Wireless 802.1x authentication integration with NPS

Implementation Cookbook

Document Version: V1.0
Date: 2023.10.19

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

- The official website of Ruijie Reyee: https://www.ruijienetworks.com/products/reyee
- Technical Support Website: https://www.ruijienetworks.com/support
- Case Portal: https://caseportal.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com

Conventions

1. GUI Symbols

Interface symbol	Description	Example
Boldface	1. Button names 2. Window names, tab name, field name and menu items 3. Link	1. Click **OK**. 2. Select **Config Wizard**. 3. Click the **Download File** link.
>	Multi-level menus items	Select **System** > **Time**.

2. Signs

This document also uses signs to indicate some important points during the operation. The meanings of these signs are as follows:

Warning

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

Note

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Instruction

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

An alert that contains a description of product or version support.

3. Instruction

This manual is used to guide users to understand the product, install the product, and complete the configuration.

- The example of the port type may be different from the actual situation. Please proceed with configuration according to the port type supported by the product.
- The example of display information may contain the content of other product series (such as model and description). Please refer to the actual display information.
- The routers and router product icons involved in this manual represent common routers and layer-3 switches running routing protocols.

Contents

1 NPS Server Deployment

This chapter will introduce how to deploy a NPS server on Windows Server 2008 R2 Enterprise to integrate AD domain authentication and Wireless dot1x authentication. AD domain server, AD license server, DNS server, WEB server (IIS) and NPS server.

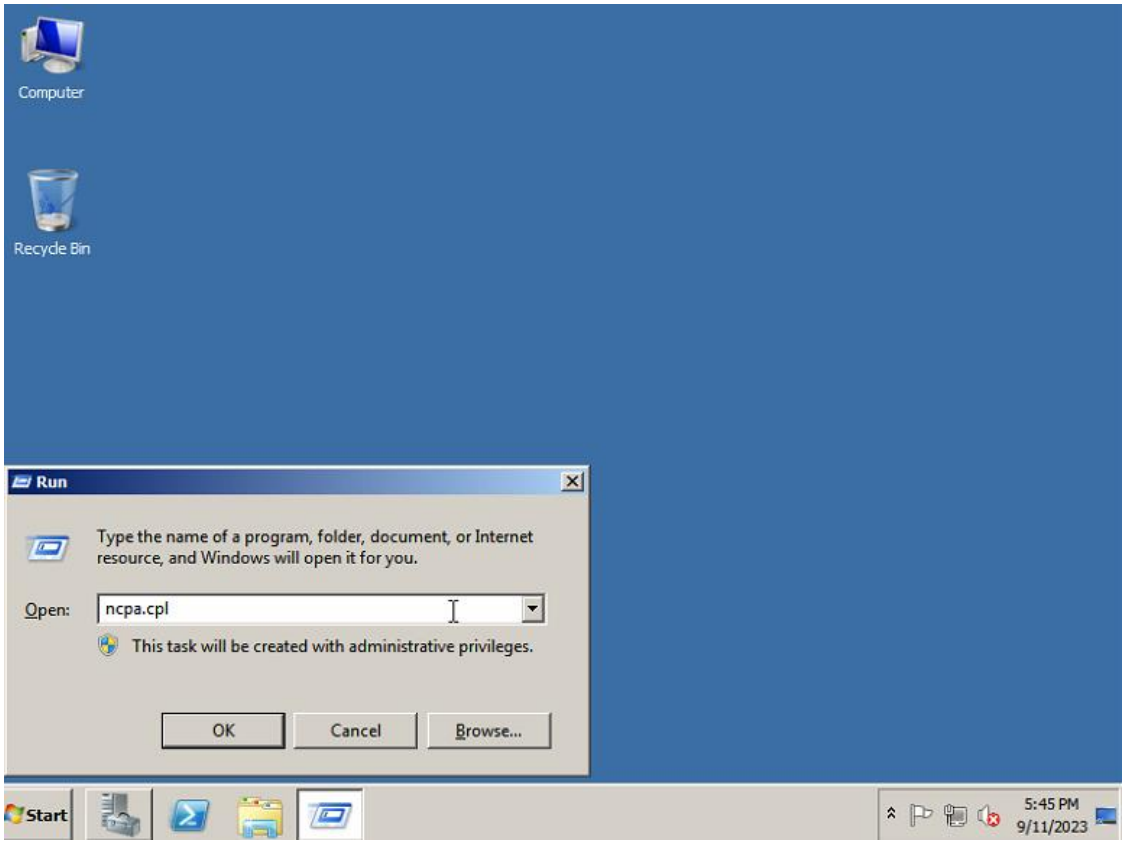
1.1 Operating System of NPS Server

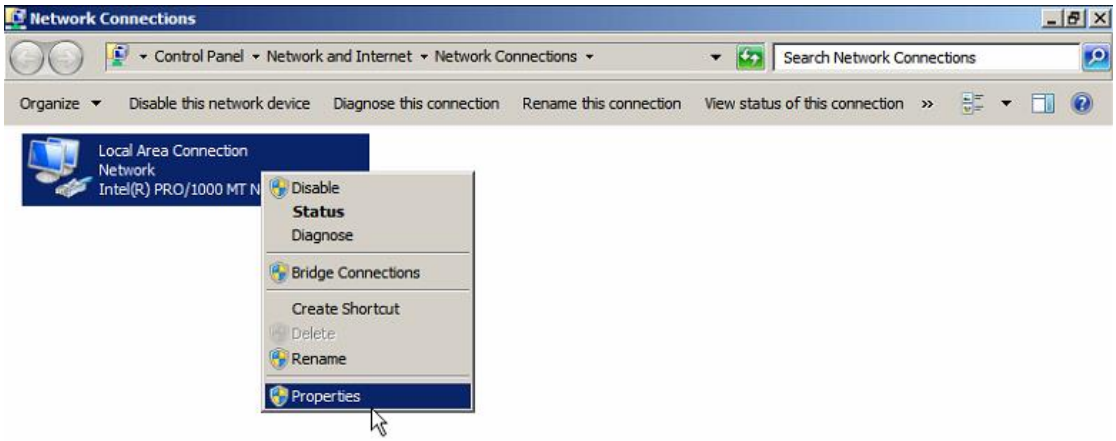
Server Type	Operating System	Note
Windows NPS Server	Windows Server 2008 R2 Enterprise	Provide certificate application, issuance, revocation and other services

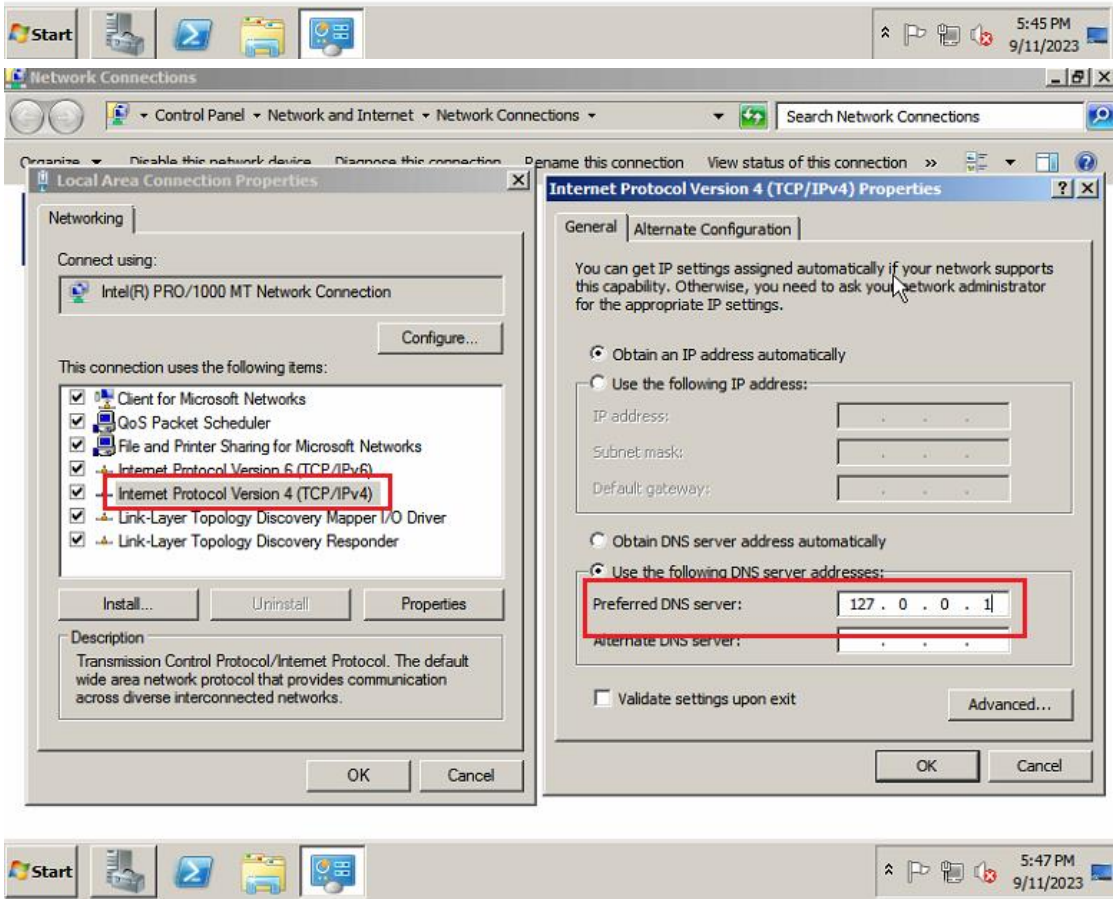
1.2 Install AD Domain Server

1.2.1 Change the DNS address of the server

Open WIN+R and input ‘ncpa.cpl’ to enter ‘Network Connection’ page. Choose the NIC and enter the configuration page by click ‘Properties’ to change the preferred DNS server as the local IP address: 127.0.0.1

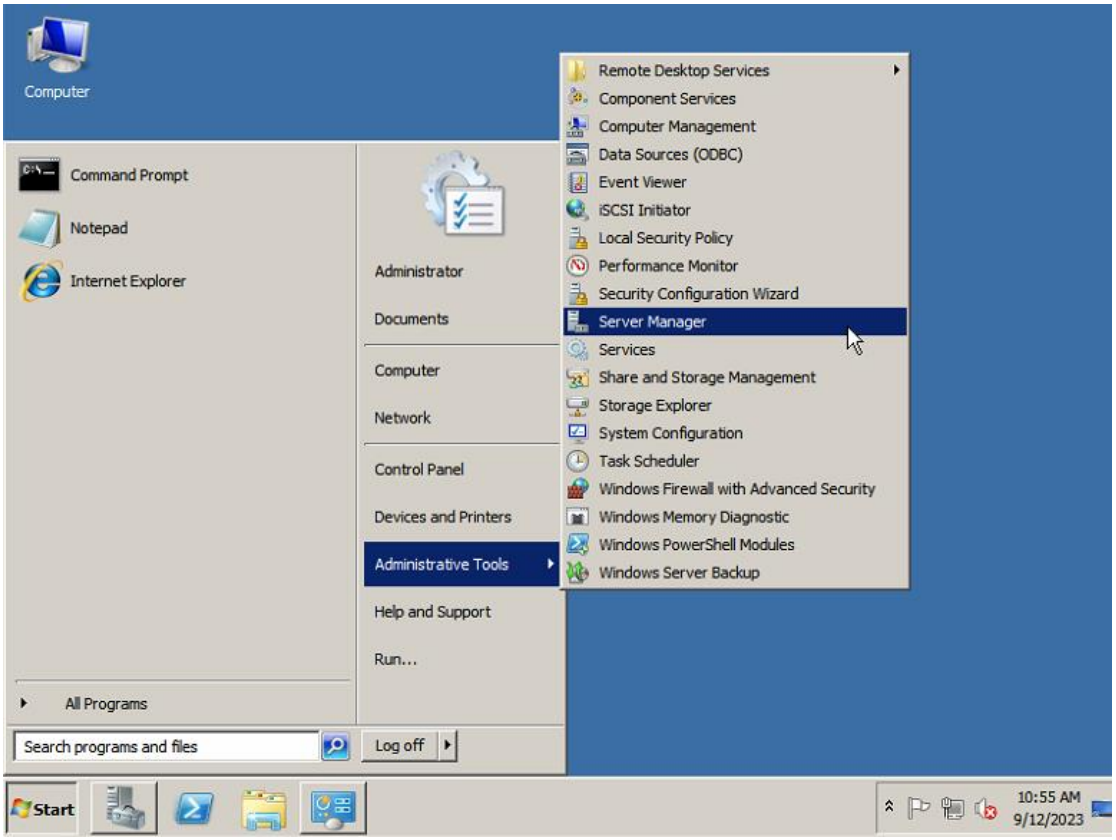



Network Connections
Control Panel ▸ Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Local Area Connection
Network
Intel(R) PRO/1000 MT N
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties

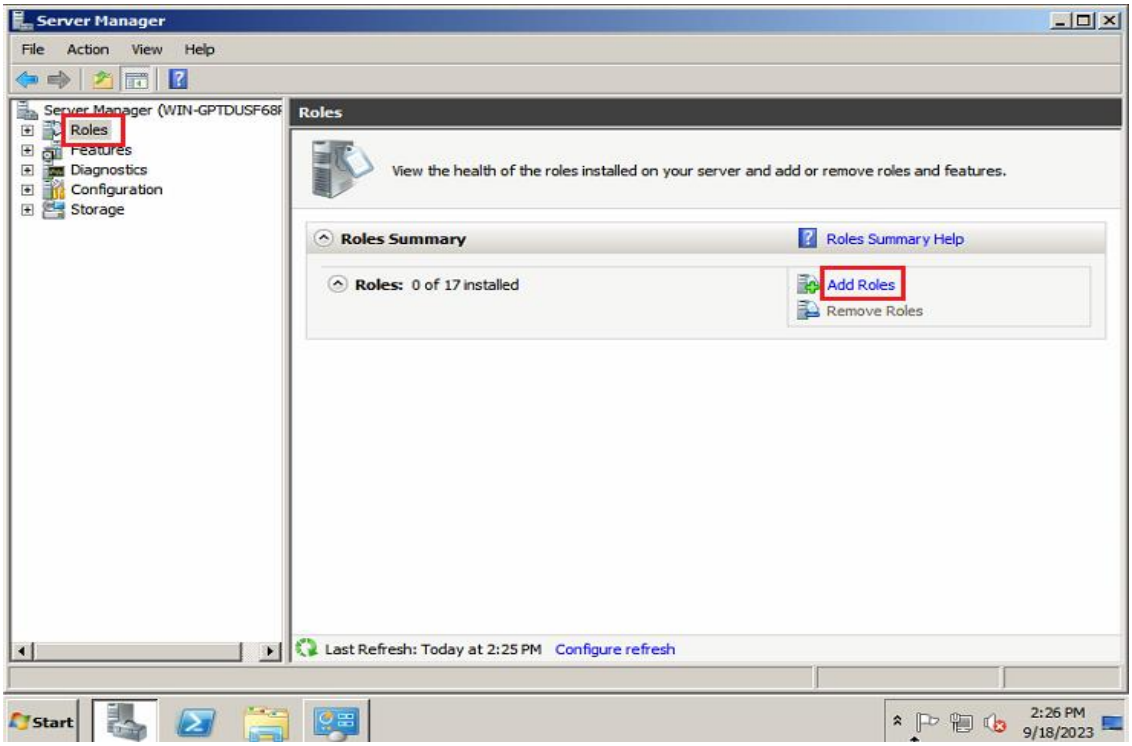

Start
5:45 PM
9/11/2023
Network Connections
Control Panel ▸ Network and Internet ▸ Network Connections ▸
Search Network Connections
Local Area Connection Properties
Networking
Connect using:
Intel(R) PRO/1000 MT Network Connection
Configure...
This connection uses the following items:
Client for Microsoft Networks
QoS Packet Scheduler
File and Printer Sharing for Microsoft Networks
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 127 . 0 . 0 . 1
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
Start
5:47 PM
9/11/2023

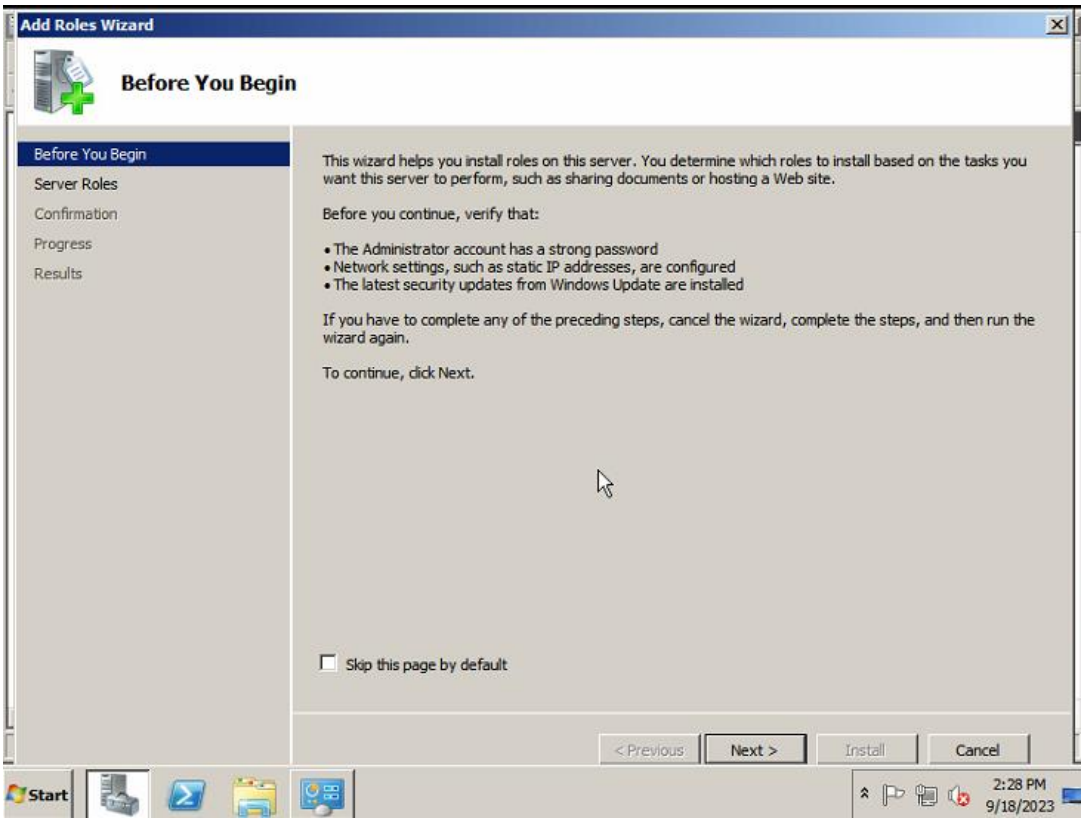
1.2.2 Add roles for ‘Active Directory Domain Server’

Click “[Start>>[Administrative Tools] >>[Server Manager]” and click [Roles] in the left menus and then click ‘Add Roles’

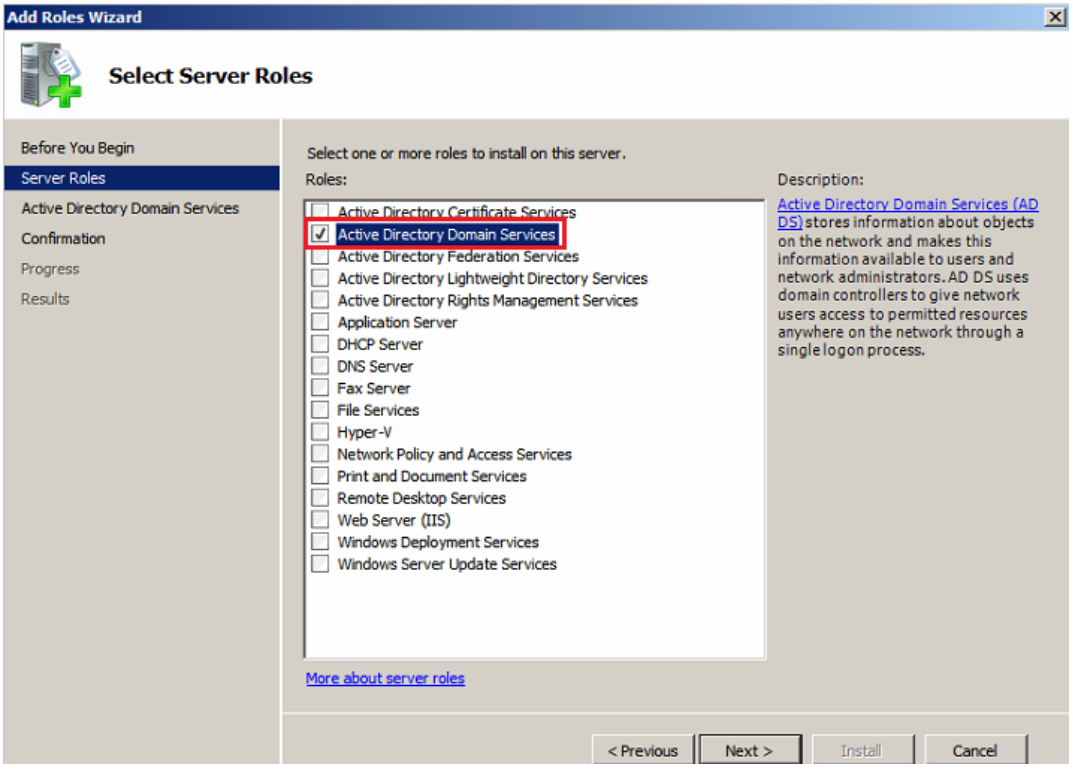


Click “Add Roles”

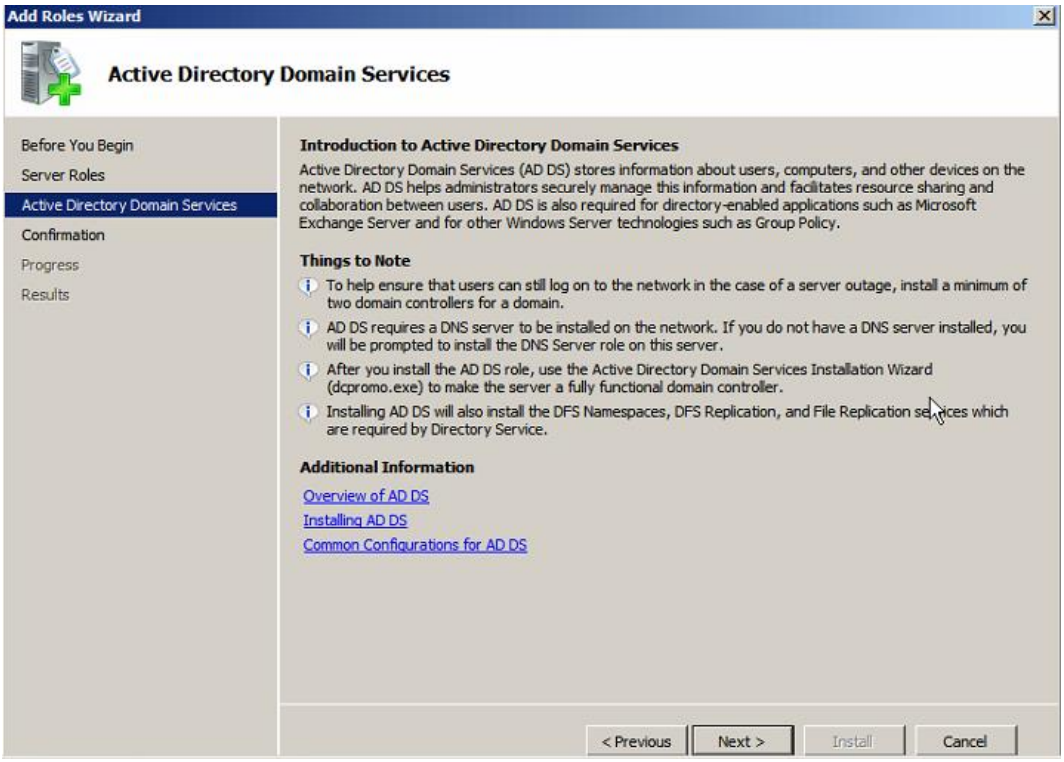




(1) Select 'Active Directory Domain Services' and click 'Next'

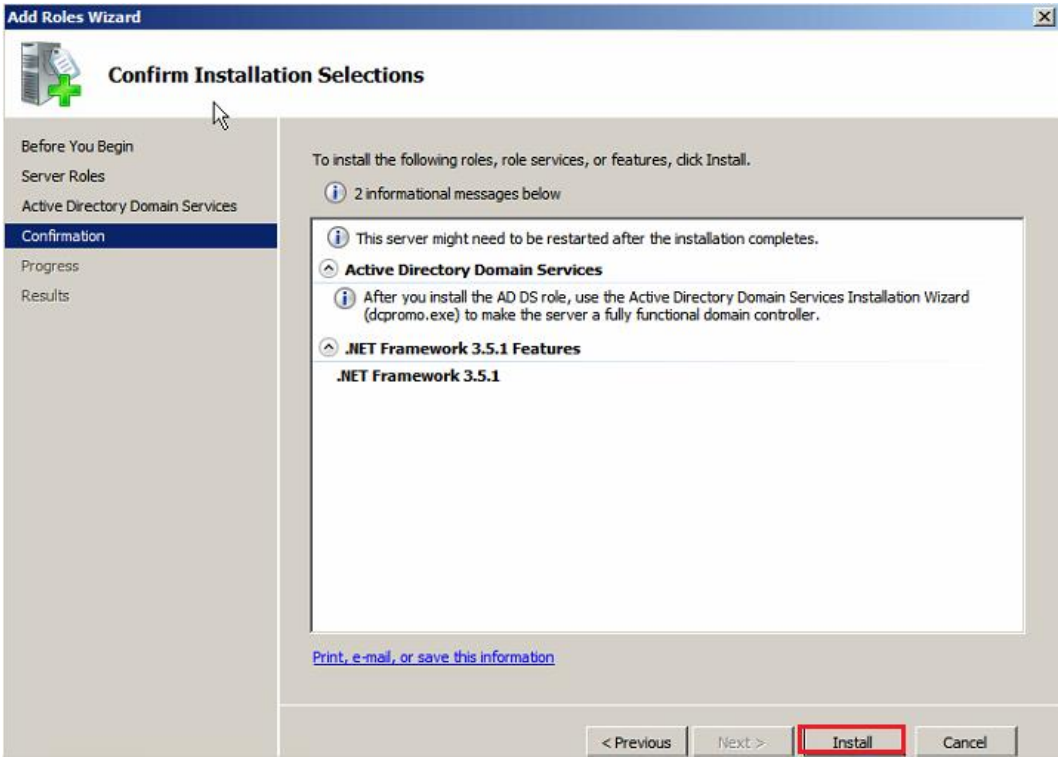


Select Server Roles

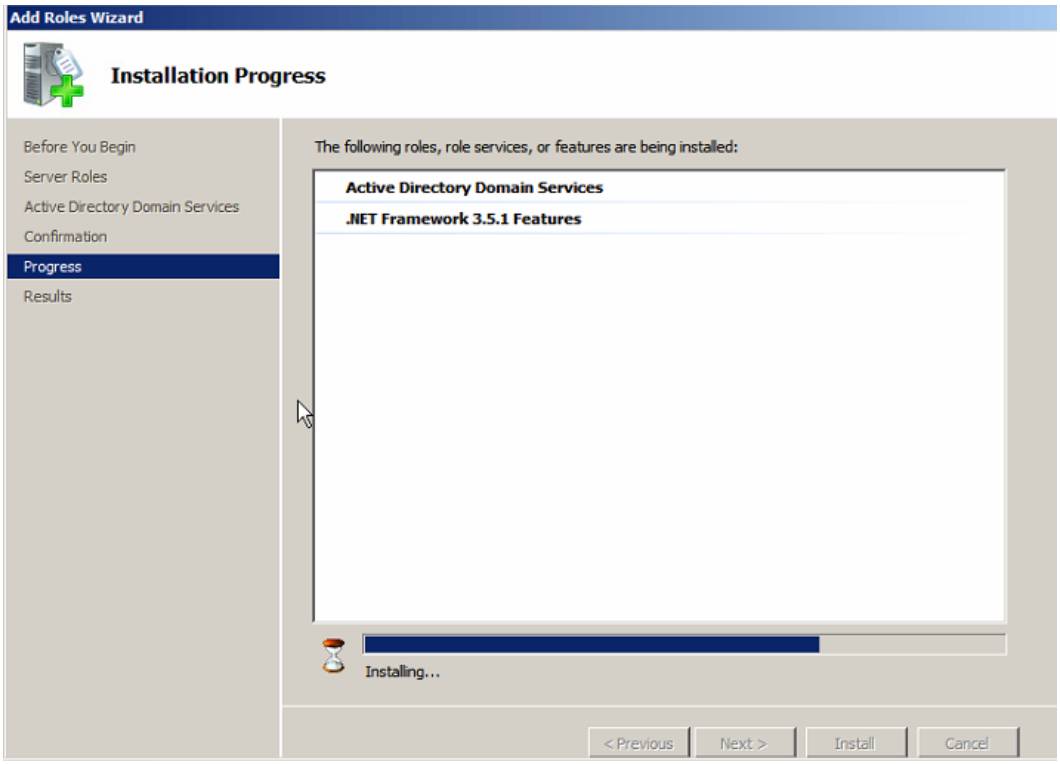


Active Directory Domain Services Introduction

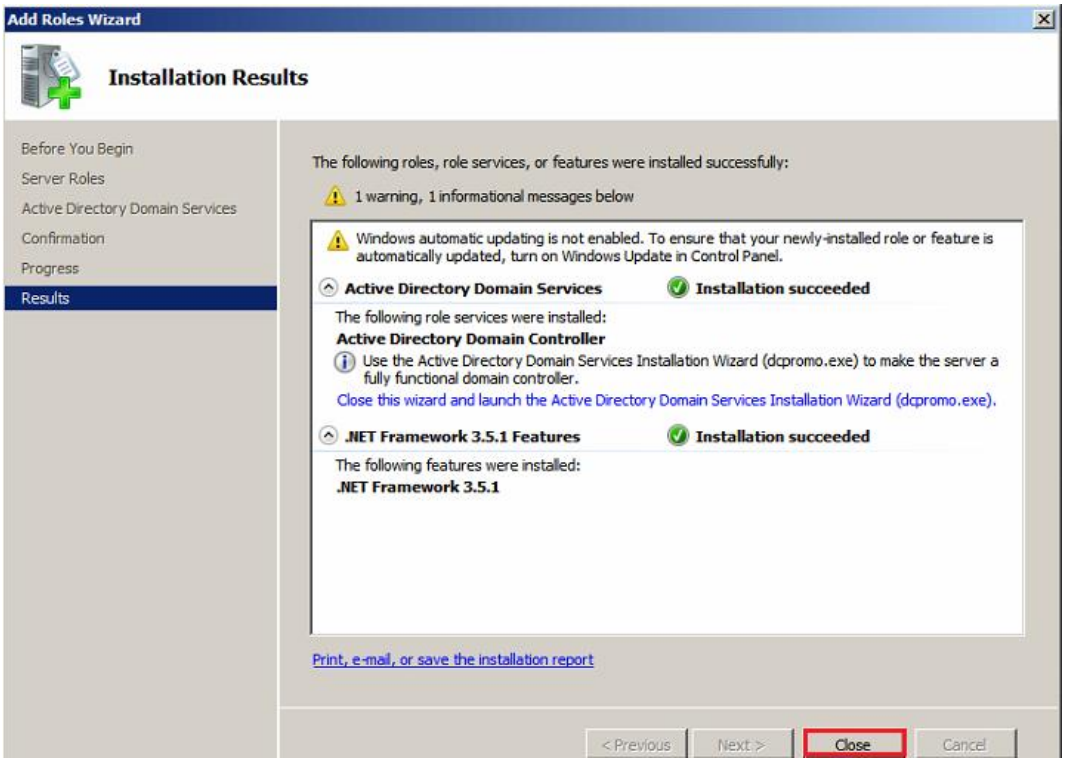
(2) Click 'Install' to install domain services



Confirm Installation Selections



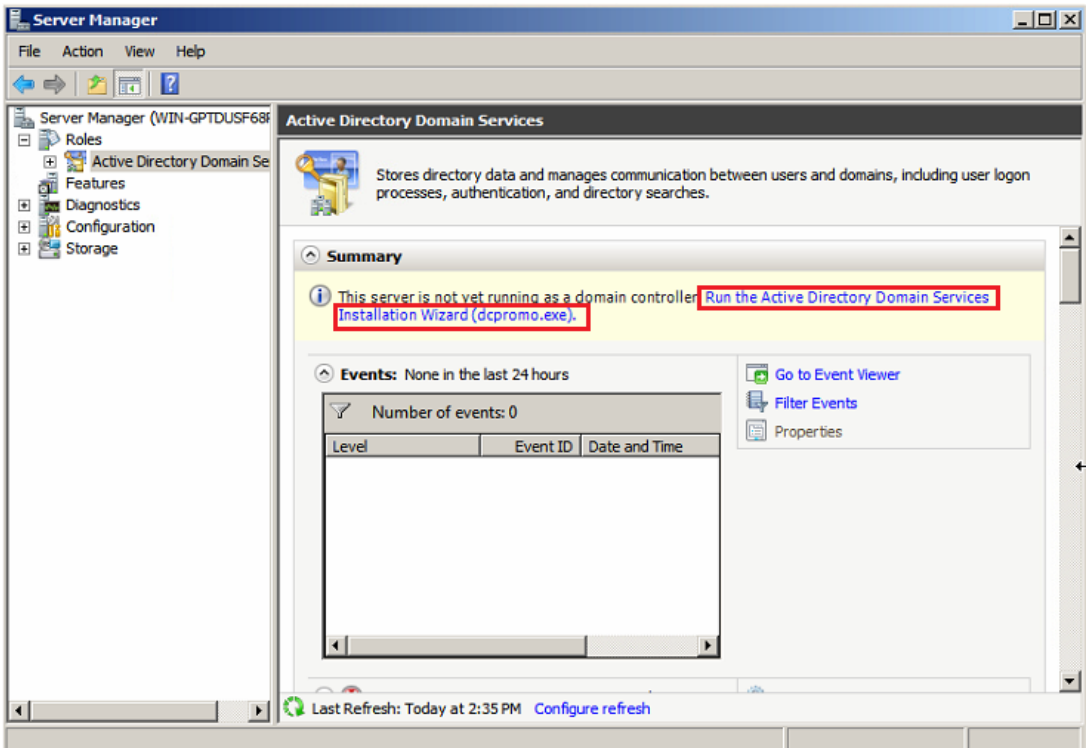
(3) Click ‘Close’ after Domain Services is installed



Installation Results

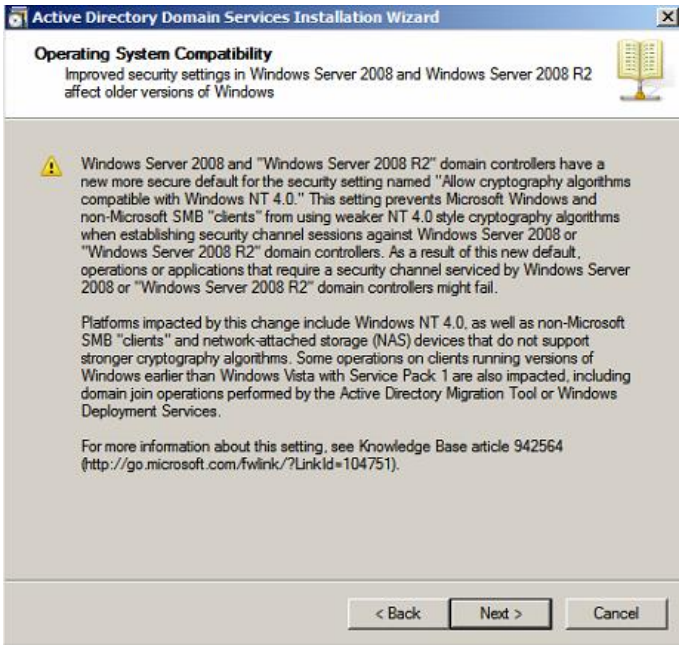
1.2.3 Install Active Directory Domain Controller

(1) [Active Directory Domain Services Installation Wizard] to click User Advanced Mode Installation’



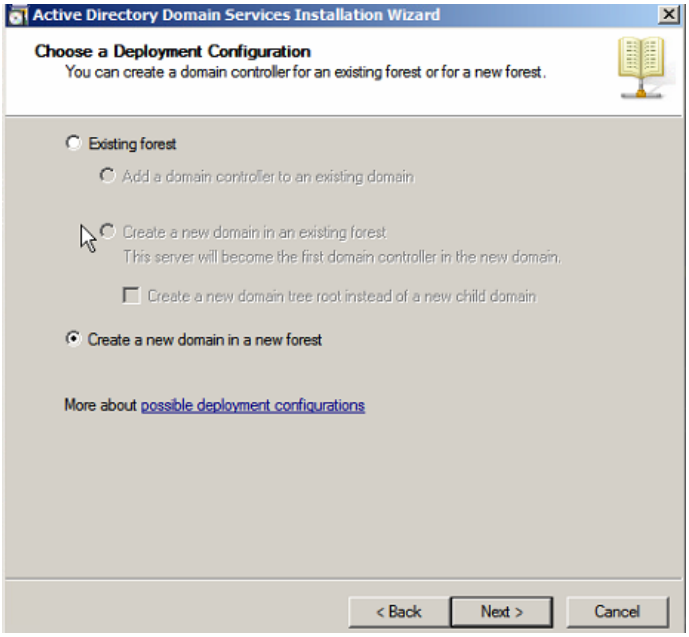
Select "Use advanced mode installation"

(2) Click 'Next' after the 'Operating System Compatibility' pops up



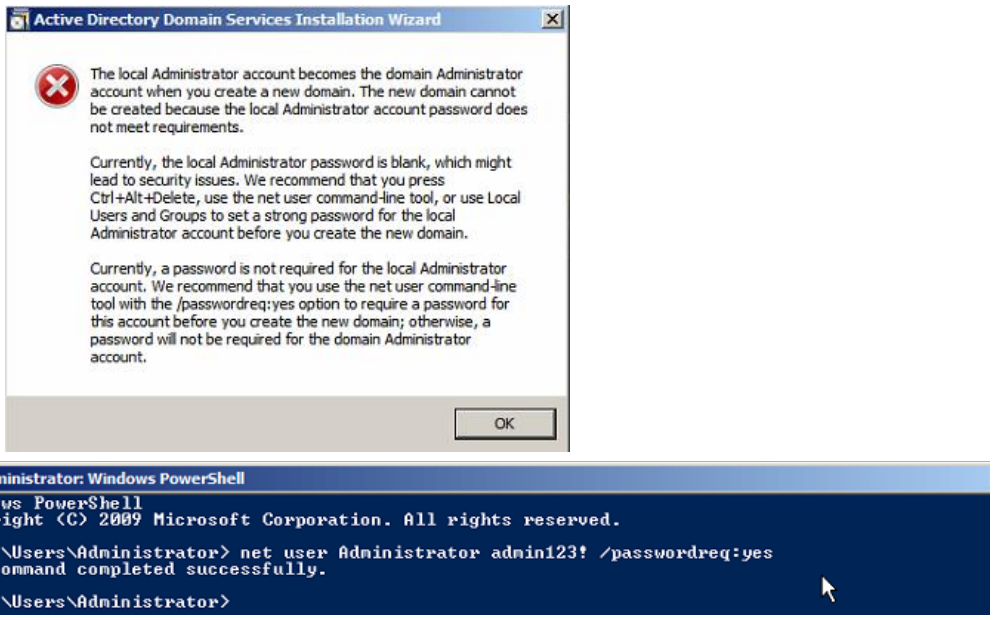
Select Operating System Compatibility

(3) Choose an domain configuration as “Create a new domain in a new forest”。



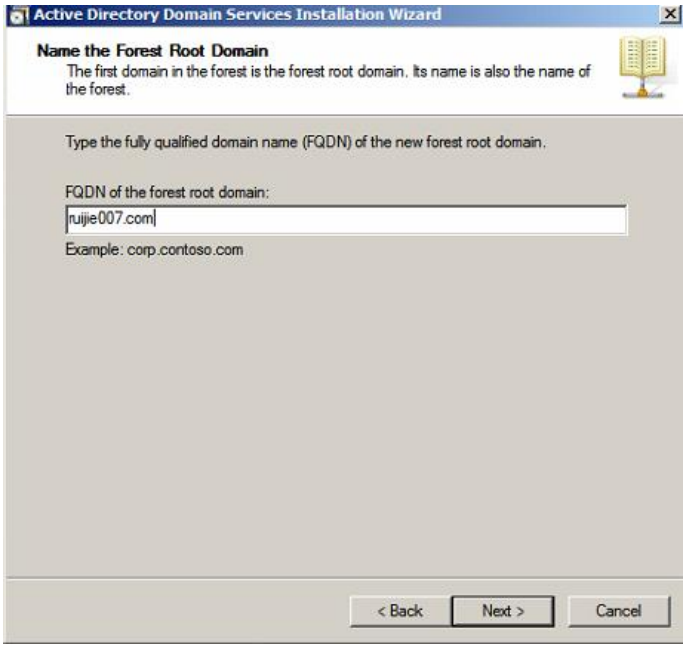
Create a new domain in a new forest

(4) If the following error message is displayed when you click Next, enter ‘net user username password /passwordreq:yes’ in the command line.



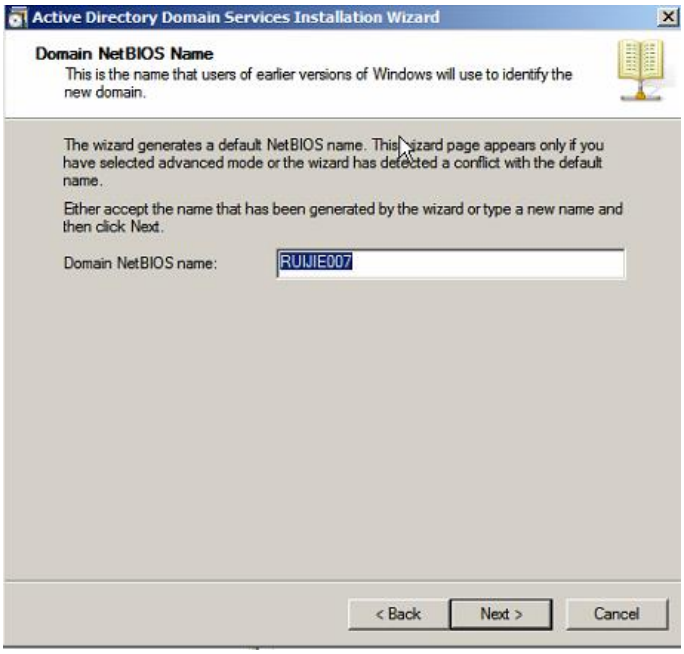
Local Administrator account does not meet requirements

(5) Name the domain: because this is the first domain in the forest, so this domain is also the root domain.



Enter Root domain name

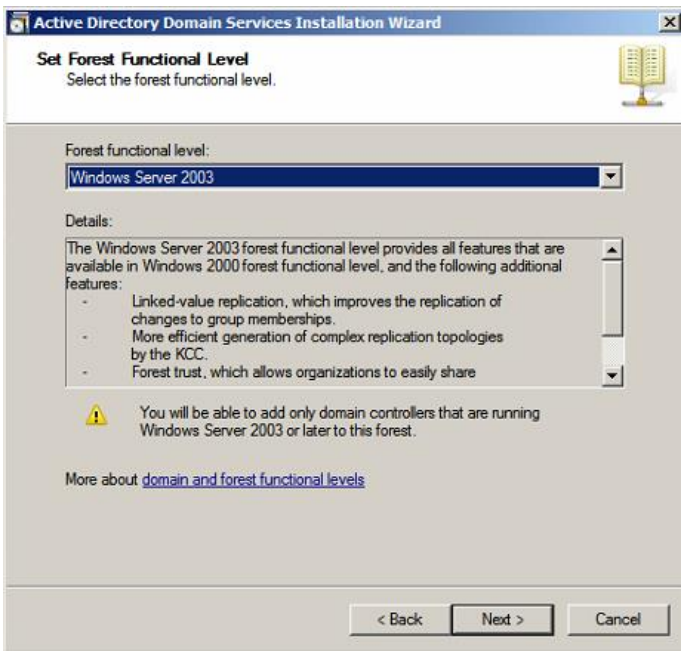
The domain is named as ruijie007.com here, but you can name based on your requirement.



Domain NetBIOS Name

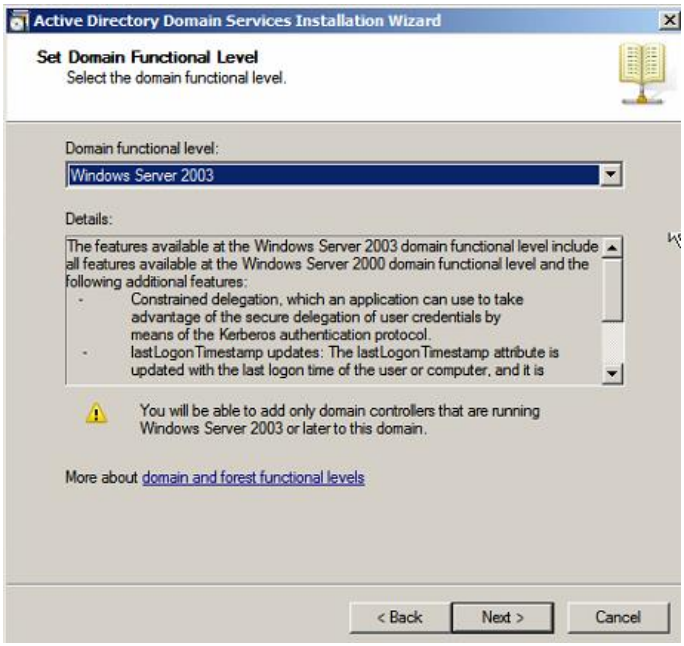
The default NetBIOS name is from the domain name before .com. So the default NetBIOS name in this test is RUIJIE007

(6) Set "Set Forest Functional Level". The forest functional level you choose here will affect the domain controller added



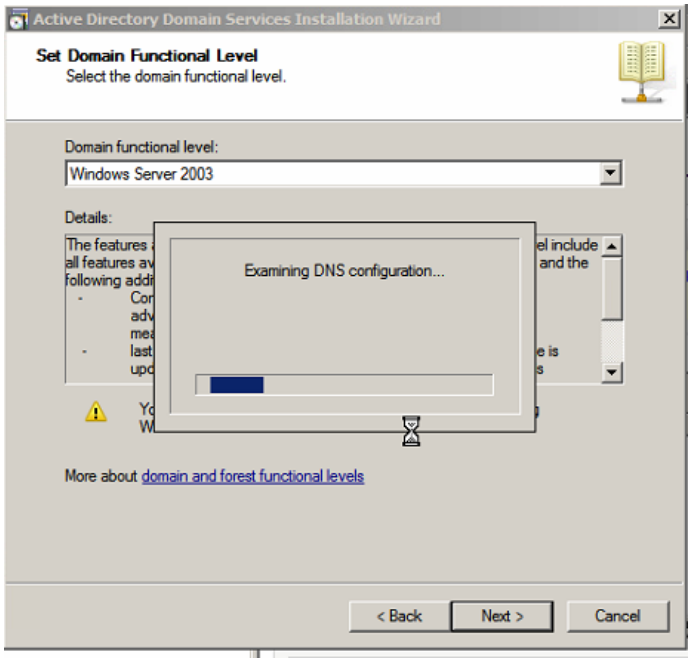
Set Forest Functional Level

Set Domain Functional Level. In order for a domain to be more powerful, the domain functional level should try to set the lowest operating system used in the domain.



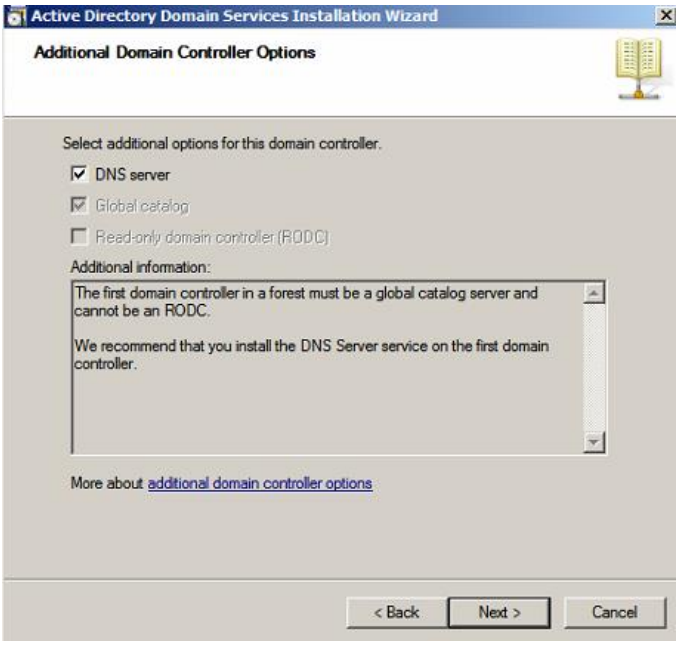
Set Domain Functional Level

(7) Check the DNS Configuration after clicking 'Next'



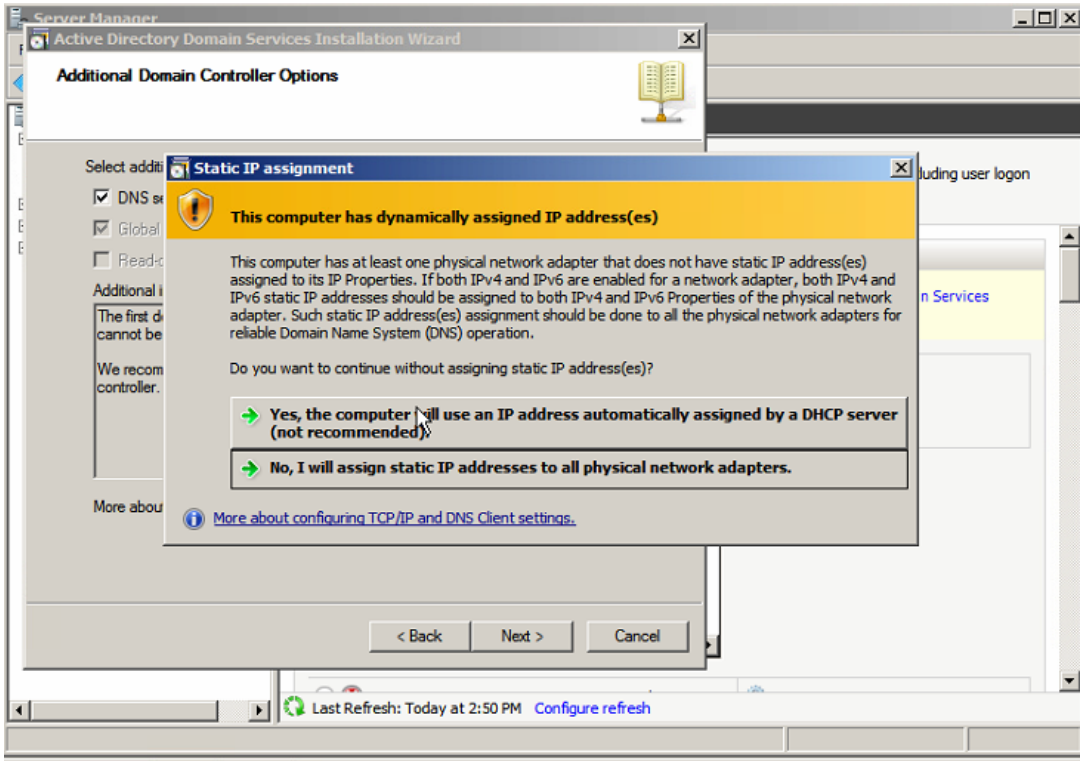
Check DNS configuration

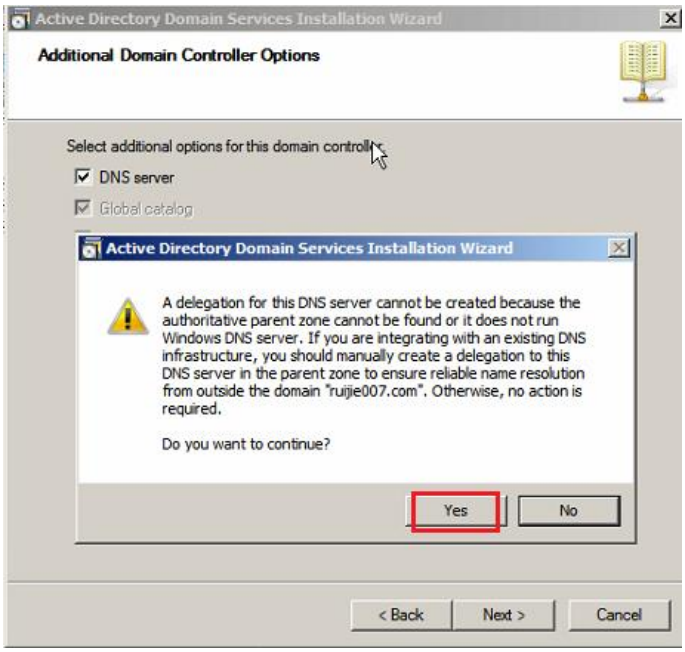
(8) Since we have not installed the DNS service yet, you will need to check "DNS Server".



Install DNS Server

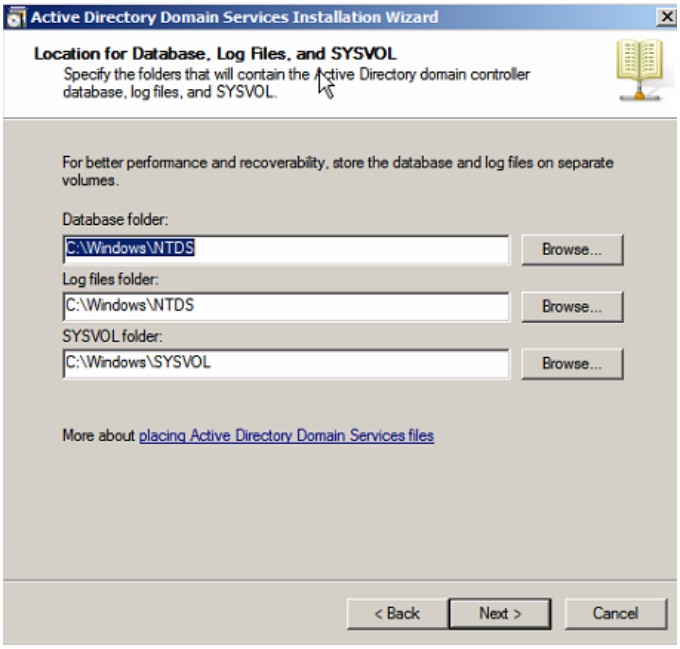
(9) Ignore the displayed warning information and click 'Yes, the computer will use an IP address automatically assigned by a DHCP server (not recommended)' and click 'Next'.





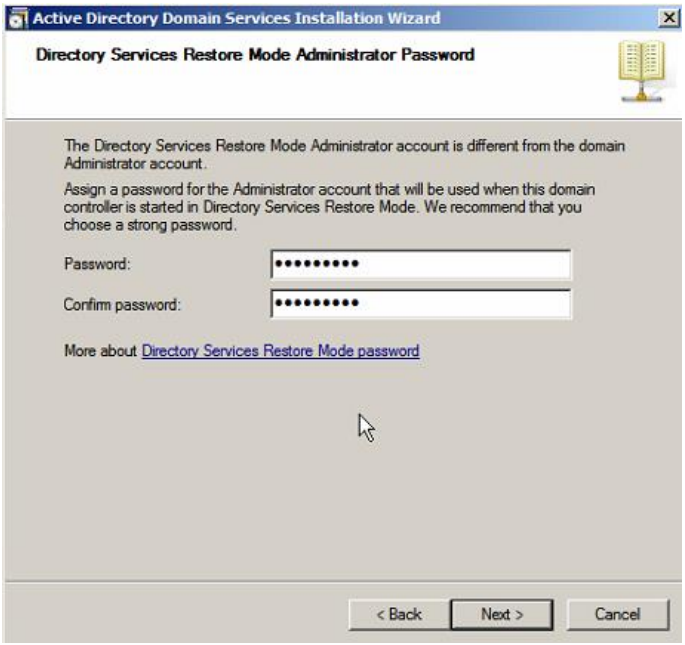
Install DNS Server

(10) Configure the location for Database, Log Files, and SYSVOL. Generally, it's recommended to set two different locations for database and log files.



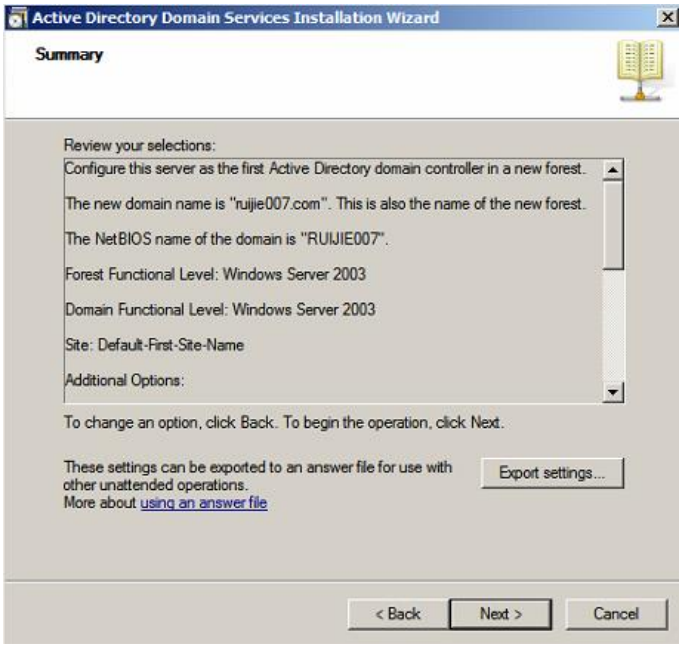
Set the location for Database, Log Files and SYSVOL

(11) Set Directory Services Restore Mode Administrator Password。It will be needed if you need to recover the Active Directory from backup.



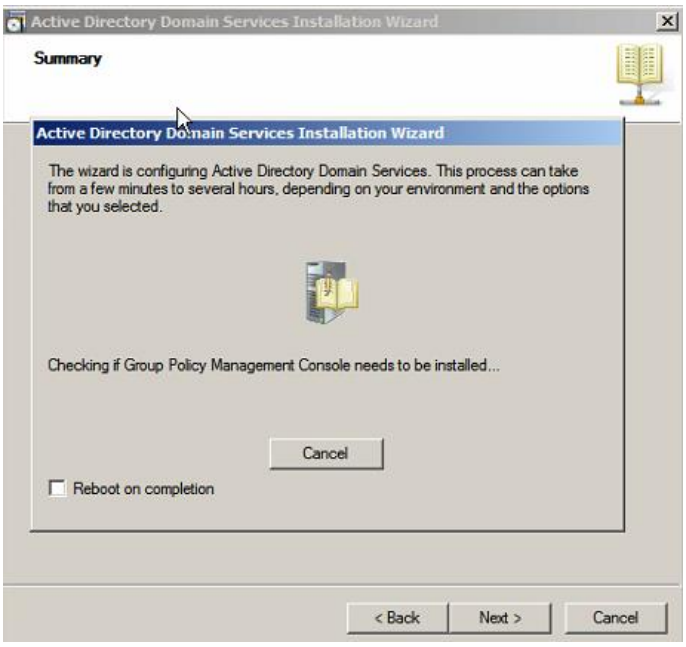
Set Directory Services Restore Mode Administrator Password

(12) When the above steps are set up, the configurations will be performed in summary form for review.



Domain Services Summary

(13) If the configuration is correct, go to the next step to start the installation.

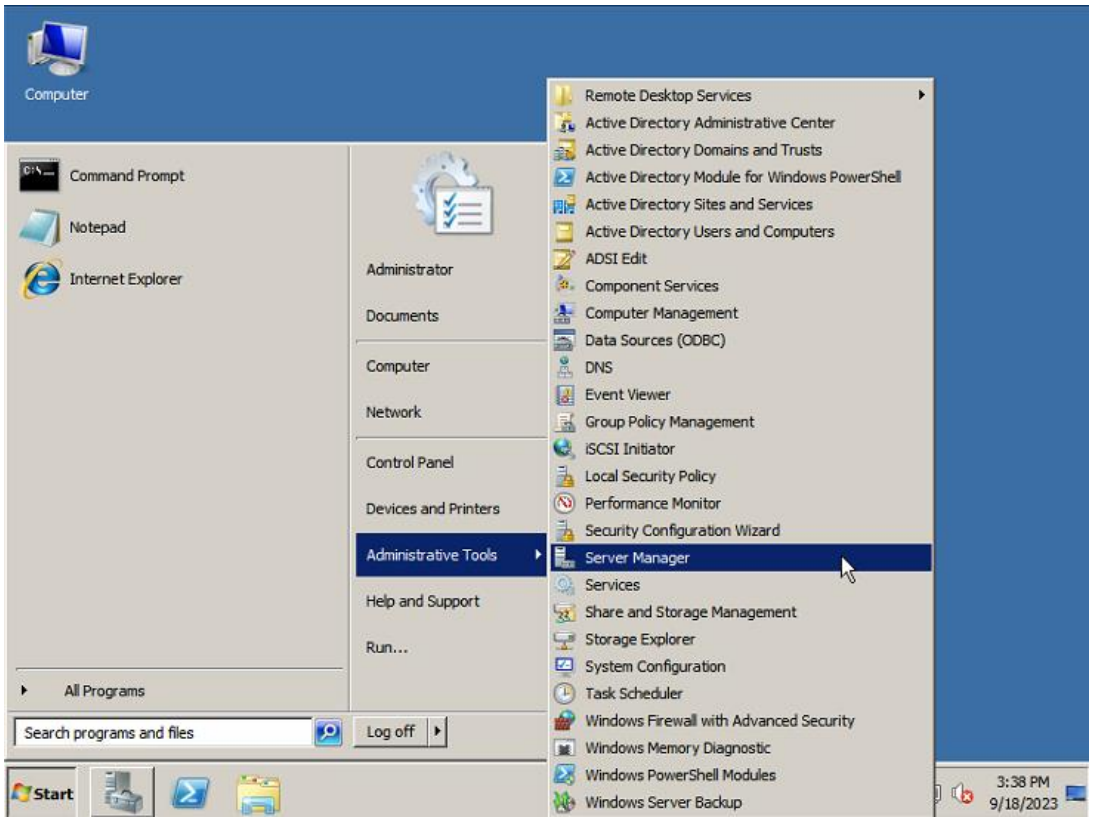


Start Installation

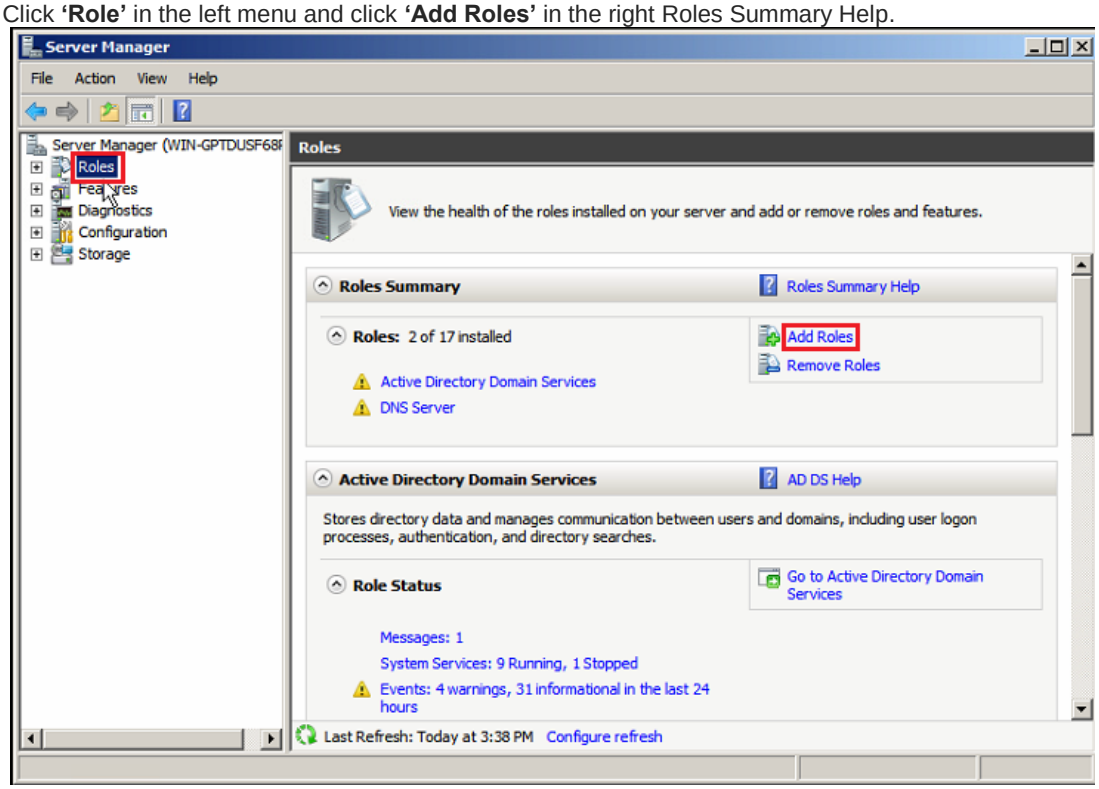
(14) When the installation is complete, you are prompted to restart the computer. The AD domain controller is set up after the restart.

1.3 Install CA Server

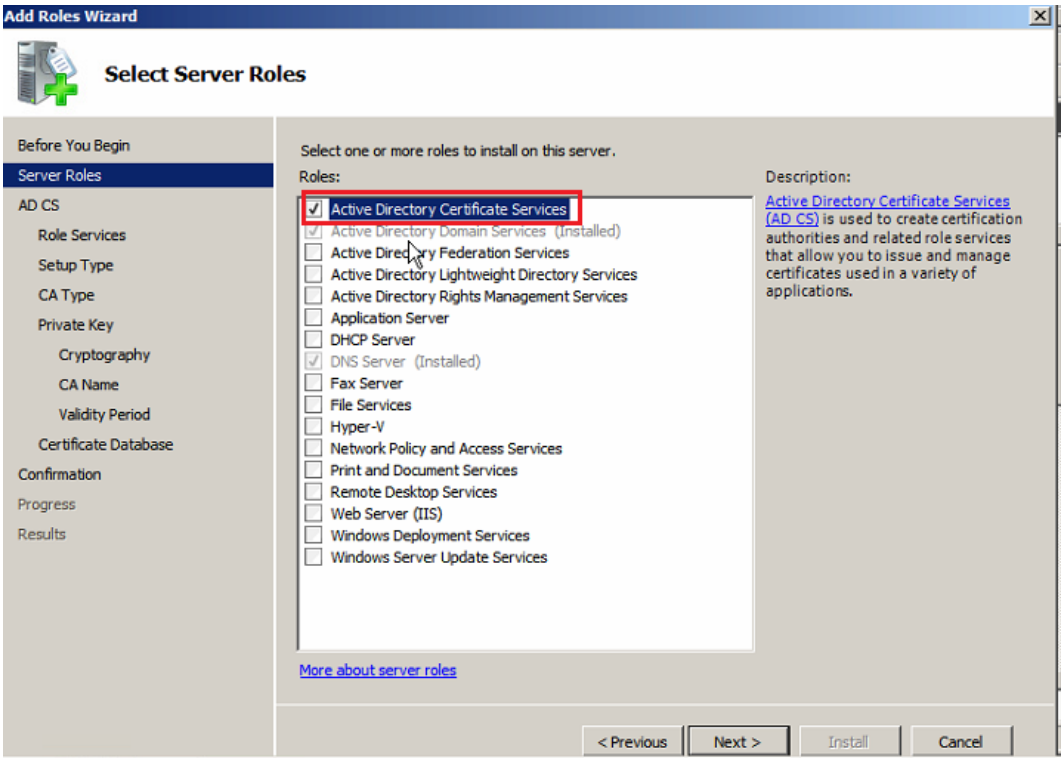
(1) Log in to the domain Server as the Administrator and click [Start]>>[Administrative Tools] >>[Server Manager] to open the server manager.



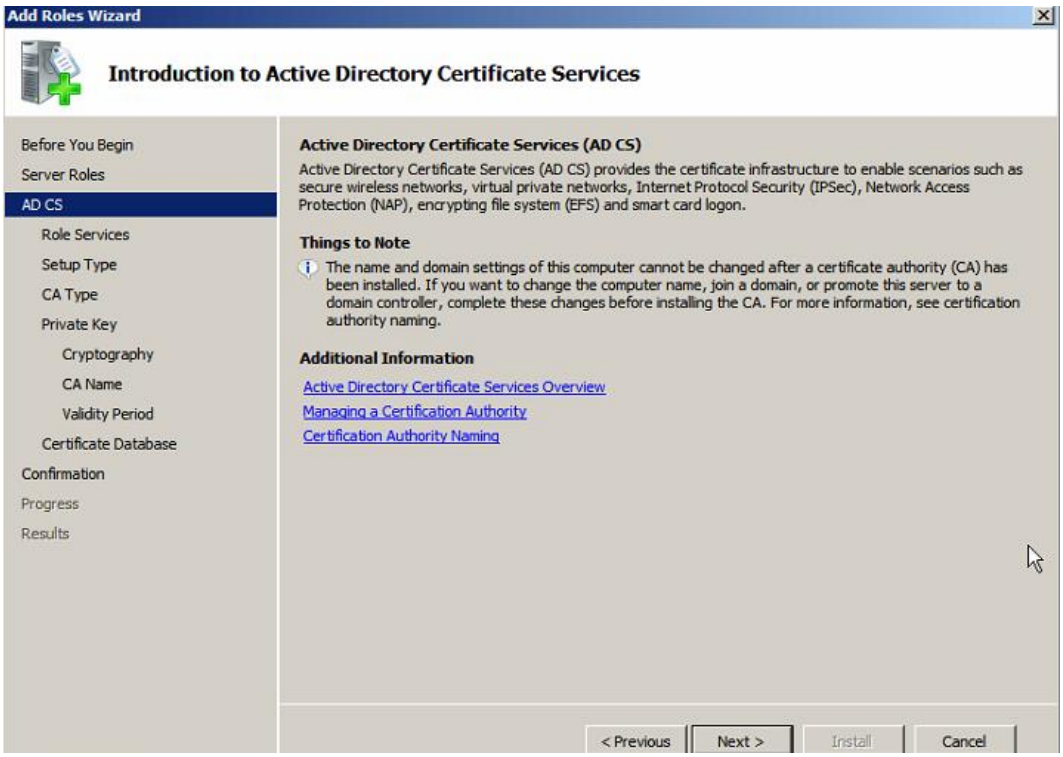
(2) Click **'Role'** in the left menu and click **'Add Roles'** in the right Roles Summary Help.



(3) Select 'Active Directory Certificate Services' in the 'Select Server Roles' page, and then click 'next' twice.

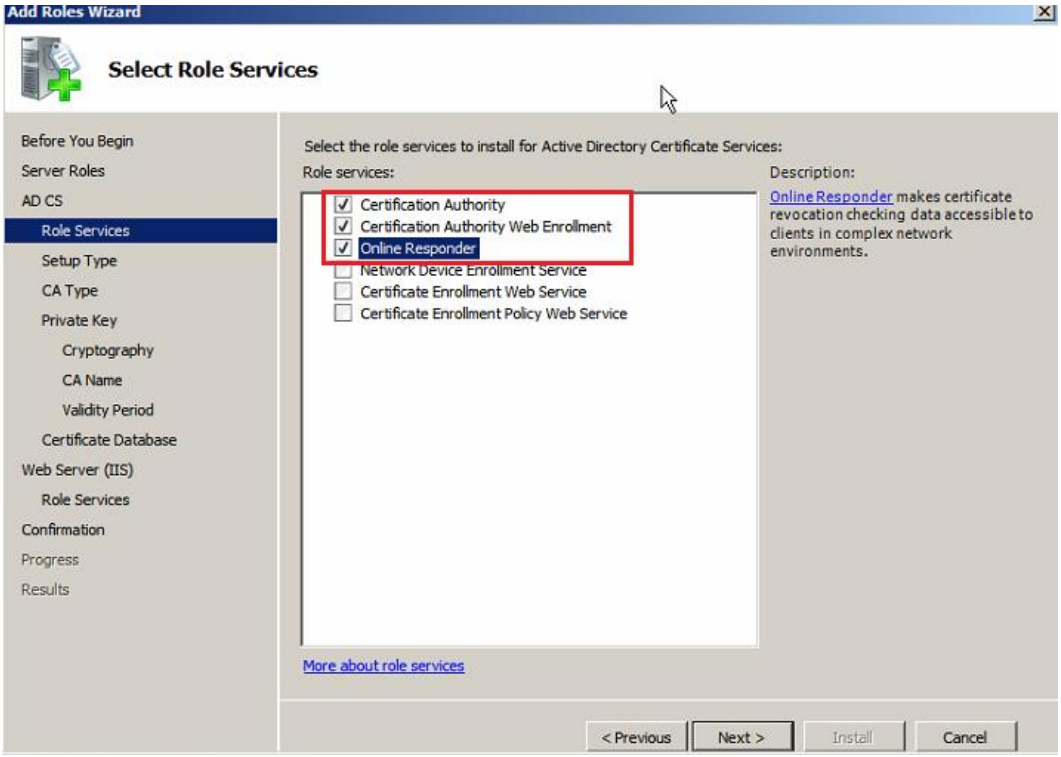


Select "Active Directory Certificates Servers"



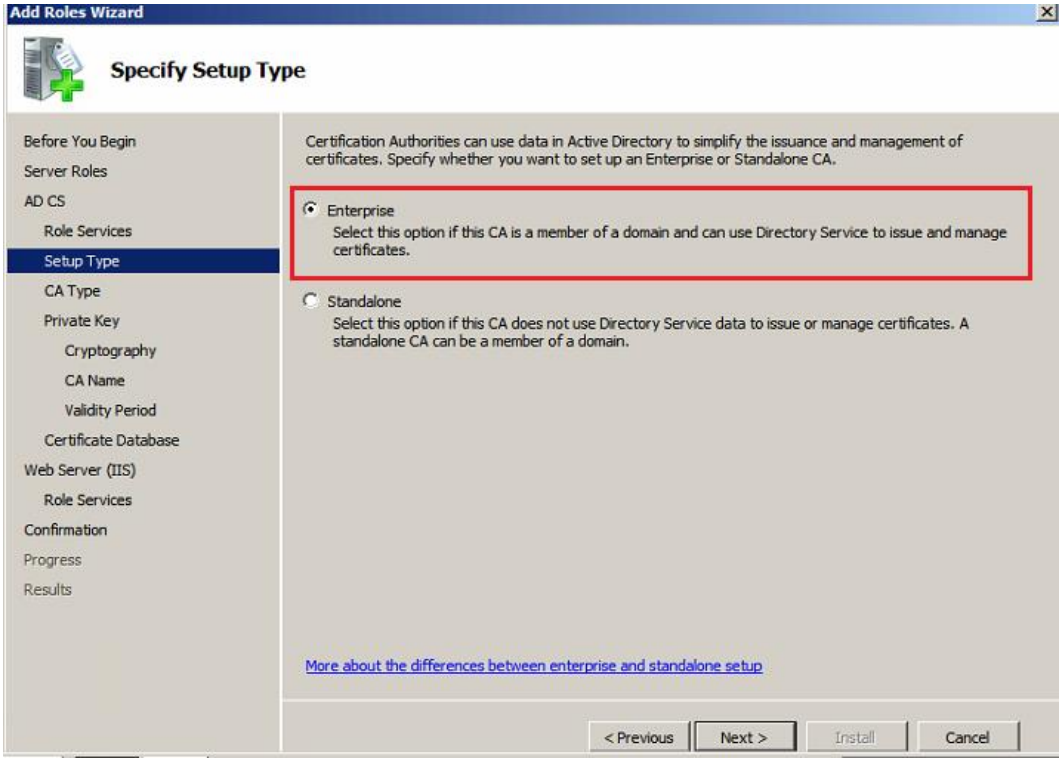
"Active Directory Certificate Services" Introduction

(4) Click 'Certification Authority', 'Certification Authority Web Enrollment and 'Online Responder' and then click 'Next'.



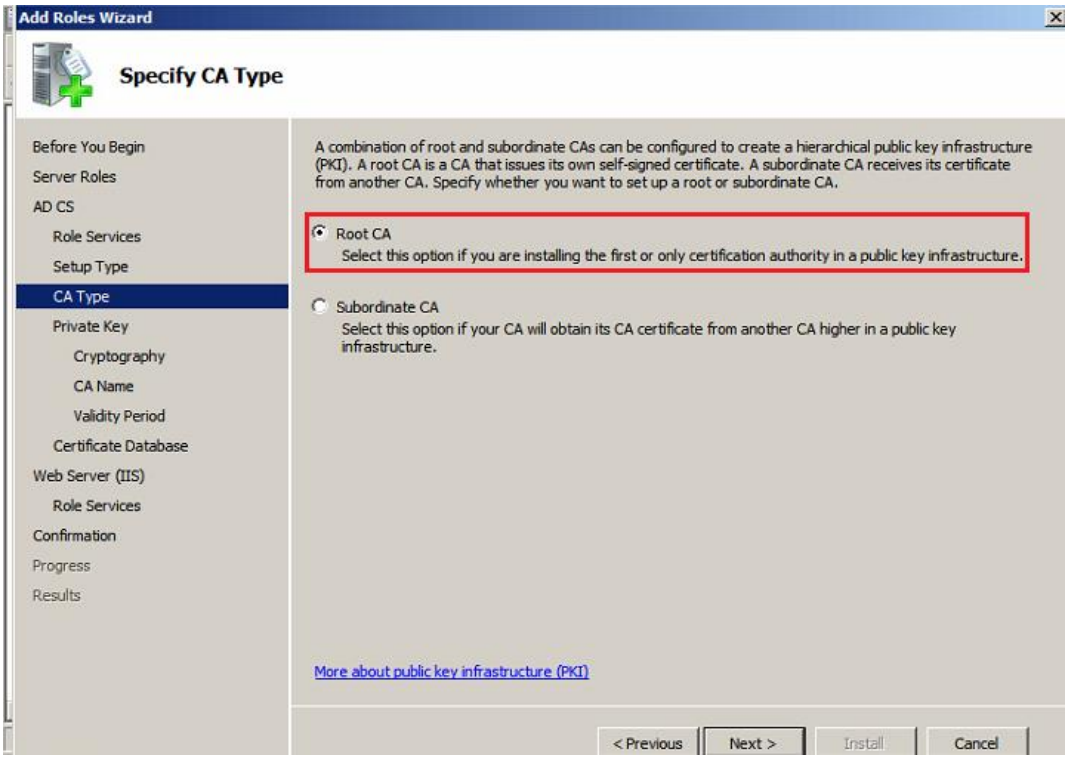
Select Role Services

(5) Click ‘Enterprise’ in the Specify Setup Type’ page, and then click ‘Next’



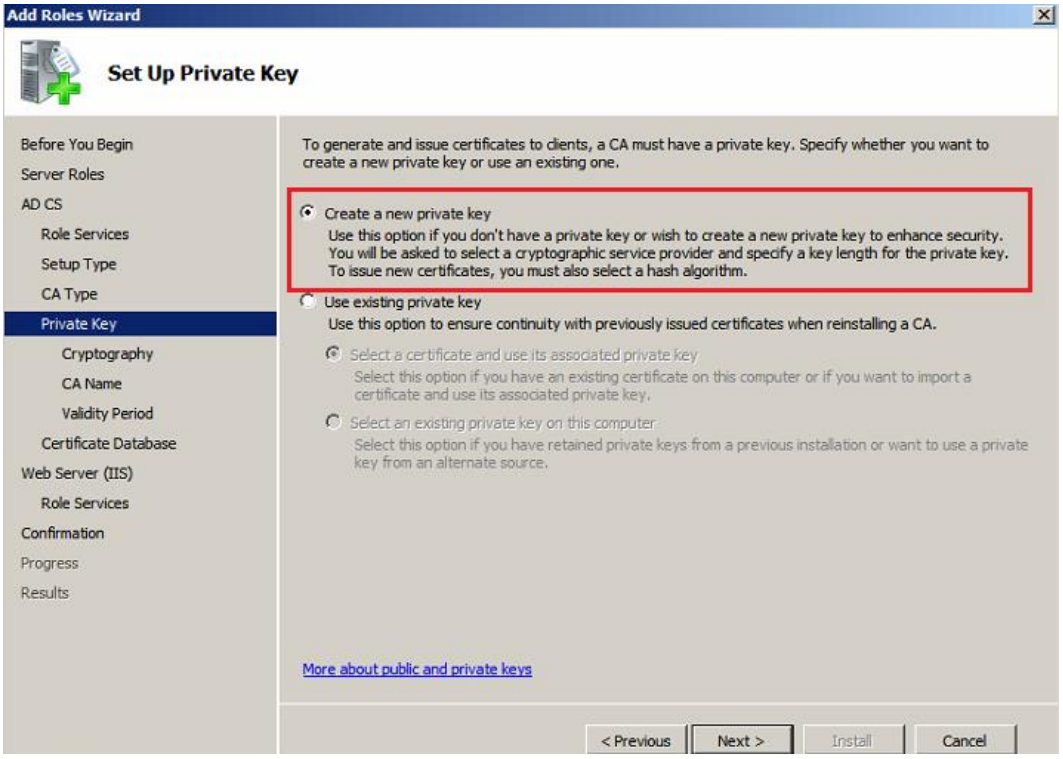
Specify Setup Type

(6) Click ‘Root CA’ in the ‘Specify CA Type’ and then click ‘Next’.



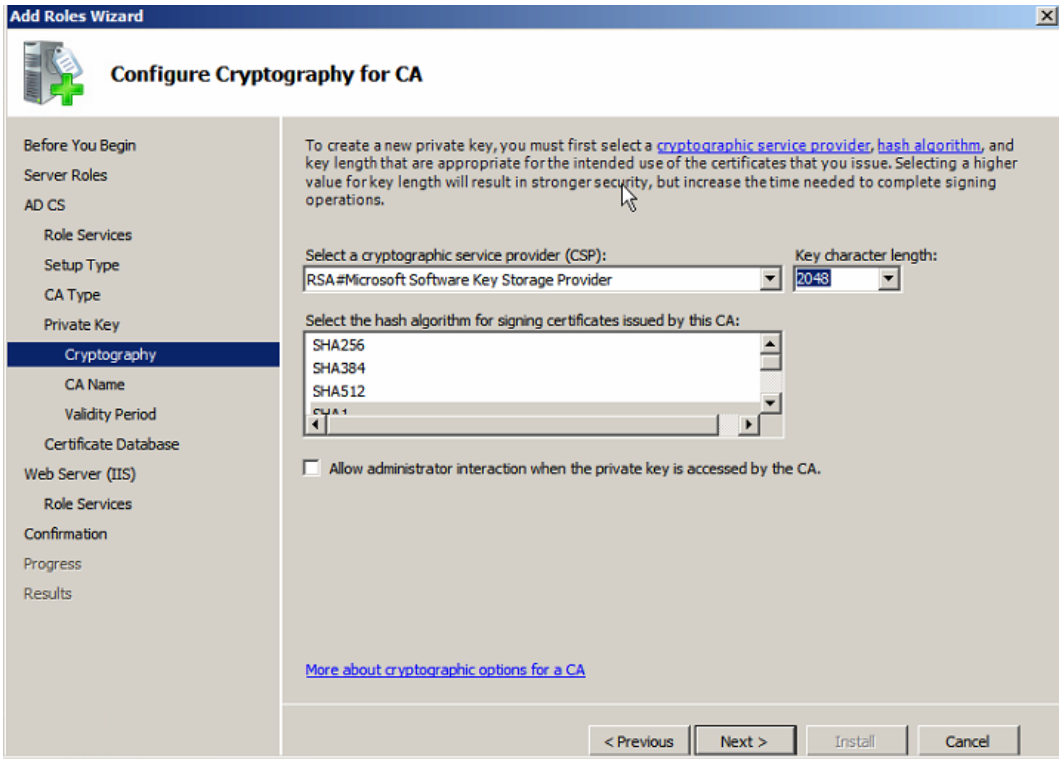
Specify CA Type

(7) You can set available settings in the ‘Set Up Private Key’ page. The default settings ‘Create a new private key’ is set here, and then click ‘Next’.



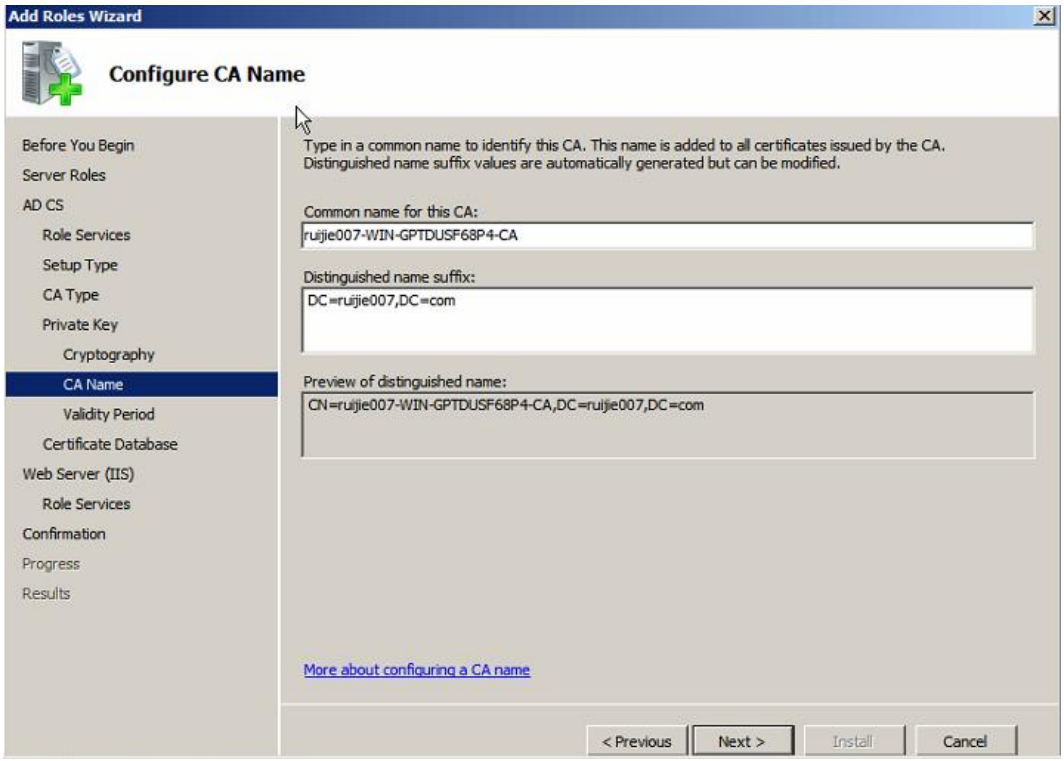
Set Up Private Key

(8) 在Configure cryptography for CA in the ‘Cryptography’ page and click ‘Next’ without changing any settings.



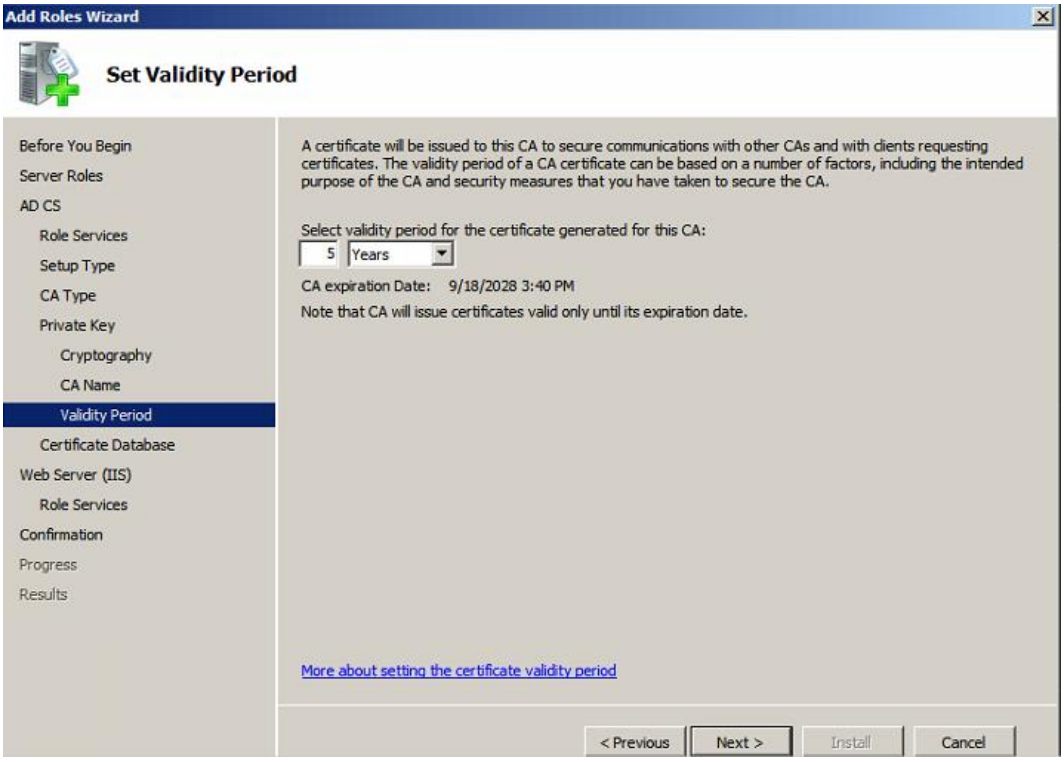
Configure Cryptography for CA

(9) You can keep the default content: 'Domain name+ Server Name' in the box of 'Common name for this CA' and then click 'Next'



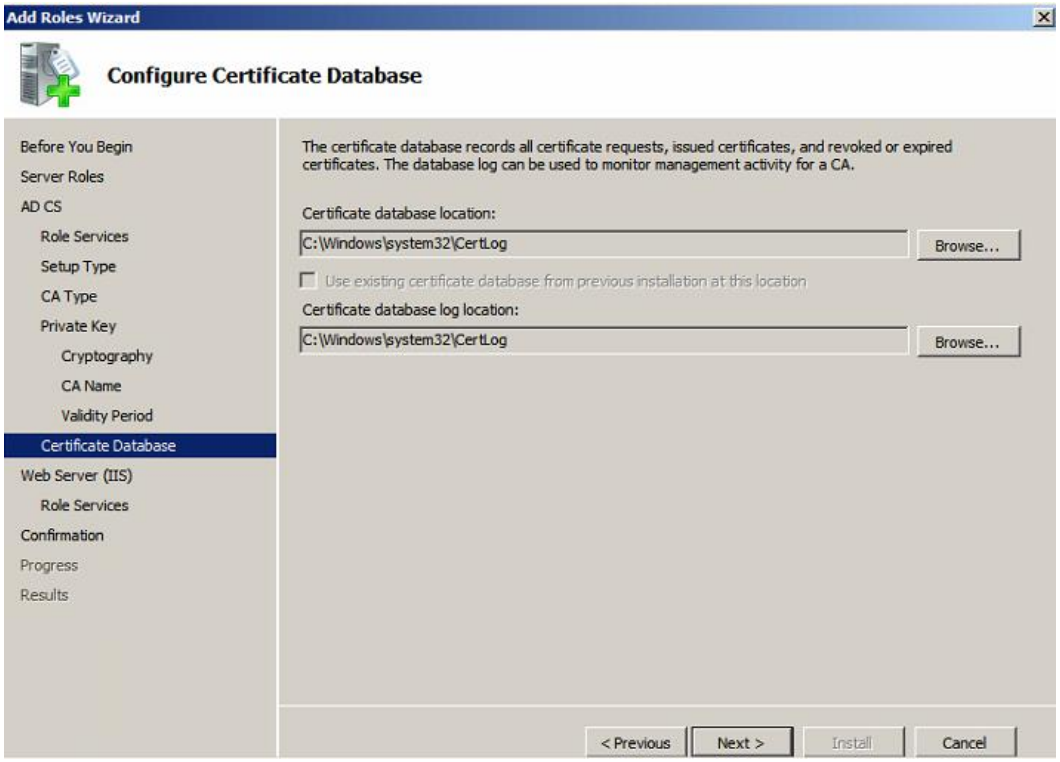
Configure CA Name

(10) In the ‘Set Validity Period’ page, accept the default validity period, and the click ‘Next’.



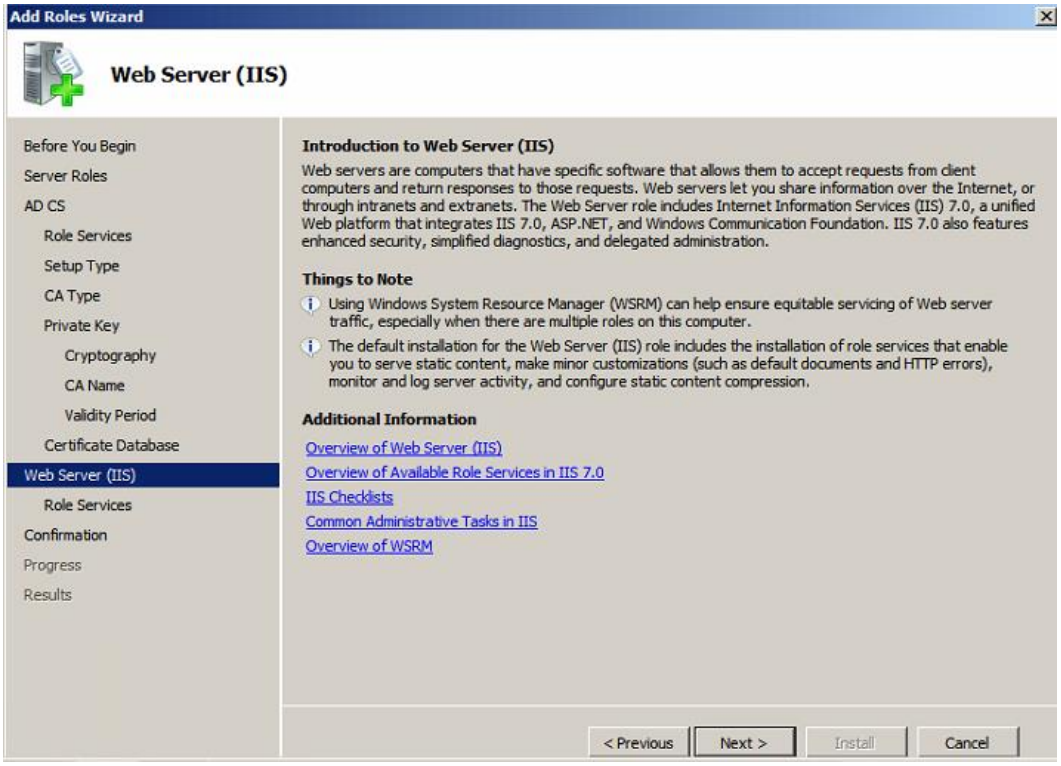
Set Validity Period

(11) In the “Configure Certificate Database” page，accept the default location or save the certificates database and certificates log in different location and then click ‘Next’.



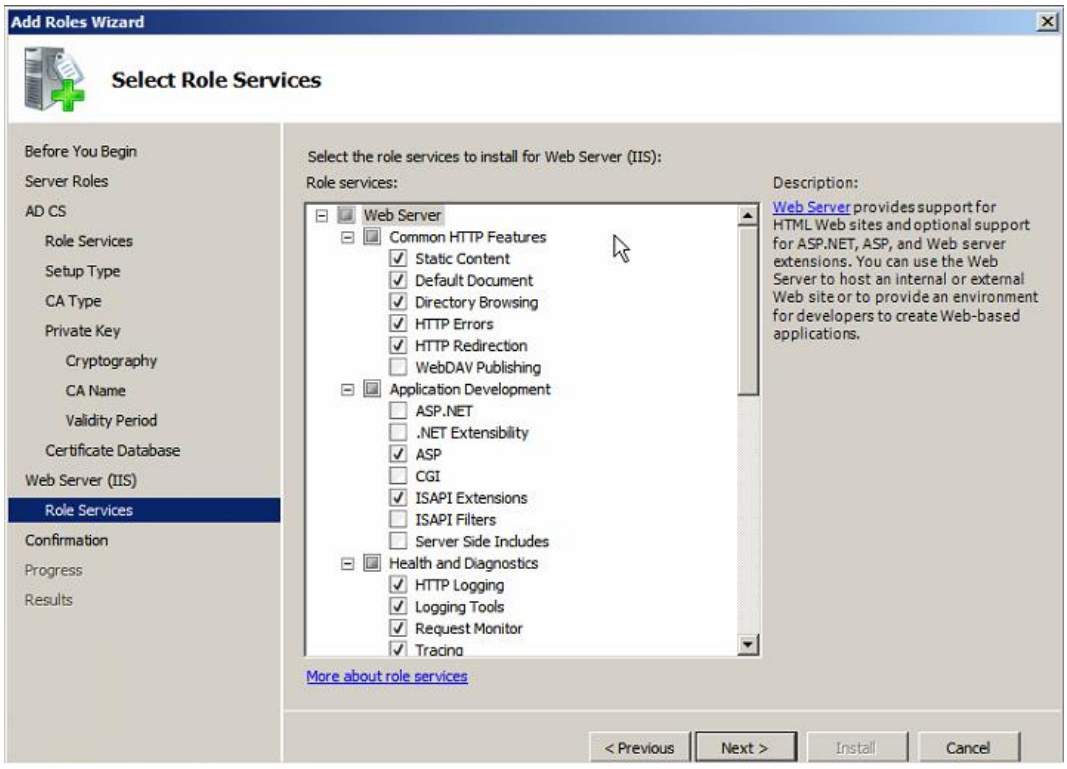
Configure Certificate Database

(12) Inter "Web Server（IIS）" page, click 'Next'



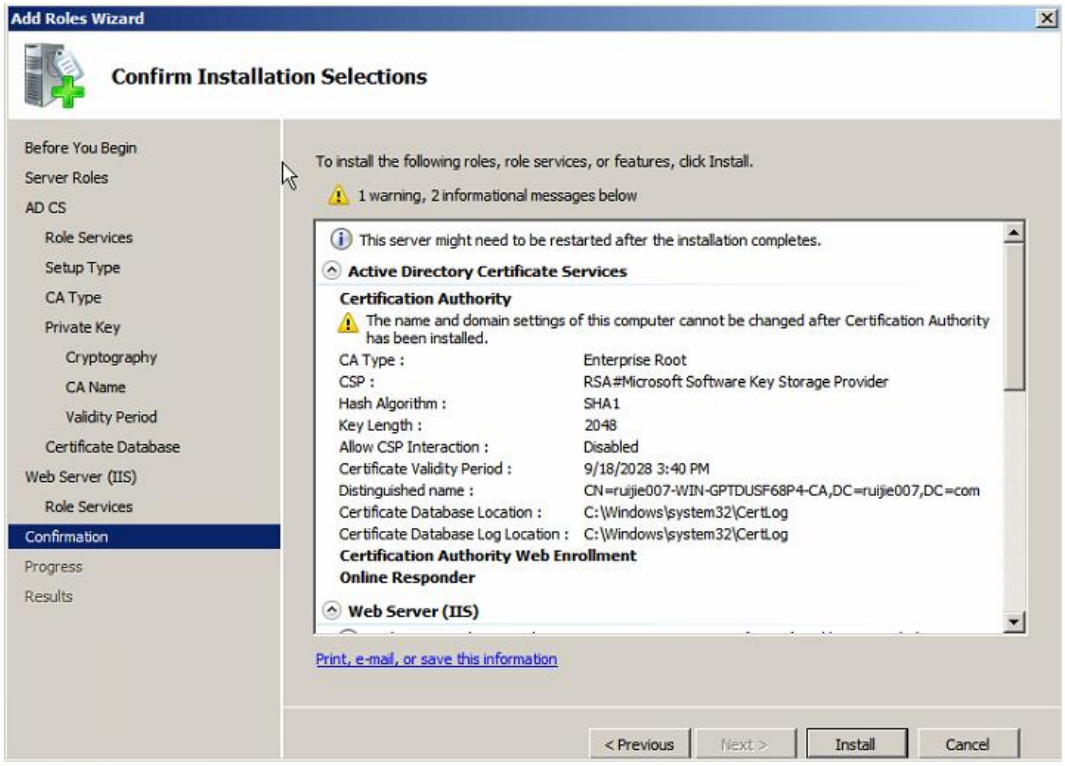
Web Server Installation

(13) In the 'Select Role Services' page， use the default configuration and then click 'Next'

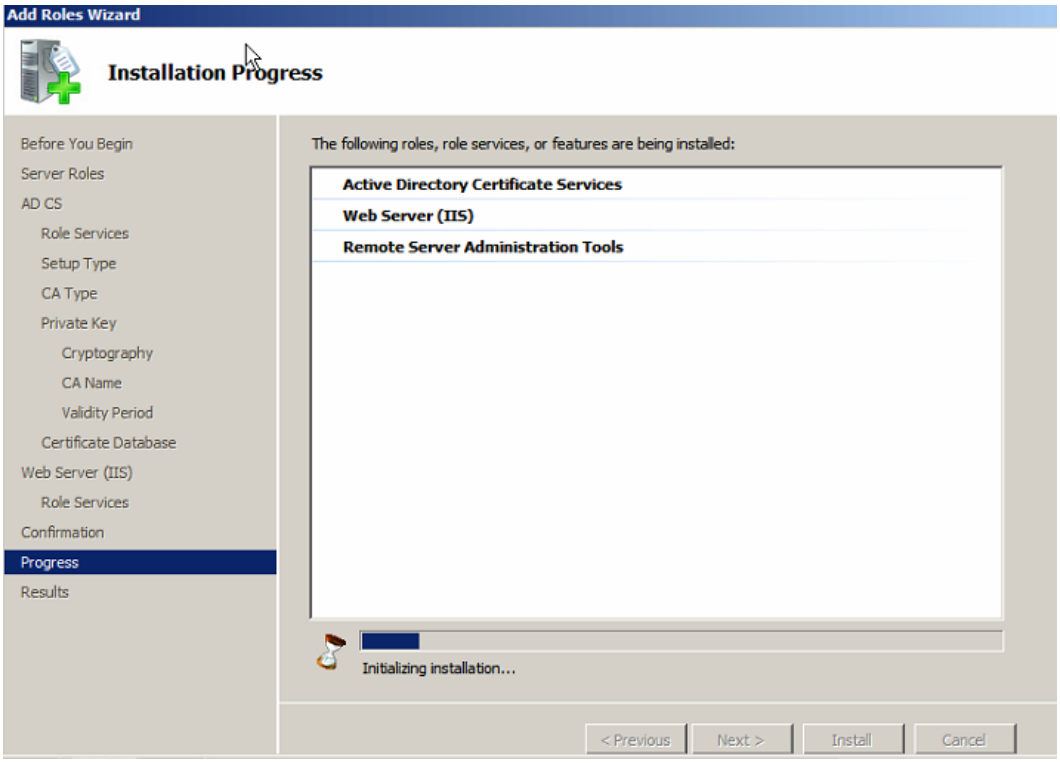


Add a Role Services for Web Server

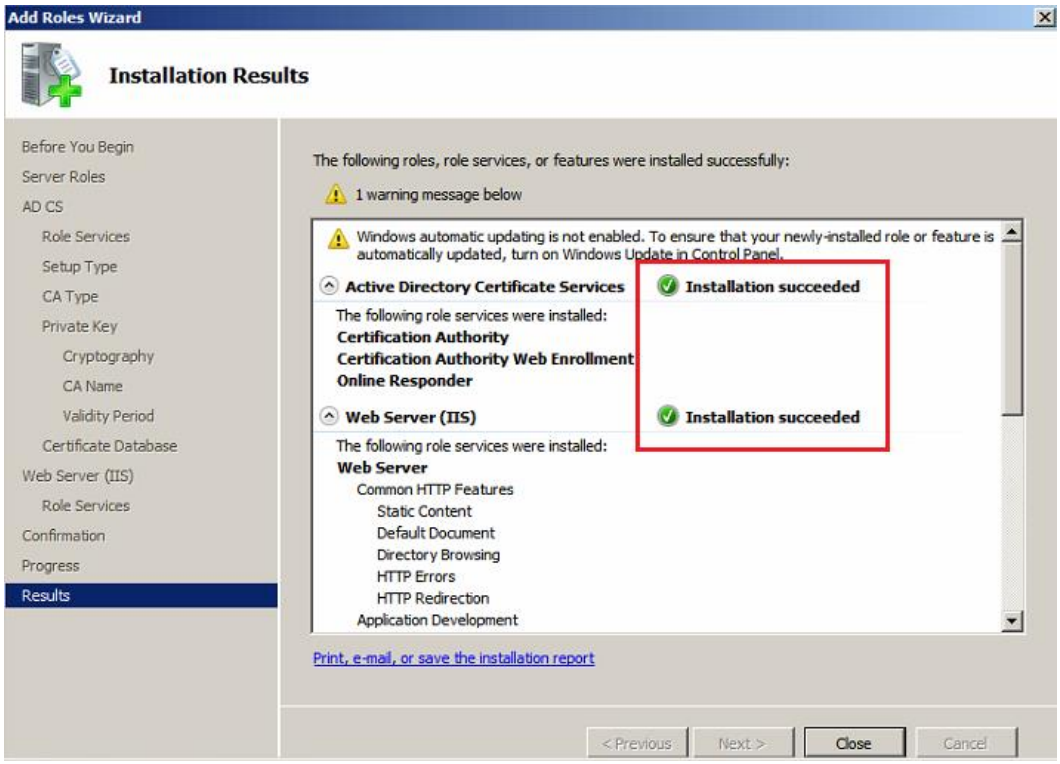
(14) After verify the information in the ‘Confirm Installation Selections’ page and click ‘install’



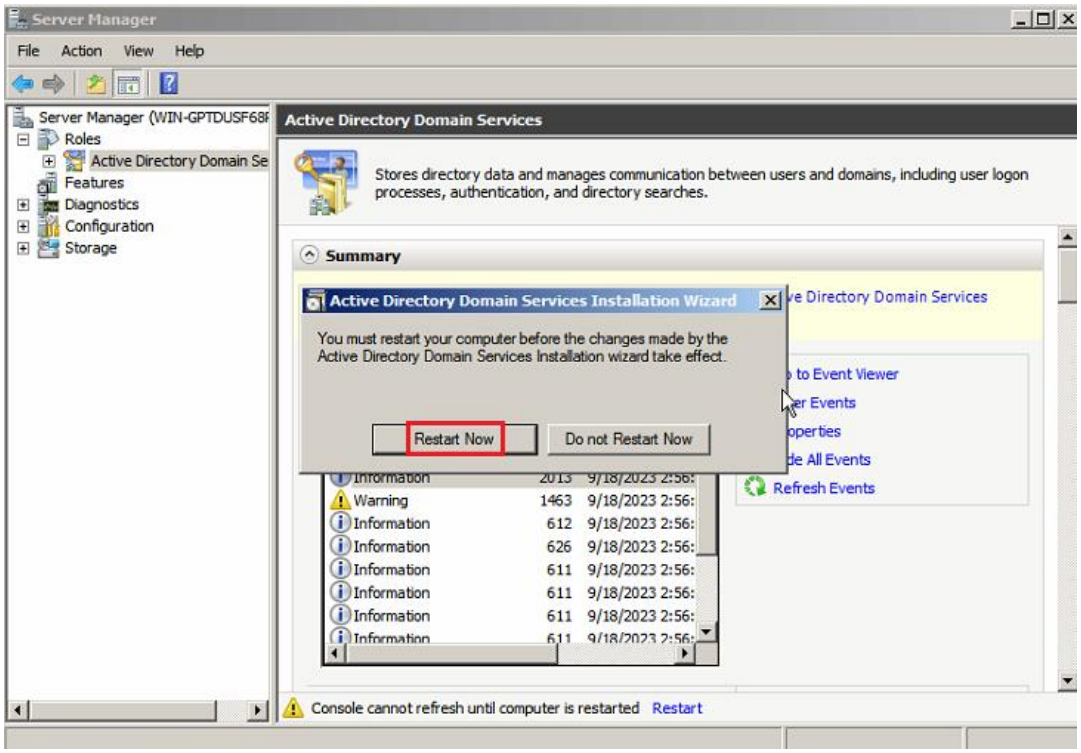
Confirm Installation Selections



(15) Check the configuration to verify where the installation is successful or not.



Confirm Installation Results

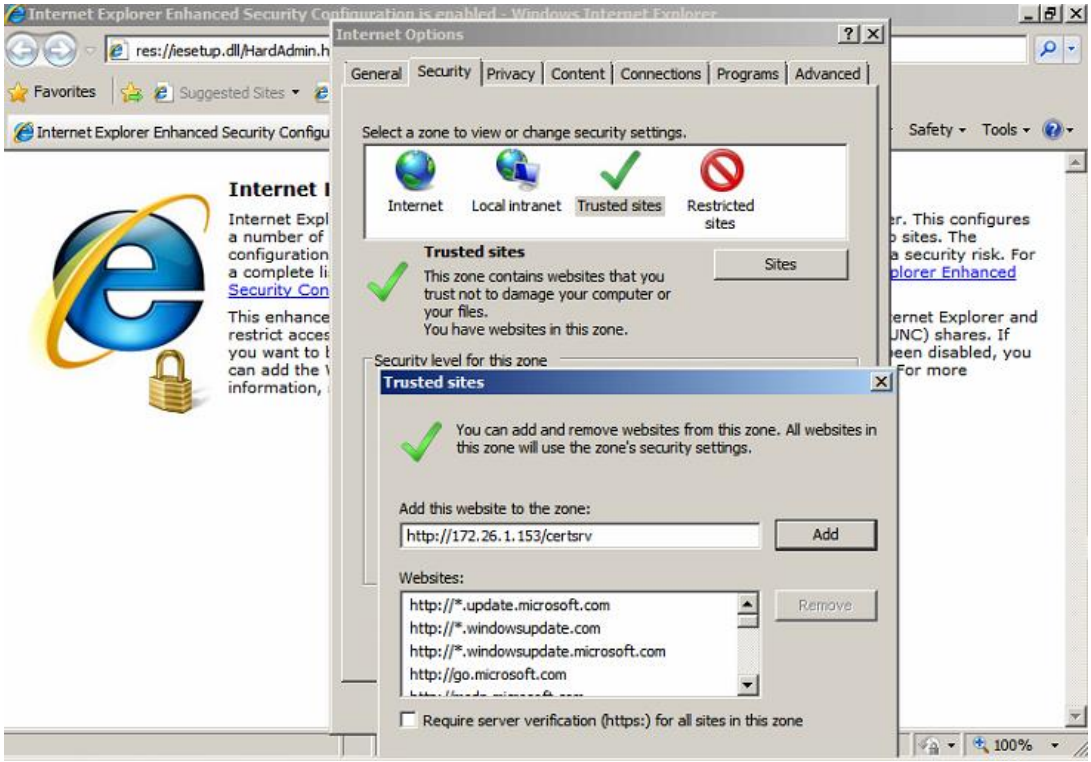


Restart the Computer

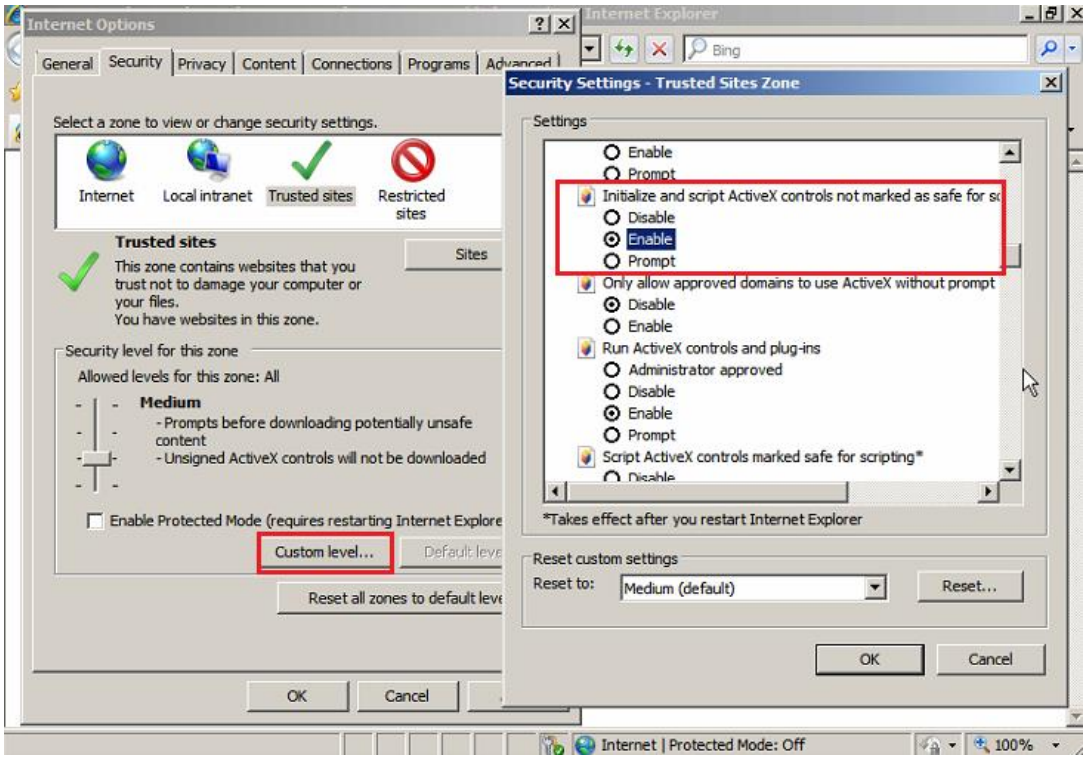
1.4 Install Server Certificates

1.4.1 Set the browser

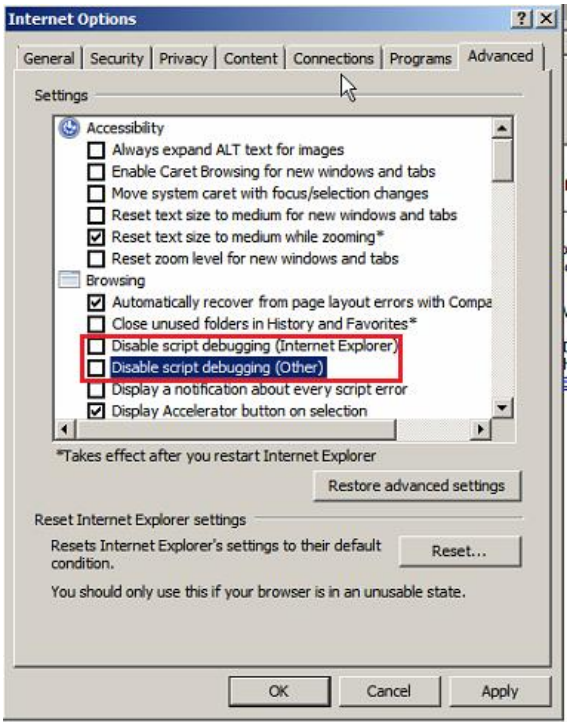
(1) Click Tools in browser->Internet Options-> Security ->Add the http://localpcip/certsrv as the trusted site .



(1) Custom level for security and enable the “Initialize and script activex controls not marked as safe for scripting” in the options of ActiveX

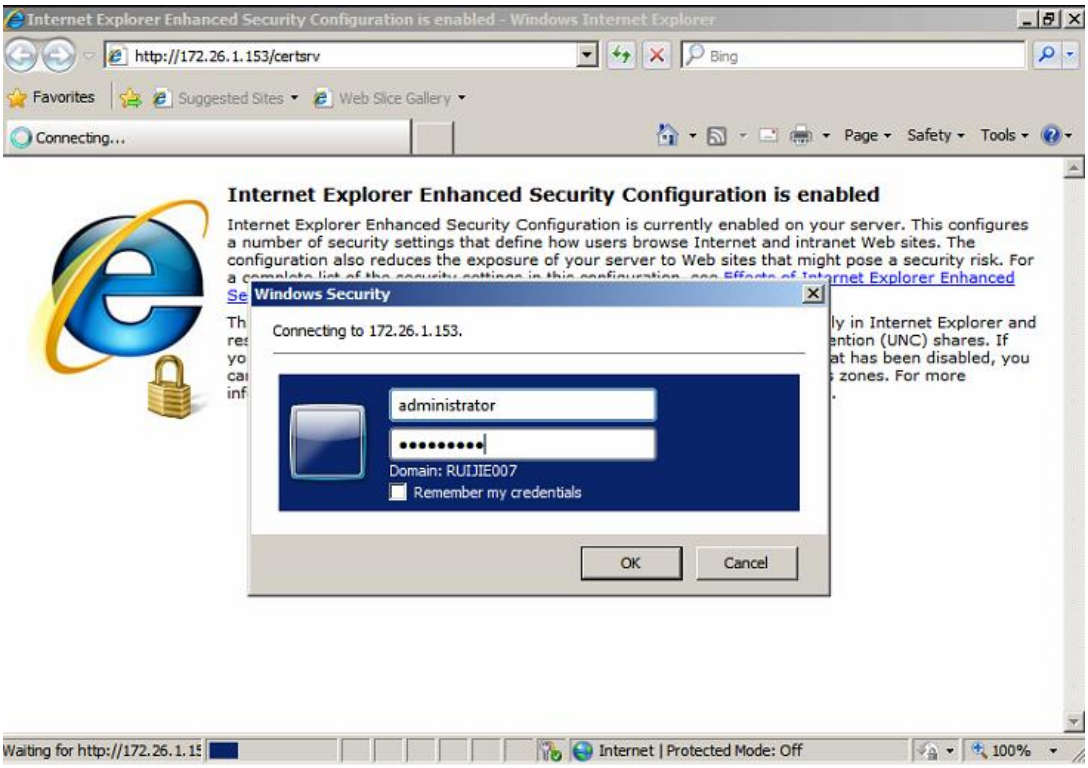


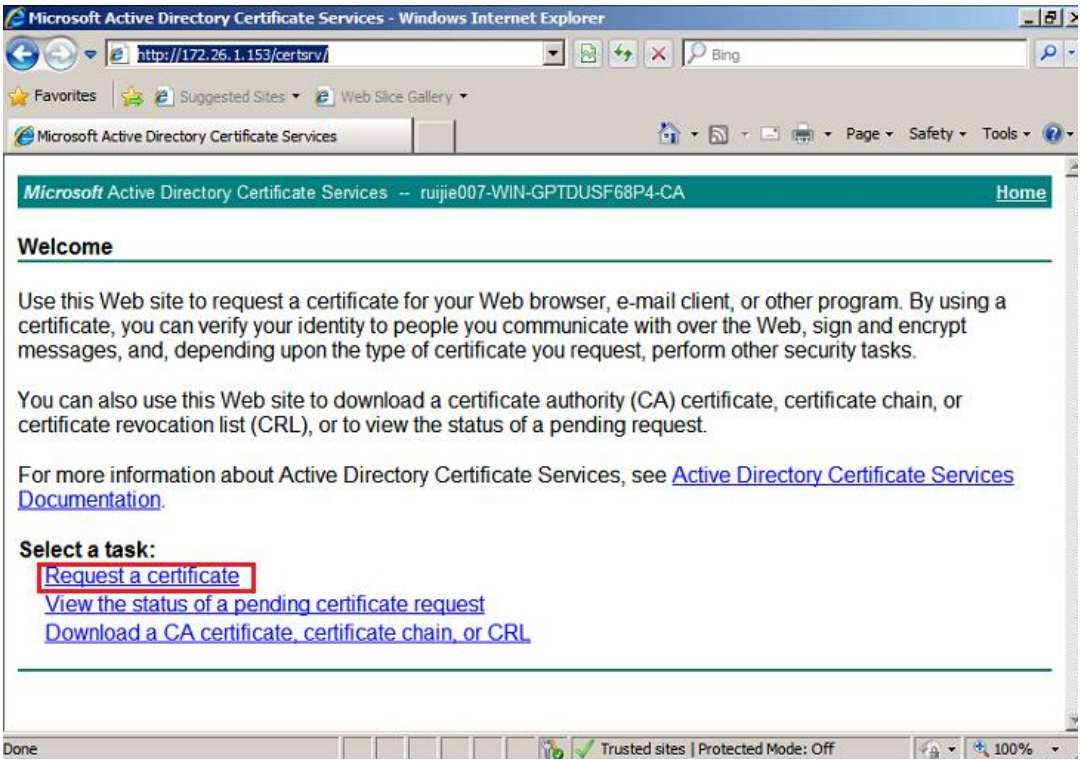
(2) Disable the option of 'Disable script debugging (Other)'

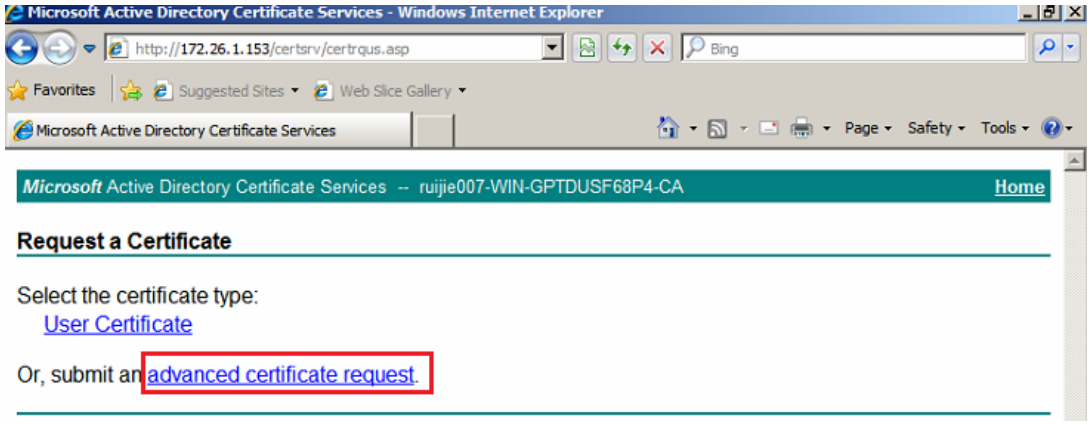


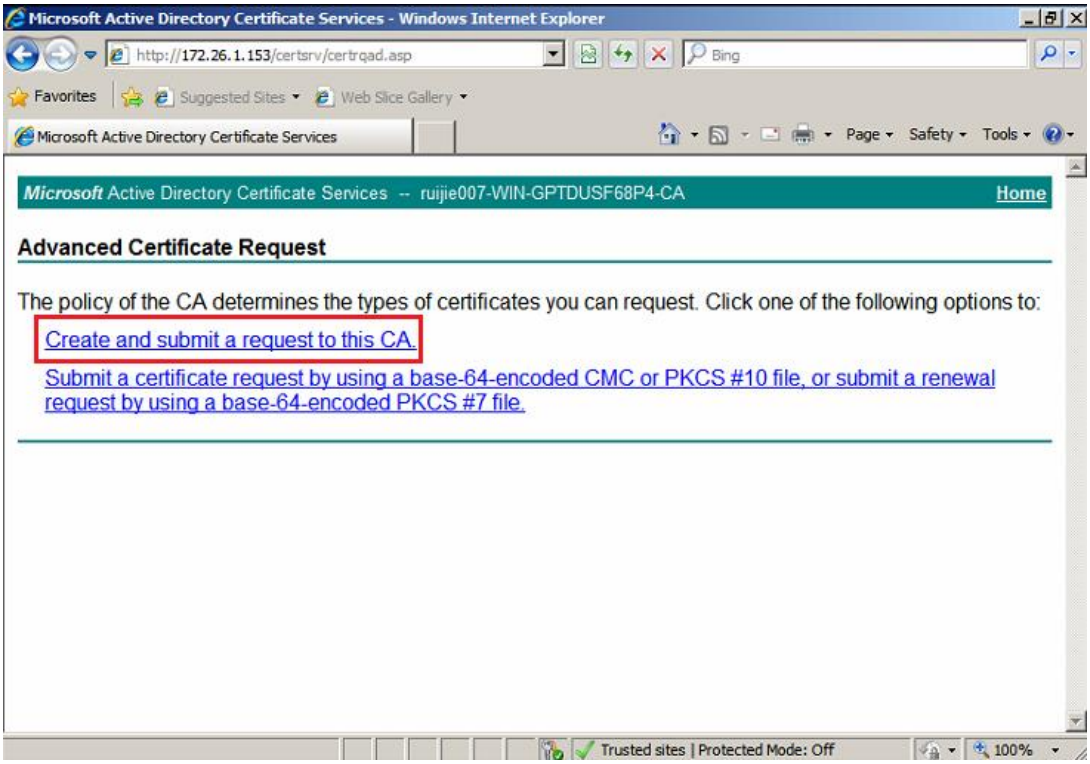
1.4.2 Apply and install the server certificates

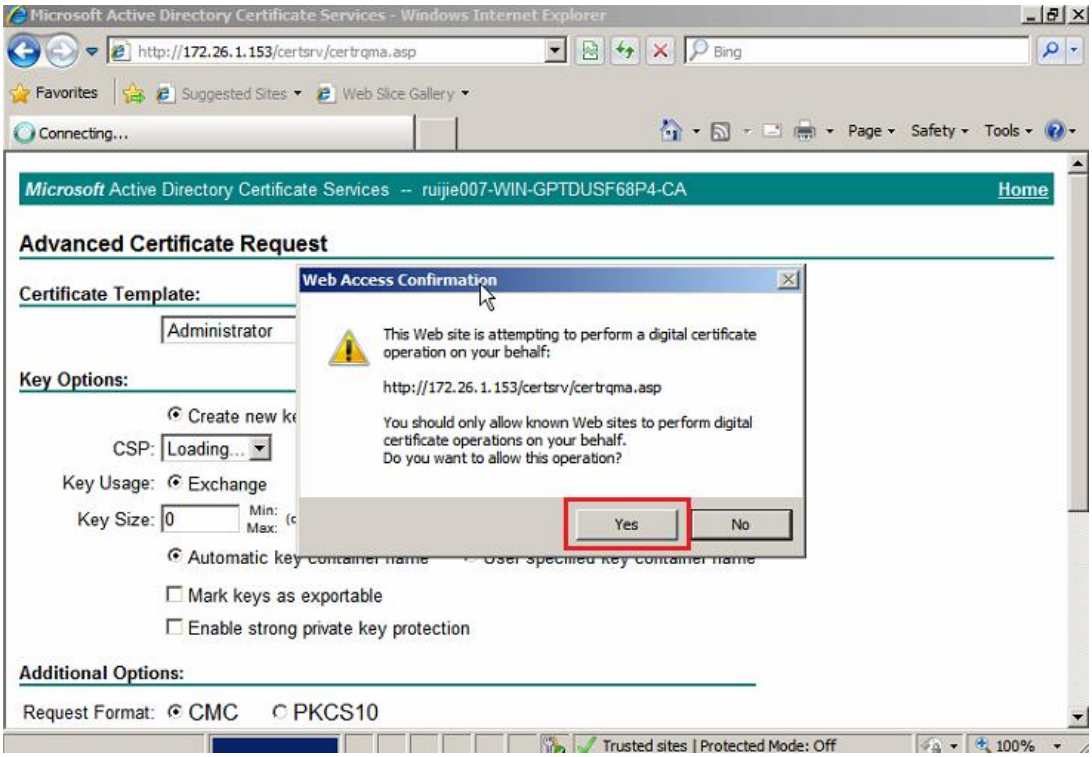
(1) Visit http://serverip/certsrv and log in with admin account, then apply the certificate by following steps.





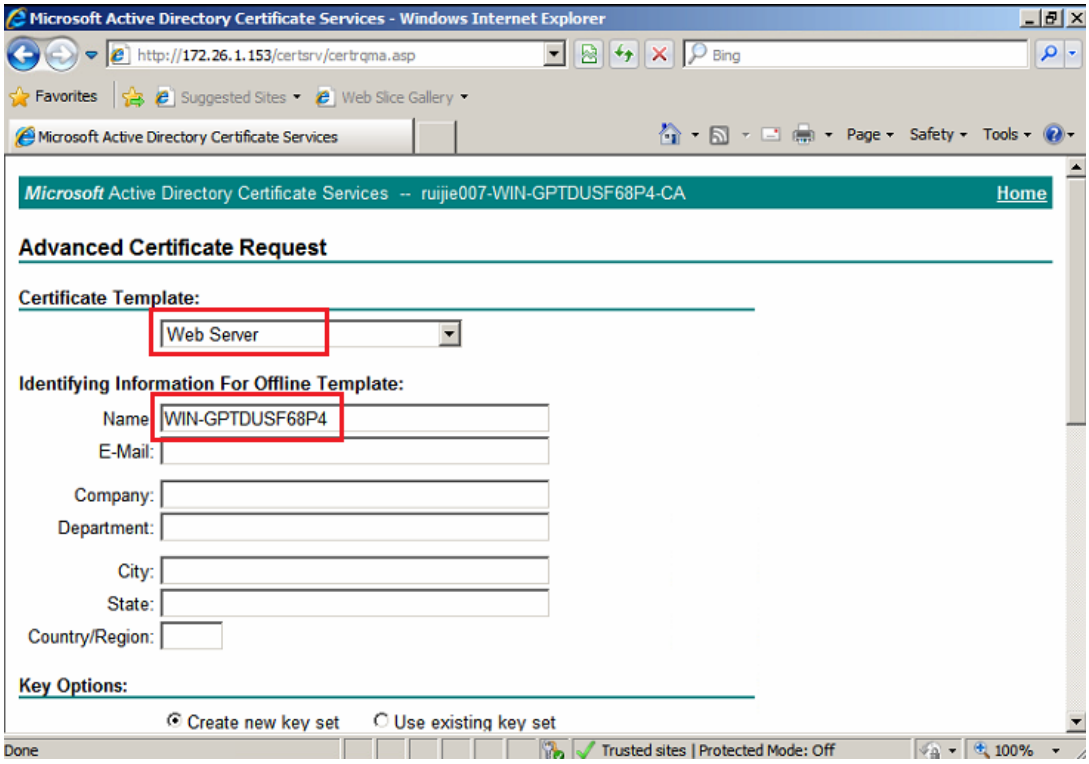

Microsoft Active Directory Certificate Services - Windows Internet Explorer
http://172.26.1.153/certsrv/certrqus.asp
Bing
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Certificate Services
Page
Safety
Tools
Microsoft Active Directory Certificate Services -- ruijie007-WIN-GPTDUSF68P4-CA
Home
Request a Certificate
Select the certificate type:
User Certificate
Or, submit an advanced certificate request.

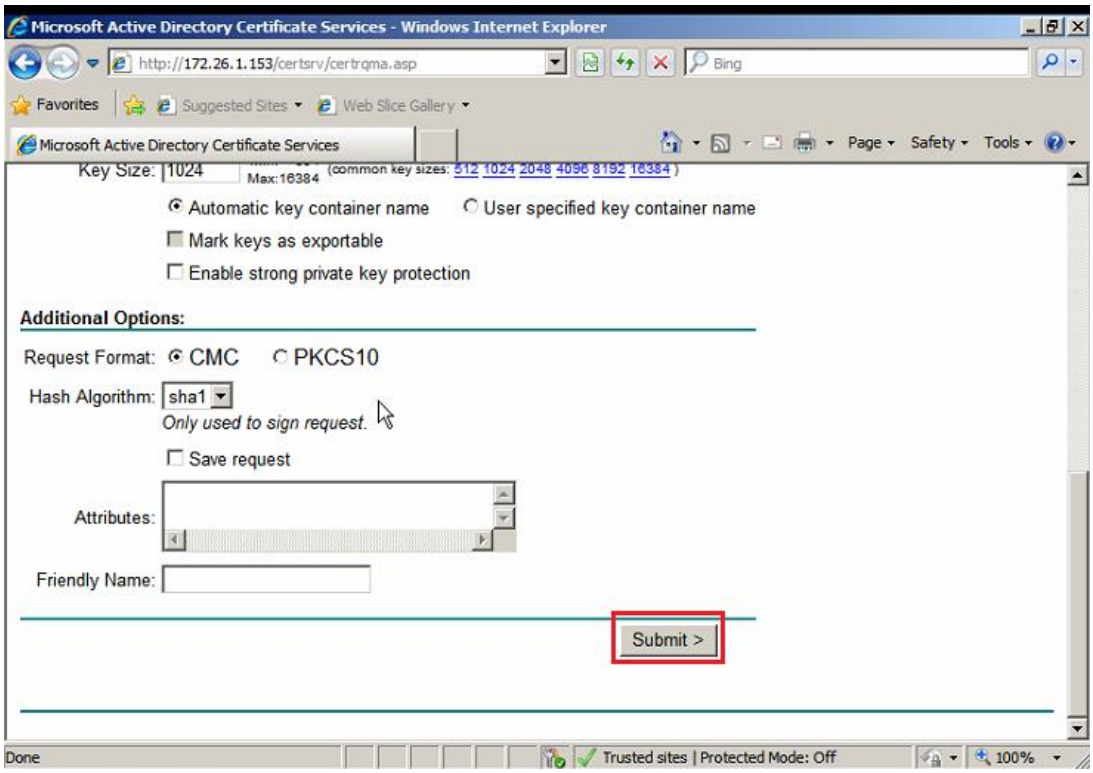

Microsoft Active Directory Certificate Services - Windows Internet Explorer
http://172.26.1.153/certsrv/certrqad.asp
Bing
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Certificate Services
Page
Safety
Tools
Microsoft Active Directory Certificate Services -- ruijie007-WIN-GPTDUSF68P4-CA
Home
Advanced Certificate Request
The policy of the CA determines the types of certificates you can request. Click one of the following options to:
Create and submit a request to this CA.
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
Trusted sites | Protected Mode: Off
100%

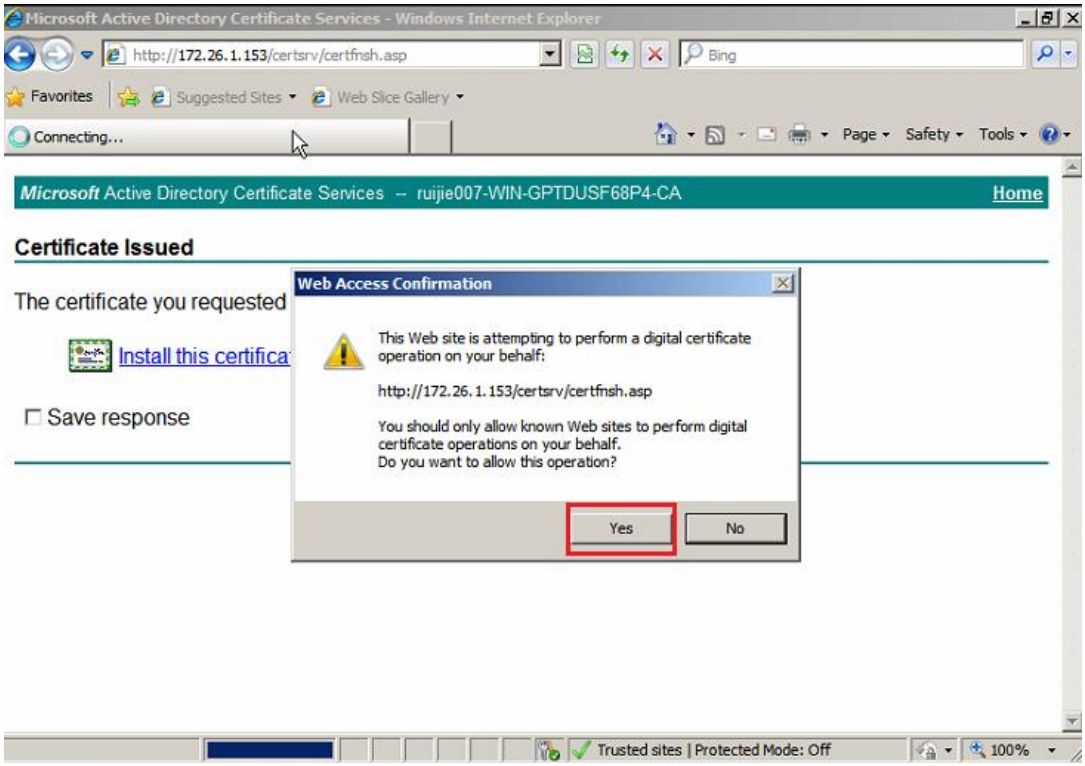


It recommended to use PC name of the server to apply for web server and other options keeps default settings.进行web

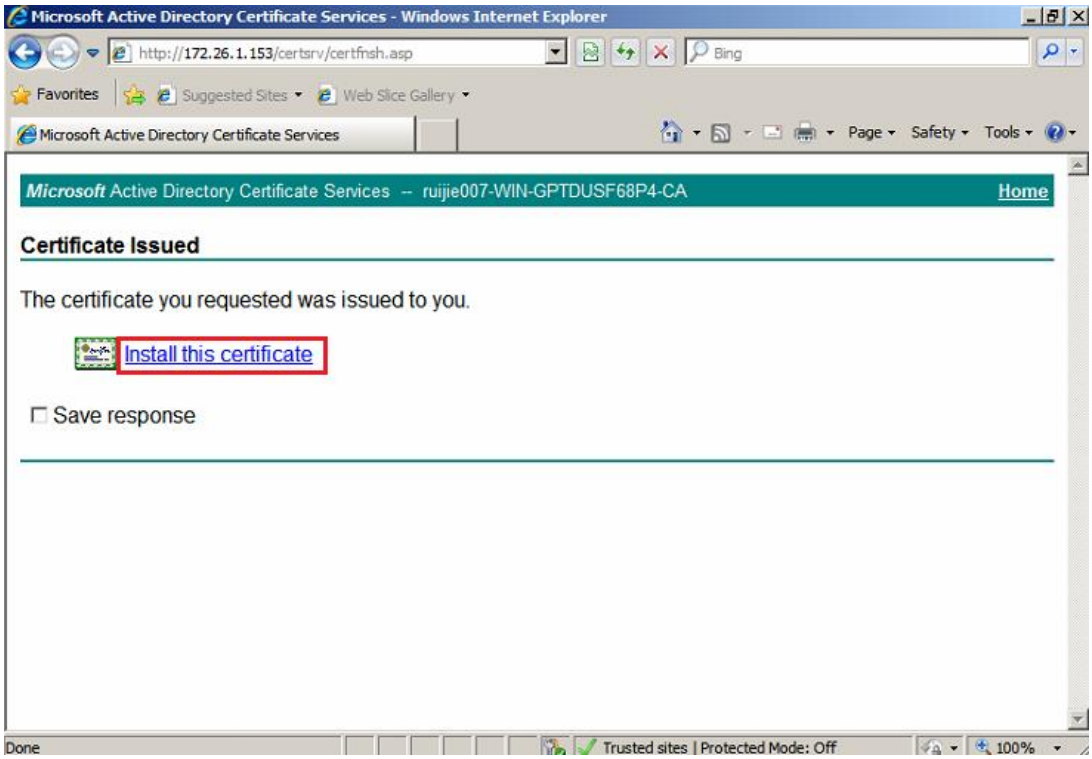
Then click Submit for ‘application’.

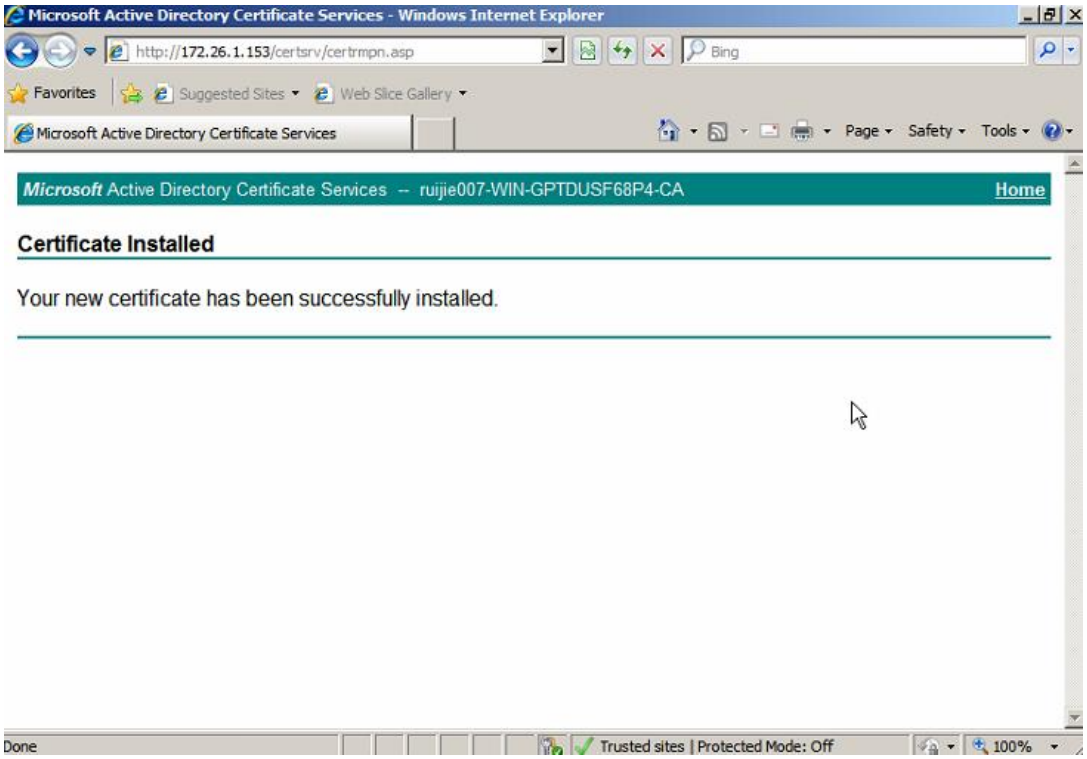




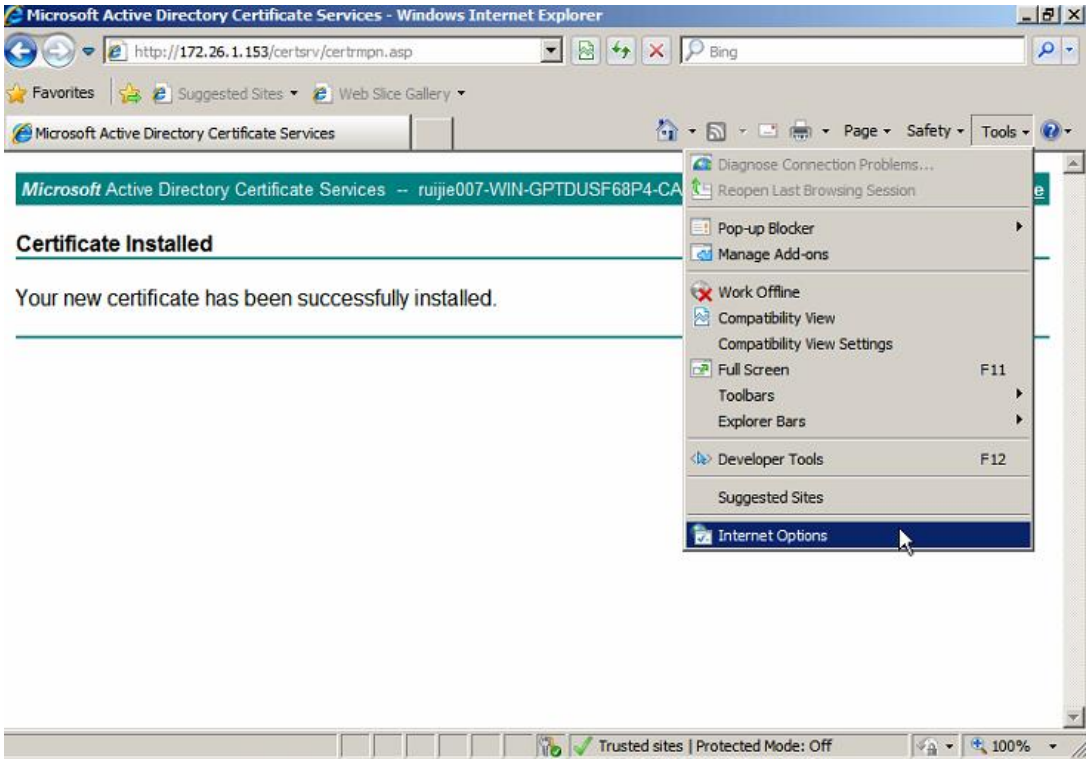


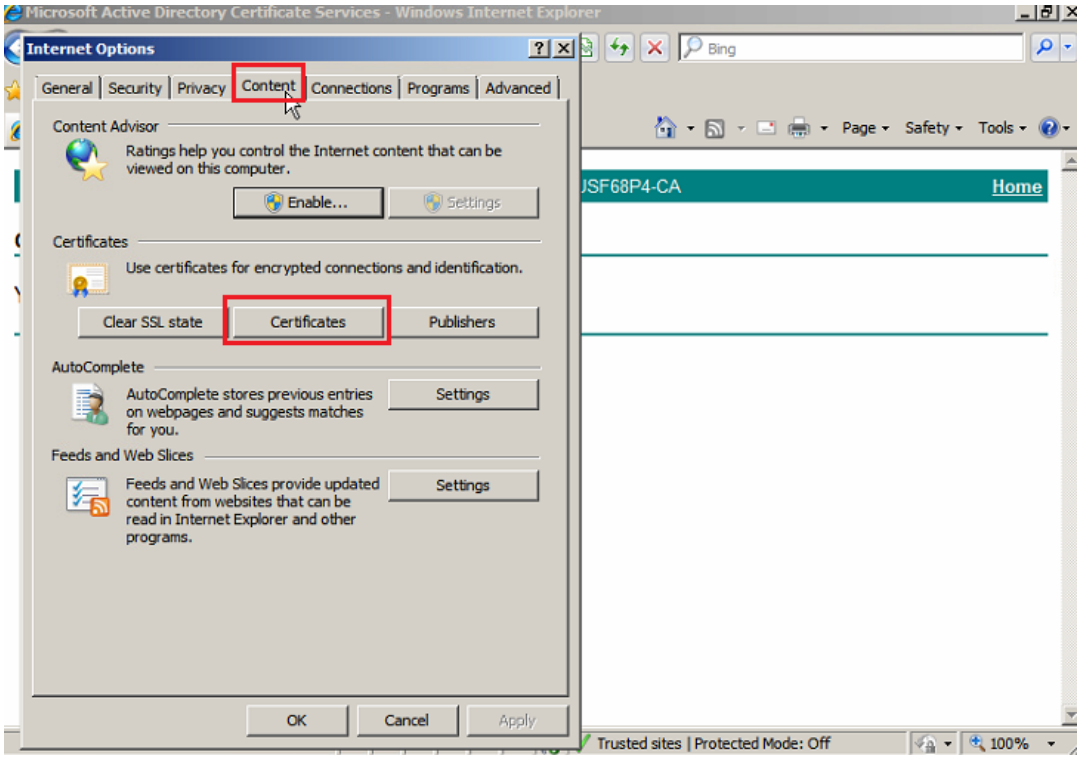
Click ‘Yes’ to apply the certification. After the application is complete, click ‘Install this certificate’ to install.

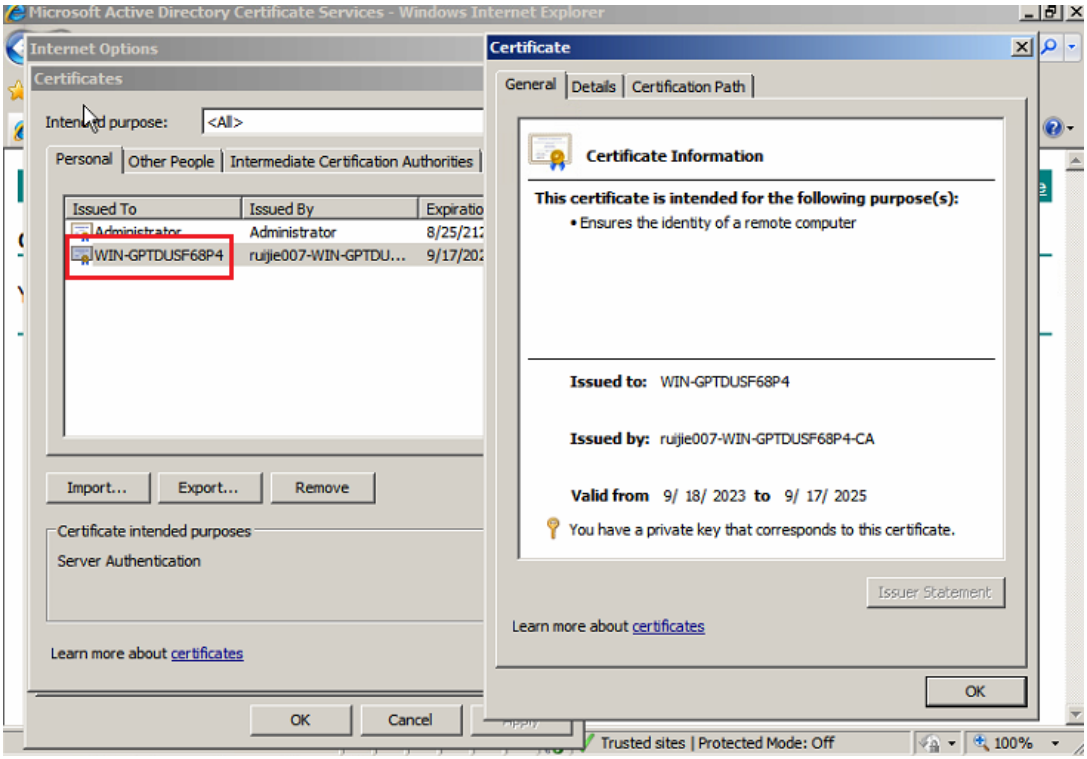




Check the certificate:


Microsoft Active Directory Certificate Services - Windows Internet Explorer
http://172.26.1.153/certsrv/certrmpn.asp
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Certificate Services
Page
Safety
Tools
Diagnose Connection Problems...
Reopen Last Browsing Session
Pop-up Blocker
Manage Add-ons
Work Offline
Compatibility View
Compatibility View Settings
Full Screen F11
Toolbars
Explorer Bars
Developer Tools F12
Suggested Sites
Internet Options
Microsoft Active Directory Certificate Services -- ruijie007-WIN-GPTDUSF68P4-CA
Certificate Installed
Your new certificate has been successfully installed.
Trusted sites | Protected Mode: Off
100%

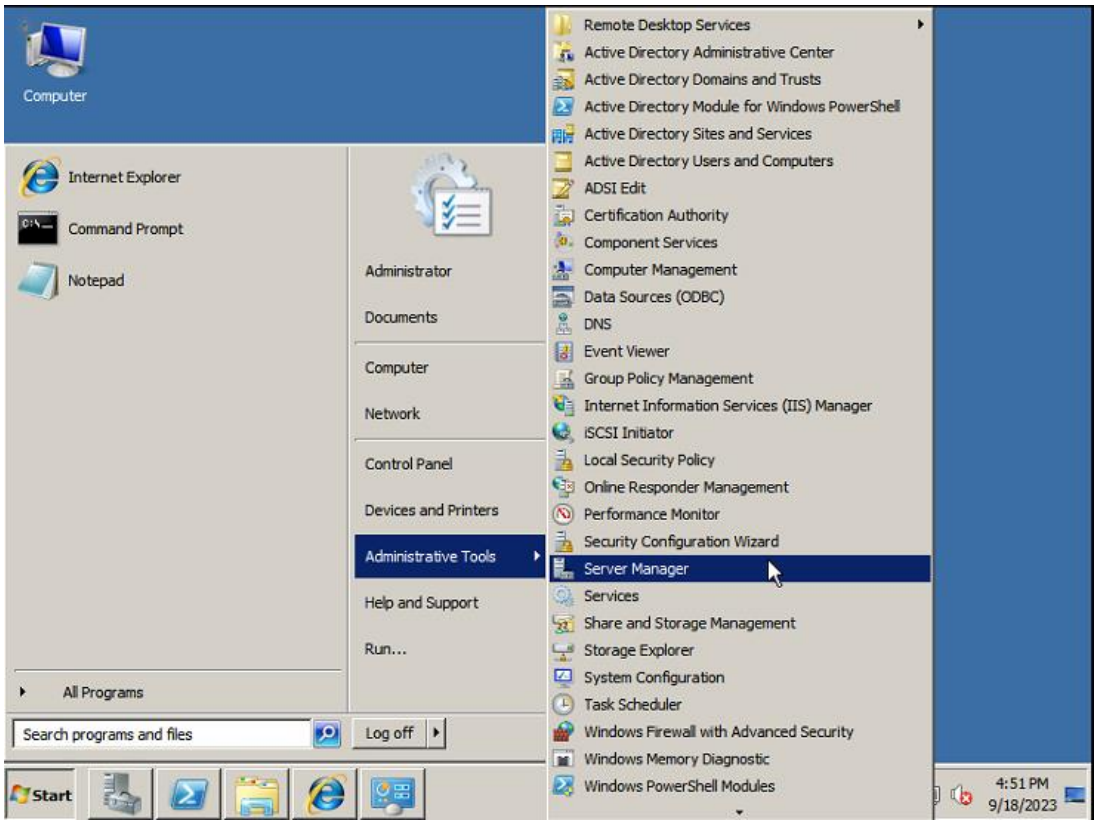

Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Content Advisor
Ratings help you control the Internet content that can be viewed on this computer.
Enable...
Settings
Certificates
Use certificates for encrypted connections and identification.
Clear SSL state
Certificates
Publishers
AutoComplete
AutoComplete stores previous entries on webpages and suggests matches for you.
Settings
Feeds and Web Slices
Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.
Settings
OK
Cancel
Apply
Home
Trusted sites | Protected Mode: Off
100%



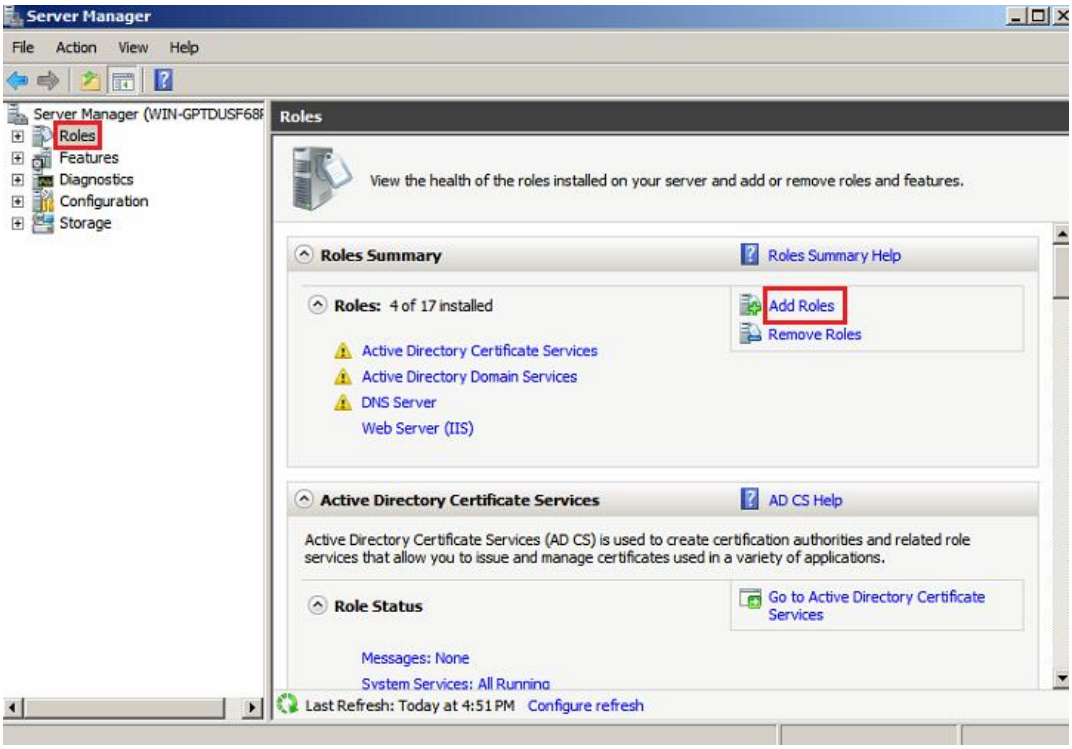
After the certificate is installed, please follow the above guides to check whether the certificate is installed successfully.

1.5 NPS Server Installation

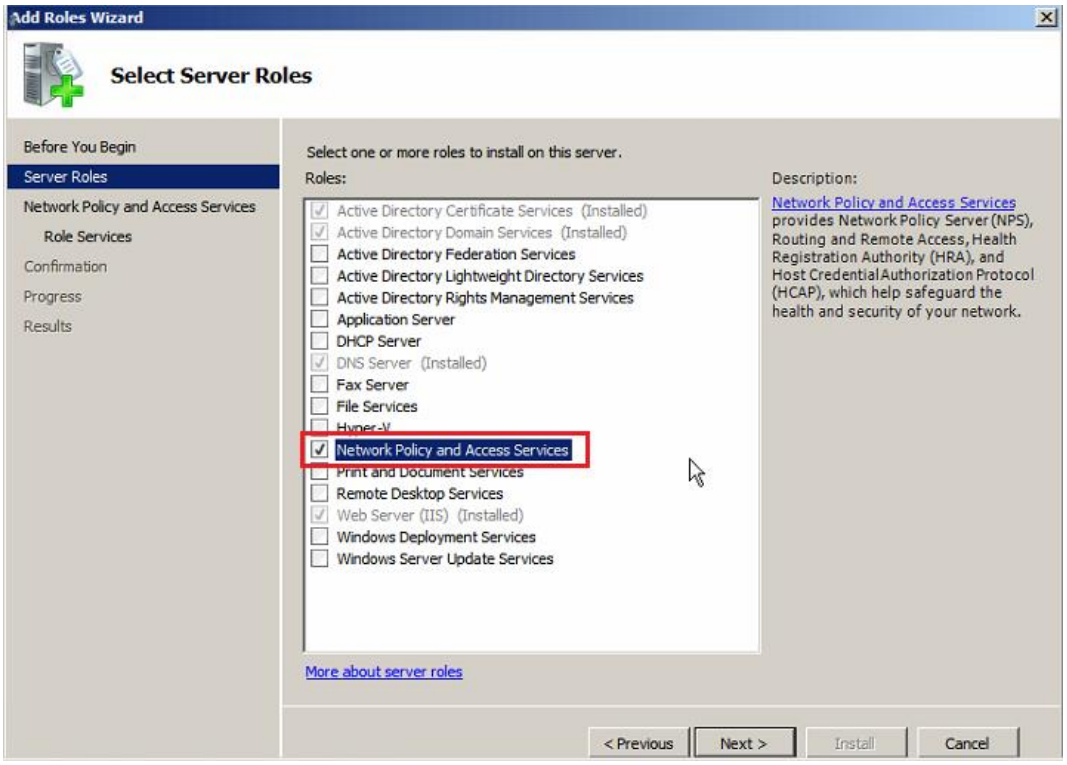
(1) Click '[Start]>>[Administrative Tools] >>[Server Manager]' to open server manager



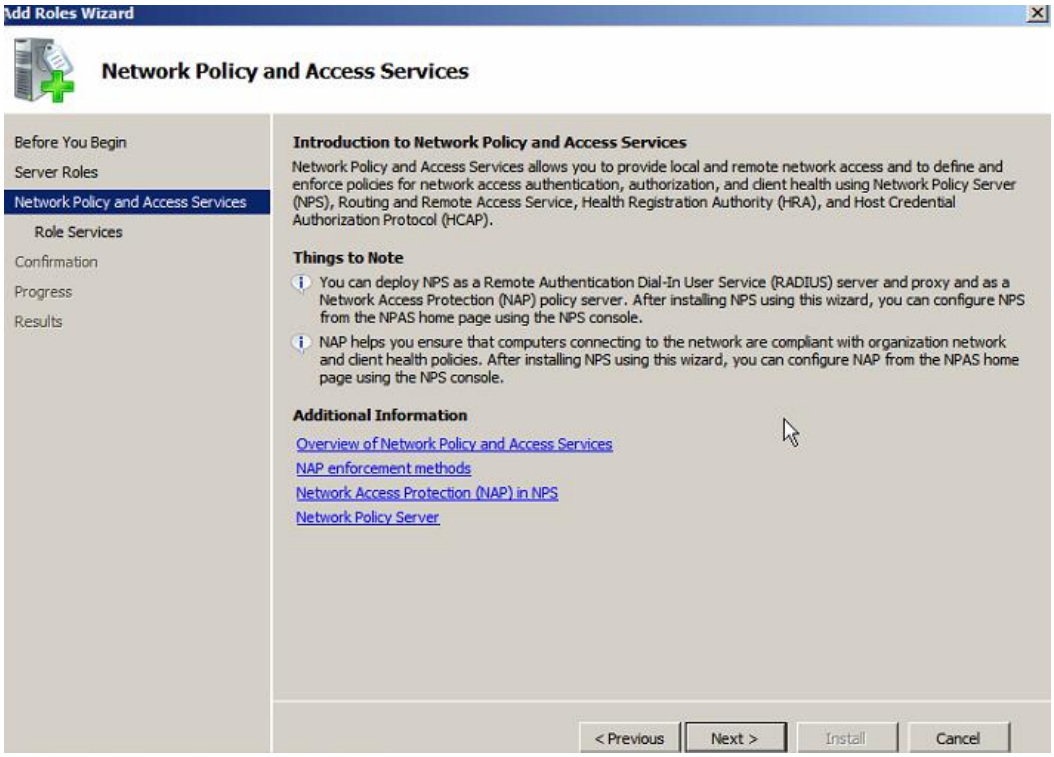
Click 'Roles' in the left menu and click 'Add Roles' in the right 'Roles Summary'.



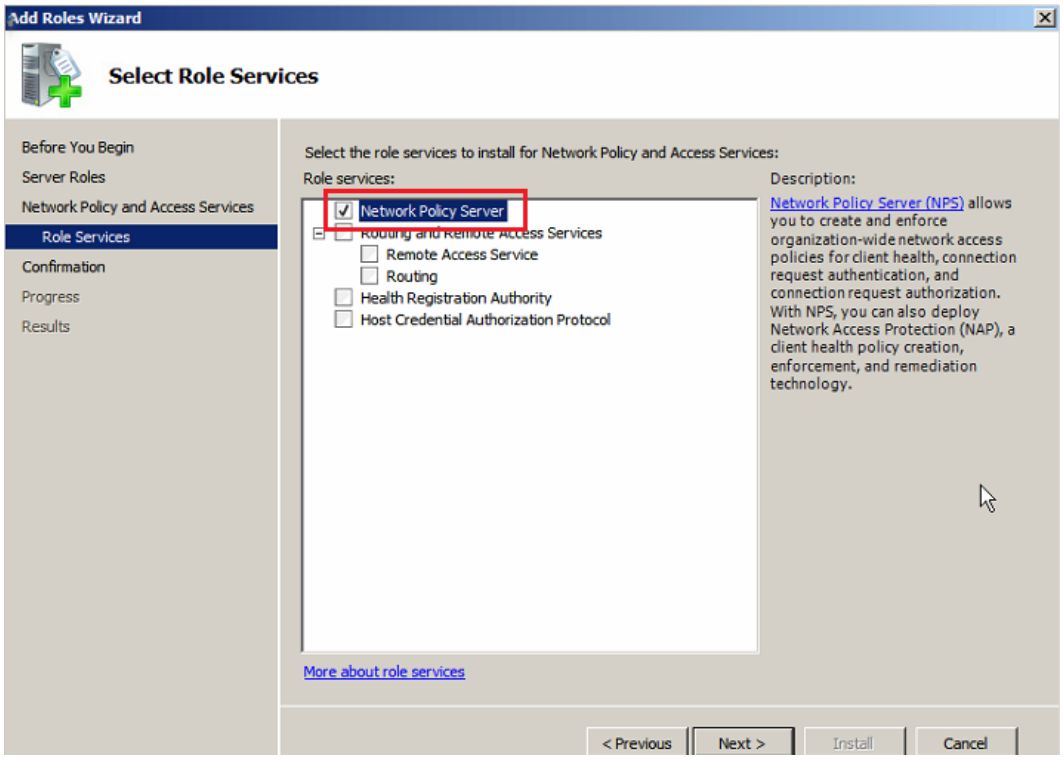
Choose Network Policy and Access Service to install.



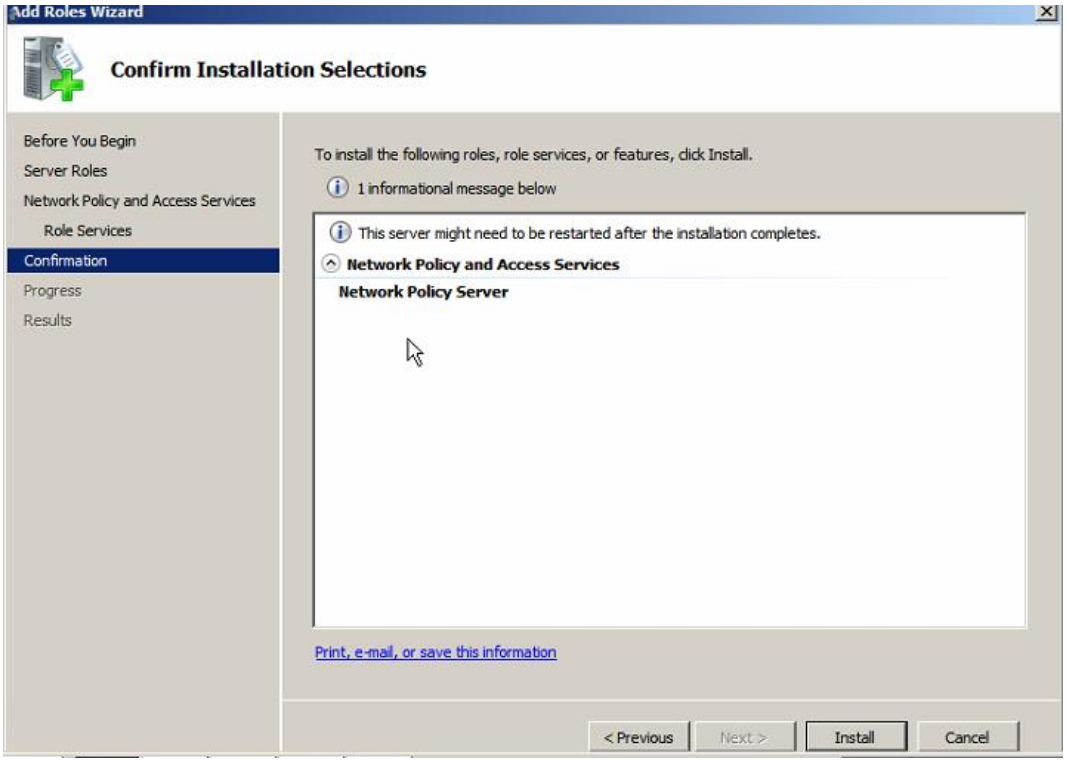
Select Network Policy and Access Service

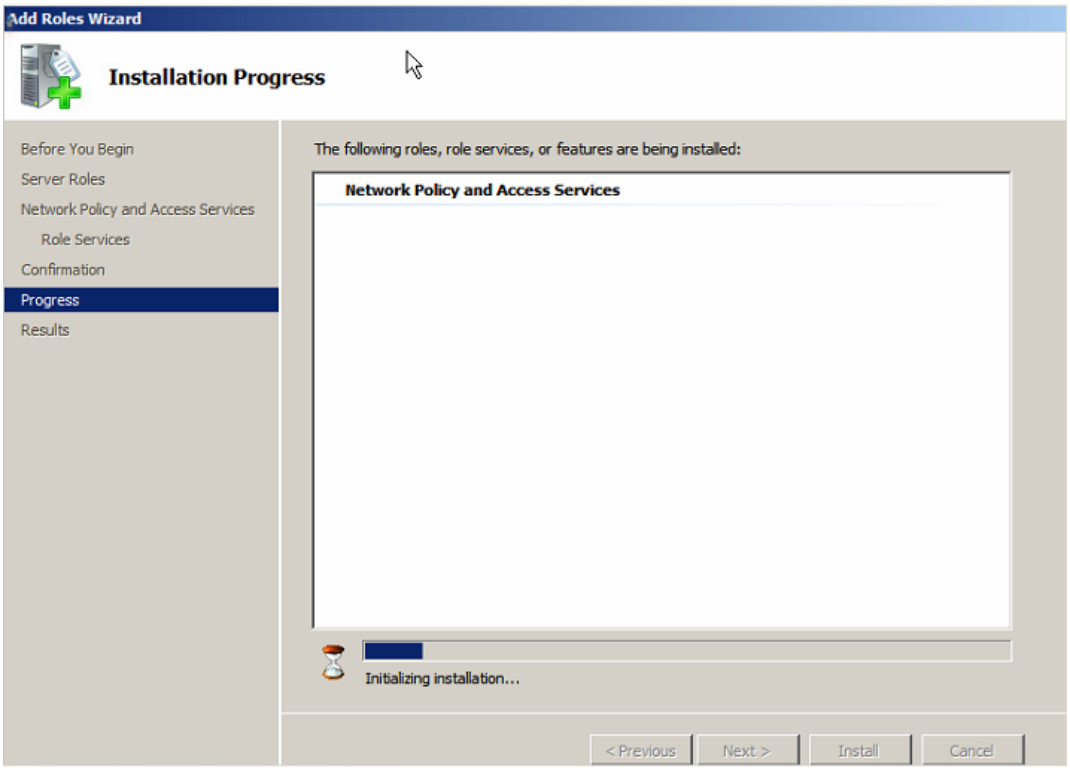


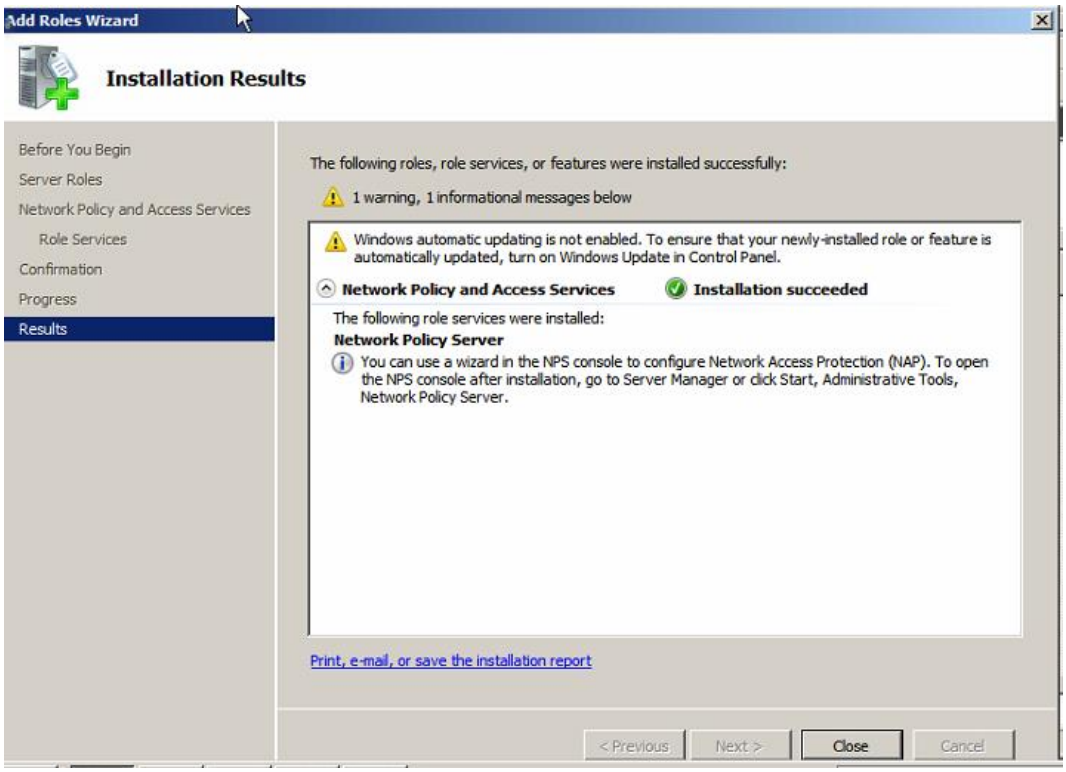
Click Next



Select Network Policy Server


Add Roles Wizard
Confirm Installation Selections
Before You Begin
Server Roles
Network Policy and Access Services
Role Services
Confirmation
Progress
Results
To install the following roles, role services, or features, click Install.
1 informational message below
This server might need to be restarted after the installation completes.
Network Policy and Access Services
Network Policy Server
Print, e-mail, or save this information
< Previous
Next >
Install
Cancel


Add Roles Wizard
Installation Progress
Before You Begin
Server Roles
Network Policy and Access Services
Role Services
Confirmation
Progress
Results
The following roles, role services, or features are being installed:
Network Policy and Access Services
Initializing installation...
< Previous
Next >
Install
Cancel



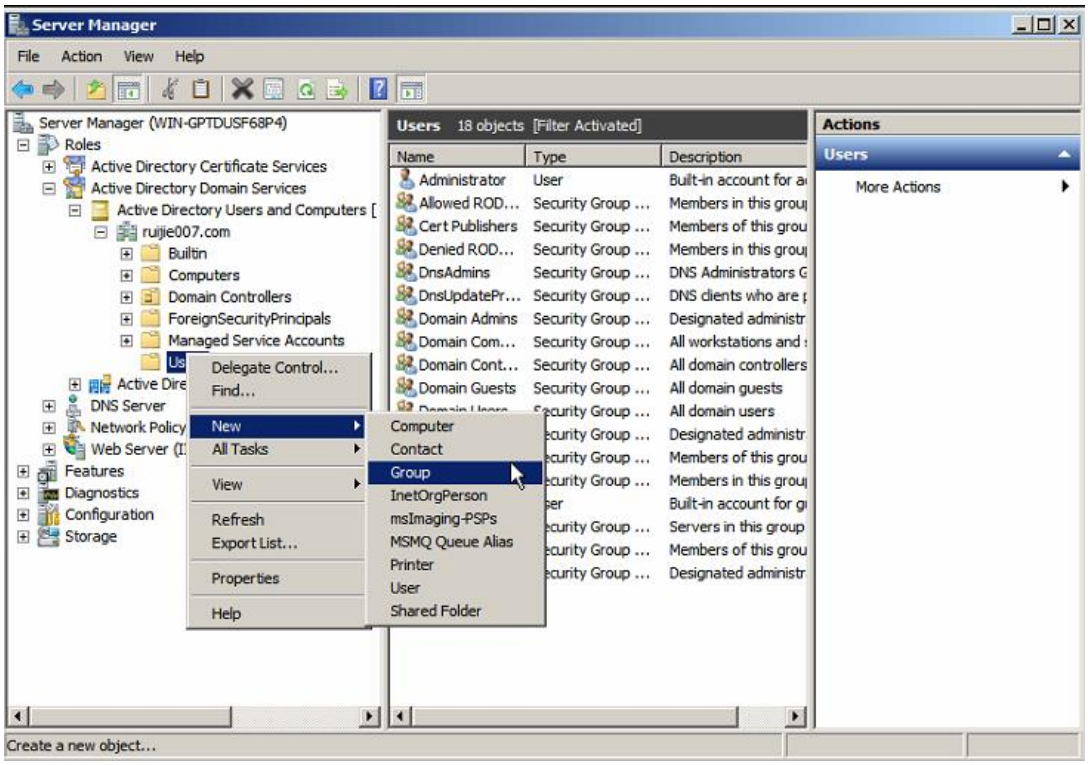
The network policy and access services are now installed. Restart the PC if it is necessary.

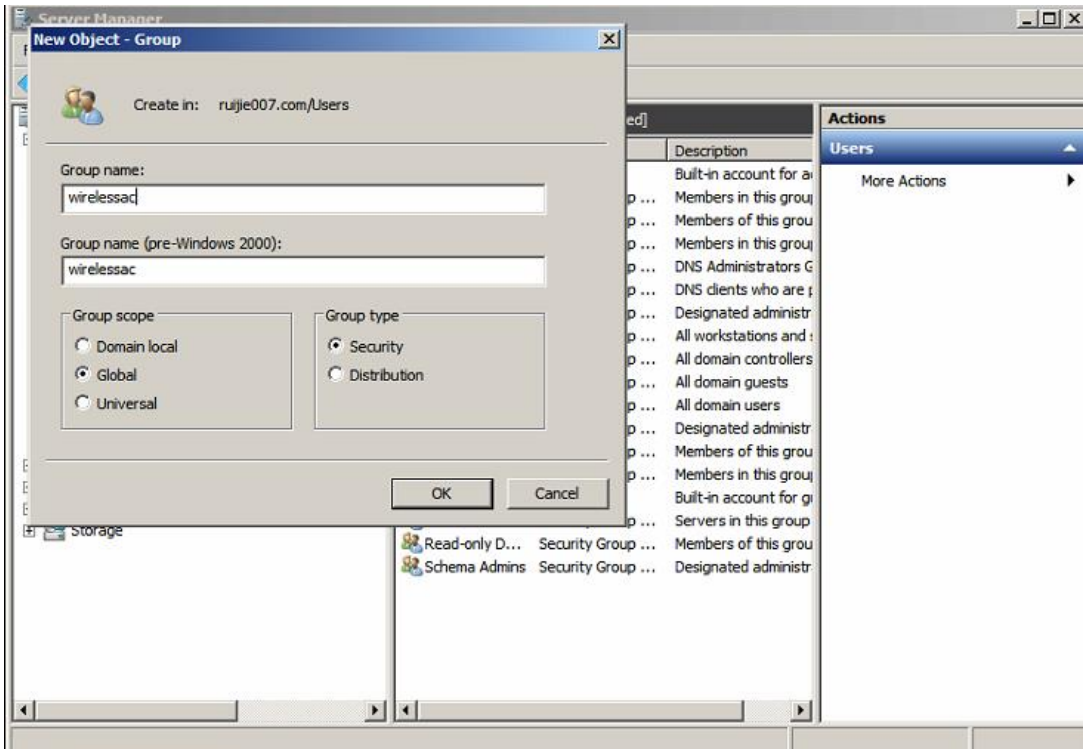
After the above steps, we have completed the installation: AD domain service, DNS service, AD Domain certificate, WEB Server (IIS), network policy, and access service.

1.6 Configure NPS Server

1.6.1 Add User and Group in the AD Domain Server.

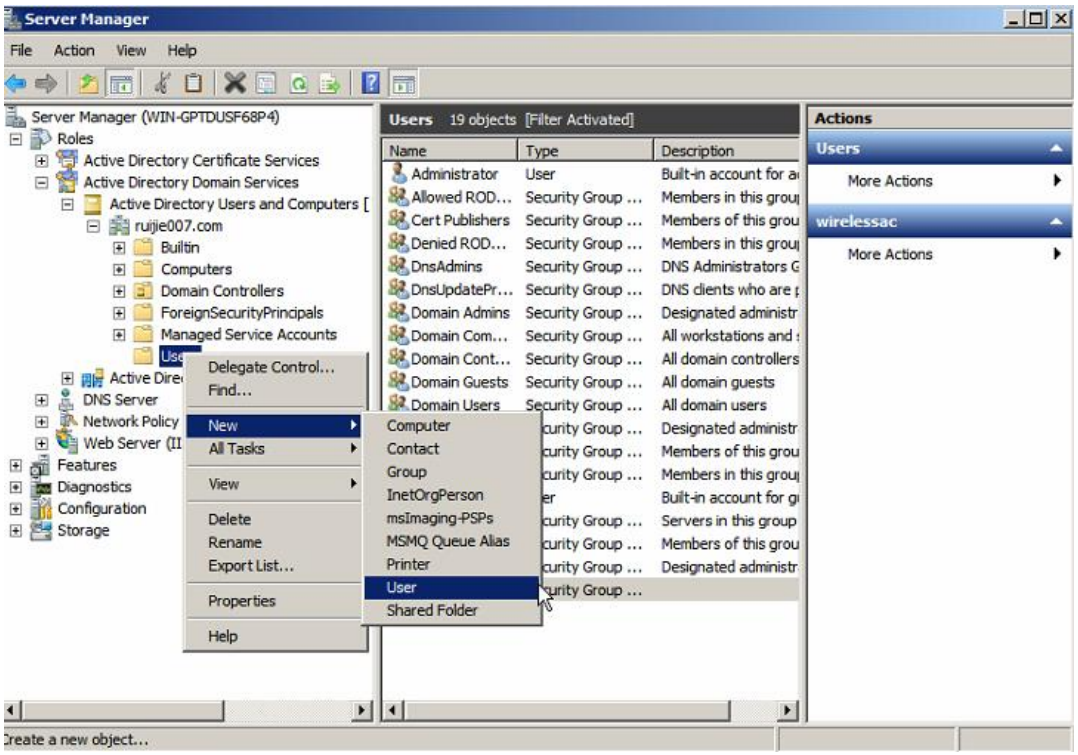
(1) Add users and group in the AD domain server. Choose user and click new-> group.

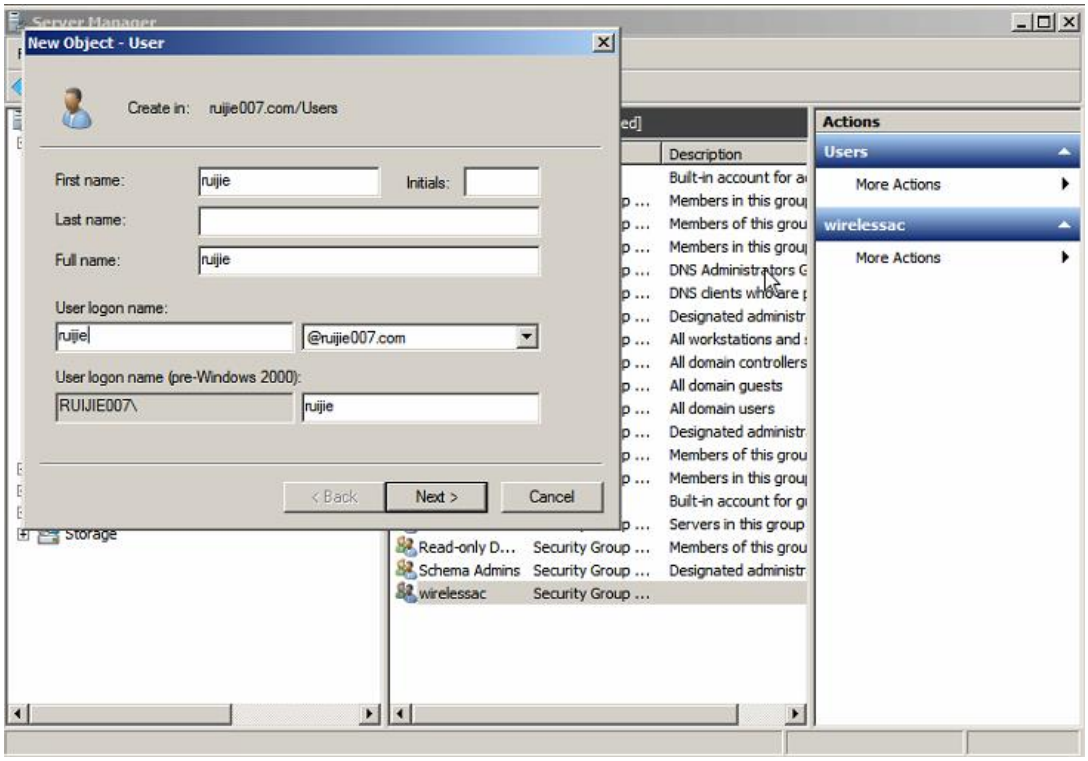




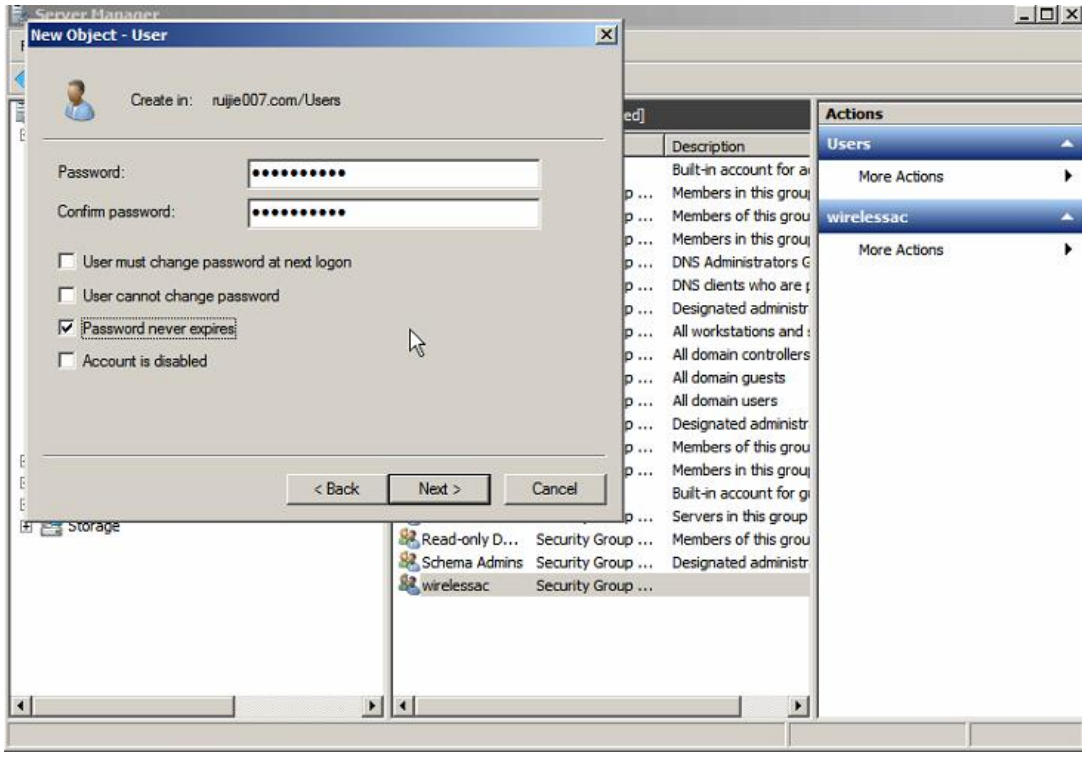
Create a group in the user of AD domain

(2) Add users after group is created. Select User and then click ‘New->User.

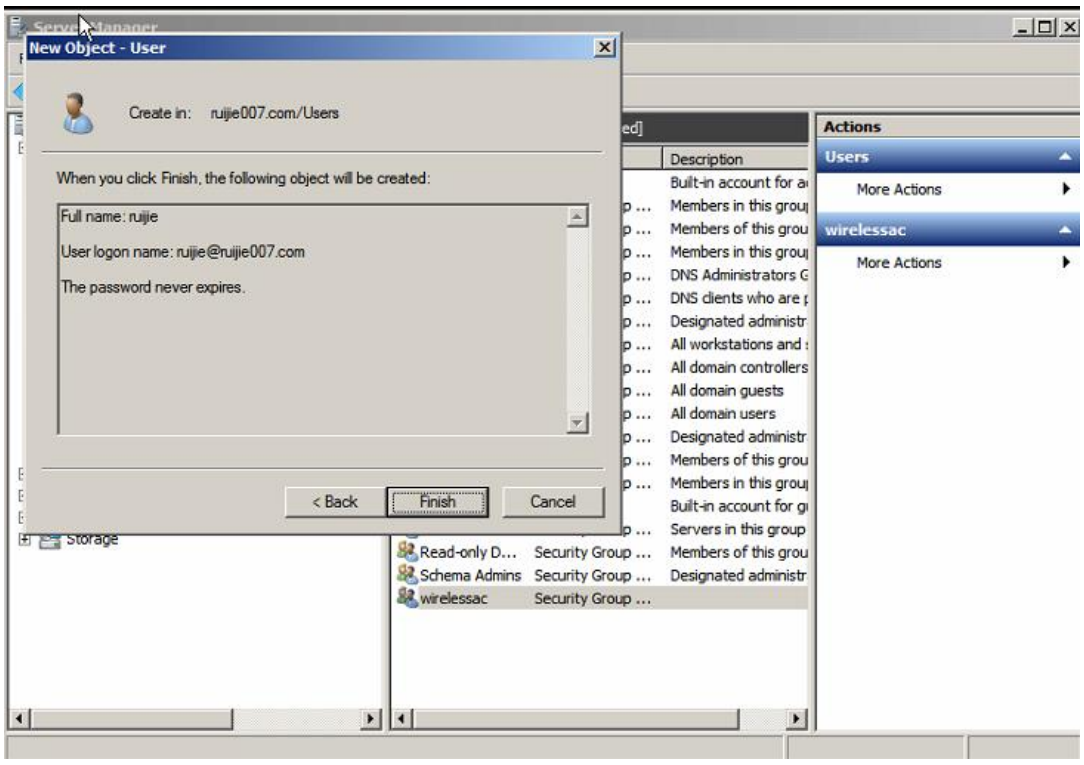




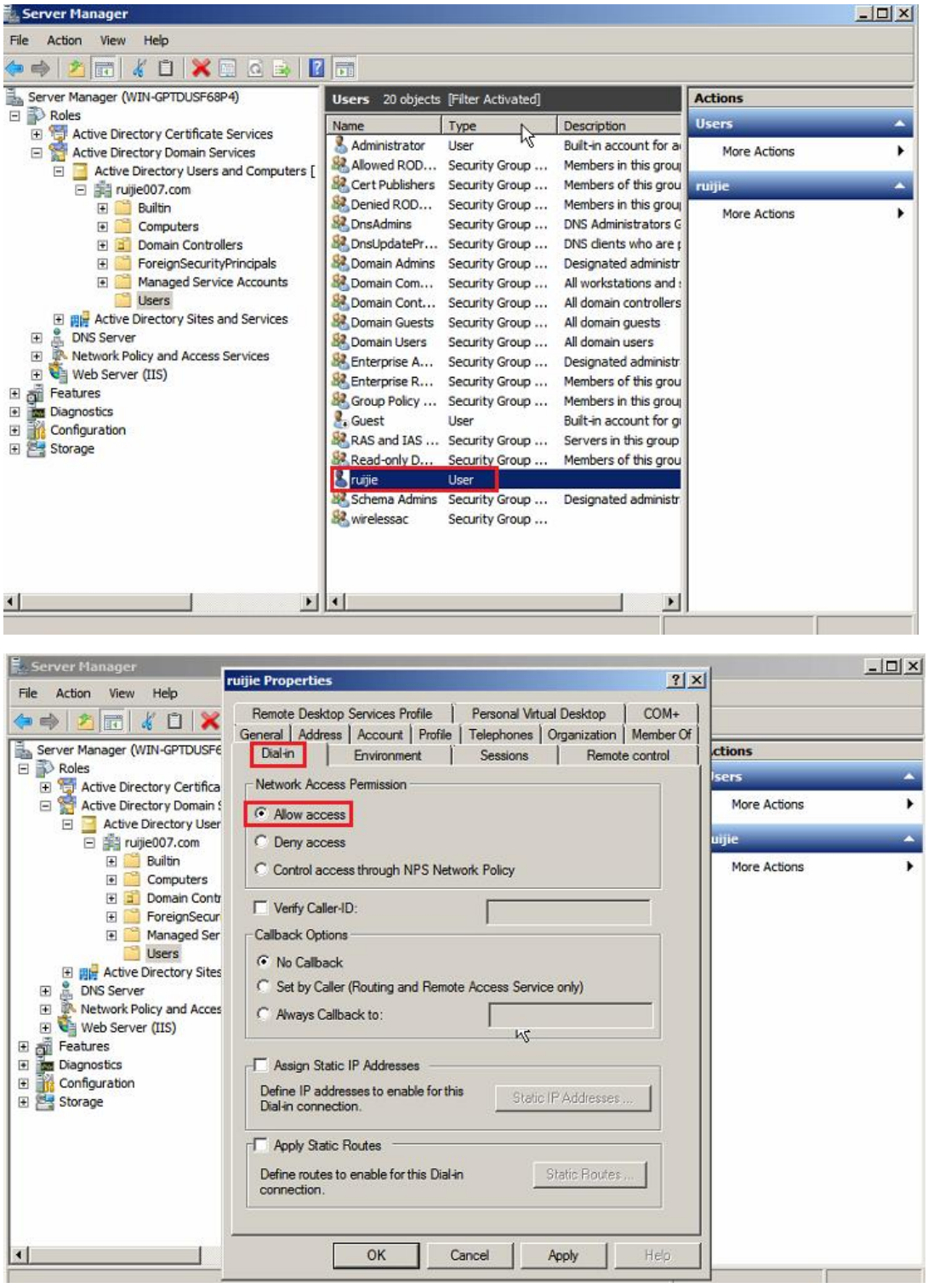
Add a new user in the user of AD domain



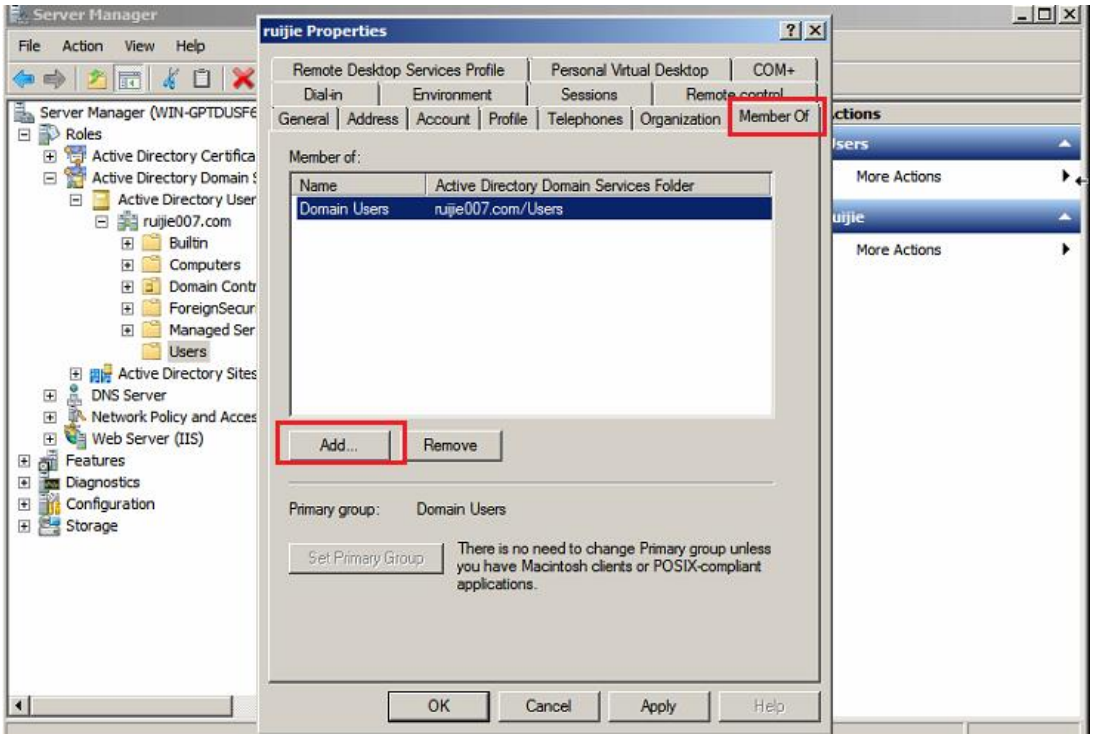
The password must contain letters, special characters, and digits

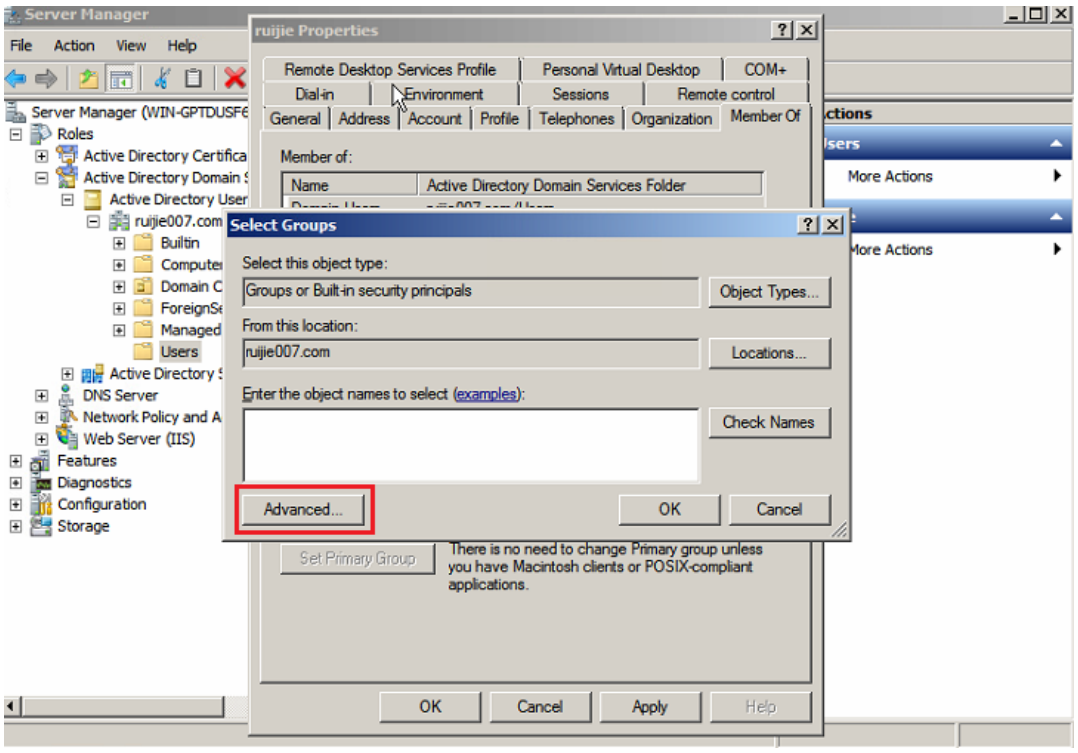


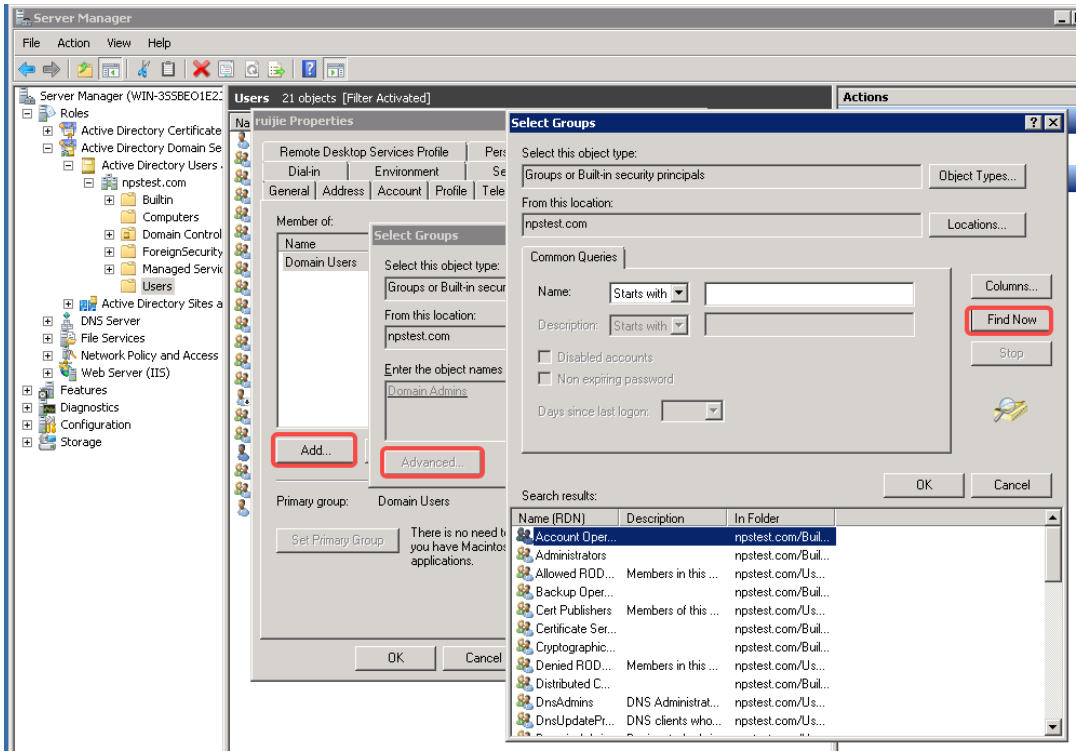
(3) Double click ruijie account to set user properties including the ‘dial-in’ properties and ‘member of’ properties

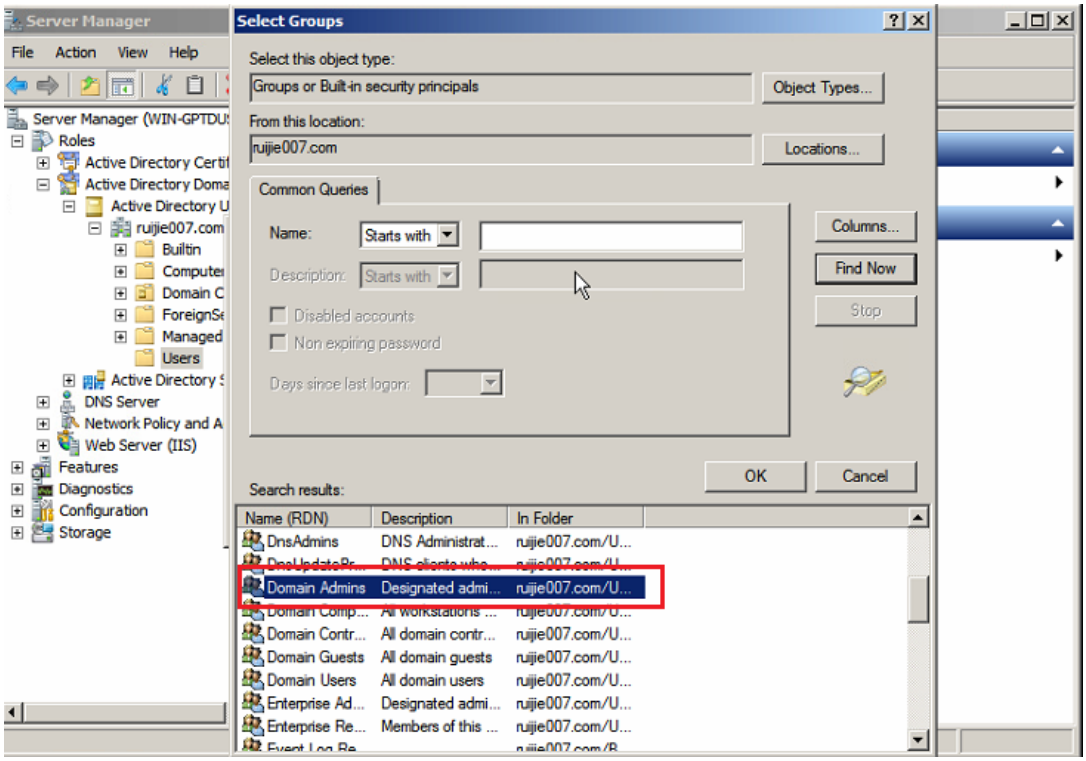


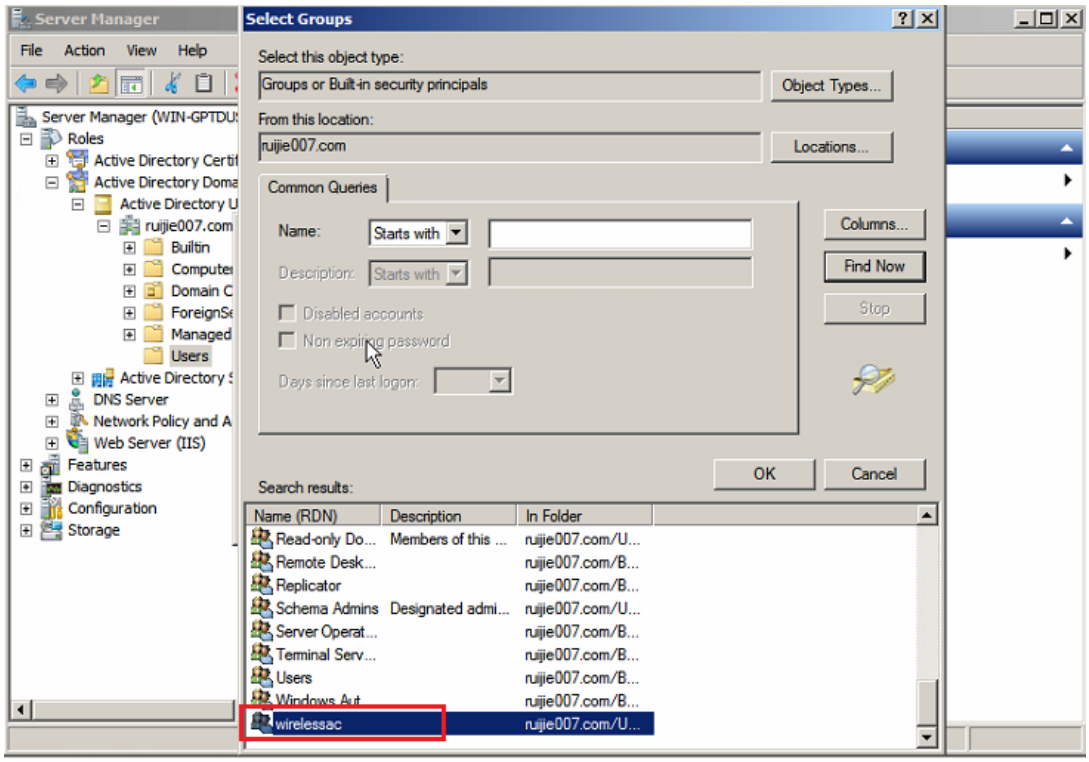
User Properties Setting

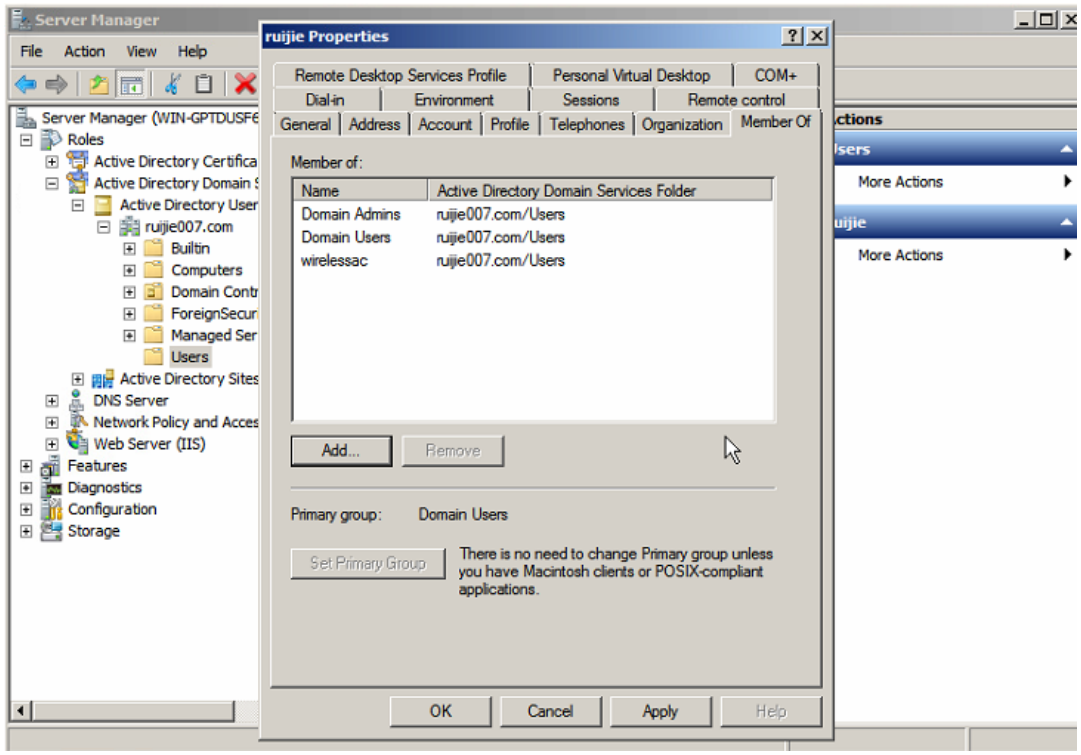

Server Manager
File Action View Help
Server Manager (WIN-GPTDUSF6
Roles
Active Directory Certifica
Active Directory Domain
Active Directory User
ruijie007.com
Builtin
Computers
Domain Contr
ForeignSecur
Managed Ser
Users
Active Directory Sites
DNS Server
Network Policy and Acces
Web Server (IIS)
Features
Diagnostics
Configuration
Storage
ruijie Properties
Remote Desktop Services Profile
Personal Virtual Desktop
COM+
Dial-in
Environment
Sessions
Remote control
General
Address
Account
Profile
Telephones
Organization
Member Of
Member of:
Name
Active Directory Domain Services Folder
Domain Users
ruijie007.com/Users
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help
More Actions
More Actions


Server Manager
File Action View Help
ruijie Properties
Remote Desktop Services Profile
Personal Virtual Desktop
COM+
Dial-in
Environment
Sessions
Remote control
General
Address
Account
Profile
Telephones
Organization
Member Of
Member of:
Name
Active Directory Domain Services Folder
Select Groups
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
ruijie007.com
Locations...
Enter the object names to select (examples):
Check Names
Advanced...
OK
Cancel
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help
More Actions

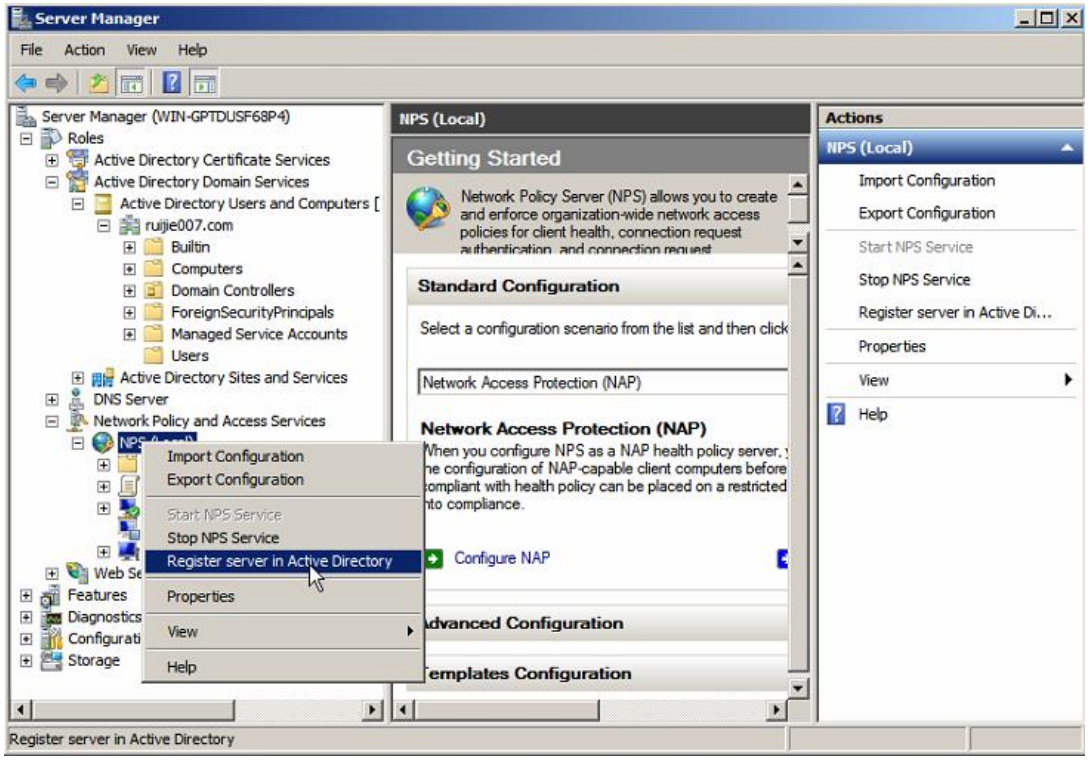

Server Manager
File Action View Help
Server Manager (WIN-3SSBEO1E2
Roles
Active Directory Certificate
Active Directory Domain Se
Active Directory Users
npstest.com
Builtin
Computers
Domain Control
ForeignSecurity
Managed Servic
Users
Active Directory Sites a
DNS Server
File Services
Network Policy and Access
Web Server (IIS)
Features
Diagnostics
Configuration
Storage
Users 21 objects [Filter Activated]
Actions
ruijie Properties
Remote Desktop Services Profile
Dial-in
Environment
General
Address
Account
Profile
Member of:
Name
Domain Users
Add...
Primary group:
Domain Users
Set Primary Group
OK
Cancel
Select Groups
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
npstest.com
Locations...
Common Queries
Name:
Starts with
Description:
Disabled accounts
Non expiring password
Days since last logon:
Columns...
Find Now
Stop
Search results:
Name (RDN)
Description
In Folder
Account Oper...
Administrators
Allowed ROD...
Members in this ...
Backup Oper...
Cert Publishers
Members of this ...
Certificate Ser...
Cryptographic...
Denied ROD...
Distributed C...
DnsAdmins
DNS Administrat...
DnsUpdatePr...
DNS clients who...
npstest.com/Buil...
npstest.com/Us...


Server Manager
File Action View Help
Server Manager (WIN-GPTDU
Roles
Active Directory Certif
Active Directory Doma
Active Directory U
ruijie007.com
Builtin
Computer
Domain C
ForeignSe
Managed
Users
Active Directory S
DNS Server
Network Policy and A
Web Server (IIS)
Features
Diagnostics
Configuration
Storage
Select Groups
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
ruijie007.com
Locations...
Common Queries
Name:
Starts with
Description:
Disabled accounts
Non expiring password
Days since last logon:
Columns...
Find Now
Stop
OK
Cancel
Search results:
Name (RDN)
Description
In Folder
DnsAdmins
DNS Administrat...
ruijie007.com/U...
Domain Admins
Designated admi...
Domain Contr...
All domain contr...
Domain Guests
All domain guests
Domain Users
All domain users
Enterprise Ad...
Designated admi...
Enterprise Re...
Members of this ...





In the process of setting the 'Member of' properties, select add->advanced->find now, select domain admin, domain users and wirelessac groups and then click 'Apply'. Now, the User name and group are added successfully.

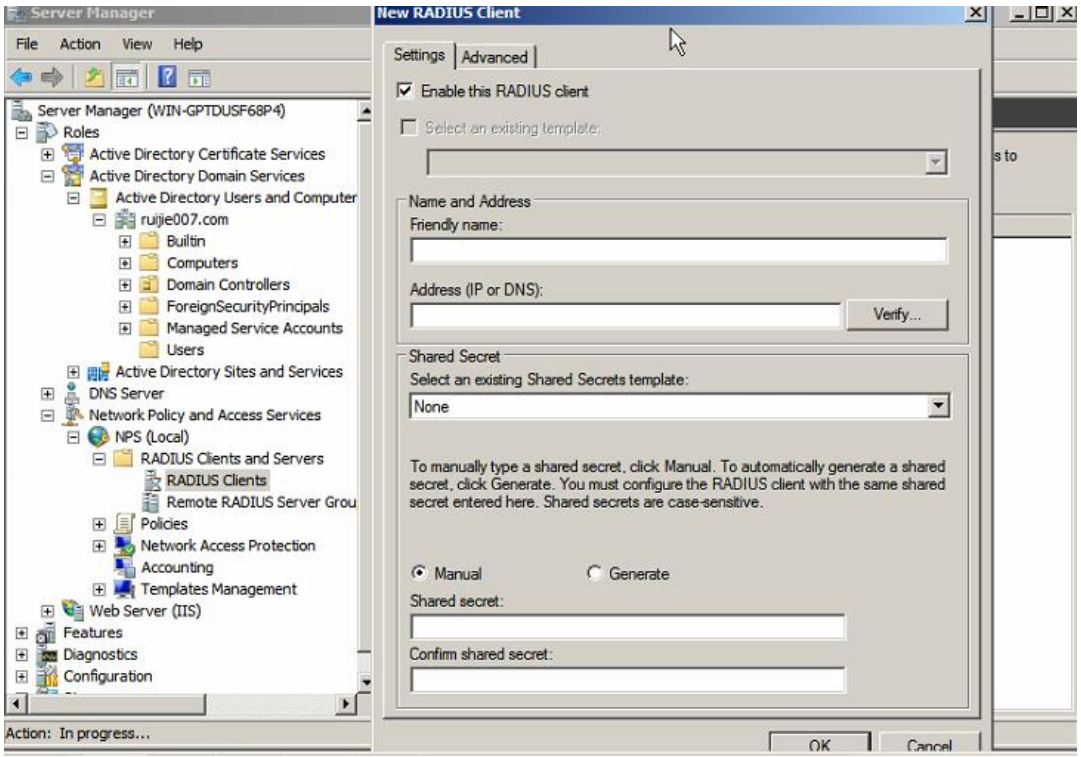


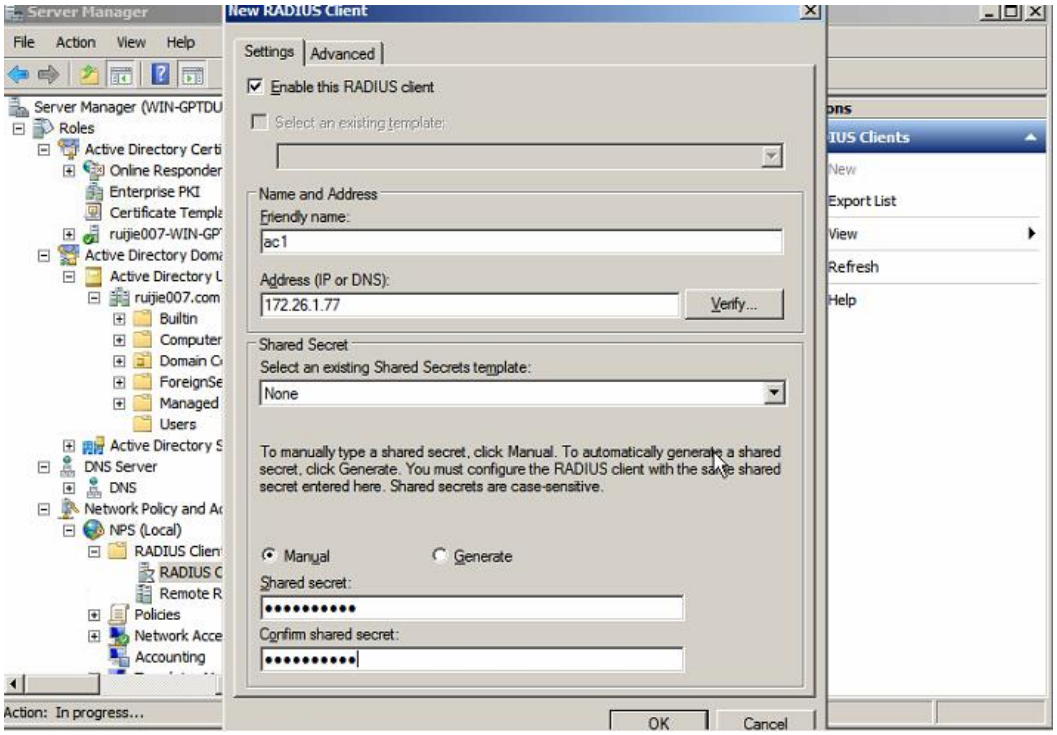
1.6.2 Enable NPS Service

Click ‘register server in active directory’. The NPS Server enable notification will be promoted when register.

1.6.3 Add radius client

Add the radius client that is the AC device we need to integrate.



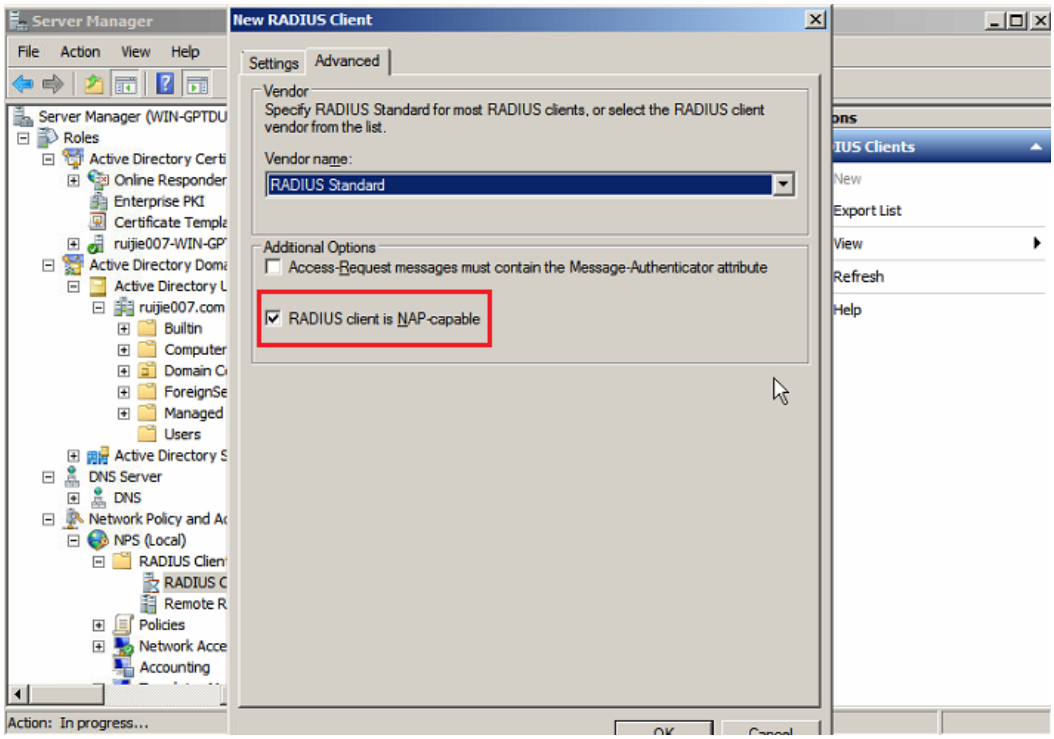


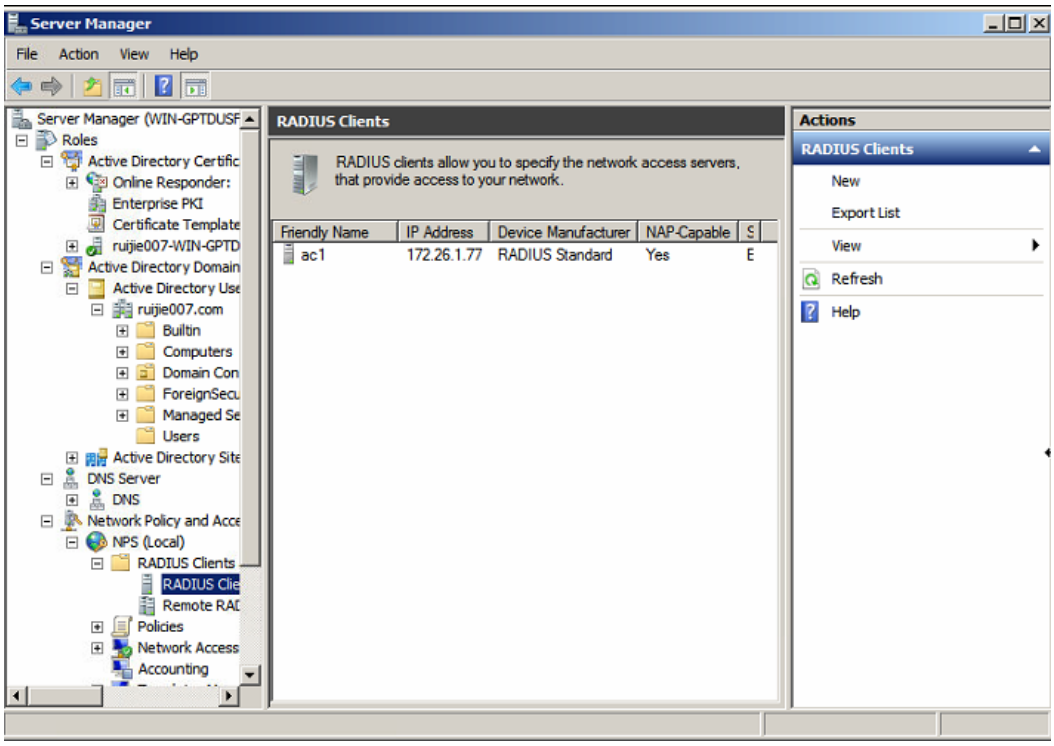
Click radius client to add the AC device. Please note that the key you configured in shared secret should be consistently with the configuration of radius-server host 172.26.1.77 key ruijie@123.

Note: When adding Radius Clients, if the radius server are in the same local area network, the address box

Note: When you add a Radius client, if the Radius Server and AC are on the same LAN, enter the AC Address in the address box. If the Radius Server is on the external network of the AC, the AC communicates with the Radius Server using an IP address after NAT. Therefore, enter the IP Address after NAT in the address box. The Address in this article is the WAN port address of EG.

In the advanced page, click RADIUS client is NAP-capable in the Additions Options.



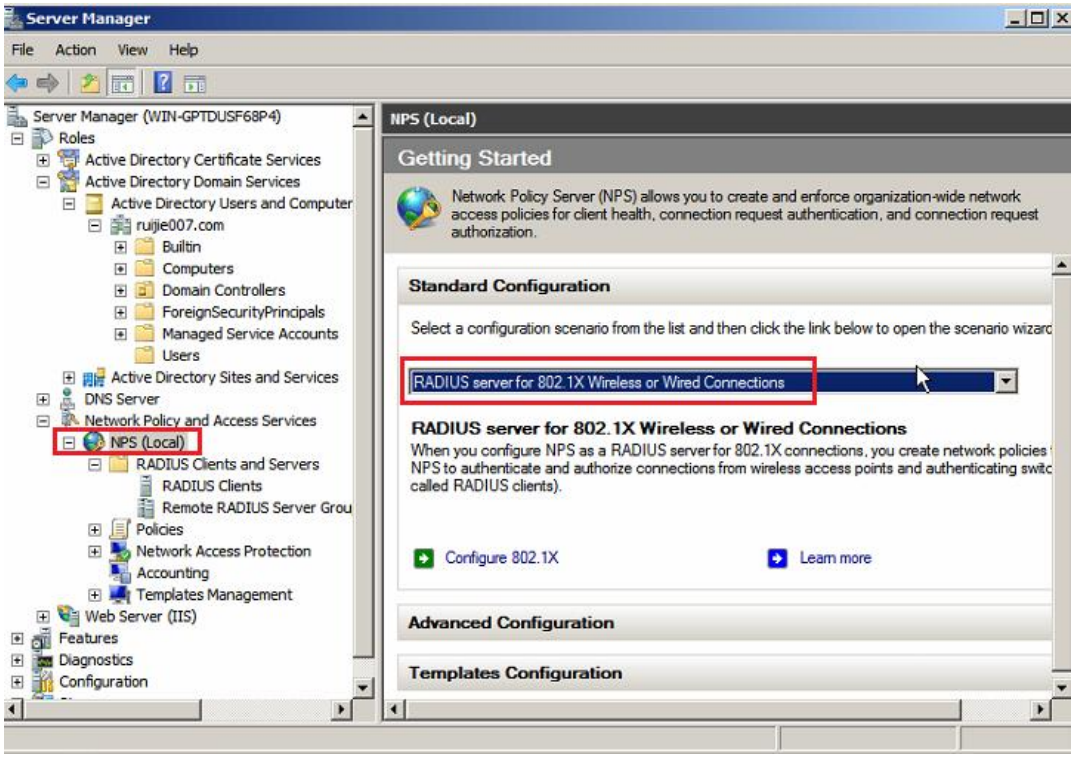


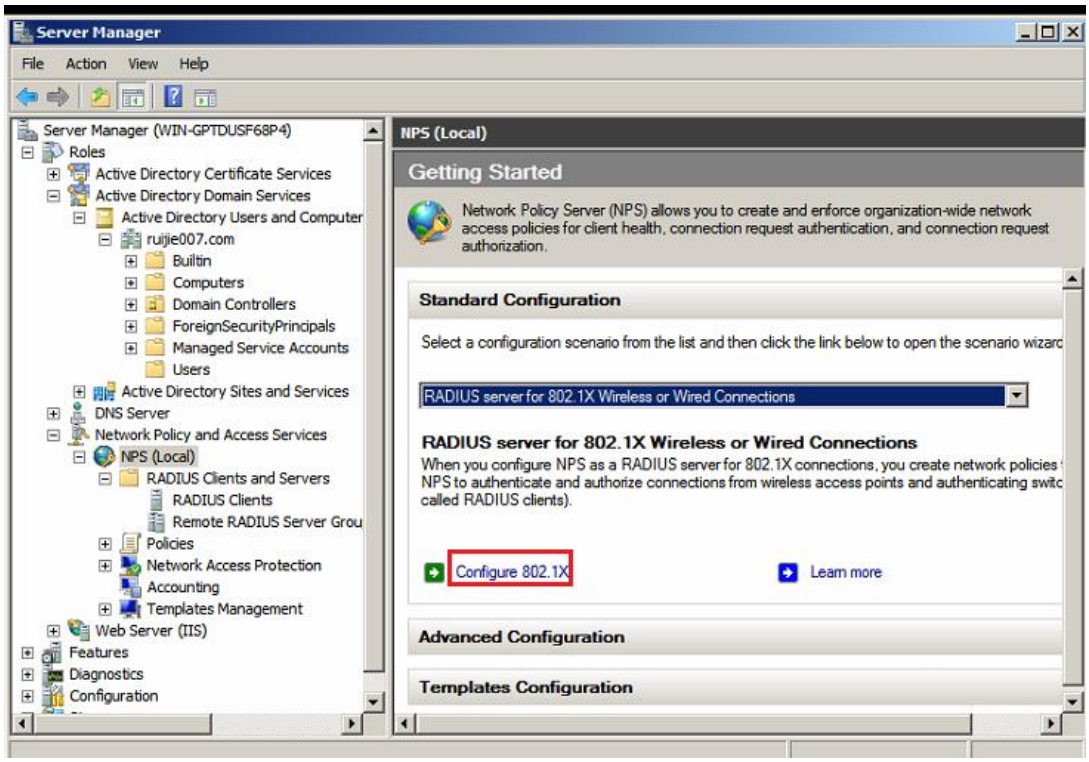
Click ‘OK’ after the settings are finished.

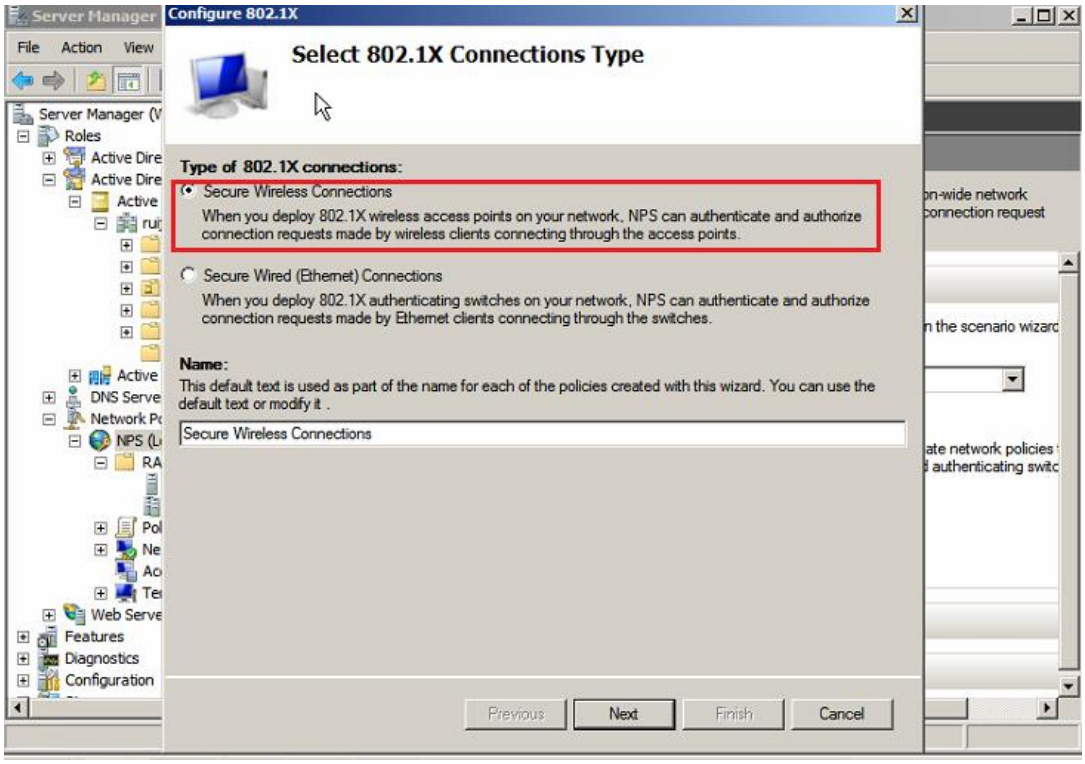
1.6.4 Set Wireless 802.1x Template

Set Wireless 802.1x template for AC

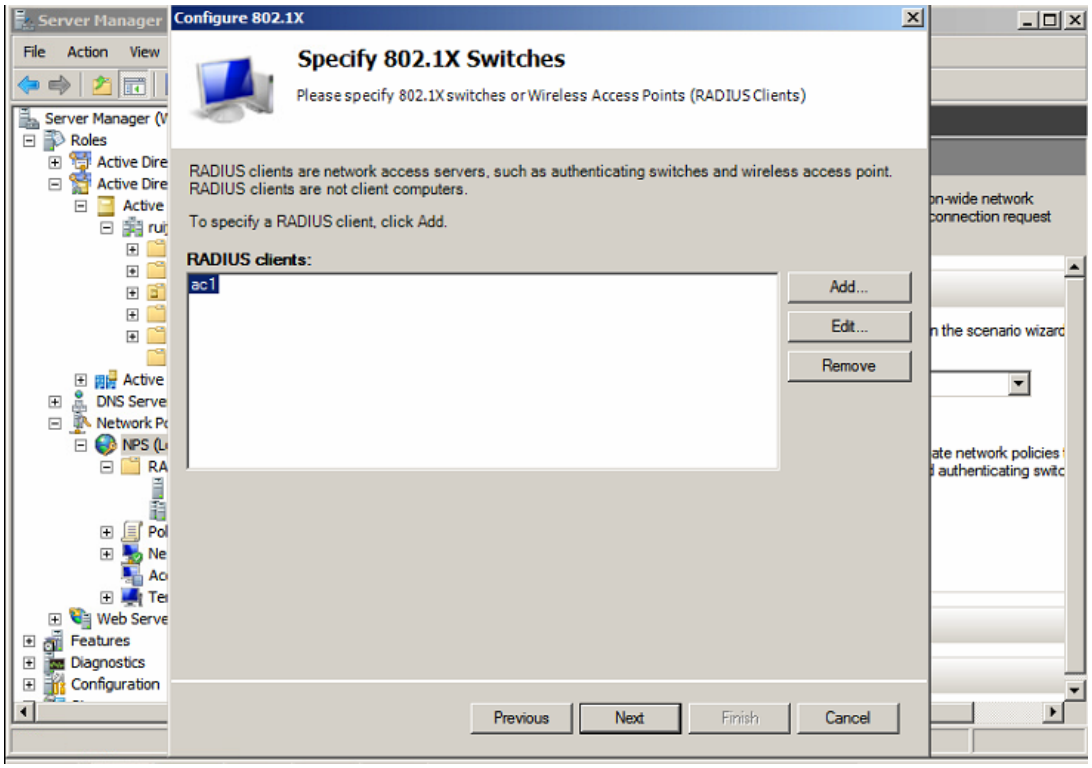
NPS(Local) > RADIUS server for 802.1x wireless or wired connections > Configure 802.1x



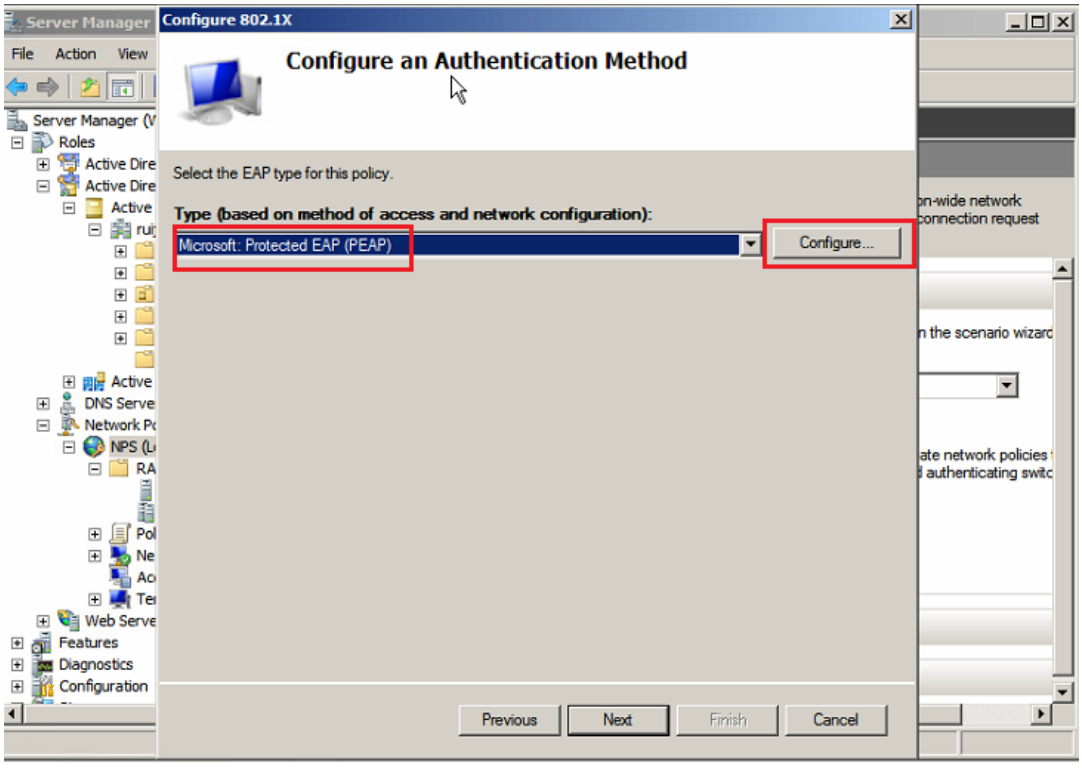




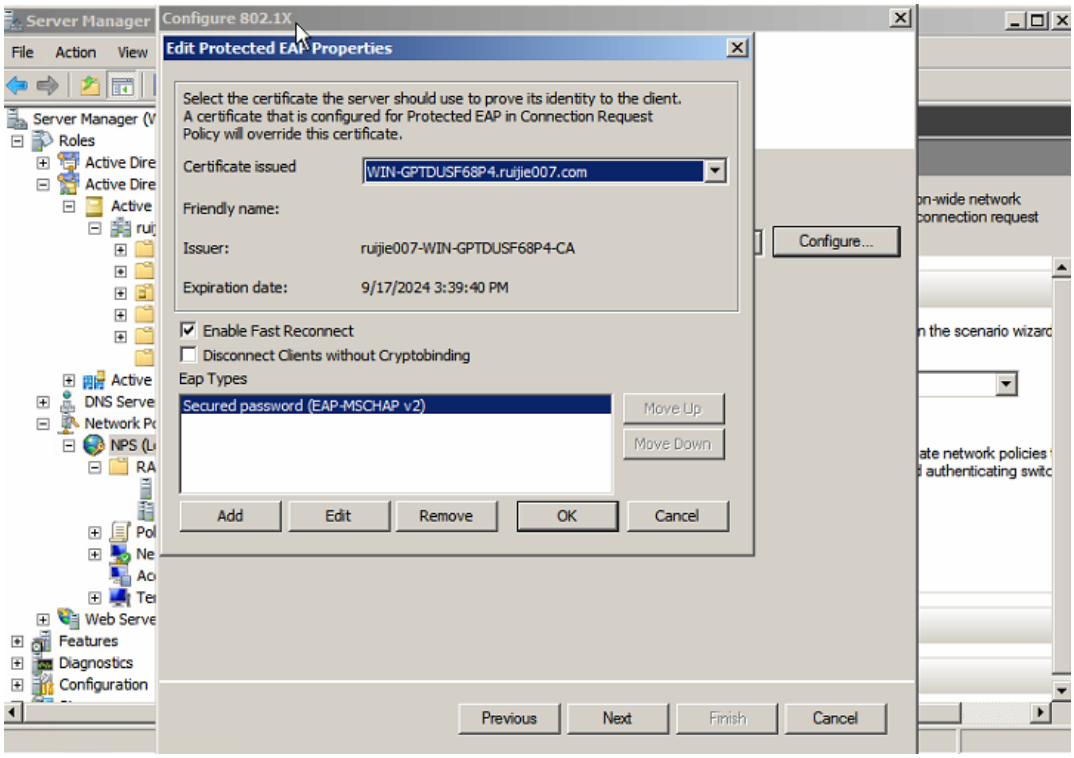
Select the AC device you need to integrate. The devices display here are the devices you have added before. If you doesn't add the devices before, you can click 'Add' to add the device.



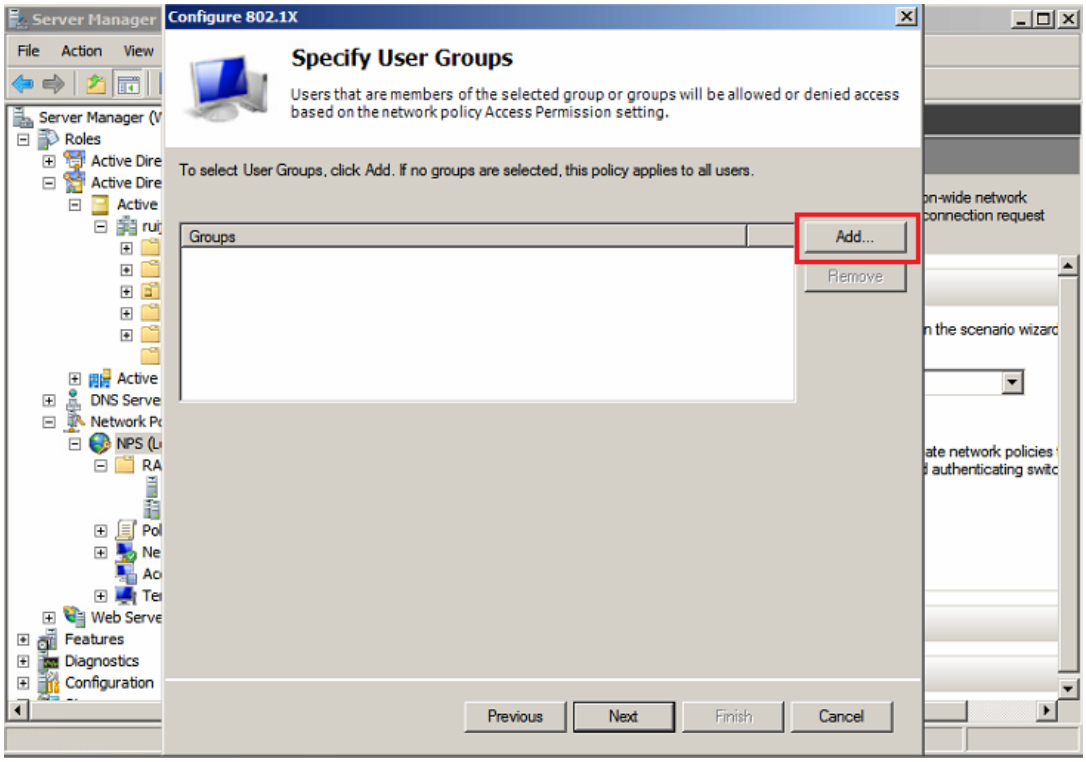
Click ‘Microsoft: Protected EAP (PEAP)’ and ‘Configure’ to set.

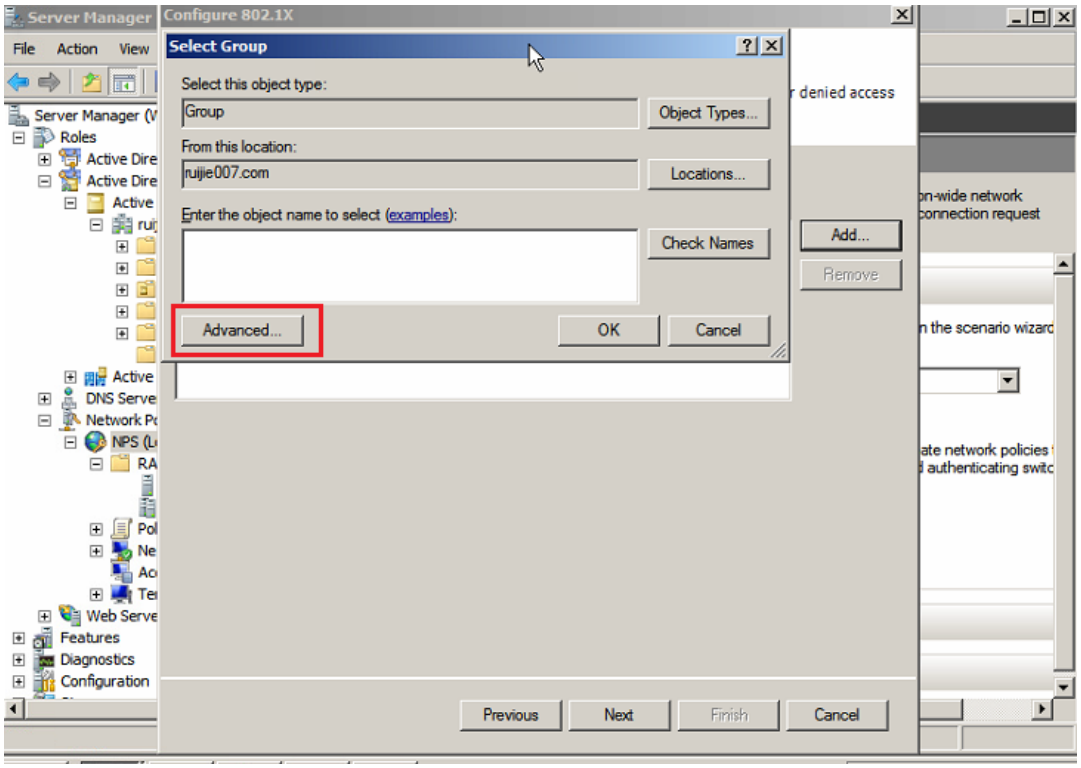


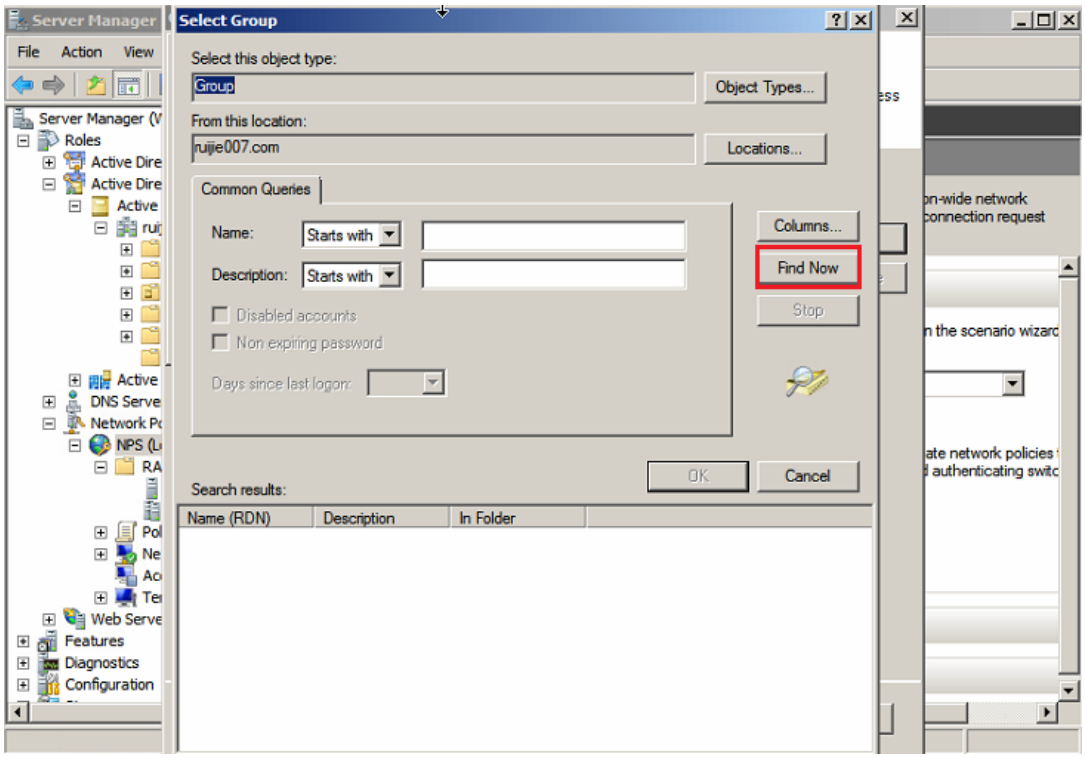
Select the server certificate applied in the figure, do not select the root certificate of another –CA. Click ‘OK’ and then go back to the configuration to click ‘Next’

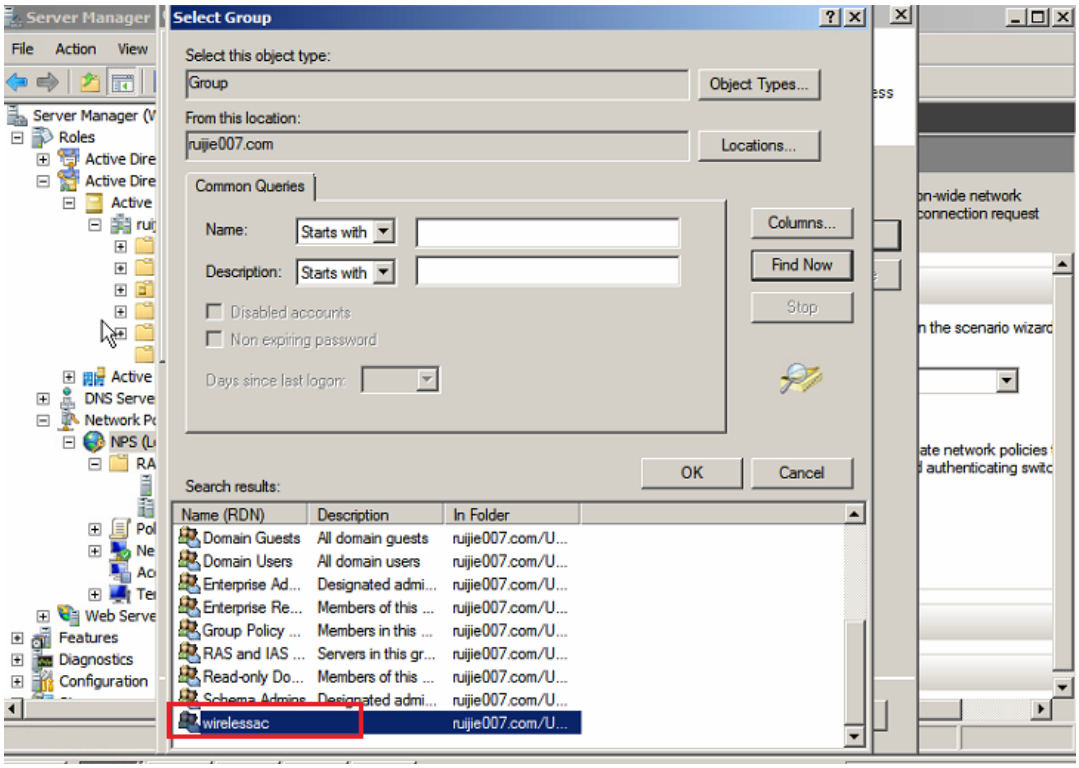


In the configuration page of Specify User Groups, click Add > Advanced > Find Now and select group you have set before, then click check name. If the follow warming is displayed, ‘Close” it and add the group more time.

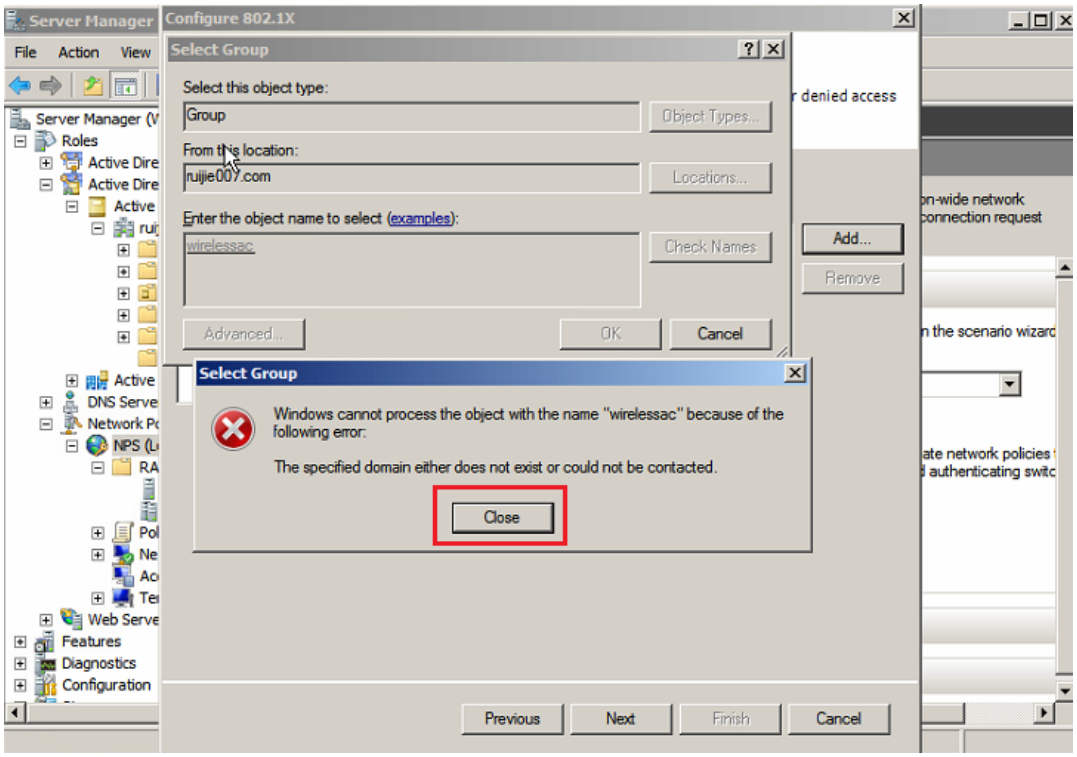


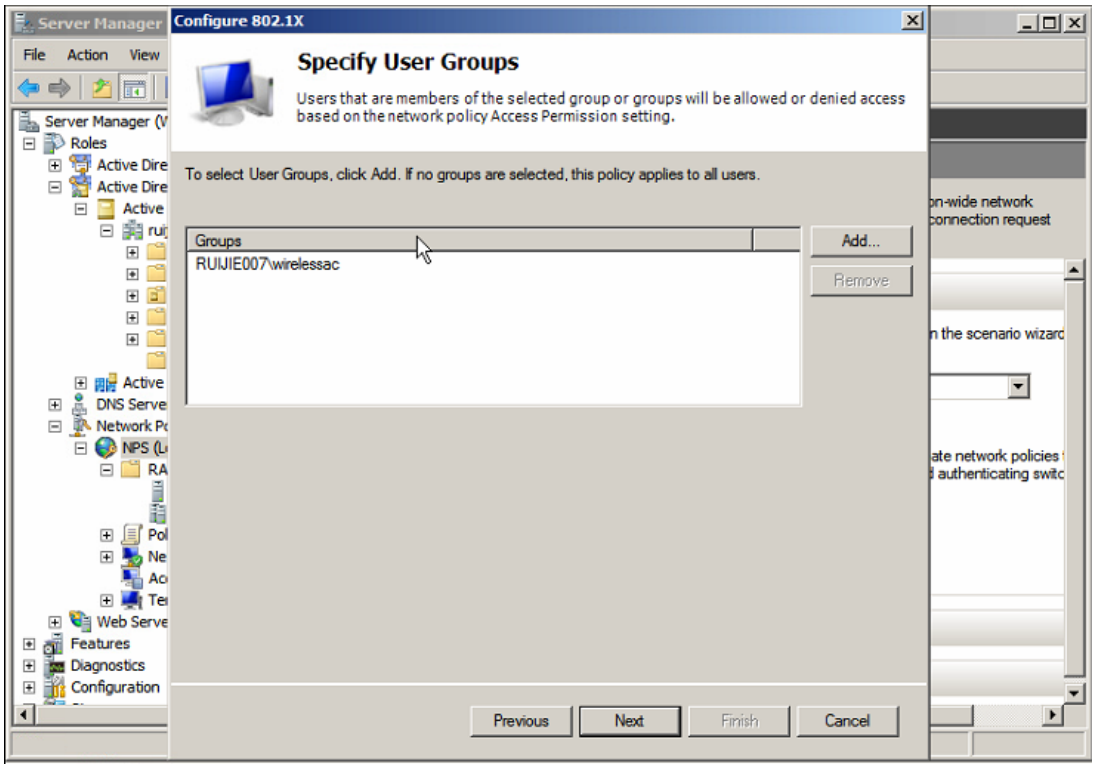

Server Manager
File Action View
Configure 802.1X
Select Group
Select this object type:
Group
Object Types...
From this location:
ruijie007.com
Locations...
Enter the object name to select (examples):
Check Names
Advanced...
OK
Cancel
Add...
Remove
Previous
Next
Finish
Cancel
Roles
Features
Diagnostics
Configuration


Server Manager
File Action View
Select Group
Select this object type:
Group
Object Types...
From this location:
ruijie007.com
Locations...
Common Queries
Name: Starts with
Description: Starts with
Disabled accounts
Non expiring password
Days since last logon:
Columns...
Find Now
Stop
OK
Cancel
Search results:
Name (RDN)
Description
In Folder
Roles
Features
Diagnostics
Configuration

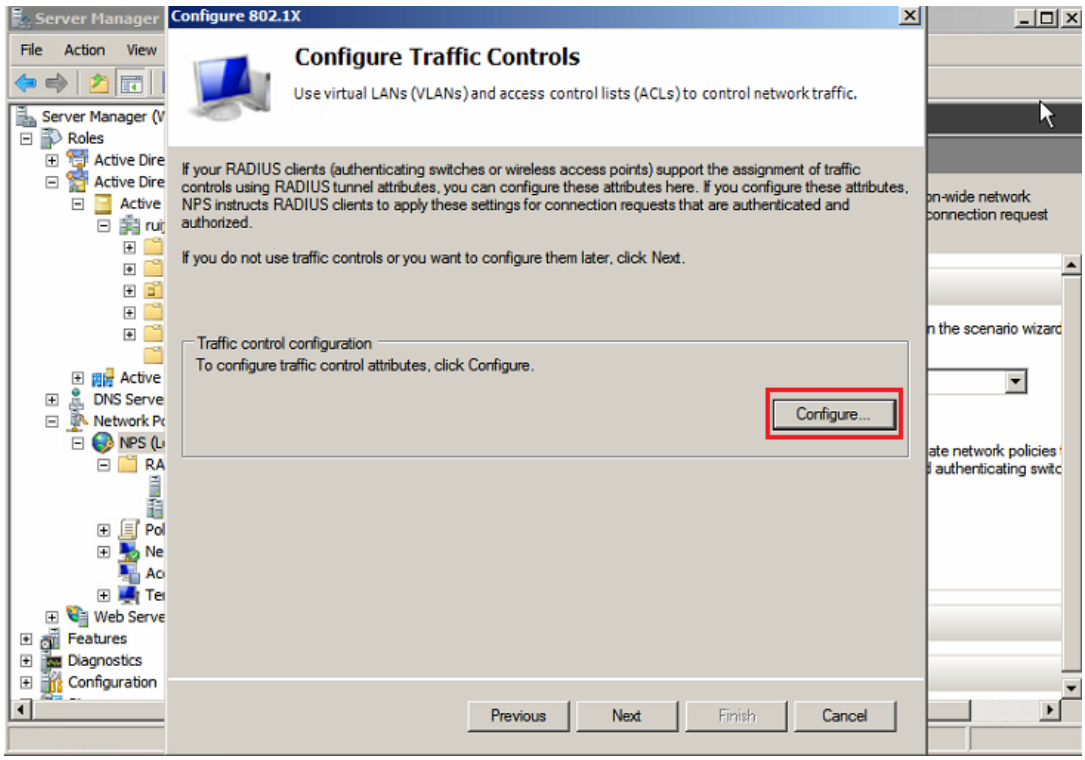


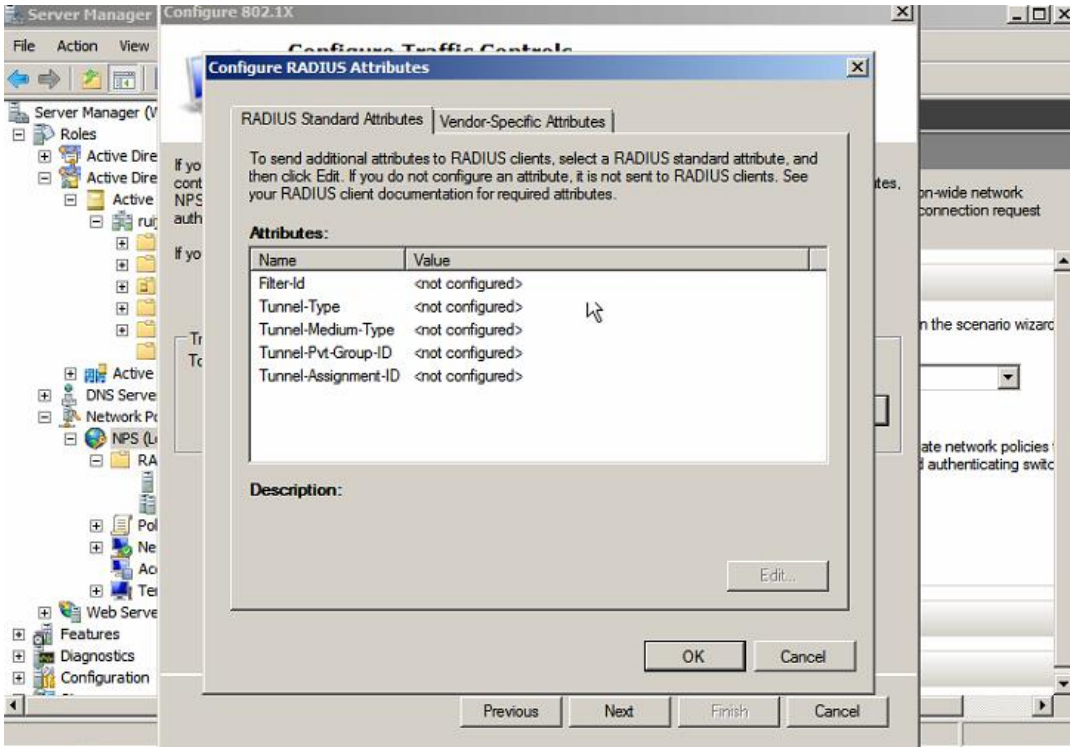
If the warming is displayed, click ‘Close’ and ‘check name’ again.

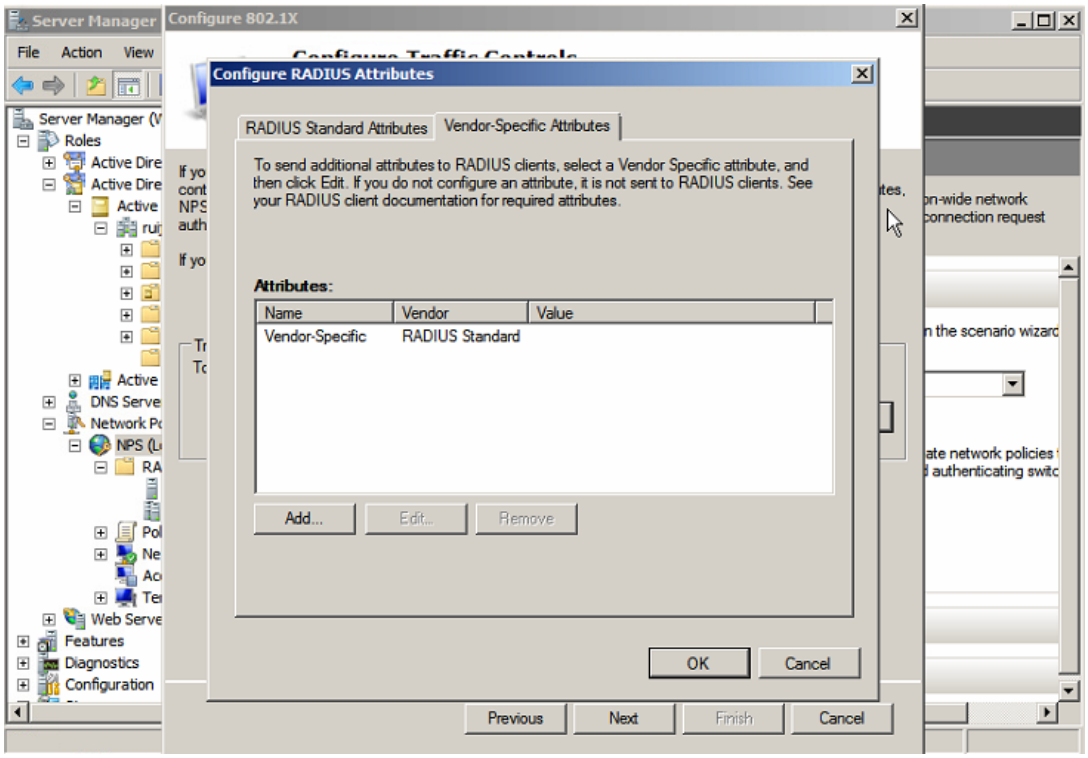


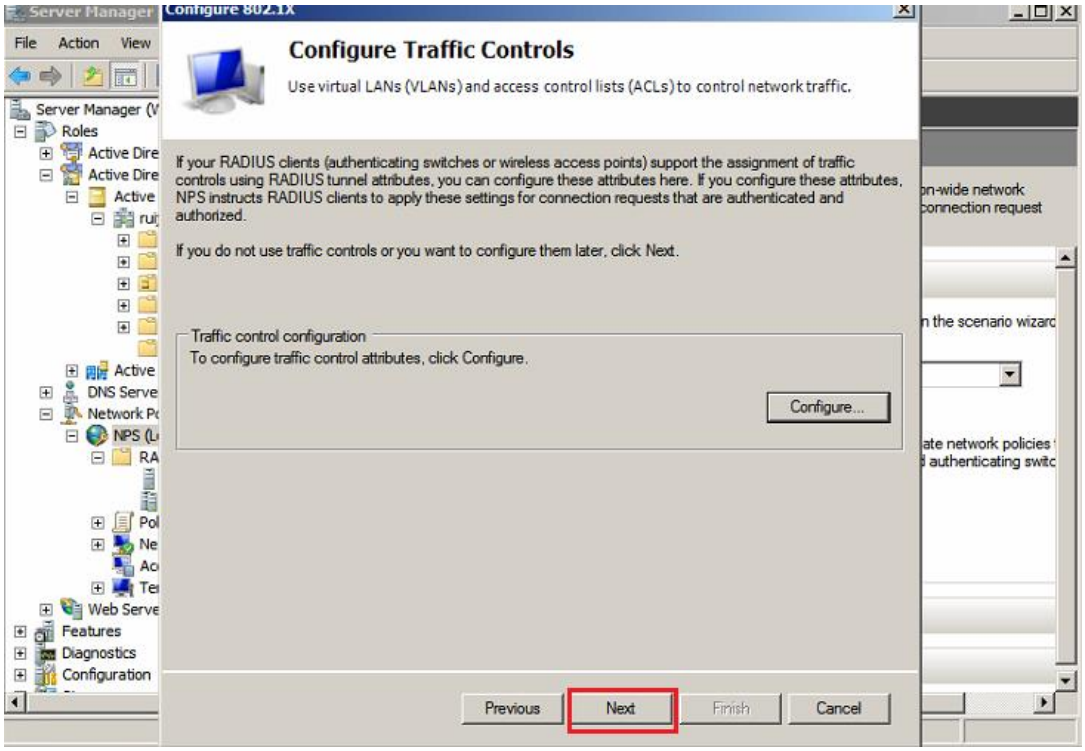


Enter the page of Traffic Control Configuration to check the radius attributes.

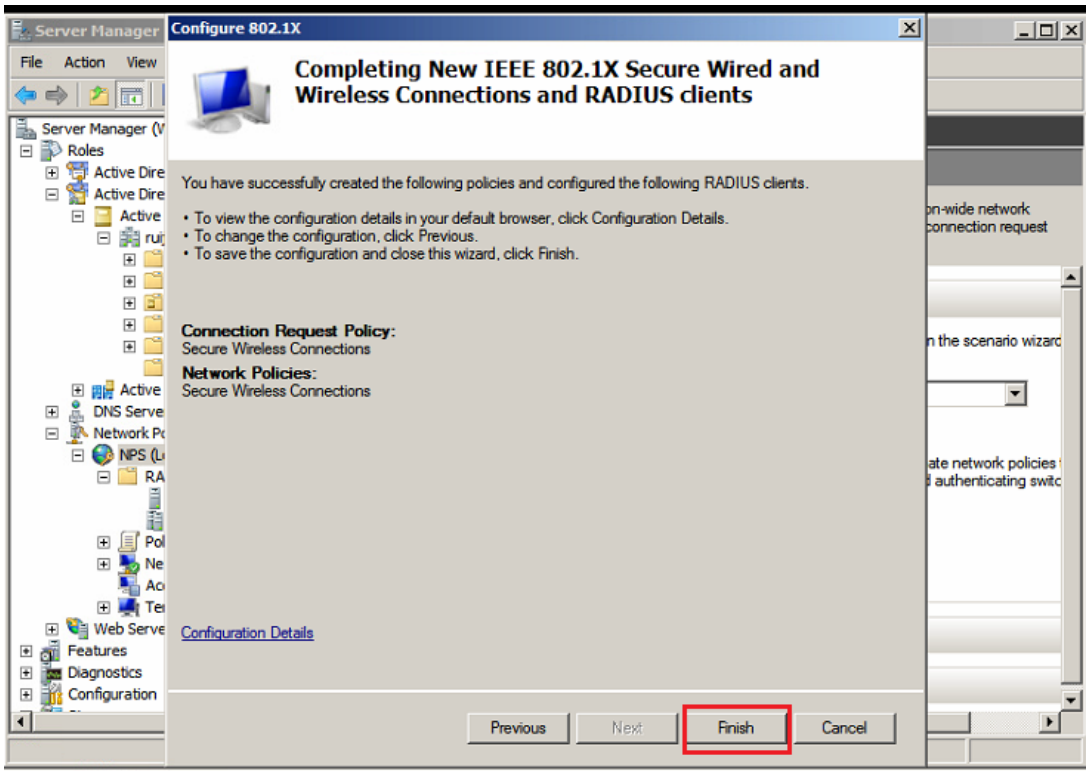



Server Manager
File Action View
Configure 802.1X
Configure RADIUS Attributes
RADIUS Standard Attributes
Vendor-Specific Attributes
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Value
Filter-Id
<not configured>
Tunnel-Type
<not configured>
Tunnel-Medium-Type
<not configured>
Tunnel-Pvt-Group-ID
<not configured>
Tunnel-Assignment-ID
<not configured>
Description:
Edit...
OK
Cancel
Previous
Next
Finish
Cancel
Roles
Active Dire
Active Dire
Active
DNS Serve
Network Pc
NPS (L
Web Serve
Features
Diagnostics
Configuration


Server Manager
File Action View
Configure 802.1X
Configure RADIUS Attributes
RADIUS Standard Attributes
Vendor-Specific Attributes
To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Vendor
Value
Vendor-Specific
RADIUS Standard
Add...
Edit...
Remove
OK
Cancel
Previous
Next
Finish
Cancel
Roles
Active Dire
Active Dire
Active
DNS Serve
Network Pc
NPS (L
Web Serve
Features
Diagnostics
Configuration

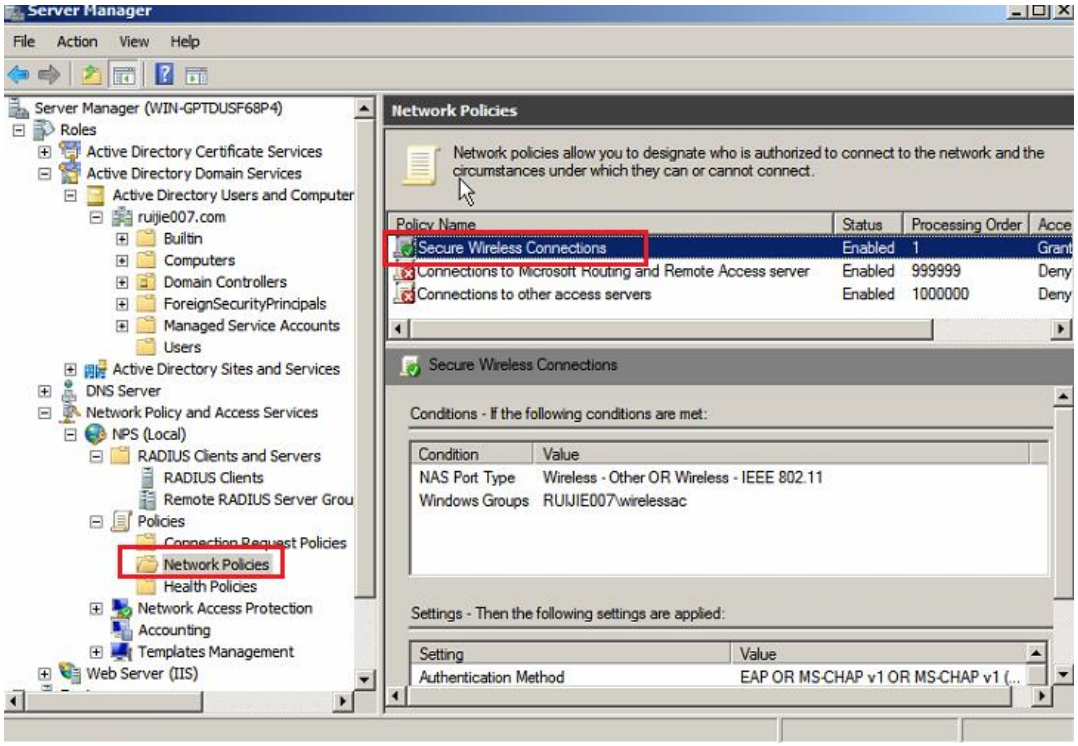


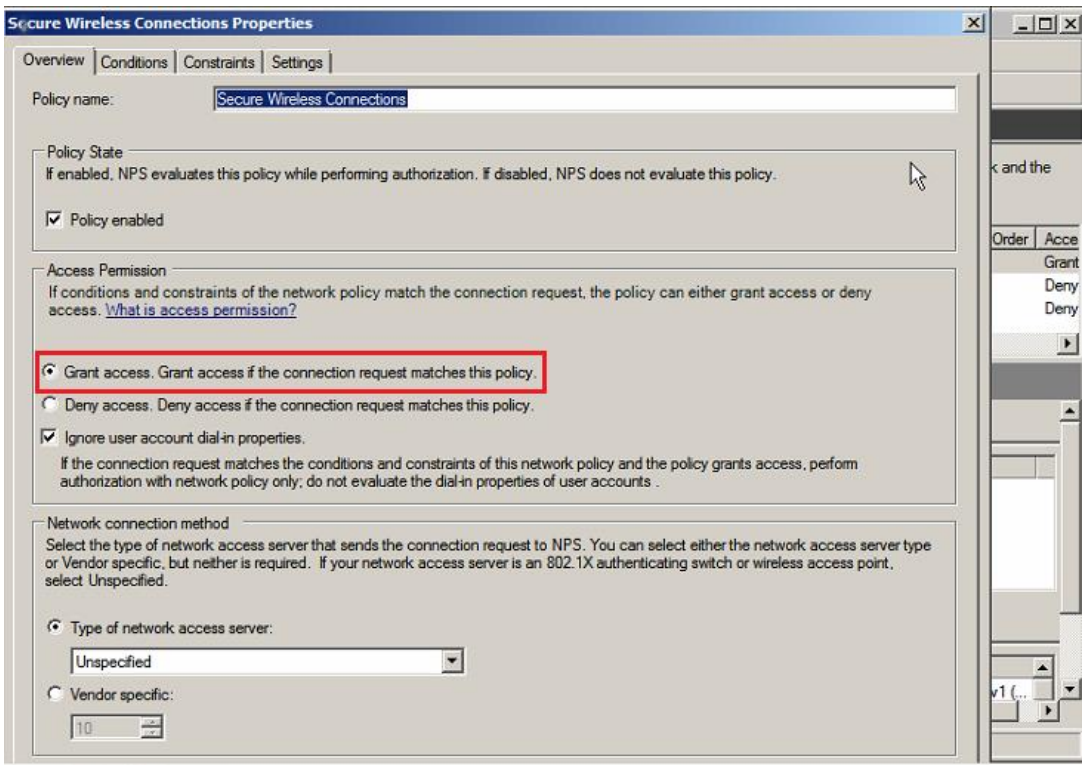
Click ‘Finish’ to finish the configuration. Now the 802.1x configuration template for AC1 is finished.

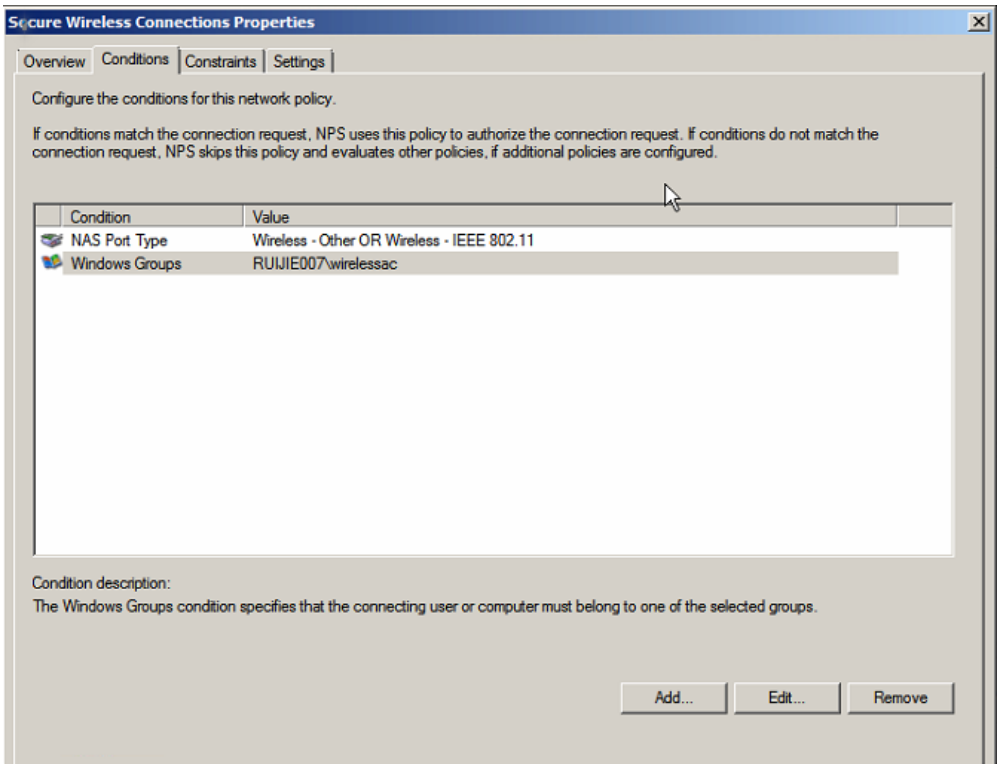


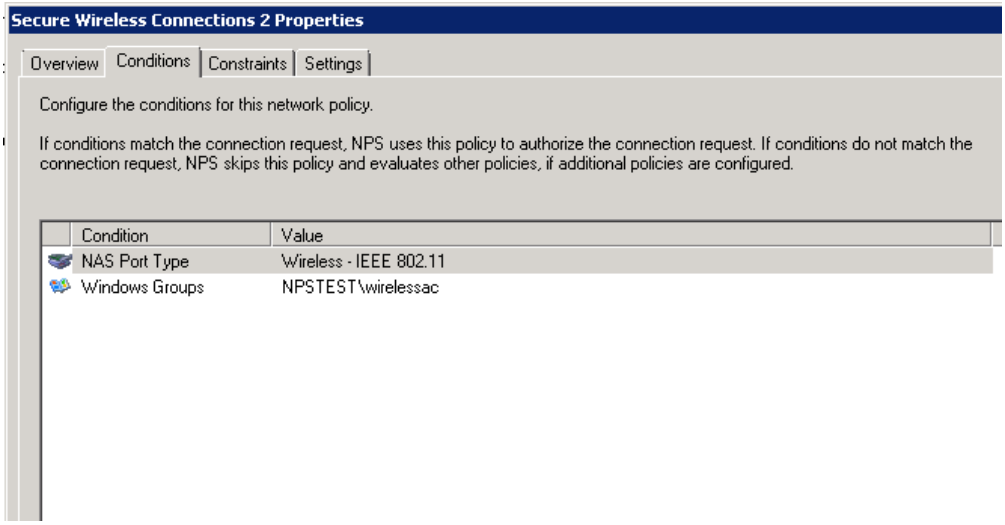
1.6.5 Set NPS Network Policy

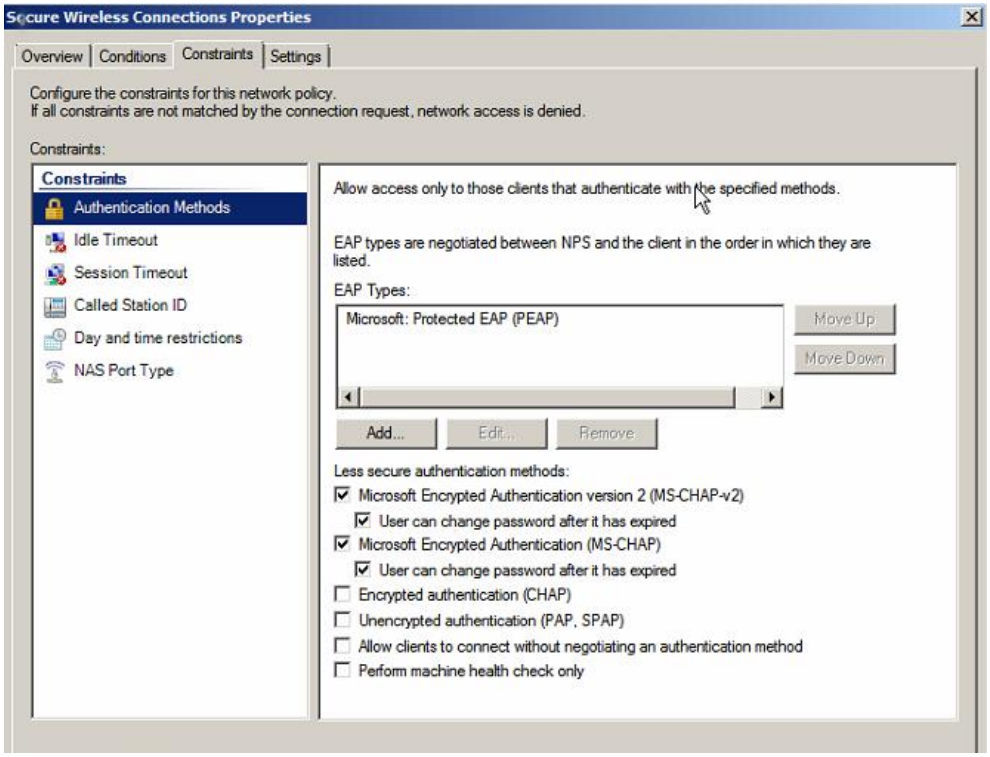
Click ‘Network Policies’ > the 802.1x configuration template you have just set > Grant access to grant the access if the connection request matches this policy.


Server Manager
File Action View Help
Server Manager (WIN-GPTDUSF68P4)
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Users and Computer
ruijie007.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Active Directory Sites and Services
DNS Server
Network Policy and Access Services
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Grou
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Templates Management
Web Server (IIS)
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
Acce
Secure Wireless Connections
Enabled
1
Grant
Connections to Microsoft Routing and Remote Access server
Enabled
999999
Deny
Connections to other access servers
Enabled
1000000
Deny
Secure Wireless Connections
Conditions - If the following conditions are met:
Condition
Value
NAS Port Type
Wireless - Other OR Wireless - IEEE 802.11
Windows Groups
RUIJIE007\wirelessac
Settings - Then the following settings are applied:
Setting
Value
Authentication Method
EAP OR MS-CHAP v1 OR MS-CHAP v1 (...

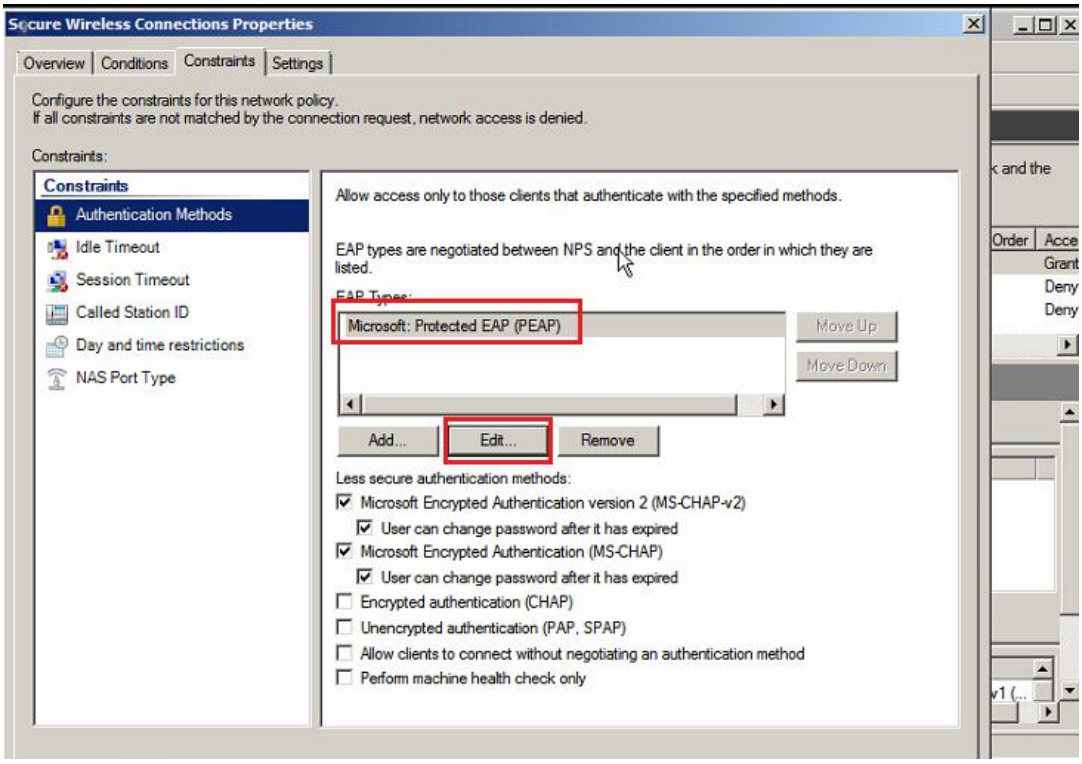

Secure Wireless Connections Properties
Overview
Conditions
Constraints
Settings
Policy name:
Secure Wireless Connections
Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.
Policy enabled
Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?
Grant access. Grant access if the connection request matches this policy.
Deny access. Deny access if the connection request matches this policy.
Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.
Type of network access server:
Unspecified
Vendor specific:
10

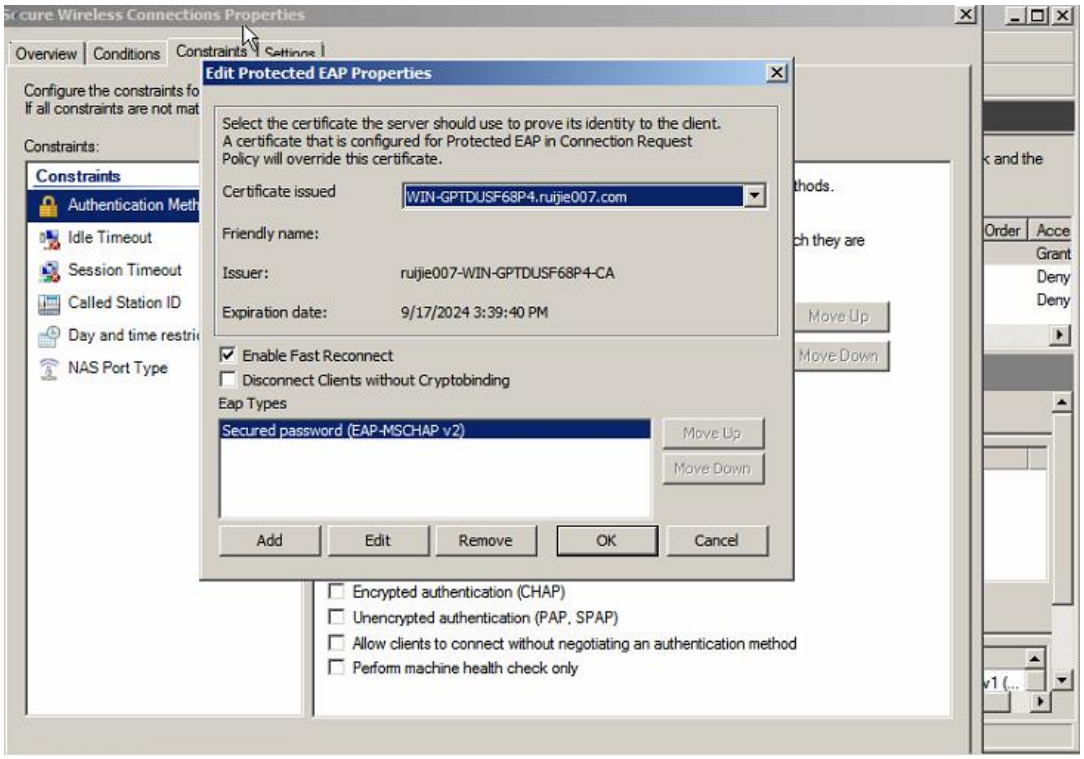

Secure Wireless Connections Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
NAS Port Type
Wireless - Other OR Wireless - IEEE 802.11
Windows Groups
RUIJIE007\wirelessac
Condition description:
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.
Add...
Edit...
Remove


Secure Wireless Connections 2 Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
NAS Port Type
Wireless - IEEE 802.11
Windows Groups
NPSTEST\wirelessac

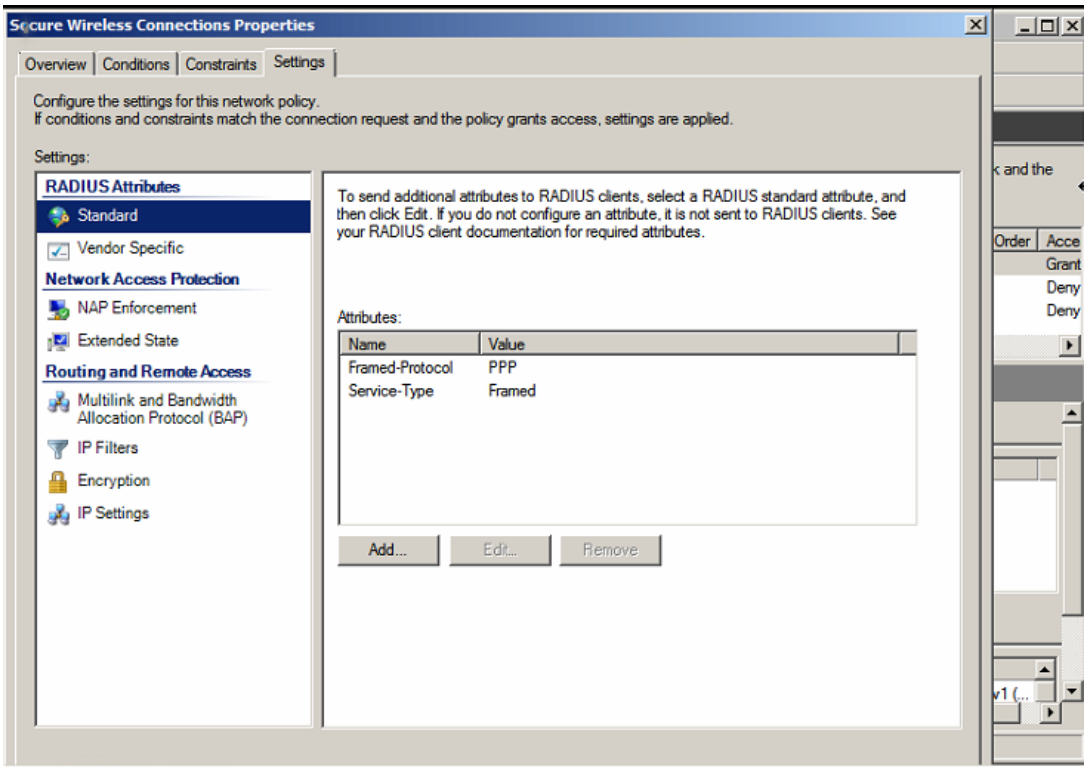


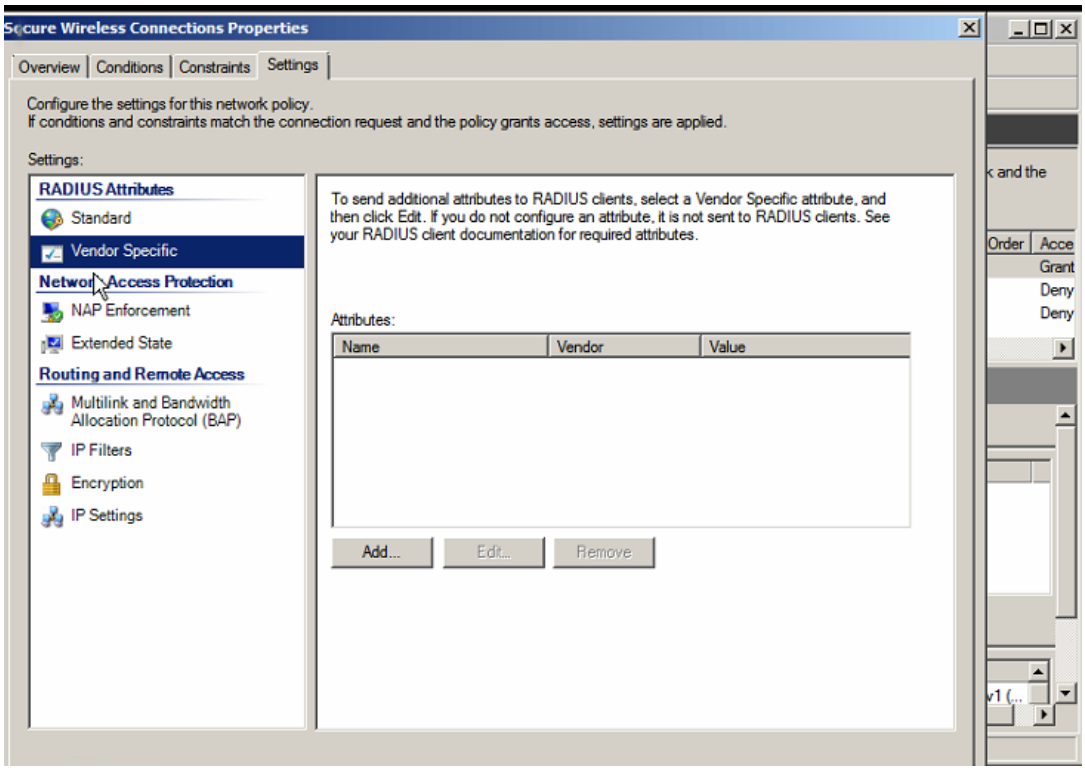
Check the settings about Microsoft: Protected EAP (PEAP) and the selected certificates are right or not.





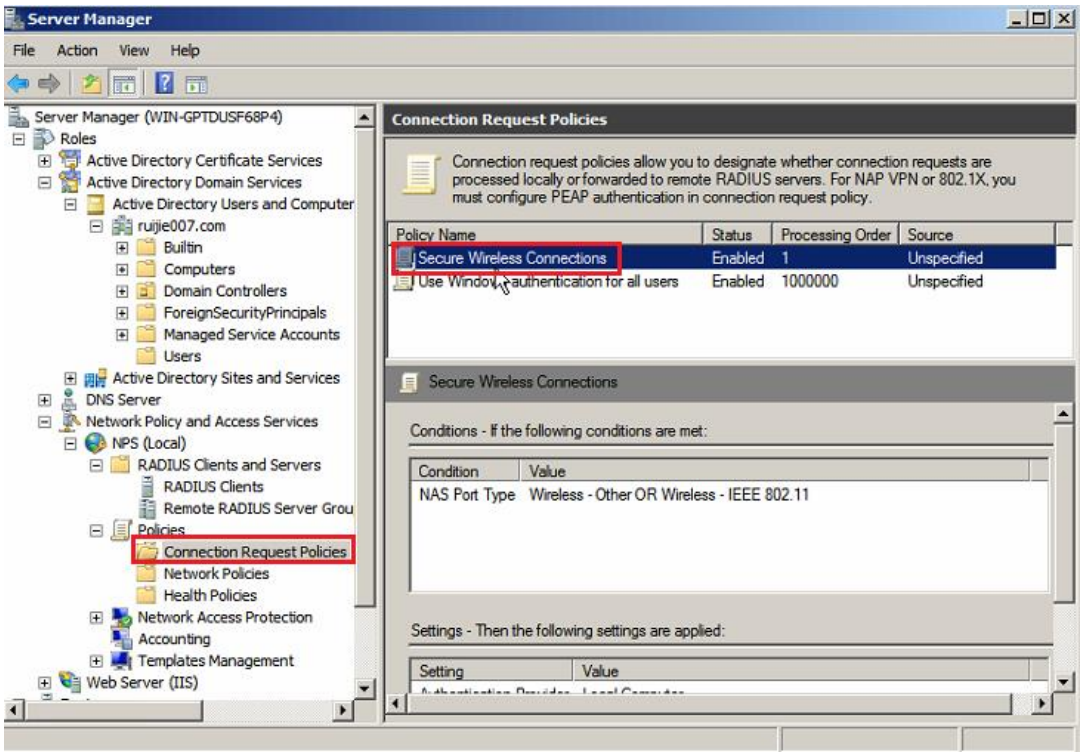
Check the Setting of Radius Attributes. The configuration is shown as below:

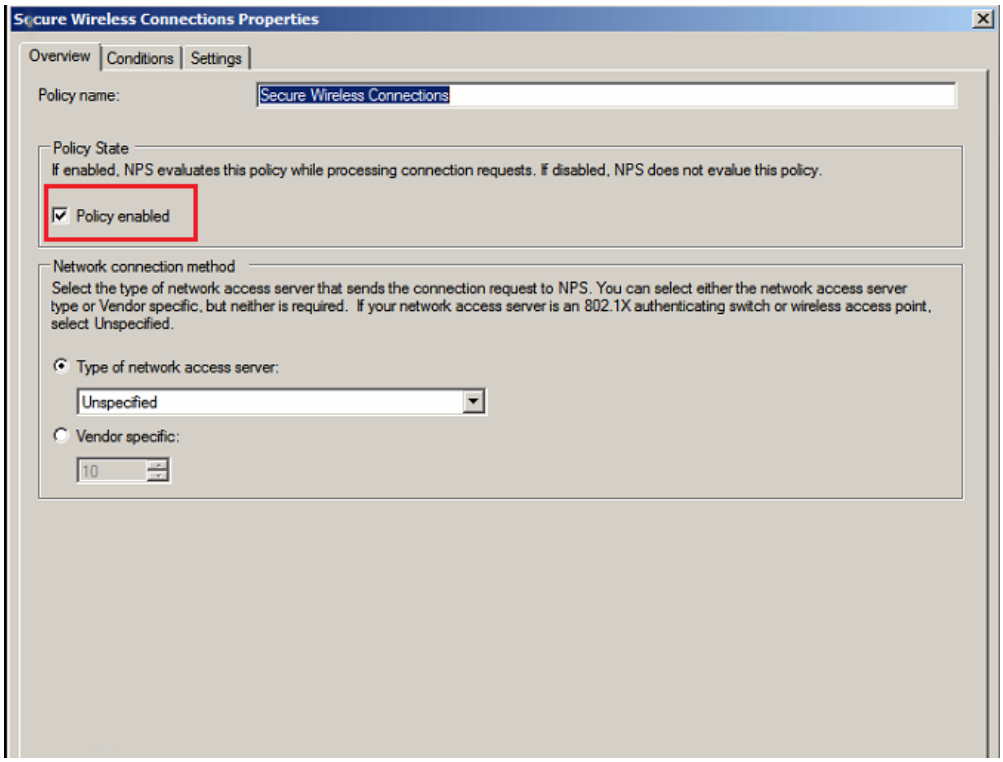


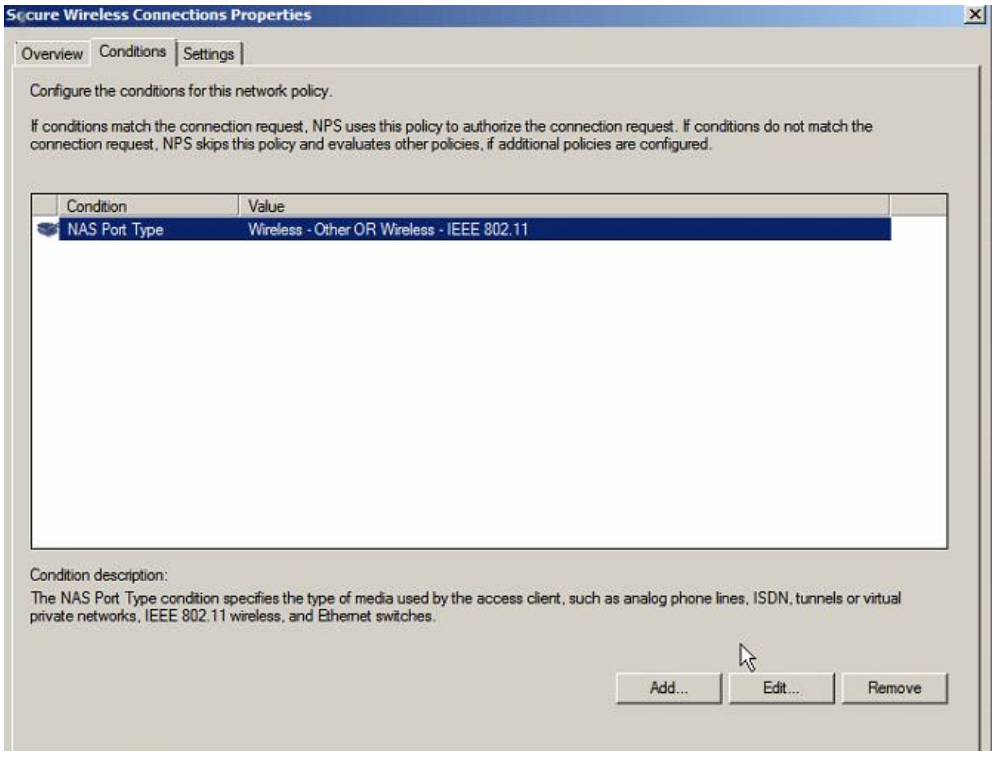


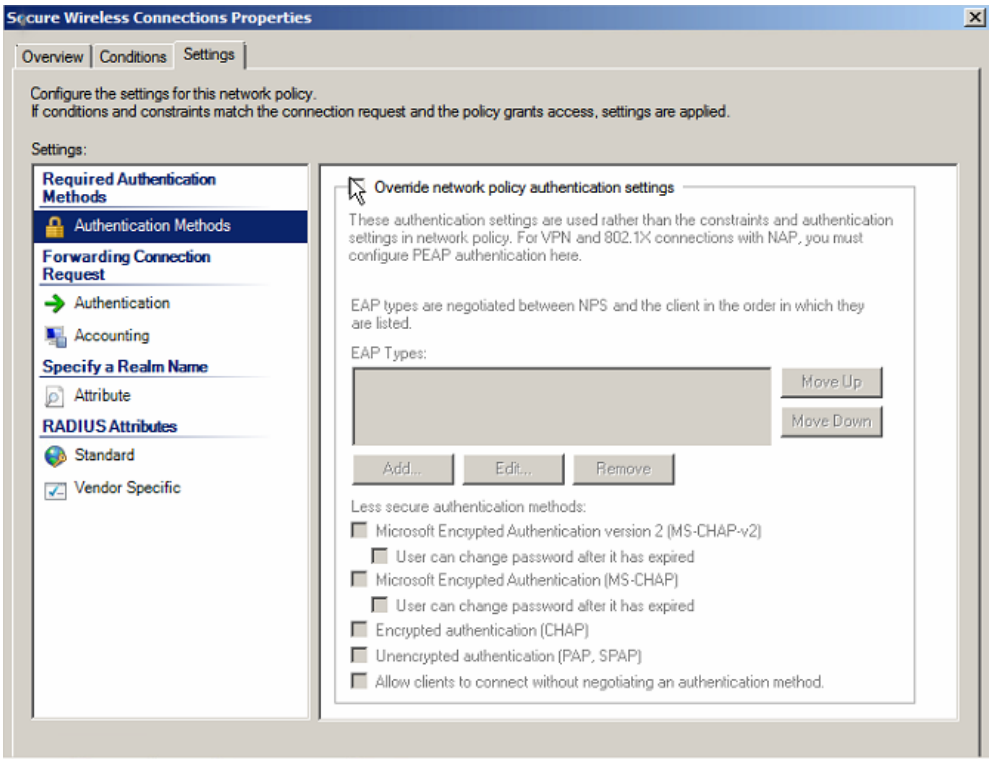
1.6.6 Set NPS Connection Request Policies

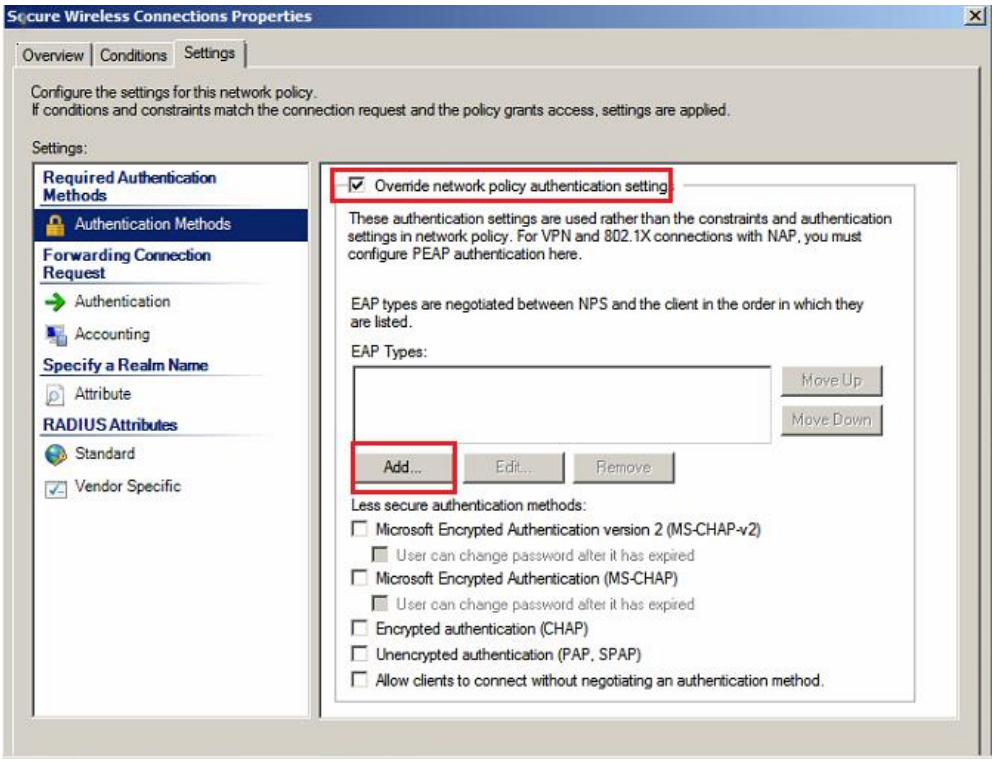
The settings steps of NPS Connection Request Policies is similar to the steps of network policies. Some settings including EAP settings need to be checked.

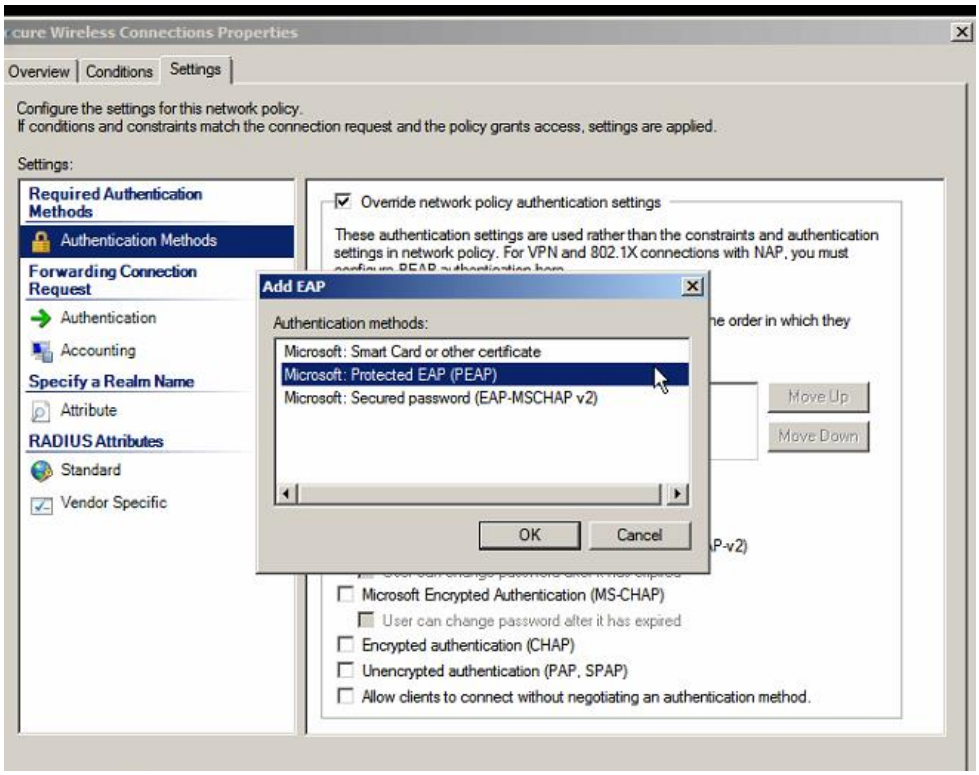


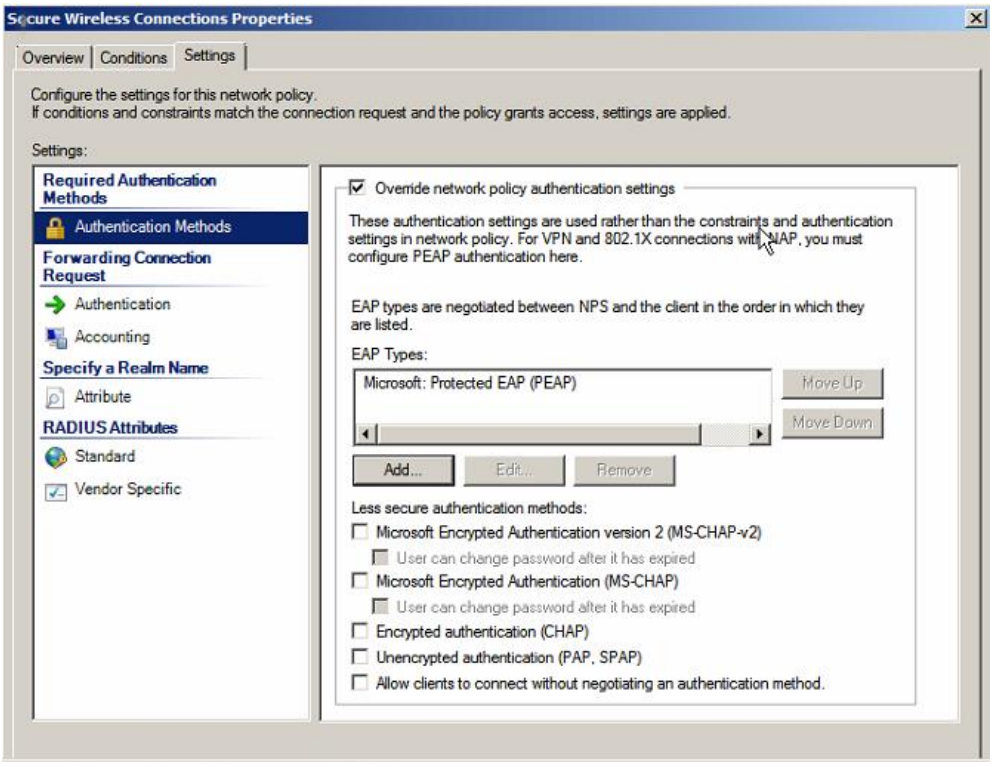

Secure Wireless Connections Properties
Overview
Conditions
Settings
Policy name:
Secure Wireless Connections
Policy State
If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy.
Policy enabled
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.
Type of network access server:
Unspecified
Vendor specific:
10


Secure Wireless Connections Properties
Overview
Conditions
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
NAS Port Type
Wireless - Other OR Wireless - IEEE 802.11
Condition description:
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.
Add...
Edit...
Remove

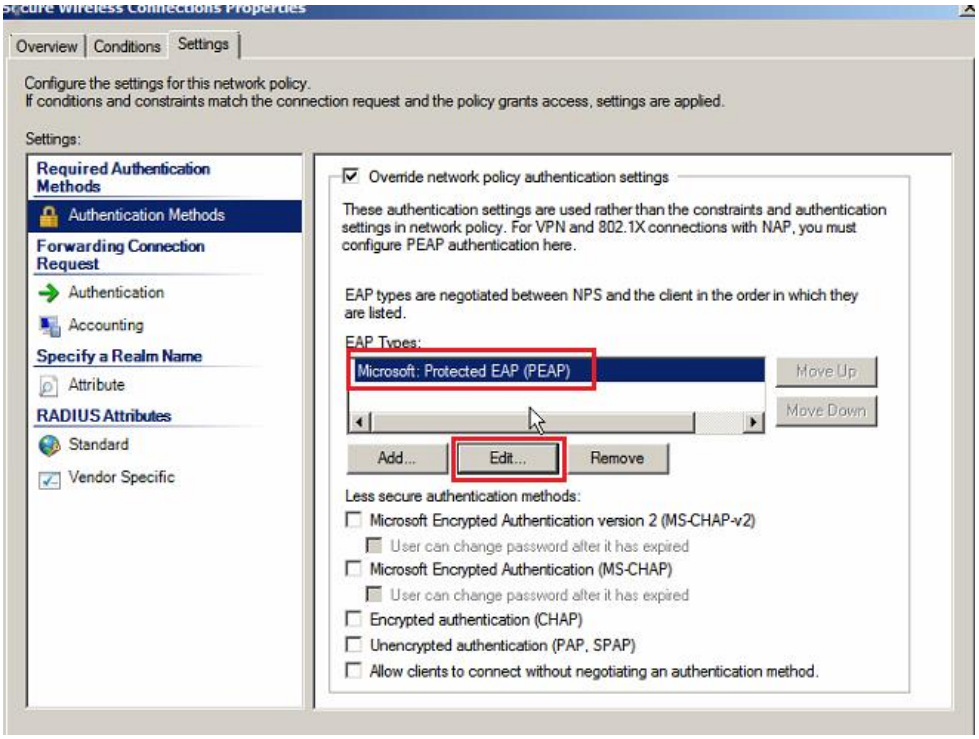

Secure Wireless Connections Properties
Overview
Conditions
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
Required Authentication Methods
Authentication Methods
Forwarding Connection Request
Authentication
Accounting
Specify a Realm Name
Attribute
RADIUS Attributes
Standard
Vendor Specific
Override network policy authentication settings
These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method.

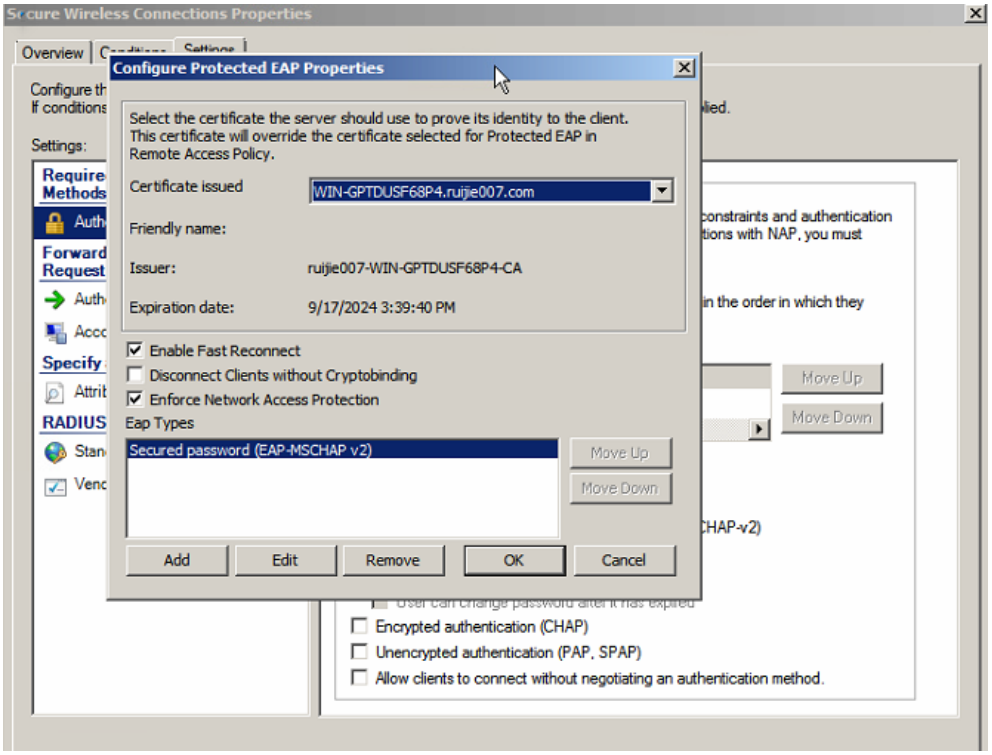

Secure Wireless Connections Properties
Overview
Conditions
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
Required Authentication Methods
Authentication Methods
Forwarding Connection Request
Authentication
Accounting
Specify a Realm Name
Attribute
RADIUS Attributes
Standard
Vendor Specific
Override network policy authentication setting
These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method.

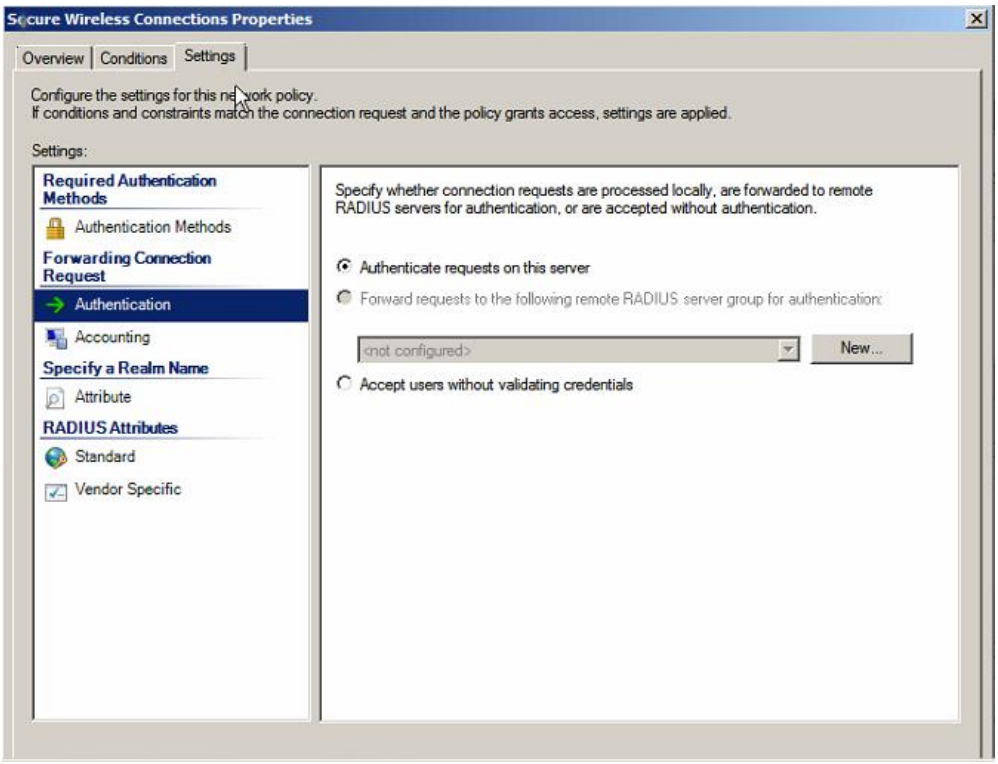


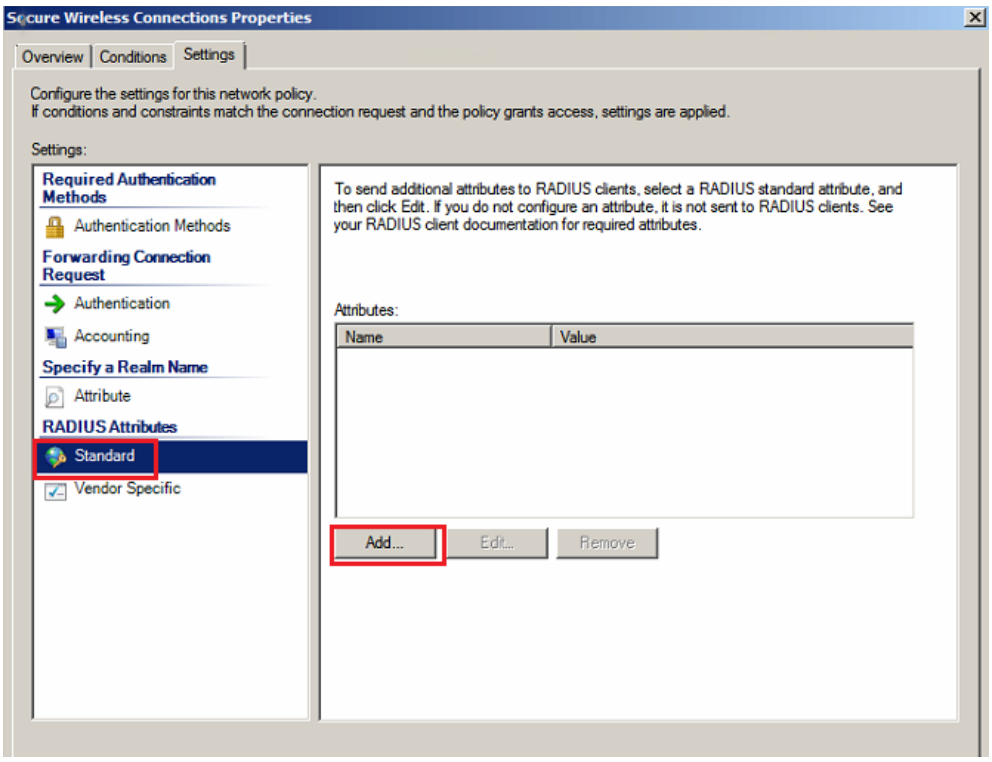


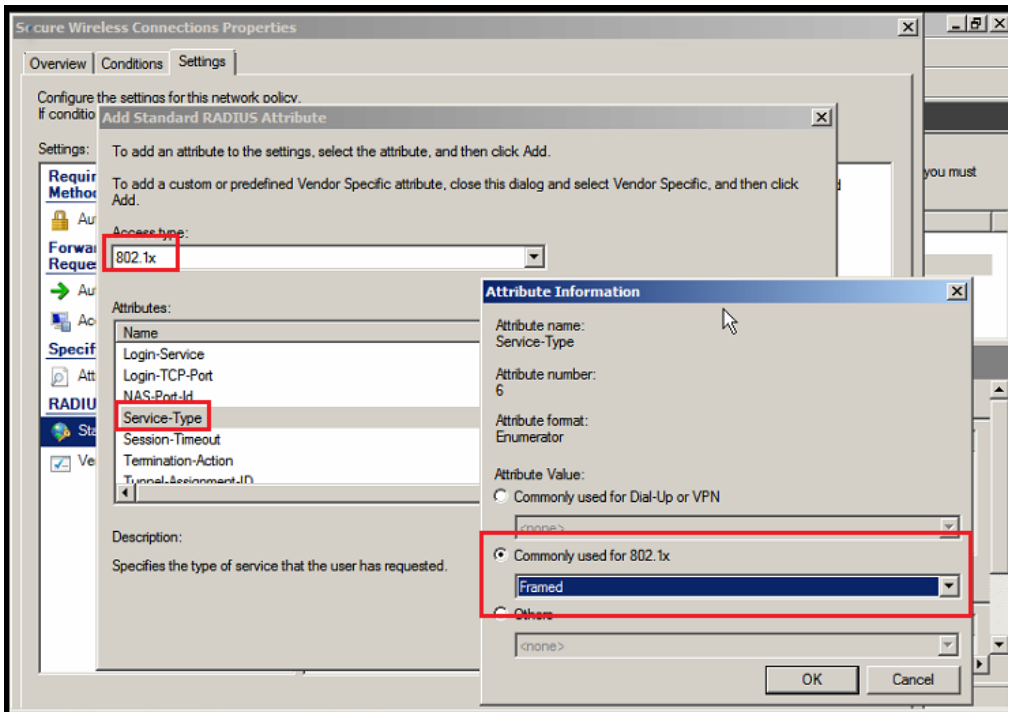
Click ‘Edit’ to check the settings of EAP, including the selected certificates are right or not.

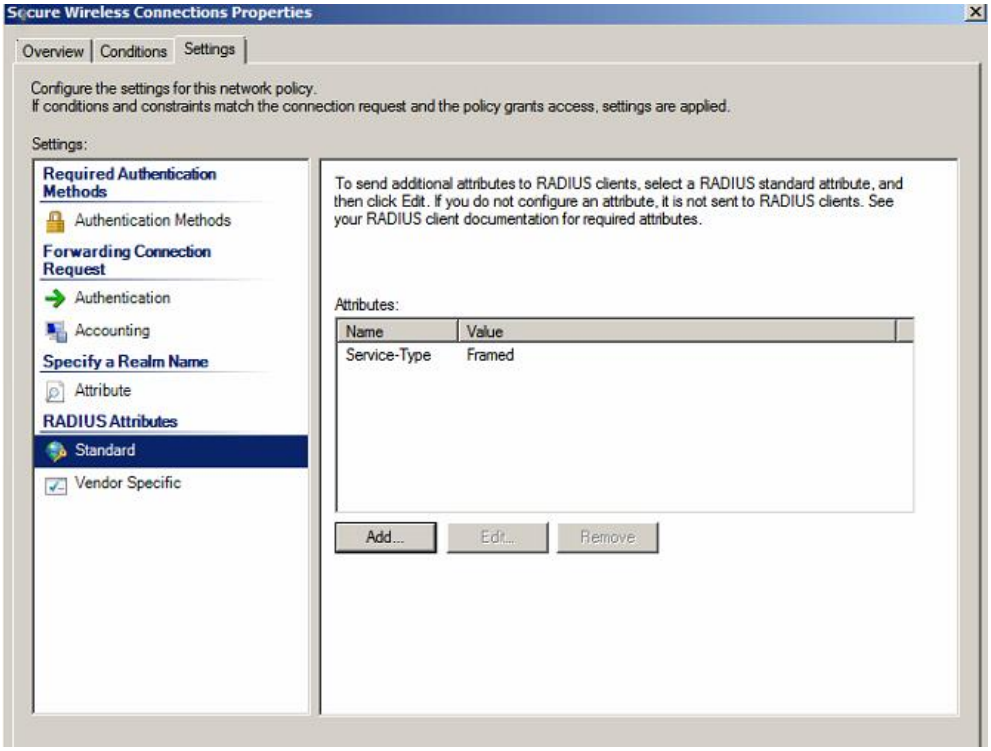

Overview
Conditions
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
Required Authentication Methods
Authentication Methods
Forwarding Connection Request
Authentication
Accounting
Specify a Realm Name
Attribute
RADIUS Attributes
Standard
Vendor Specific
Override network policy authentication settings
These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Microsoft: Protected EAP (PEAP)
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method.

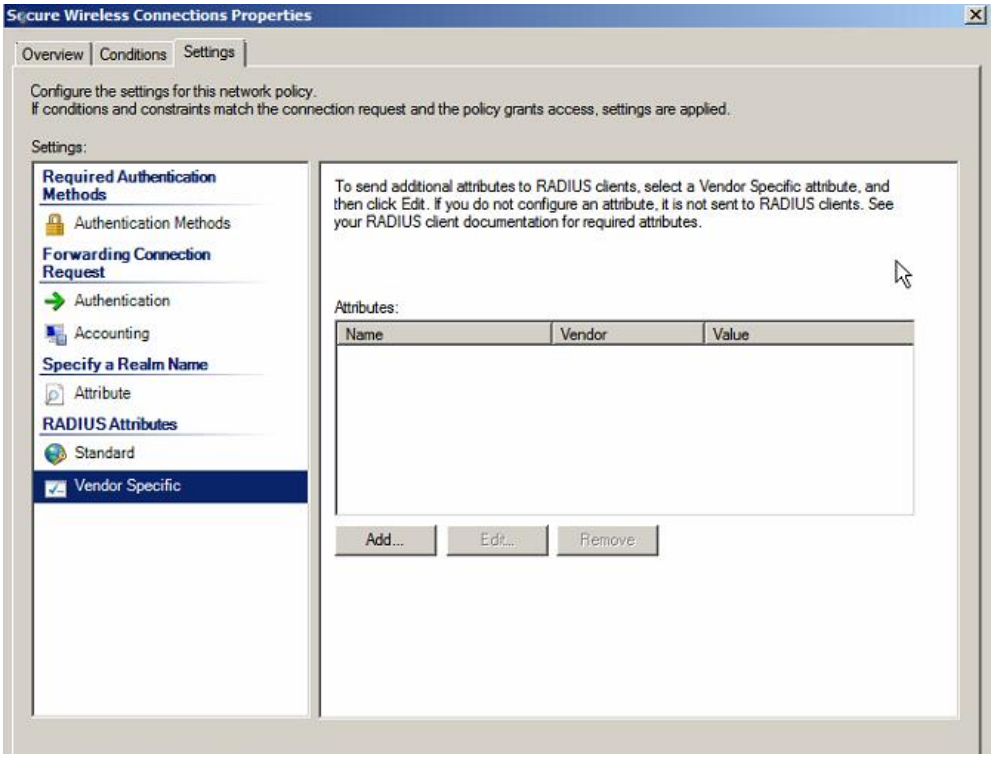

Secure Wireless Connections Properties
Configure Protected EAP Properties
Select the certificate the server should use to prove its identity to the client.
This certificate will override the certificate selected for Protected EAP in Remote Access Policy.
Certificate issued
WIN-GPTDUSF68P4.ruijie007.com
Friendly name:
Issuer:
ruijie007-WIN-GPTDUSF68P4-CA
Expiration date:
9/17/2024 3:39:40 PM
Enable Fast Reconnect
Disconnect Clients without Cryptobinding
Enforce Network Access Protection
Eap Types
Secured password (EAP-MSCHAP v2)
Move Up
Move Down
Add
Edit
Remove
OK
Cancel
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method.


Secure Wireless Connections Properties
Overview
Conditions
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
Required Authentication Methods
Authentication Methods
Forwarding Connection Request
Authentication
Accounting
Specify a Realm Name
Attribute
RADIUS Attributes
Standard
Vendor Specific
Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.
Authenticate requests on this server
Forward requests to the following remote RADIUS server group for authentication:
<not configured>
New...
Accept users without validating credentials


Secure Wireless Connections Properties
Overview
Conditions
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
Required Authentication Methods
Authentication Methods
Forwarding Connection Request
Authentication
Accounting
Specify a Realm Name
Attribute
RADIUS Attributes
Standard
Vendor Specific
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Value
Add...
Edit...
Remove


Secure Wireless Connections Properties
Overview
Conditions
Settings
Configure the settings for this network policy.
If conditio
Add Standard RADIUS Attribute
Settings:
To add an attribute to the settings, select the attribute, and then click Add.
To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.
Access type:
802.1x
Attributes:
Name
Login-Service
Login-TCP-Port
NAS-Port-Id
Service-Type
Session-Timeout
Termination-Action
Description:
Specifies the type of service that the user has requested.
Attribute Information
Attribute name:
Service-Type
Attribute number:
6
Attribute format:
Enumerator
Attribute Value:
Commonly used for Dial-Up or VPN
Commonly used for 802.1x
Framed
Others
OK
Cancel


Secure Wireless Connections Properties
Overview
Conditions
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
Required Authentication Methods
Authentication Methods
Forwarding Connection Request
Authentication
Accounting
Specify a Realm Name
Attribute
RADIUS Attributes
Standard
Vendor Specific
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Value
Service-Type
Framed
Add...
Edit...
Remove



Now, all configurations are finished.

2 The integration Configuration Example of Ruijie AC and NPS (Network Policy Server)

2.1 Wireless 802.1x Authentication Introduction

802.1x is a port-based network access control protocol in Client/Server mode. Through its Extensible Authentication Protocol (EAP) authentication framework, all clients can be authenticated and their network access permissions can be controlled at the LAN access interface level.

When the 802.1X application is used for wireless network access authentication, a secure channel is established between the authentication client and the authentication server through the encryption mechanism of the PEAP certificate technology to ensure that the data inside the EAP is encrypted using the certificate, which greatly improves the security and reliability of the 802.1X authentication in the wireless application. It is applicable to scenarios where a new network is created, users are concentrated, and information security requirements are strict.

Product and Software Version

Table 2-1

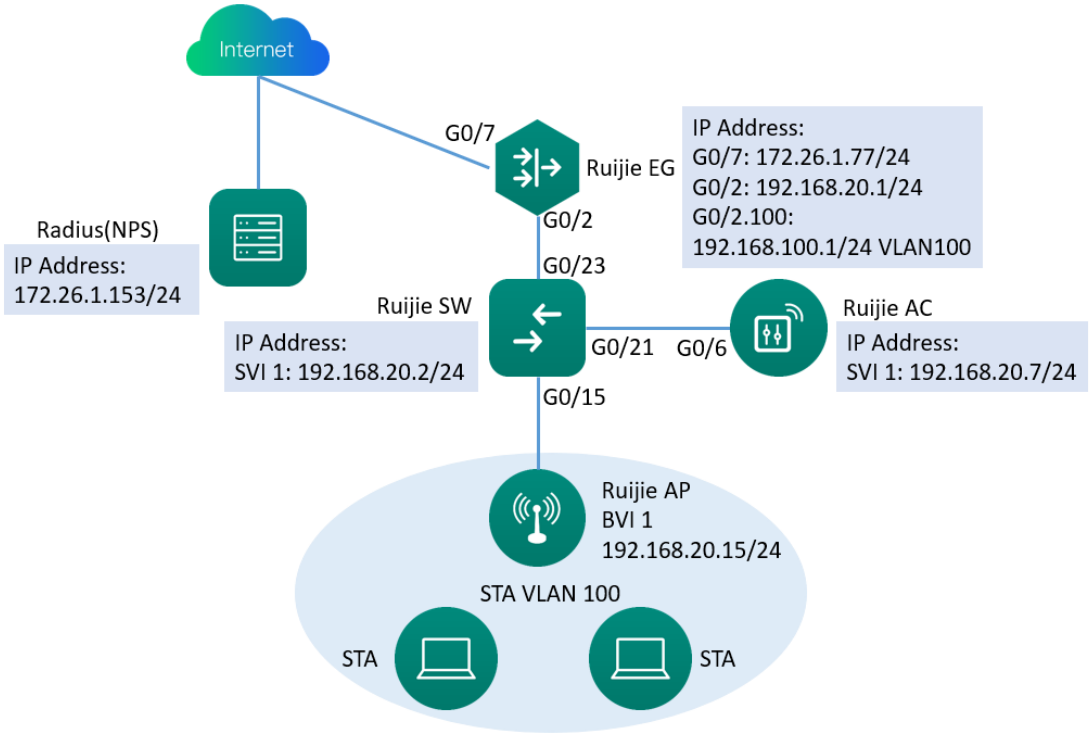
Device Type	Device Model	Version
WLAN AC	RG-WS6008	AC_RGOS 11.9(6)W1B1, Release(09192520)
Certificate Server	NPS(network policy server)	Establish on WIN SERVER2008R2

2.2 Network Requirement

For the information security, Users are required to access the network to pass the 802.1x authentication via account and password.

- Install 802.1x client version on the users' terminals(Generally, the operation （The operation system will have the 802.1x client version by default. If no, you can download other 802.1x client version client version）
- AC supports 802.1x protocol.
- Certificate Server support standard RADIUS.

2.3 Topology



Topology Note：

- Ruijie EG as a gateway, is play a role as a DHCP server to assign the IP address for AP and STA and also can do the NAT translation.
- AP and AC connects to Ruijie SW and SW supplies power for AP.
- The WLAN authentication for wireless users is 802.1x

Table 2-2 The Configuration of AC

Item	Note
Manageable VLAN of AC	VLAN 1
Manageable IP of AC	192.168.20.7
IP address of AC for Establishing CAPWAP Tunnel.	192.168.20.7
Manageable VLAN of AP	VLAN 1
Business VLAN of STA	VLAN 100
STA Address Pool	192.168.100.0/24(The address pool is on the EG)
SSID	nps1xtest
RADIUS Authentication Parameter	RADIUS authentication server group: npstest RADIUS authentication server: 172.26.1153 Authentication and accounting shared key: ruijie@123 AD domain name：ruijie007.com
AAA Method List	Authentication method list: nps Account method list: nps
Authentication Account	ruijie/Abc.123456(User needs to add认证时填写用户需 the domain name when authentication, that is: ruijie@ruijie007.com)

2.4 Configuration Points

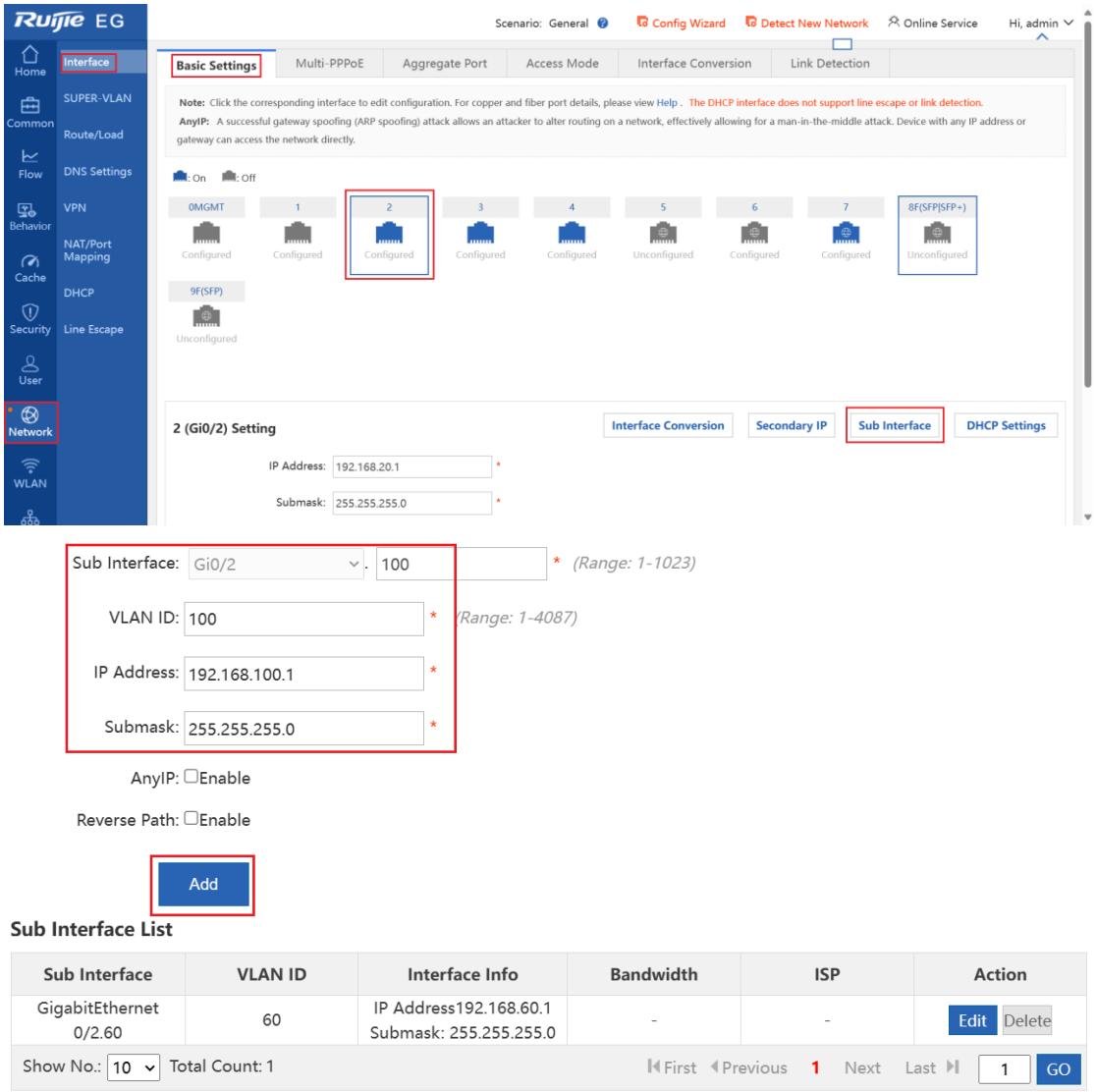
- Create a sub-interface and address pool of WLAN 100 to assign address for STA. Option 138 must be set in the address pool configuration to specify the capwap tunnel address.
- On the switch and AC, VLAN 100 should be created and allow them pass through.
- Configure the capwap tunnel address, 802.1x Authentication Parameter (Radius authentication server and AAA Method List) to enable the 802.1x authentication.

2.5 Configuration Steps

2.5.1 EG Configuration

Create a sub-interface and address pool of WLAN 100 to assign address for STA. Option 138 must be set in the address pool configuration to specify the capwap tunnel address.

Create a sub-interface:



Sub Interface List

Sub Interface	VLAN ID	Interface Info	Bandwidth	ISP	Action
GigabitEthernet 0/2.60	60	IP Address192.168.60.1 Submask: 255.255.255.0	-	-	Edit Delete

Show No.: 10 Total Count: 1 First Previous 1 Next Last 1 GO

Sub Interface: Gi0/2 . 1 * (Range: 1-1023)

VLAN ID: 1 * (Range: 1-4087)

IP Address: *

Submask: *

AnyIP: Enable

Reverse Path: Enable

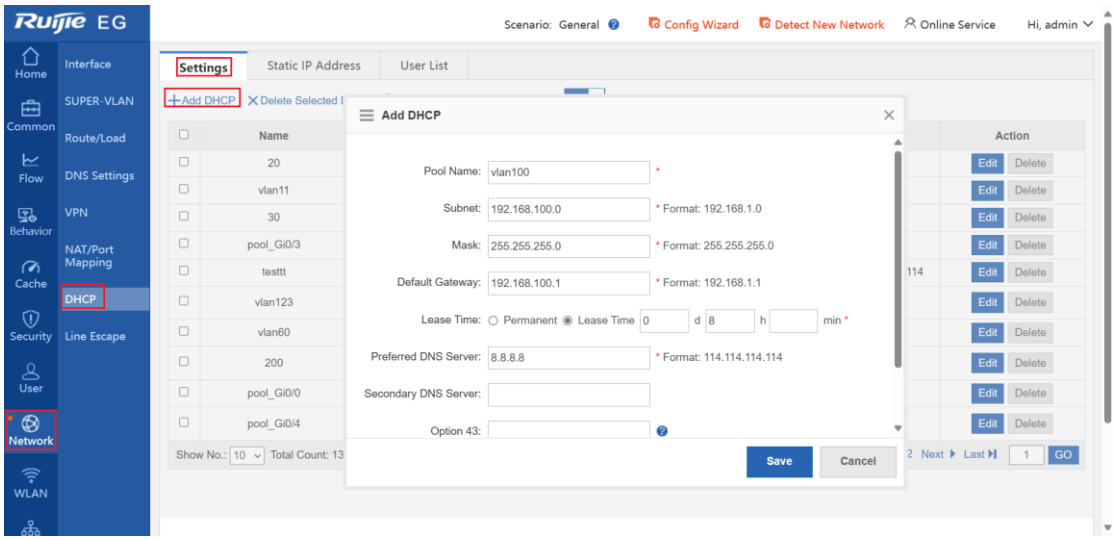
Add

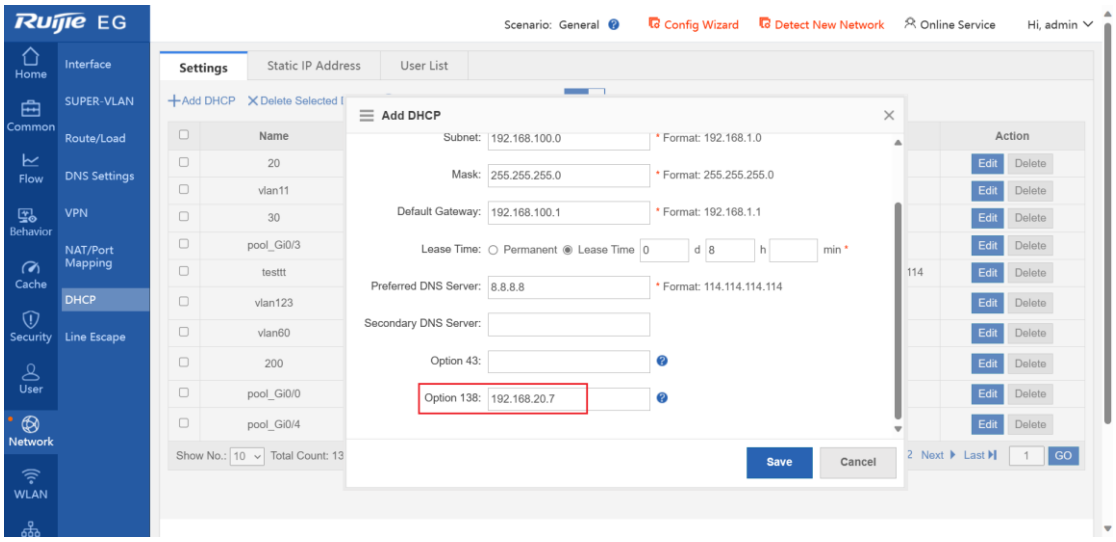
Sub Interface List

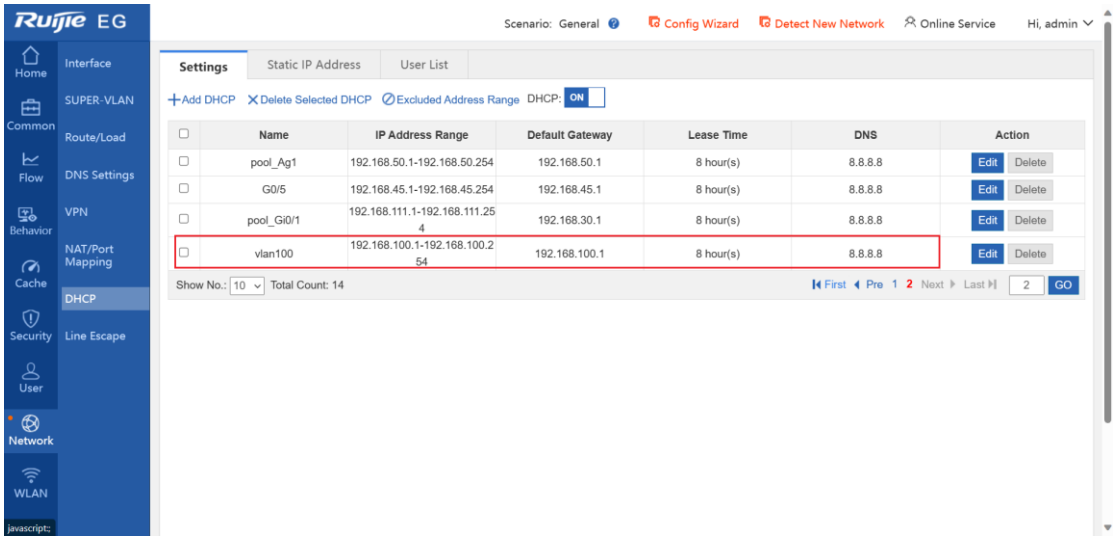
Sub Interface	VLAN ID	Interface Info	Bandwidth	ISP	Action
GigabitEthernet 0/2.100	100	IP Address192.168.100.1 Submask: 255.255.255.0	-	-	Edit Delete
GigabitEthernet 0/2.60	60	IP Address192.168.60.1 Submask: 255.255.255.0	-	-	Edit Delete

Show No.: 10 Total Count: 2 First Previous 1 Next Last 1 GO

Create an address pool

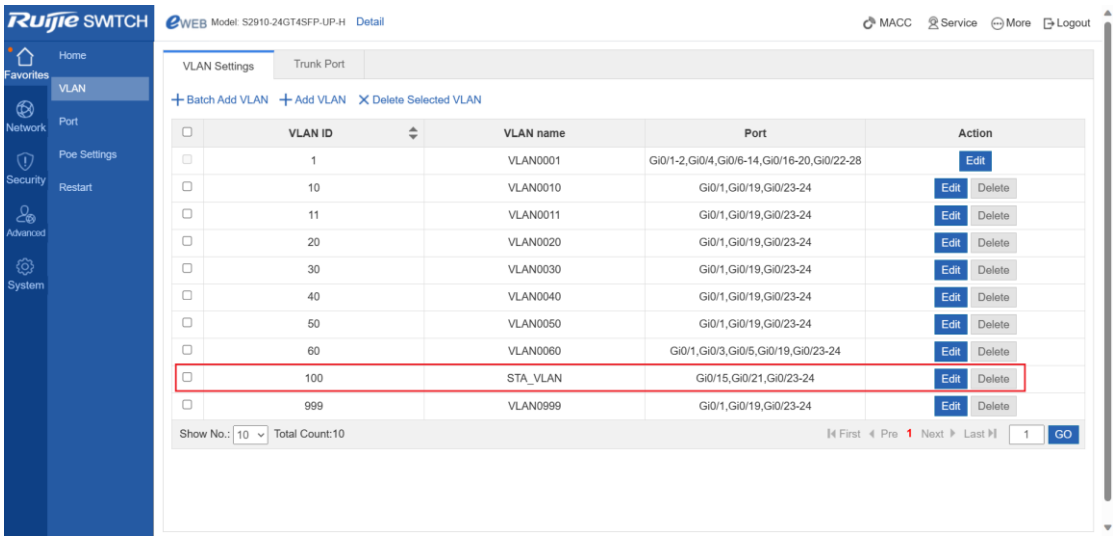






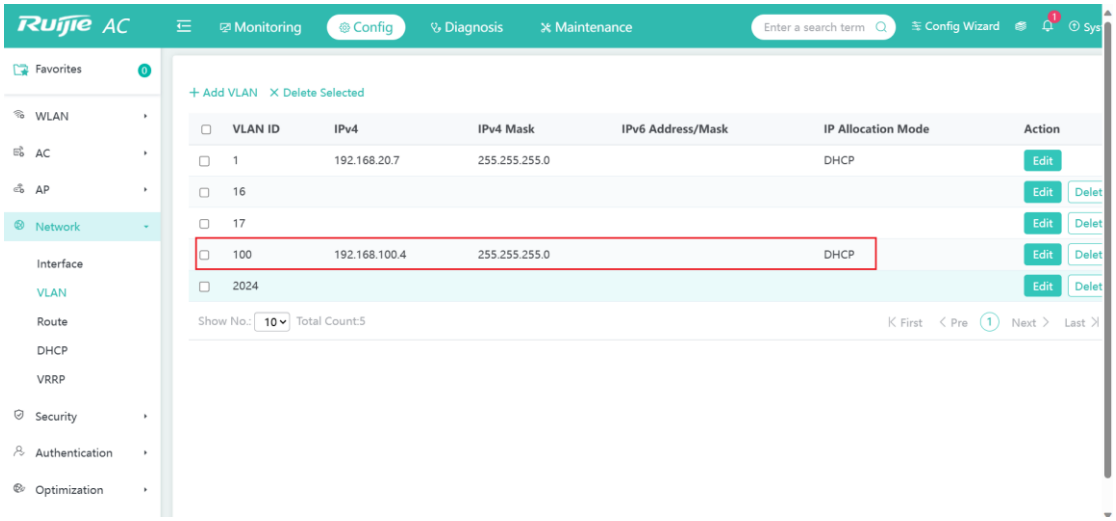
2.5.2 Create VLAN 100 and allow VLAN 100 to pass through on switch and AC

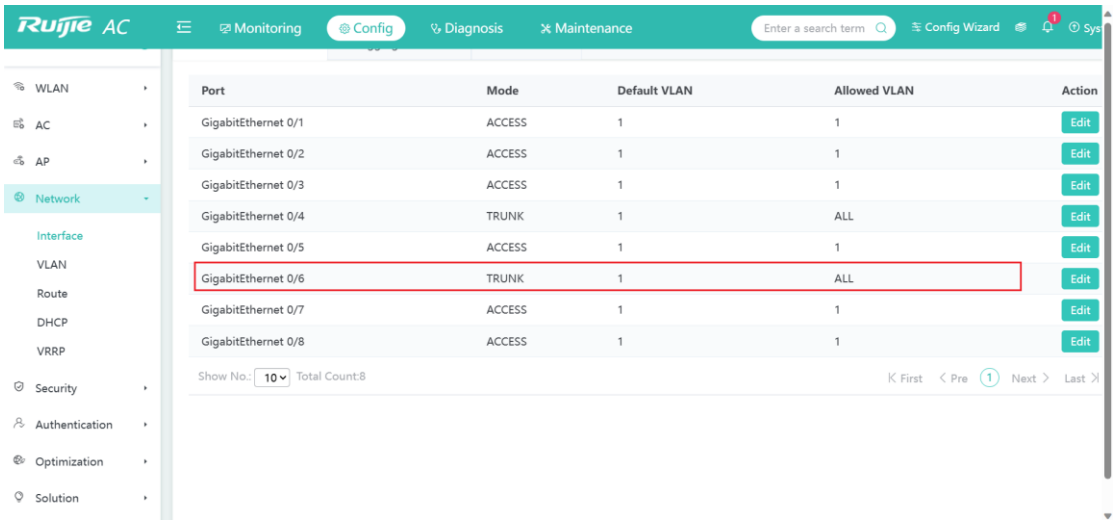
Create VLAN 100 on switch and connect AP and AC with switch. EG port should be set as Trunk and allow VLAN100 to pass through



Port	Up/Down	Port Type	Access VLAN	Native VLAN	Permit VLAN	Description	Action
Gi0/15	Up	TRUNK	1	1	1-4094		Edit Detail
Gi0/16	Up	ACCESS	1	1			Edit Detail
Gi0/17	Up	ACCESS	1	1			Edit Detail
Gi0/18	Up	ACCESS	1	1			Edit Detail
Gi0/19	Up	TRUNK	1	1	1-99,101-4094		Edit Detail
Gi0/20	Up	ACCESS	1	1			Edit Detail
Gi0/21	Up	TRUNK	1	1	1-4094		Edit Detail
Gi0/22	Up	ACCESS	1	1			Edit Detail
Gi0/23	Up	TRUNK	1	1	1-4094		Edit Detail

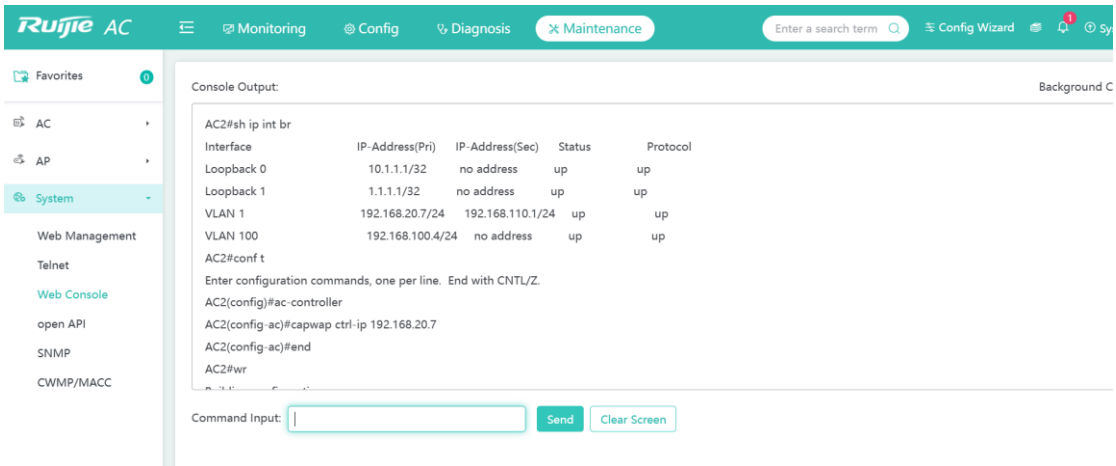
On the AC:



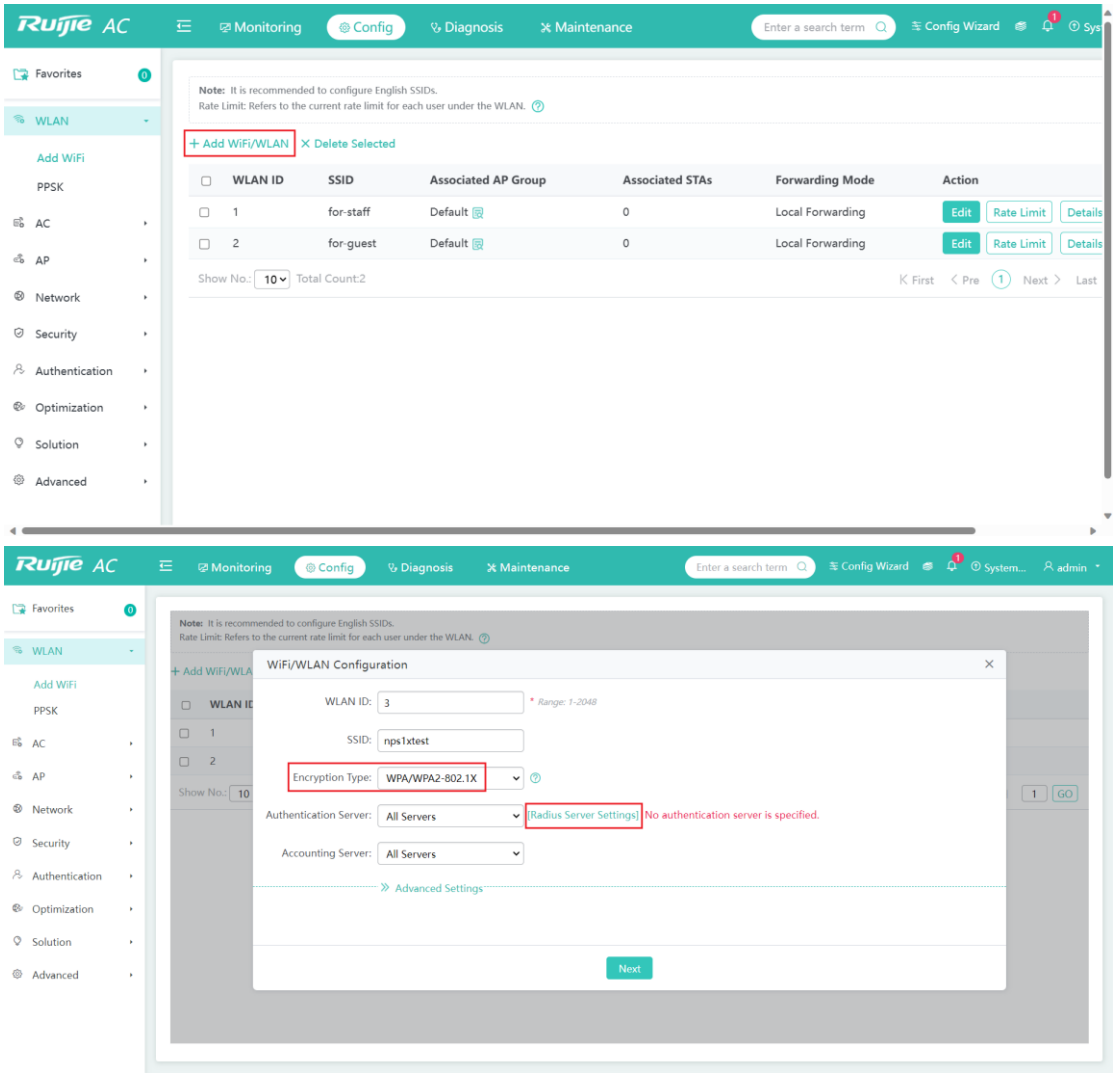


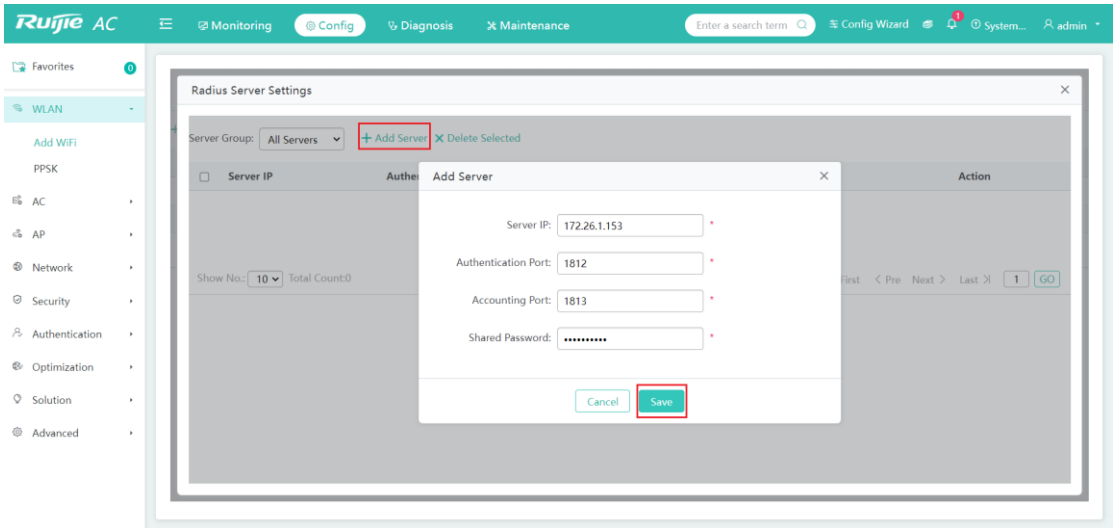
2.5.3 Configure the capwap tunnel address, 802.1x Authentication Parameter (Radius authentication server and AAA Method List) to enable the 802.1x authentication.

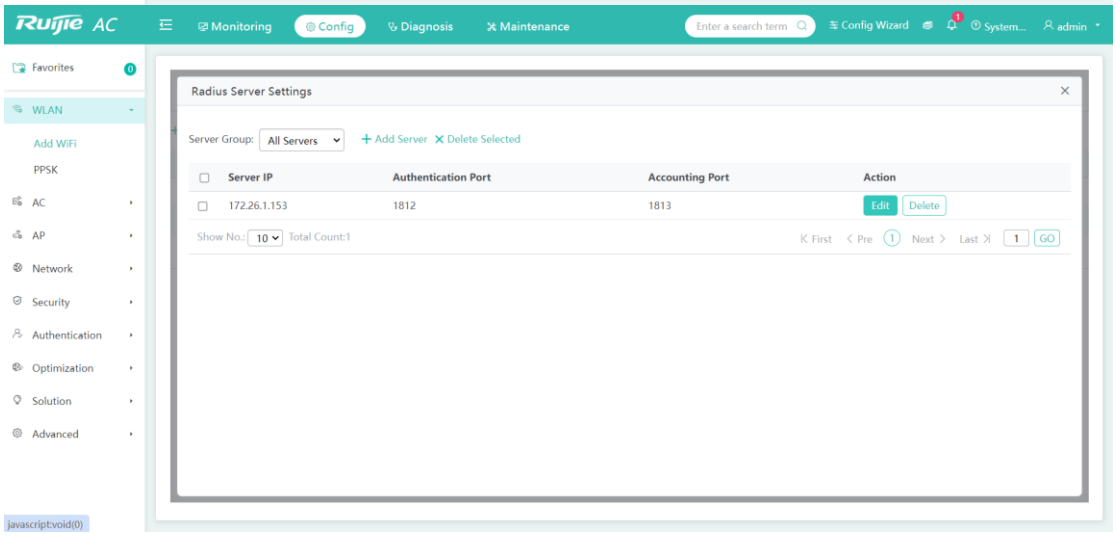
- Configure the capwap tunnel address on AC

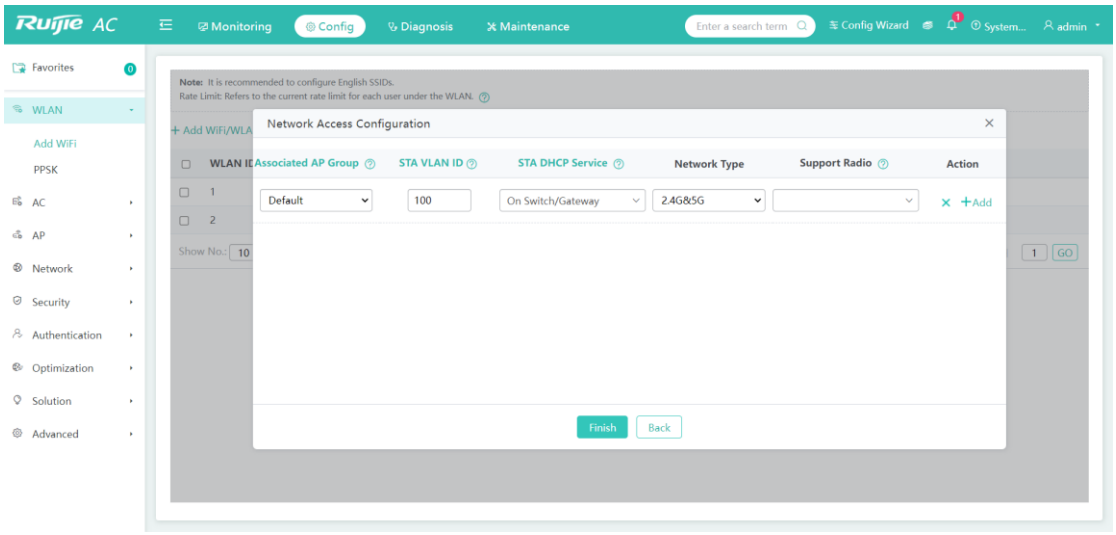


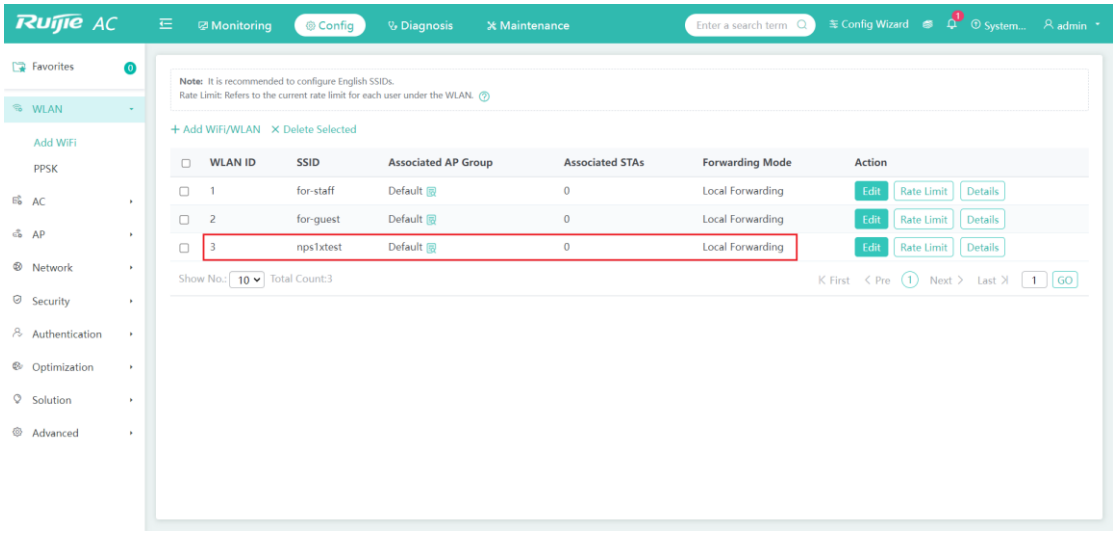
- 802.1x Authentication Parameter (Radius authentication server and AAA Method List)


Ruijie AC
Monitoring
Config
Diagnosis
Maintenance
Enter a search term
Config Wizard
Favorites
WLAN
Add WiFi
PPSK
AC
AP
Network
Security
Authentication
Optimization
Solution
Advanced
Note: It is recommended to configure English SSIDs.
Rate Limit: Refers to the current rate limit for each user under the WLAN.
+ Add WiFi/WLAN
Delete Selected
WLAN ID
SSID
Associated AP Group
Associated STAs
Forwarding Mode
Action
1
for-staff
Default
0
Local Forwarding
Edit
Rate Limit
Details
2
for-guest
Default
0
Local Forwarding
Edit
Rate Limit
Details
Show No.: 10
Total Count:2
First
Pre
Next
Last
WiFi/WLAN Configuration
WLAN ID: 3
* Range: 1-2048
SSID: nps1xtest
Encryption Type: WPA/WPA2-802.1X
Authentication Server: All Servers
[Radius Server Settings] No authentication server is specified.
Accounting Server: All Servers
Advanced Settings
Next

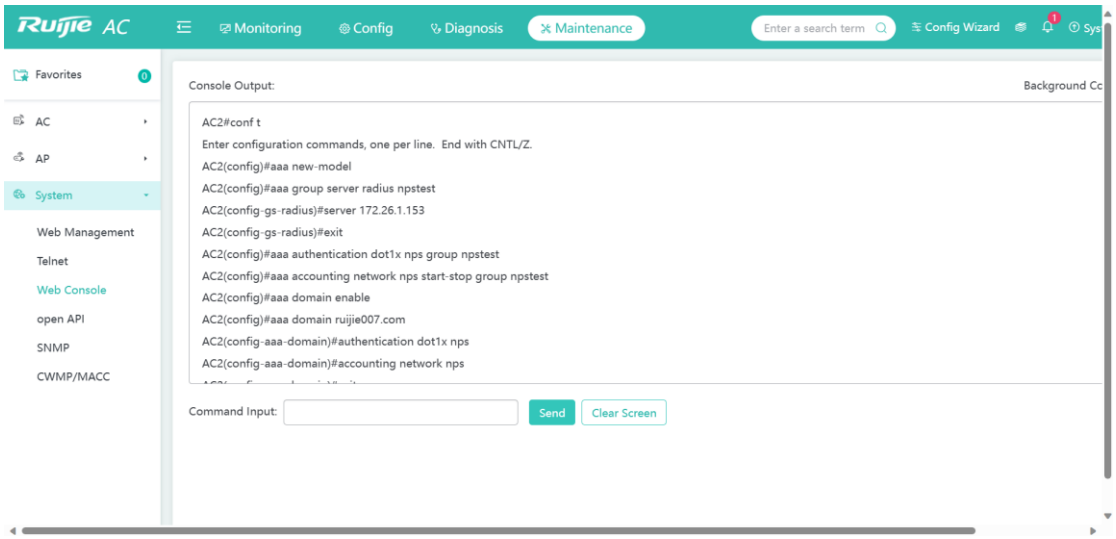

Ruijie AC
Monitoring
Config
Diagnosis
Maintenance
Enter a search term
Config Wizard
System...
admin
Favorites
WLAN
Add WiFi
PPSK
AC
AP
Network
Security
Authentication
Optimization
Solution
Advanced
Radius Server Settings
Server Group:
All Servers
Add Server
Delete Selected
Server IP
Action
Add Server
Server IP:
172.26.1.153
Authentication Port:
1812
Accounting Port:
1813
Shared Password:
Cancel
Save

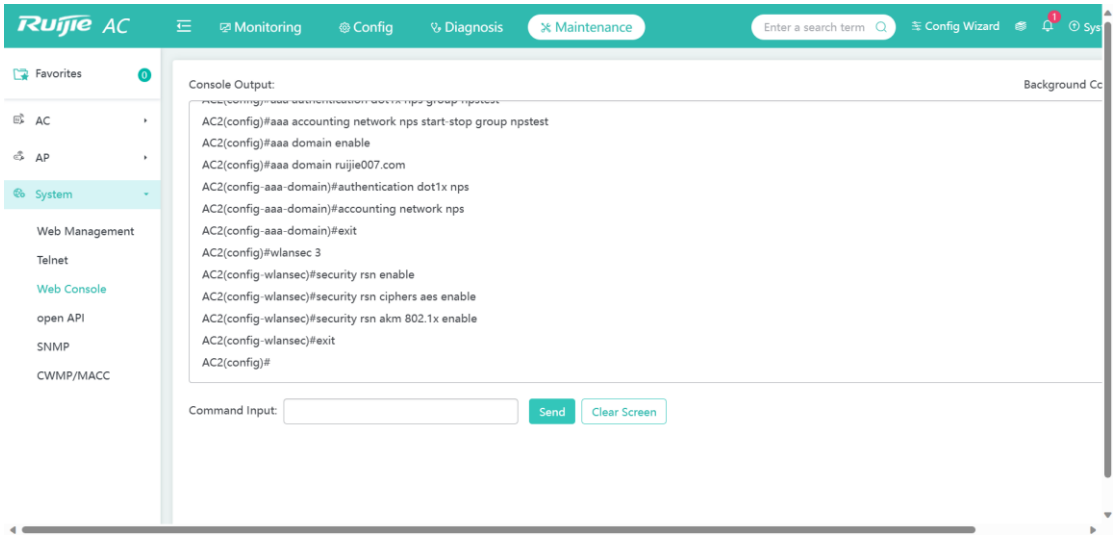

Ruijie AC
Monitoring
Config
Diagnosis
Maintenance
Enter a search term
Config Wizard
System...
admin
Favorites
WLAN
Add WiFi
PPSK
AC
AP
Network
Security
Authentication
Optimization
Solution
Advanced
Radius Server Settings
Server Group:
All Servers
Add Server
Delete Selected
Server IP
Authentication Port
Accounting Port
Action
172.26.1.153
1812
1813
Edit
Delete
Show No.:
10
Total Count:1
First
Pre
Next
Last
GO
javascript:void(0)


Ruijie AC
Monitoring
Config
Diagnosis
Maintenance
Enter a search term
Config Wizard
System...
admin
Favorites
WLAN
Add WiFi
PPSK
AC
AP
Network
Security
Authentication
Optimization
Solution
Advanced
Note: It is recommended to configure English SSIDs.
Rate Limit: Refers to the current rate limit for each user under the WLAN.
Network Access Configuration
WLAN ID
Associated AP Group
STA VLAN ID
STA DHCP Service
Network Type
Support Radio
Action
Default
100
On Switch/Gateway
2.4G&5G
Add
Finish
Back



To do the CLI configuration






```
AC2(config)#aaa new-model

AC2(config)#aaa group server radius npstest

AC2(config-gs-radius)#server 172.26.1.153
```

```
AC2(config-gs-radius)#exit
AC2(config)#aaa authentication dot1x nps group npstest
AC2(config)#aaa accounting network nps start-stop group npstest
AC2(config)#aaa domain enable
AC2(config)#aaa domain ruijie007.com  // the domain name setted in nps 上设置的域名
AC2(config-aaa-domain)#authentication dot1x nps
AC2(config-aaa-domain)#accounting network nps
AC2(config-aaa-domain)#exit
AC2(config)#wlansec 3        //corresponding wlansec number of nps1xtest SSID,
that is WLAN ID
AC2(config-wlansec)#security rsn enable
AC2(config-wlansec)#security rsn ciphers aes enable
AC2(config-wlansec)#security rsn akm 802.1x enable
AC2(config-wlansec)#exit
AC2(config)#end
AC2#wr
Building configuration...
[OK]
AC2#
```

2.6 Result Verification

STA connect to the SSID and pass the authentication successfully.