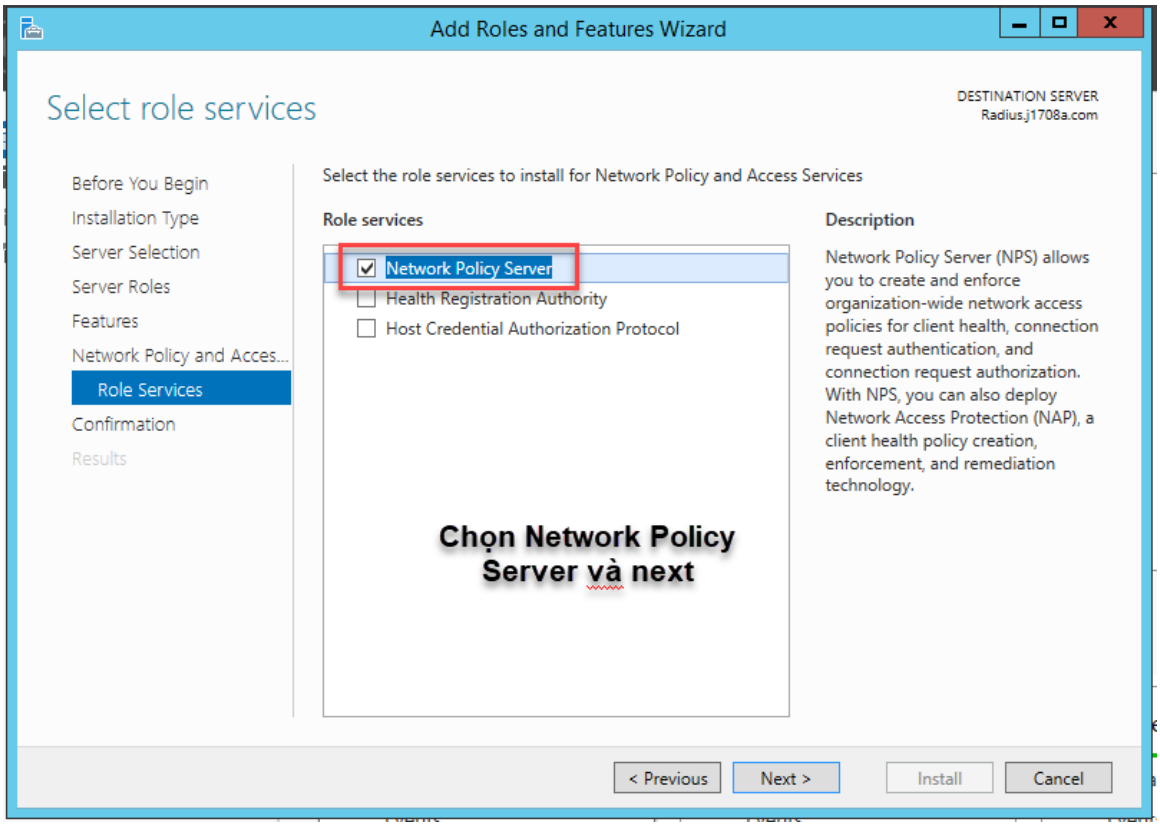

AD CS Configuration
CA Database
DESTINATION SERVER
WIN-IPAL39BJJ1A.j1708a.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the database locations
Certificate database location:
C:\Windows\system32\CertLog
Certificate database log location:
C:\Windows\system32\CertLog
Nơi lưu file log dịch vụ
More about CA Database
< Previous
Next >
Configure
Cancel

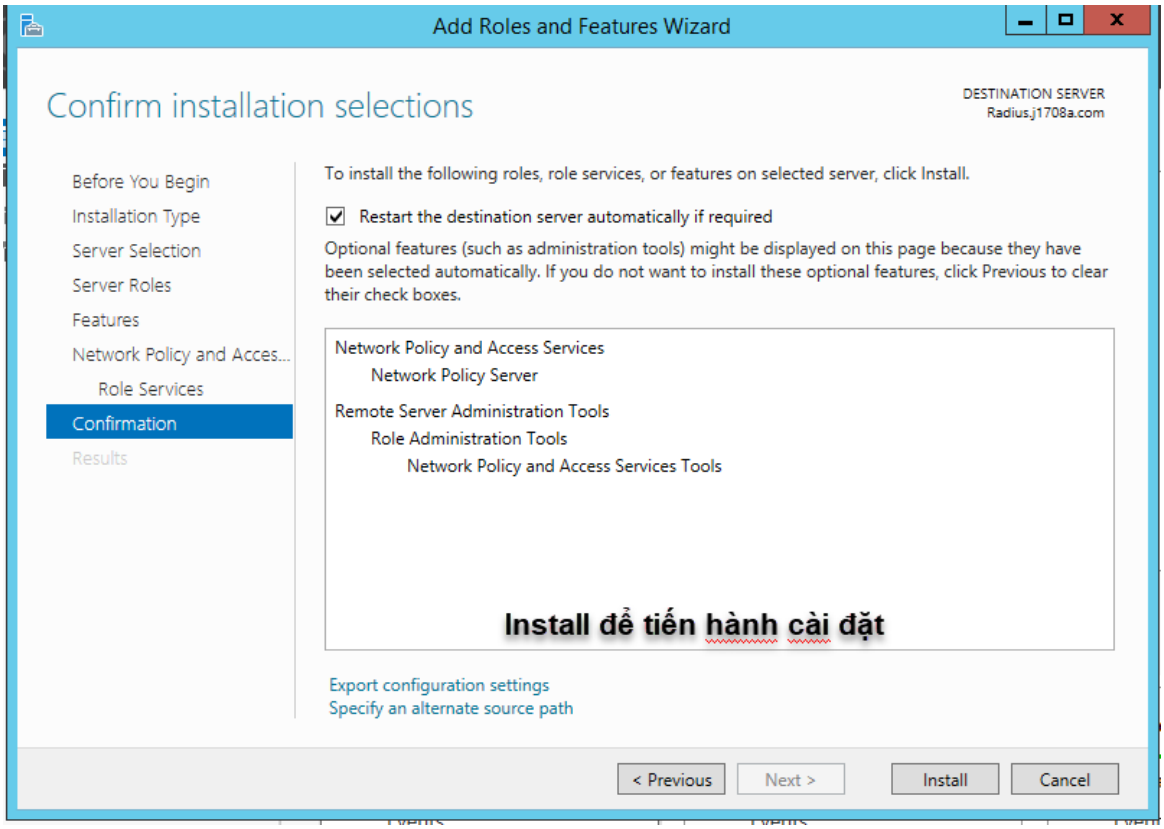

AD CS Configuration
Confirmation
DESTINATION SERVER
WIN-IPAL39BJJ1A.j1708a.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
To configure the following roles, role services, or features, click Configure.
Active Directory Certificate Services
Certification Authority
CA Type: Enterprise Root
Cryptographic provider: RSA#Microsoft Software Key Storage Provider
Hash Algorithm: SHA1
Key Length: 2048
Allow Administrator Interaction: Disabled
Certificate Validity Period: 10/17/2023 4:01:00 AM
Distinguished Name: CN=Root CA,DC=j1708a,DC=com
Certificate Database Location: C:\Windows\system32\CertLog
Certificate Database Log Location: C:\Windows\system32\CertLog
Certification Authority Web Enrollment
Configure để tiến hành cấu hình
< Previous
Next >
Configure
Cancel

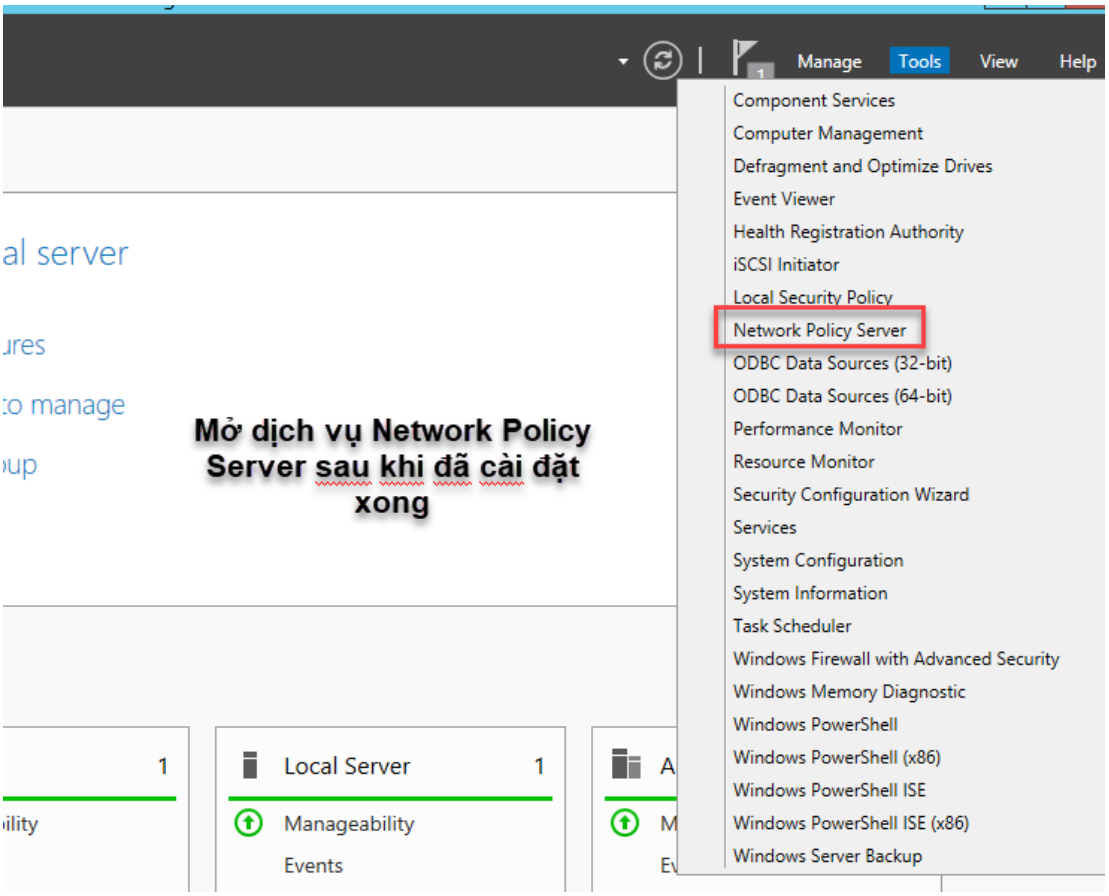


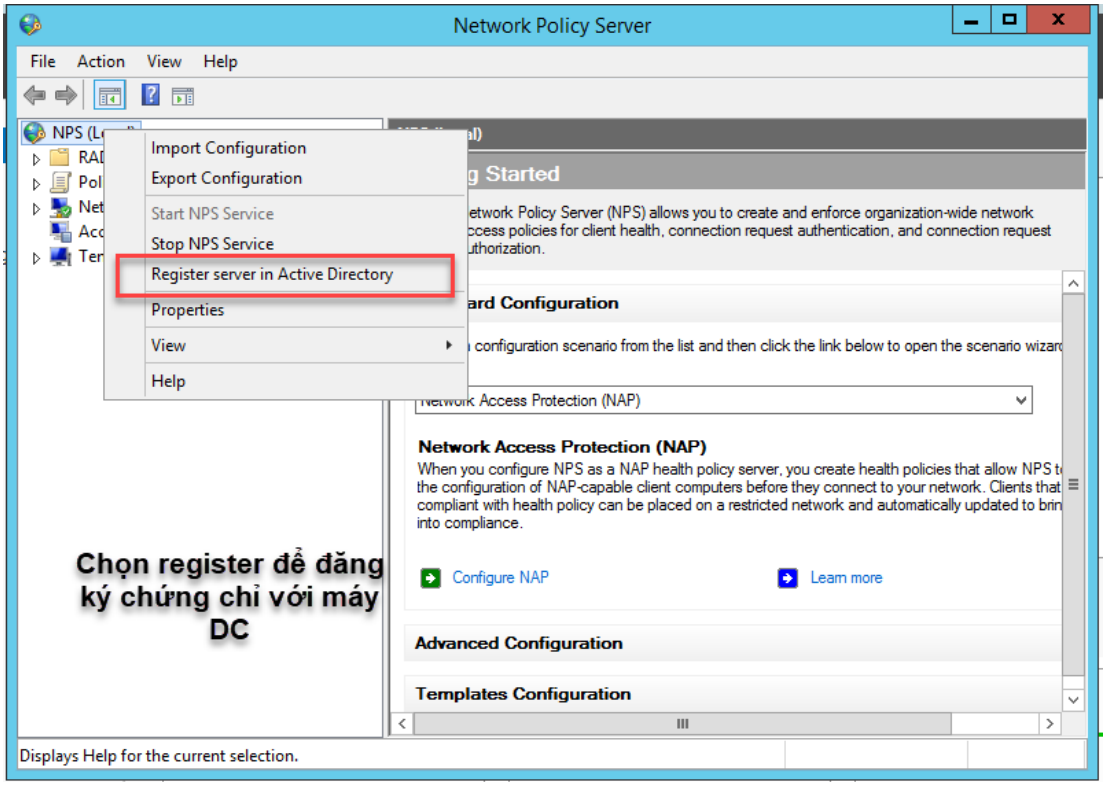
+ Trên máy RADIUS server

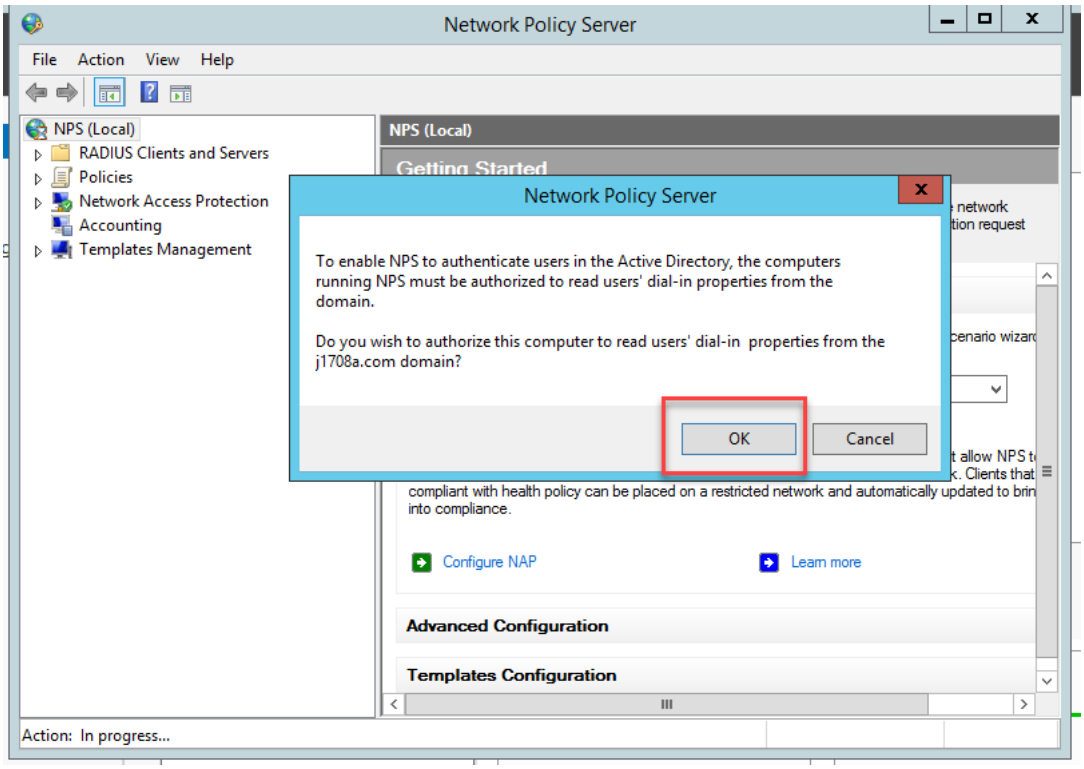


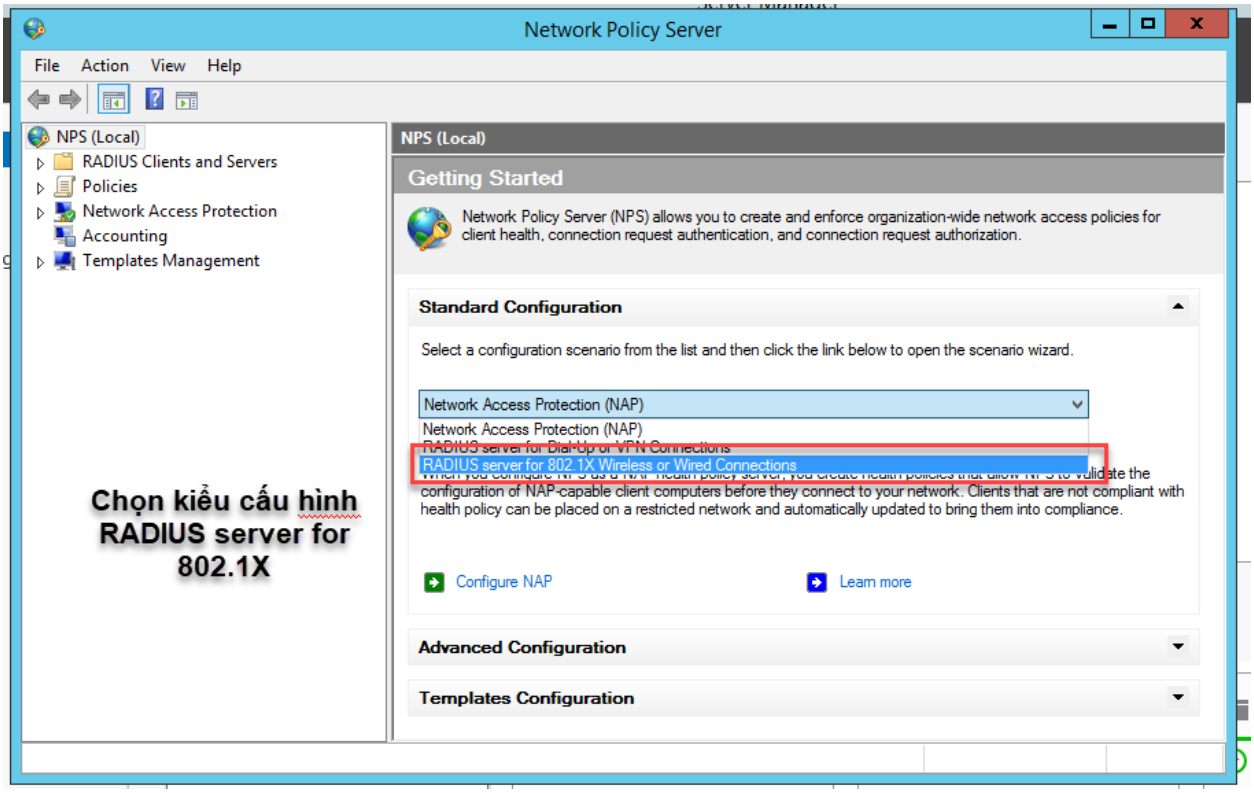

Add Roles and Features Wizard
Select role services
DESTINATION SERVER
Radius.j1708a.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Network Policy and Acces...
Role Services
Confirmation
Results
Select the role services to install for Network Policy and Access Services
Role services
Network Policy Server
Health Registration Authority
Host Credential Authorization Protocol
Description
Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization. With NPS, you can also deploy Network Access Protection (NAP), a client health policy creation, enforcement, and remediation technology.
Chọn Network Policy Server và next
< Previous
Next >
Install
Cancel

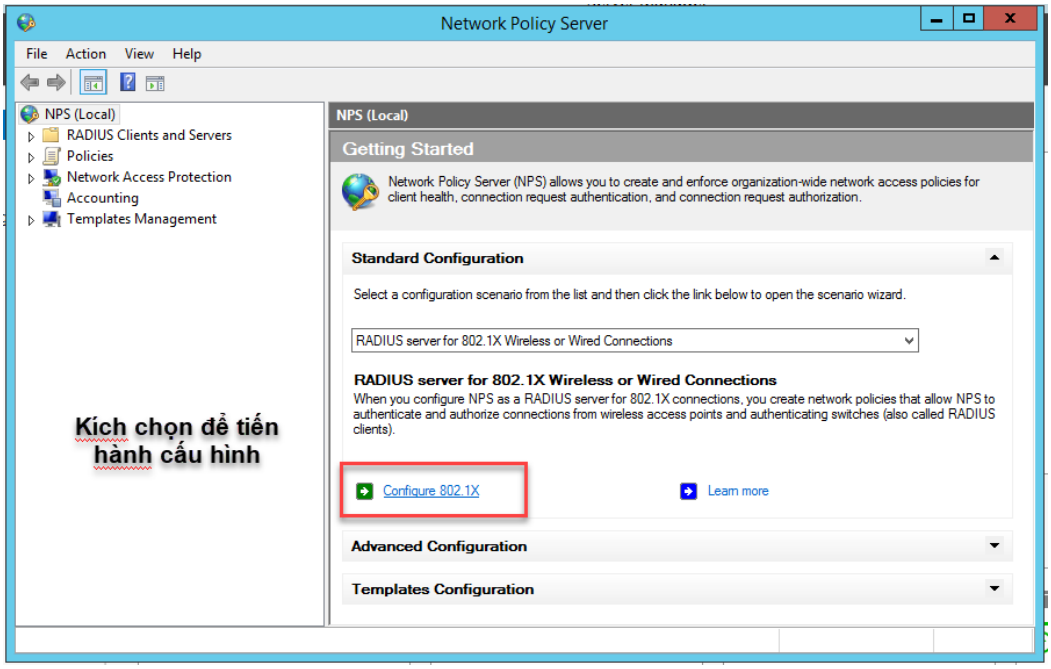

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
Radius.j1708a.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Network Policy and Acces...
Role Services
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Network Policy and Access Services
Network Policy Server
Remote Server Administration Tools
Role Administration Tools
Network Policy and Access Services Tools
Install để tiến hành cài đặt
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

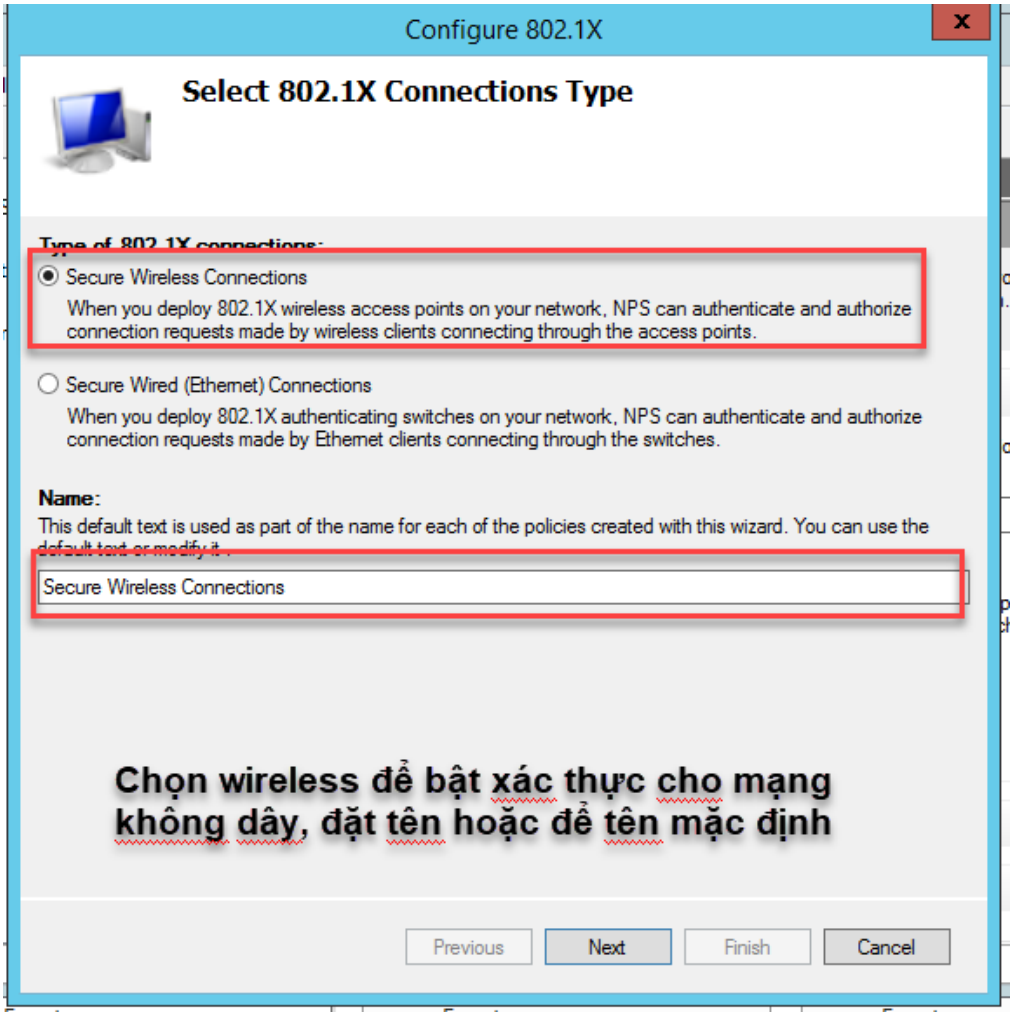

Manage
Tools
View
Help
Component Services
Computer Management
Defragment and Optimize Drives
Event Viewer
Health Registration Authority
iSCSI Initiator
Local Security Policy
Network Policy Server
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor
Security Configuration Wizard
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup
Local Server
1
Manageability
Events
Mở dịch vụ Network Policy Server sau khi đã cài đặt xong

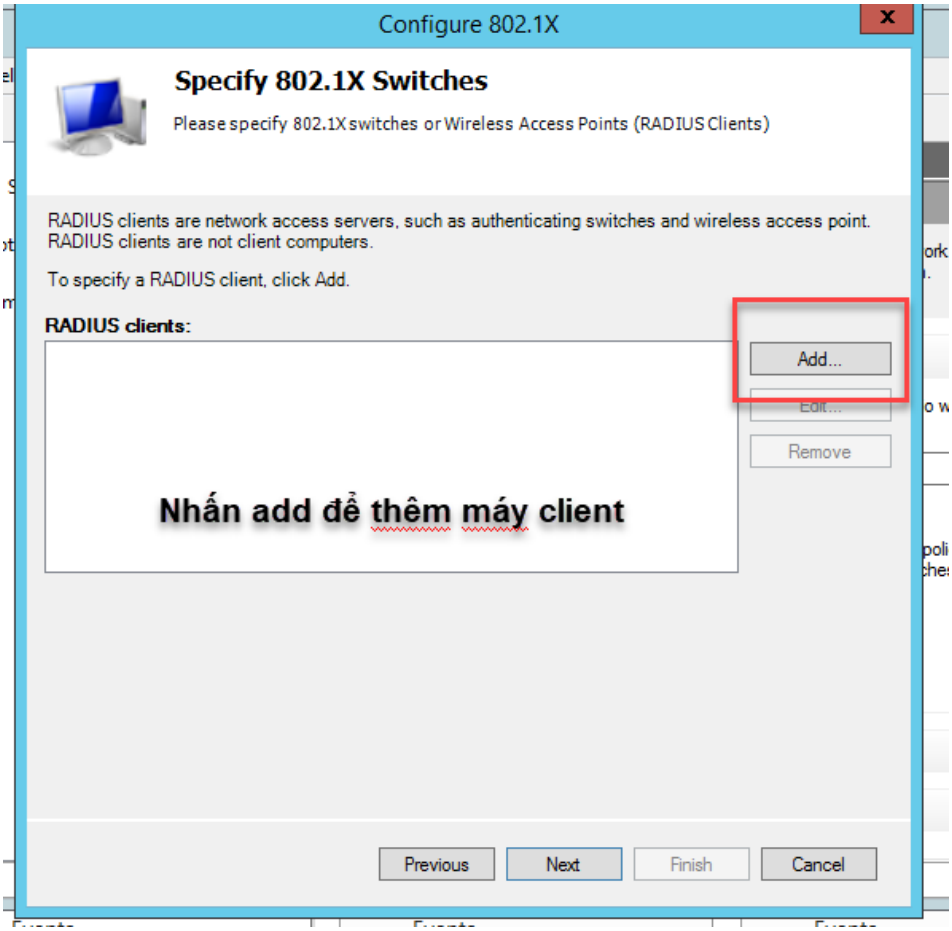

Network Policy Server
File
Action
View
Help
Import Configuration
Export Configuration
Start NPS Service
Stop NPS Service
Register server in Active Directory
Properties
View
Help
Network Access Protection (NAP)
Configure NAP
Learn more
Advanced Configuration
Templates Configuration
Displays Help for the current selection.
Chọn register để đăng ký chứng chỉ với máy DC

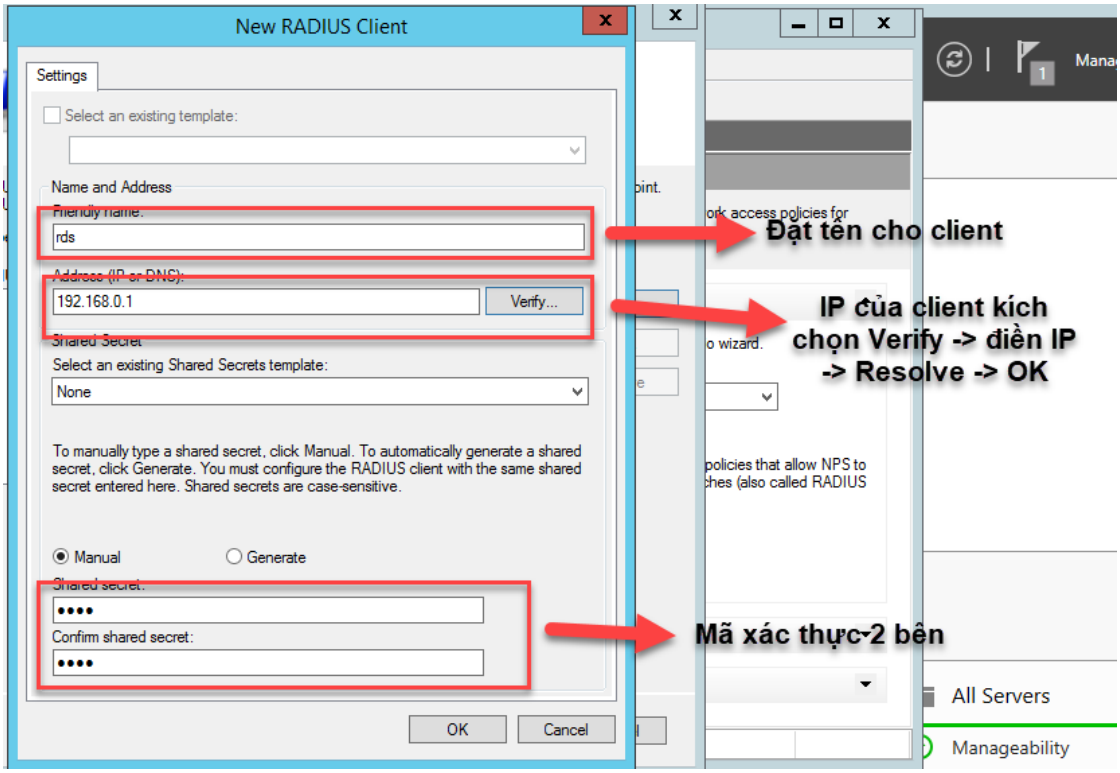

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
Policies
Network Access Protection
Accounting
Templates Management
NPS (Local)
Getting Started
Network Policy Server
To enable NPS to authenticate users in the Active Directory, the computers running NPS must be authorized to read users' dial-in properties from the domain.
Do you wish to authorize this computer to read users' dial-in properties from the j1708a.com domain?
OK
Cancel
compliant with health policy can be placed on a restricted network and automatically updated to brin into compliance.
Configure NAP
Learn more
Advanced Configuration
Templates Configuration
Action: In progress...

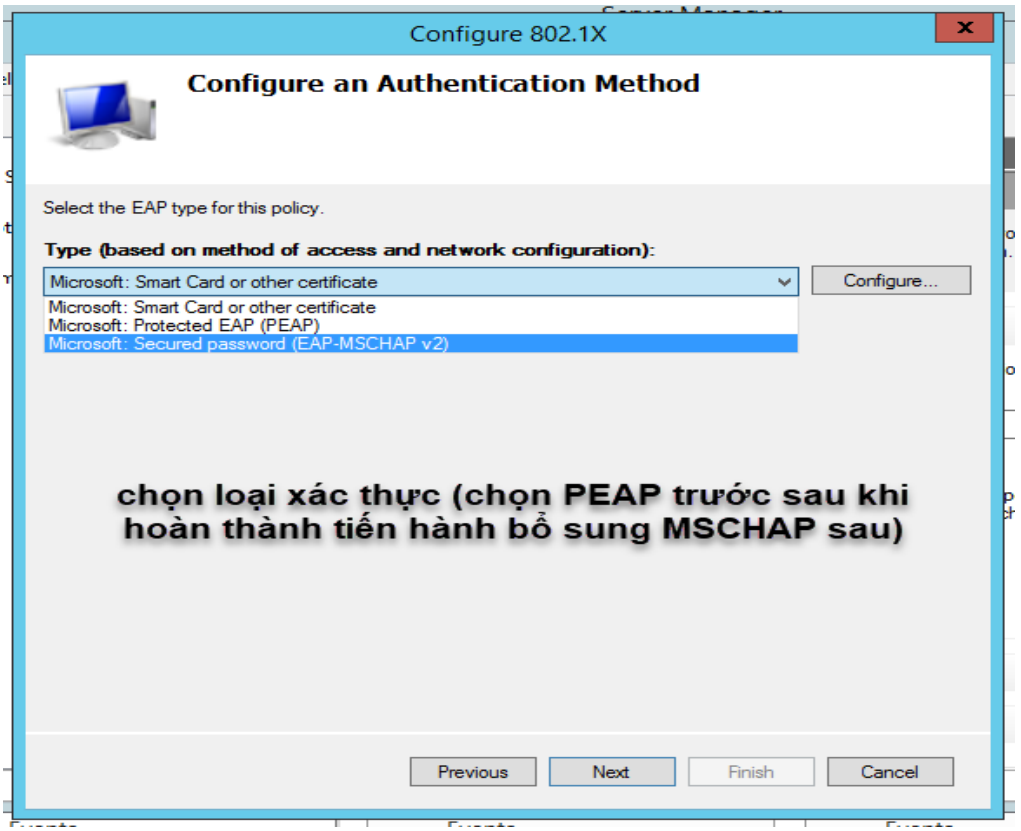

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
Policies
Network Access Protection
Accounting
Templates Management
NPS (Local)
Getting Started
Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.
Standard Configuration
Select a configuration scenario from the list and then click the link below to open the scenario wizard.
Network Access Protection (NAP)
Network Access Protection (NAP)
RADIUS server for 802.1X Wireless or Wired Connections
configuration of NAP-capable client computers before they connect to your network. Clients that are not compliant with health policy can be placed on a restricted network and automatically updated to bring them into compliance.
Configure NAP
Learn more
Advanced Configuration
Templates Configuration
Chọn kiểu cấu hình RADIUS server for 802.1X

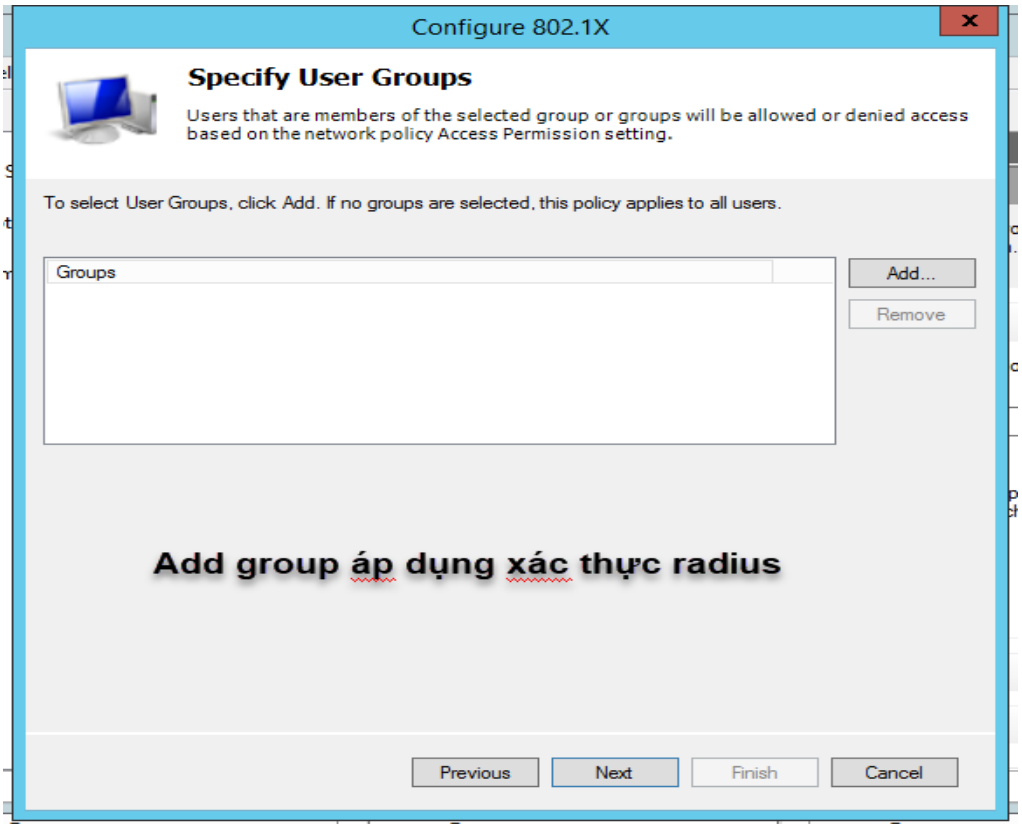

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
Policies
Network Access Protection
Accounting
Templates Management
NPS (Local)
Getting Started
Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.
Standard Configuration
Select a configuration scenario from the list and then click the link below to open the scenario wizard.
RADIUS server for 802.1X Wireless or Wired Connections
RADIUS server for 802.1X Wireless or Wired Connections
When you configure NPS as a RADIUS server for 802.1X connections, you create network policies that allow NPS to authenticate and authorize connections from wireless access points and authenticating switches (also called RADIUS clients).
Configure 802.1X
Learn more
Advanced Configuration
Templates Configuration
Kích chọn để tiến hành cấu hình

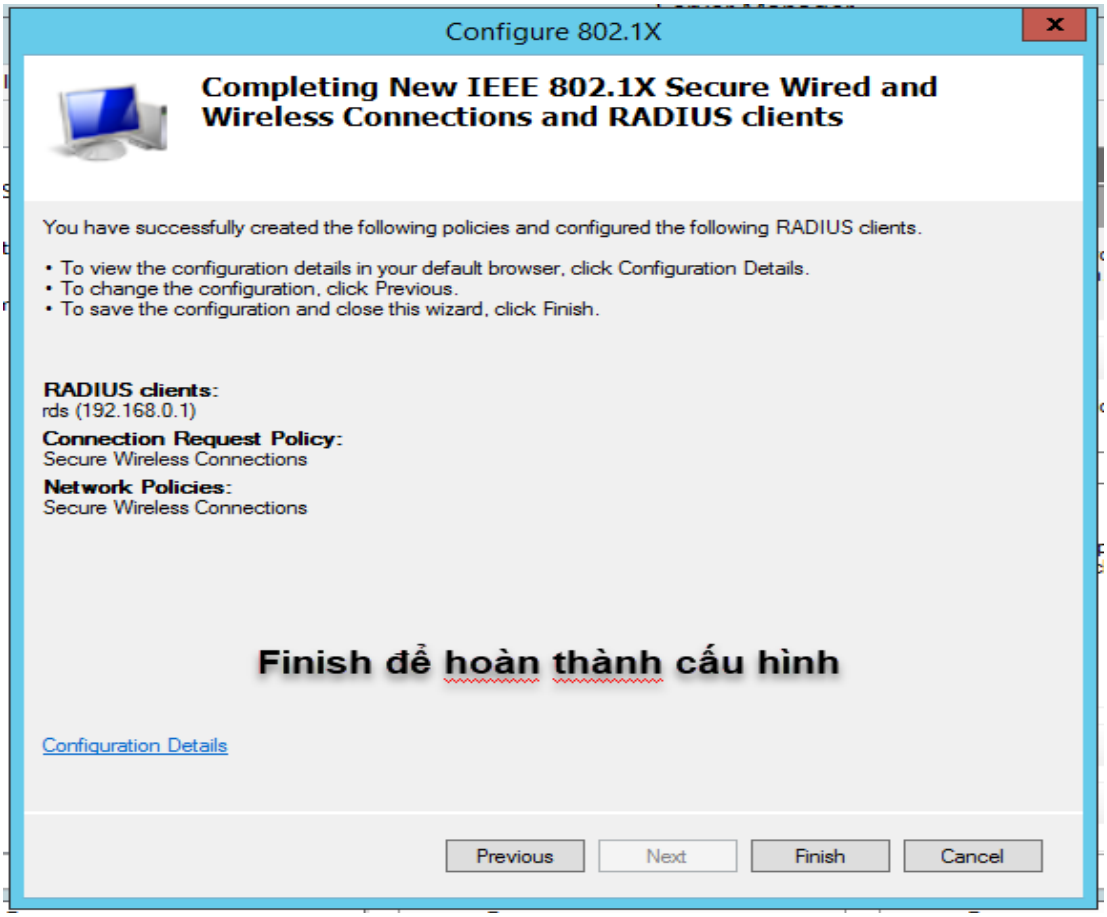

Configure 802.1X
Select 802.1X Connections Type
Type of 802.1X connections:
Secure Wireless Connections
When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize connection requests made by wireless clients connecting through the access points.
Secure Wired (Ethernet) Connections
When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethernet clients connecting through the switches.
Name:
This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it.
Secure Wireless Connections
Chọn wireless để bật xác thực cho mạng không dây, đặt tên hoặc để tên mặc định
Previous
Next
Finish
Cancel

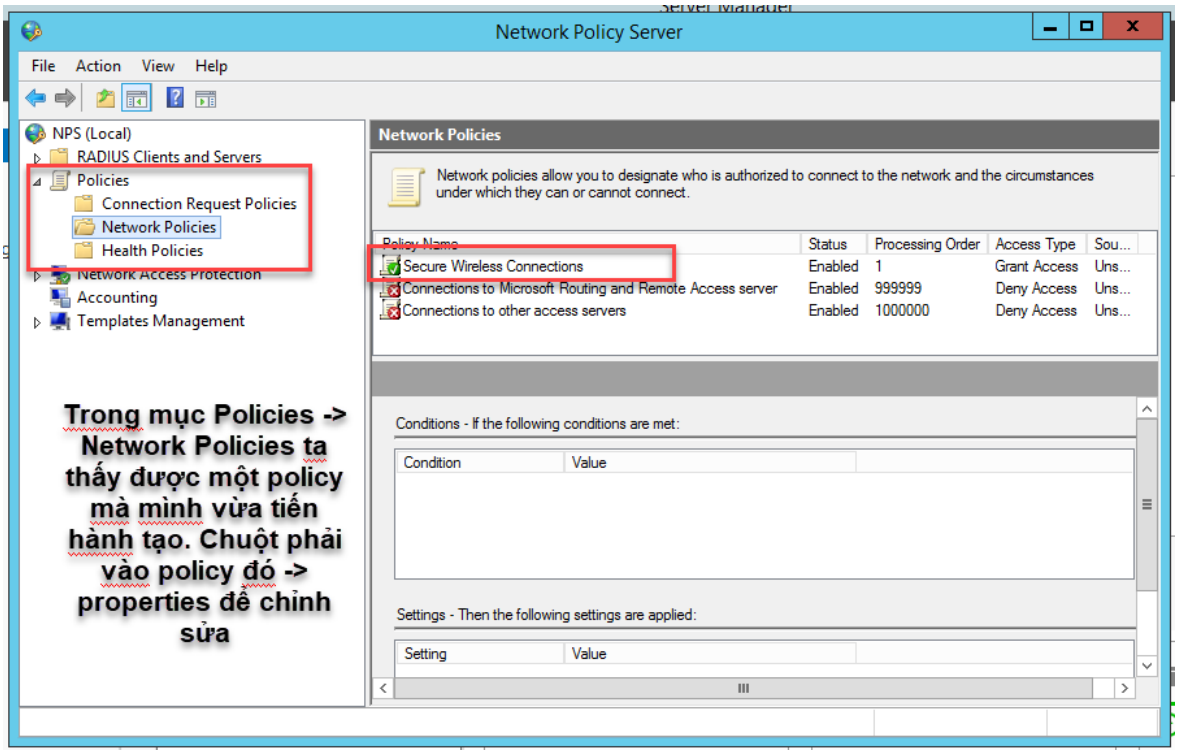

Configure 802.1X
Specify 802.1X Switches
Please specify 802.1X switches or Wireless Access Points (RADIUS Clients)
RADIUS clients are network access servers, such as authenticating switches and wireless access point. RADIUS clients are not client computers.
To specify a RADIUS client, click Add.
RADIUS clients:
Add...
Edit...
Remove
Nhấn add để thêm máy client
Previous
Next
Finish
Cancel

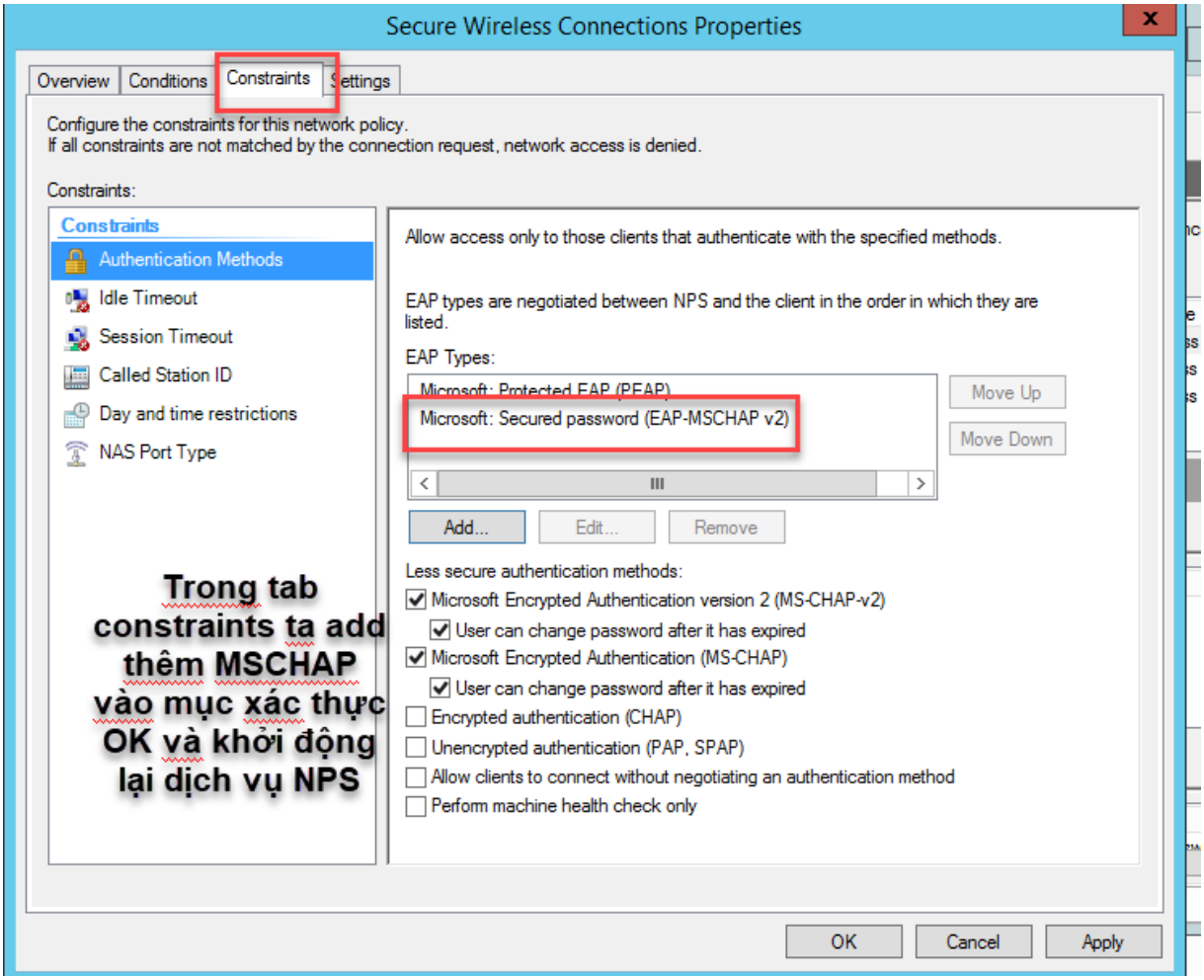

New RADIUS Client
Settings
Select an existing template:
Name and Address
Friendly name:
rds
Address (IP or DNS):
192.168.0.1
Verify...
Shared Secret
Select an existing Shared Secrets template:
None
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
Manual
Generate
Shared secret:
Confirm shared secret:
OK
Cancel
Đặt tên cho client
IP của client kích chọn Verify -> điền IP -> Resolve -> OK
Mã xác thực 2 bên
All Servers
Manageability


Configure 802.1X
Configure an Authentication Method
Select the EAP type for this policy.
Type (based on method of access and network configuration):
Microsoft: Smart Card or other certificate
Configure...
Microsoft: Smart Card or other certificate
Microsoft: Protected EAP (PEAP)
Microsoft: Secured password (EAP-MSCHAP v2)
chọn loại xác thực (chọn PEAP trước sau khi hoàn thành tiến hành bổ sung MSCHAP sau)
Previous
Next
Finish
Cancel

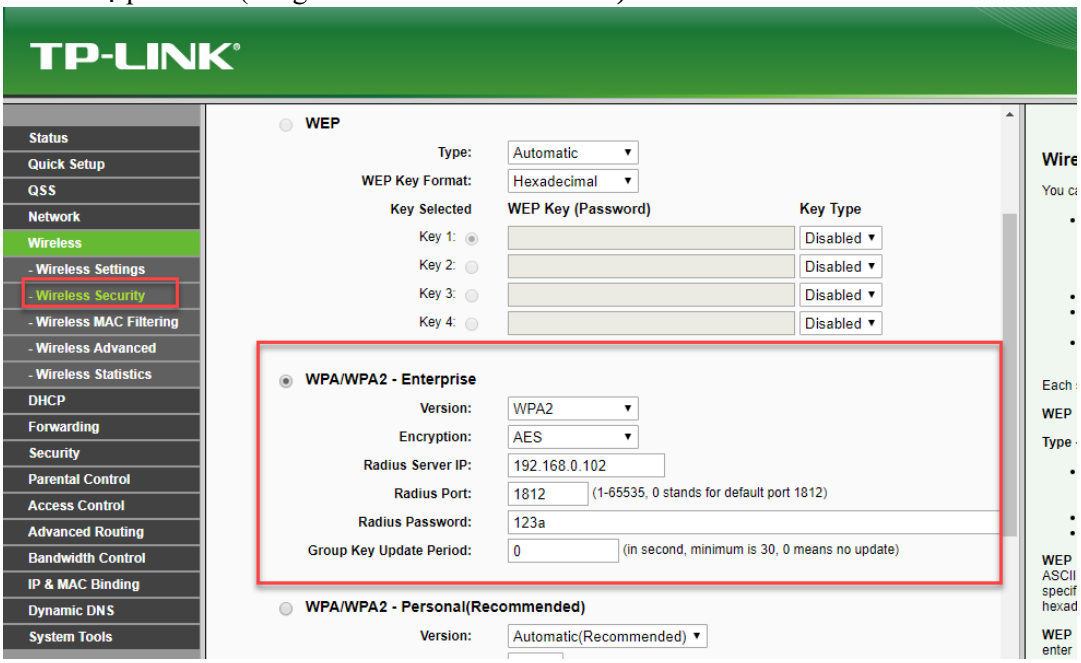

Configure 802.1X
Specify User Groups
Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.
To select User Groups, click Add. If no groups are selected, this policy applies to all users.
Groups
Add...
Remove
Add group áp dụng xác thực radius
Previous
Next
Finish
Cancel


Configure 802.1X
Completing New IEEE 802.1X Secure Wired and Wireless Connections and RADIUS clients
You have successfully created the following policies and configured the following RADIUS clients.
• To view the configuration details in your default browser, click Configuration Details.
• To change the configuration, click Previous.
• To save the configuration and close this wizard, click Finish.
RADIUS clients:
rds (192.168.0.1)
Connection Request Policy:
Secure Wireless Connections
Network Policies:
Secure Wireless Connections
Finish để hoàn thành cấu hình
Configuration Details
Previous
Next
Finish
Cancel


Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Templates Management
Network Policies
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.
Policy Name
Status
Processing Order
Access Type
Secure Wireless Connections
Enabled
1
Grant Access
Connections to Microsoft Routing and Remote Access server
Enabled
999999
Deny Access
Connections to other access servers
Enabled
1000000
Deny Access
Conditions - If the following conditions are met:
Condition
Value
Settings - Then the following settings are applied:
Setting
Value
Trong mục Policies -> Network Policies ta thấy được một policy mà mình vừa tiến hành tạo. Chuột phải vào policy đó -> properties để chỉnh sửa



+ Trên bộ phát wifi (đóng vai trò là các radius client)



+ Cấu hình phát wifi.Trong mục wireless security chọn kiểu xác thực WPA/WPA2 – enterprise điền địa chỉ IP của máy radius server, điền pass xác thực và tiến hành lưu lại cấu hình.
+ Đăng nhập vào wifi bằng user đã được tạo trong group wifi