

Using Windows 2008 With Aruba Controllers

Version 1.0

Tobias Rice

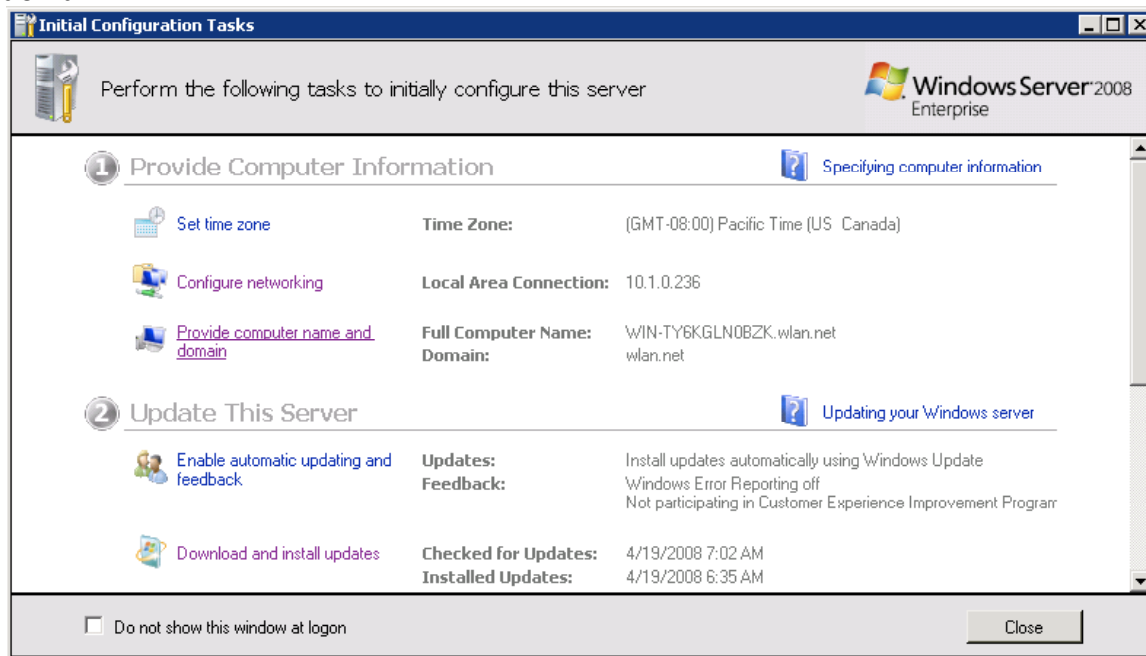
This will be a basic setup using Windows 2008 Server to allow dot1x auth with an Aruba controller. Steps to have a basic installation include:

1. Rename the server
2. Setting server as Domain Controller
3. Installing Certificate Services
4. Request Certificates (optional)
5. Installing Network Policy Services (previously IAS)
6. Creating Group Policies

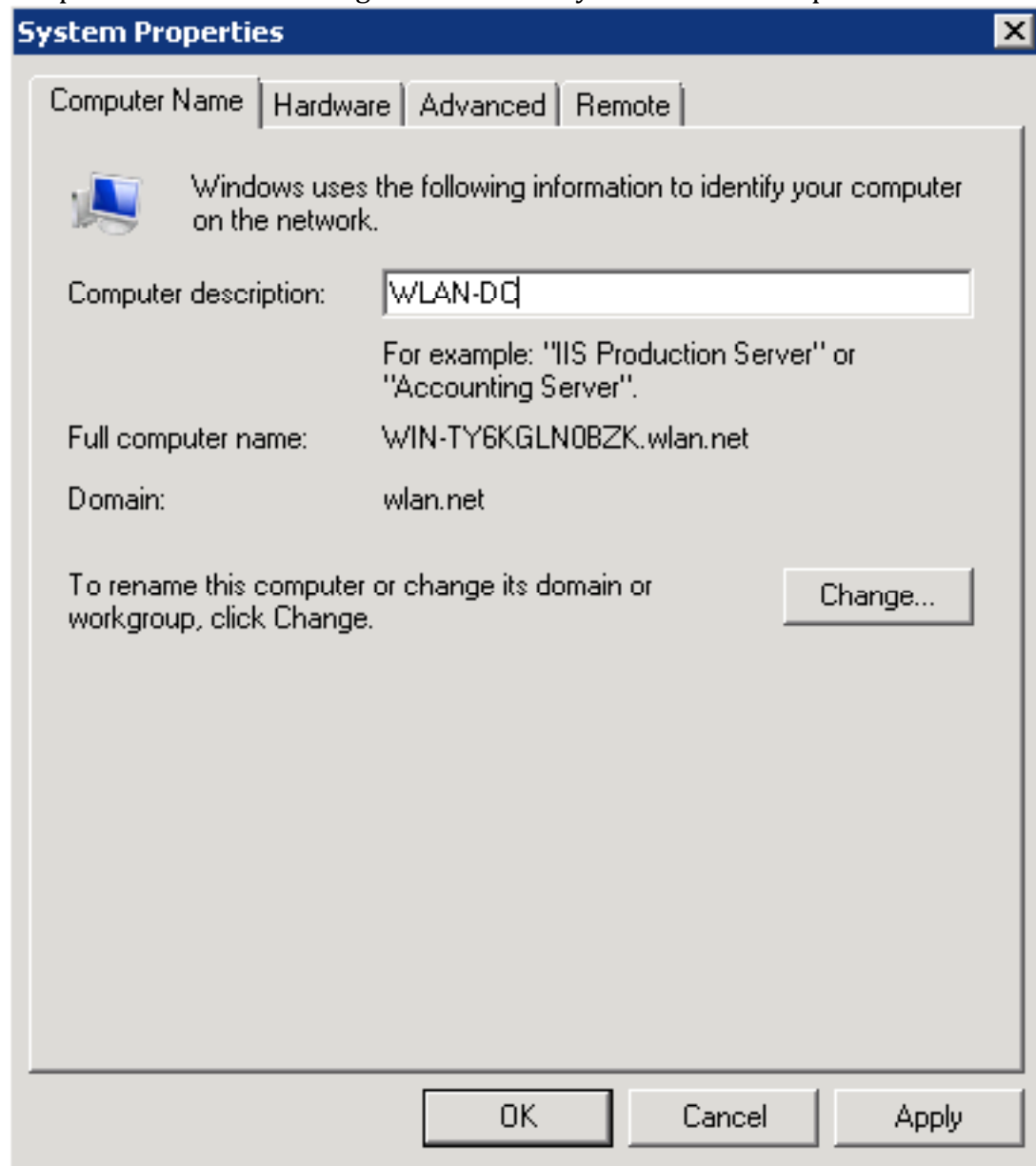
Rename The Server

Something different about Windows 2008 Server is that the server name is auto-generated and you are not given a chance during the install to name the server so you must do **before** installing Active Directory or Certificate Services.

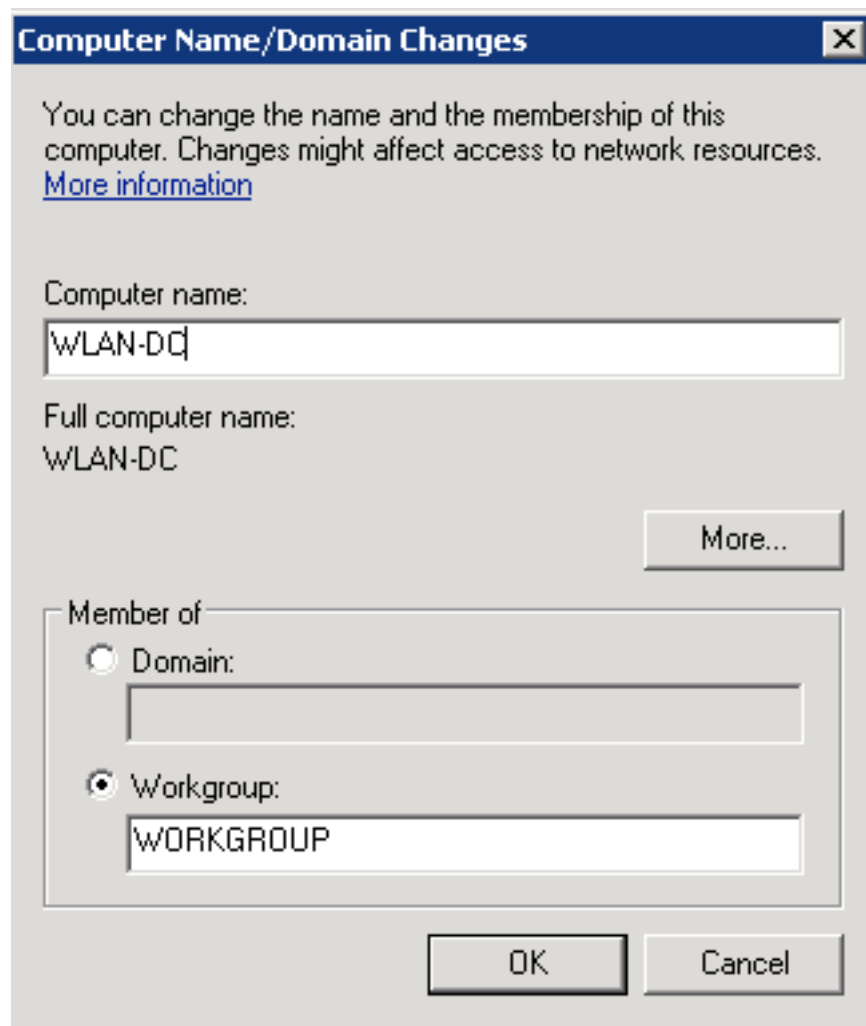
In the “Initial Configuration Tasks” window, click the “Provide computer name and domain” link.



Enter a Computer description and click the "Change..." button to change the computer name. I'll be using WLAN-DC as my name and description.



Enter the Computer name and click “OK” and reboot when prompted.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.
[More information](#)

Computer name:
WLAN-DC

Full computer name:
WLAN-DC

More...

Member of

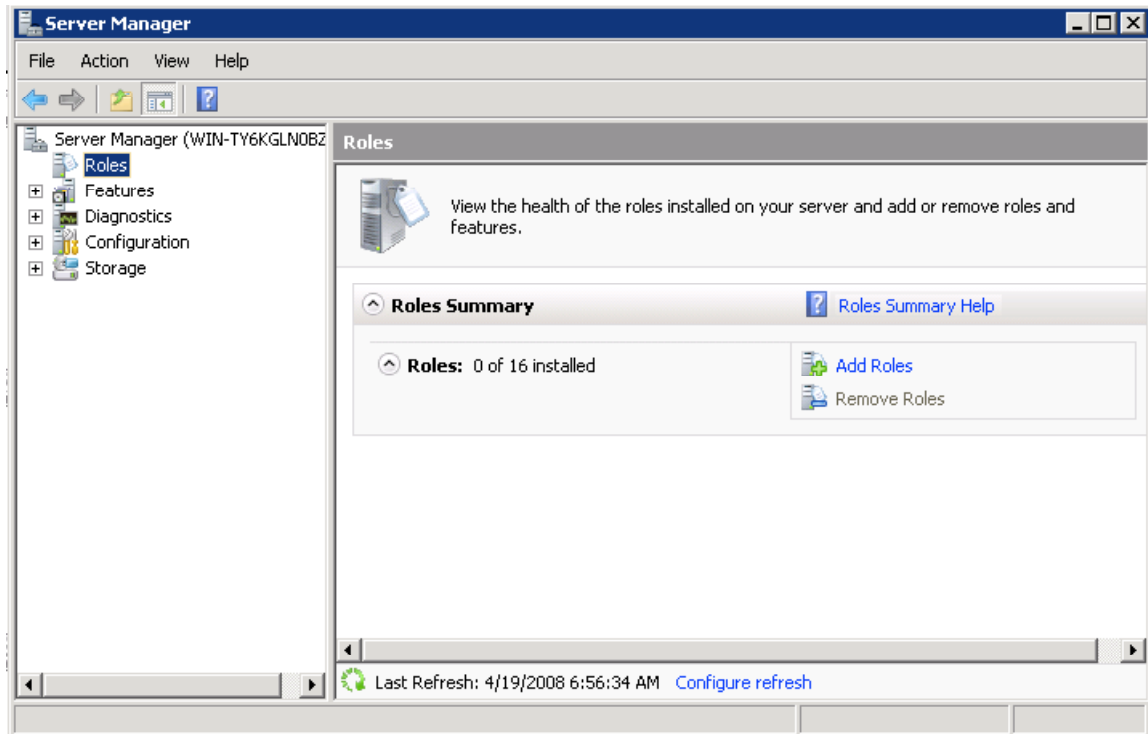
☐ Domain:
[Empty text box]

☒ Workgroup:
WORKGROUP

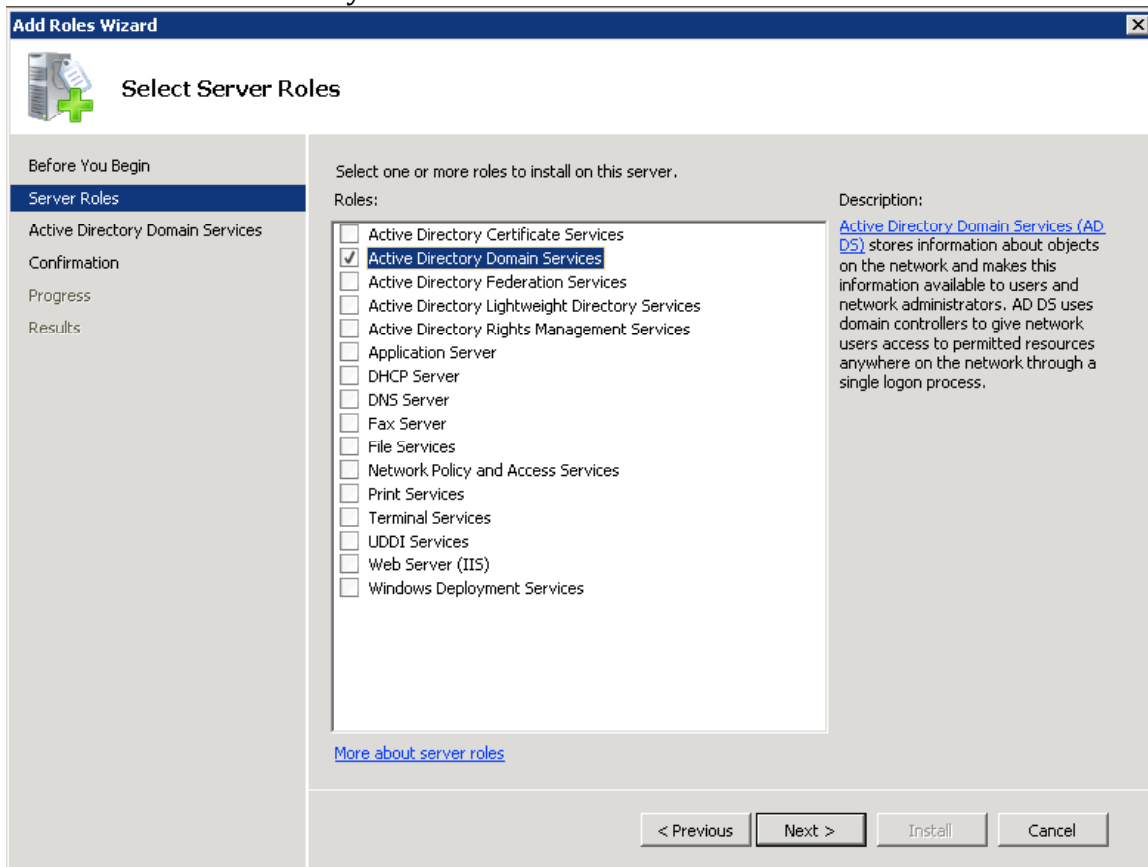
OK Cancel

Setting Server as a Domain Controller

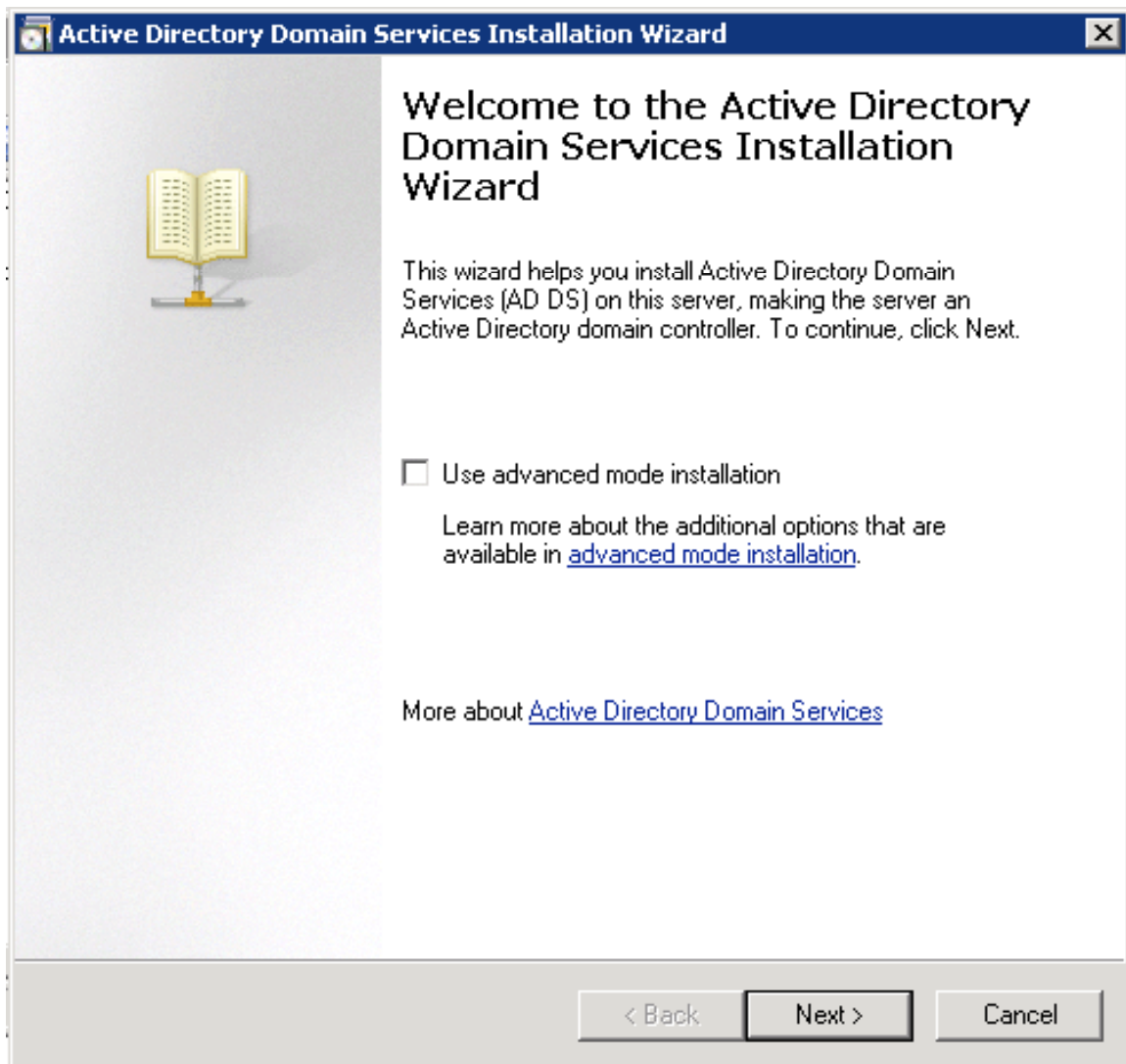
For this example we setup a new forest for the wlan.net domain. Server 2008 abstracts most server function into “Roles” so we’ll be adding the Active Directory Domain Services Role with the Server Manager by clicking “Roles” and clicking “Add Roles.”



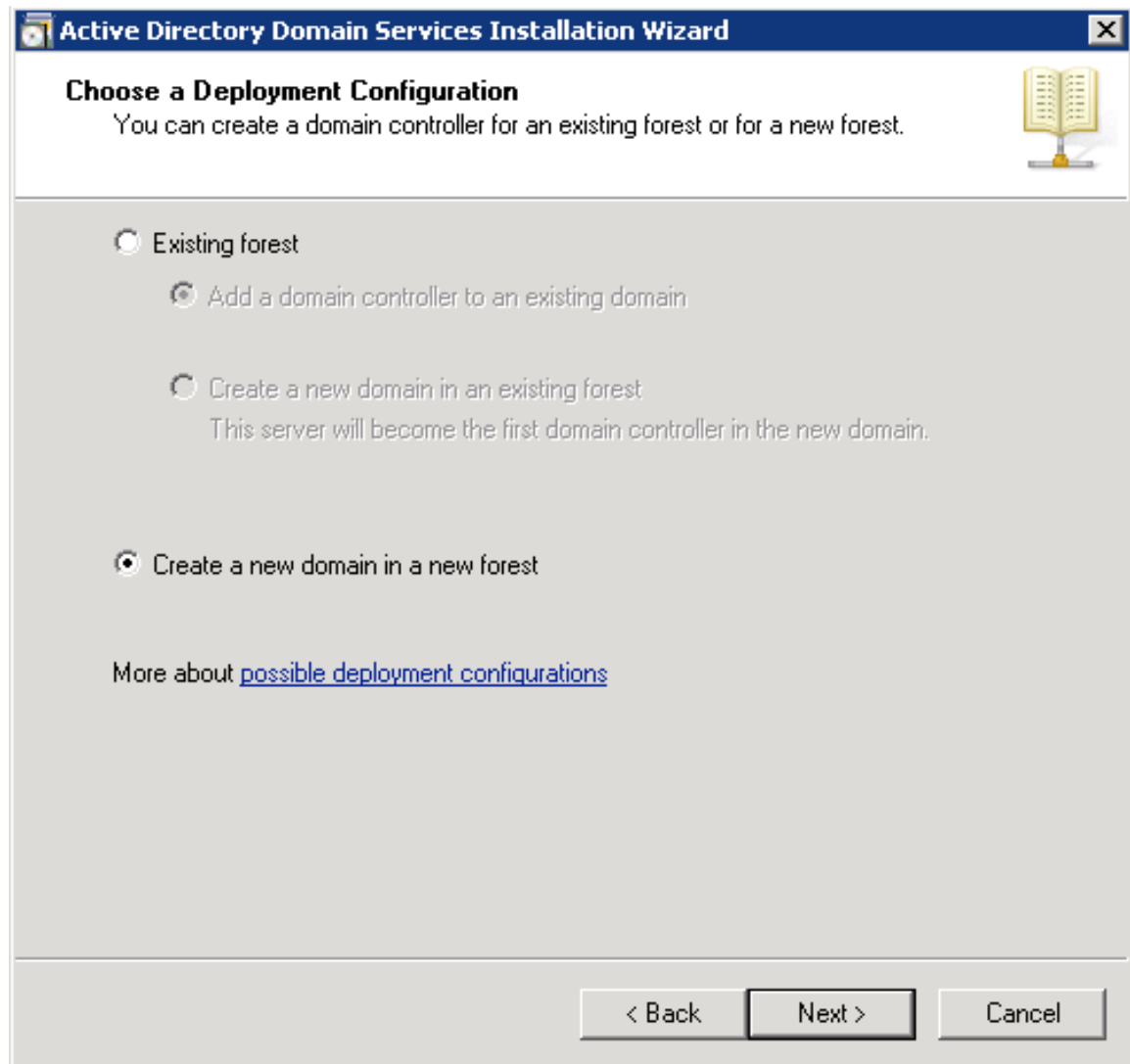
Select the Active Directory Domain Services Role.



Click through the confirmation screens and click Install. You should get see an installation progress screen and finally an “installation success” message that asks you to run the command “dcpromo.exe” which will configure your domain. So click the link to run “dcpromo” or click the “Start” button, select “Run” and enter “dcpromo.exe”. You should now see the “Active Directory Domain Service” install wizard. Click “Next “ to continue.



Choose “Create a new domain in a new forest” and click “Next”.



The image shows a Windows-style dialog box titled "Active Directory Domain Services Installation Wizard". The title bar is blue with a small icon on the left and a close button (X) on the right. The main content area has a white background. At the top, the text "Choose a Deployment Configuration" is followed by the instruction "You can create a domain controller for an existing forest or for a new forest." To the right of this text is a small icon of an open book. Below this, there are three radio button options. The first option is "Existing forest", which is currently unselected. It has two sub-options: "Add a domain controller to an existing domain" (also unselected) and "Create a new domain in an existing forest" (also unselected). The second sub-option has a descriptive text: "This server will become the first domain controller in the new domain." The third option is "Create a new domain in a new forest", which is selected with a black dot. At the bottom of the main area, there is a link: "More about [possible deployment configurations](#)". At the very bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted with a black border.

Active Directory Domain Services Installation Wizard

Choose a Deployment Configuration
You can create a domain controller for an existing forest or for a new forest.

☐ Existing forest

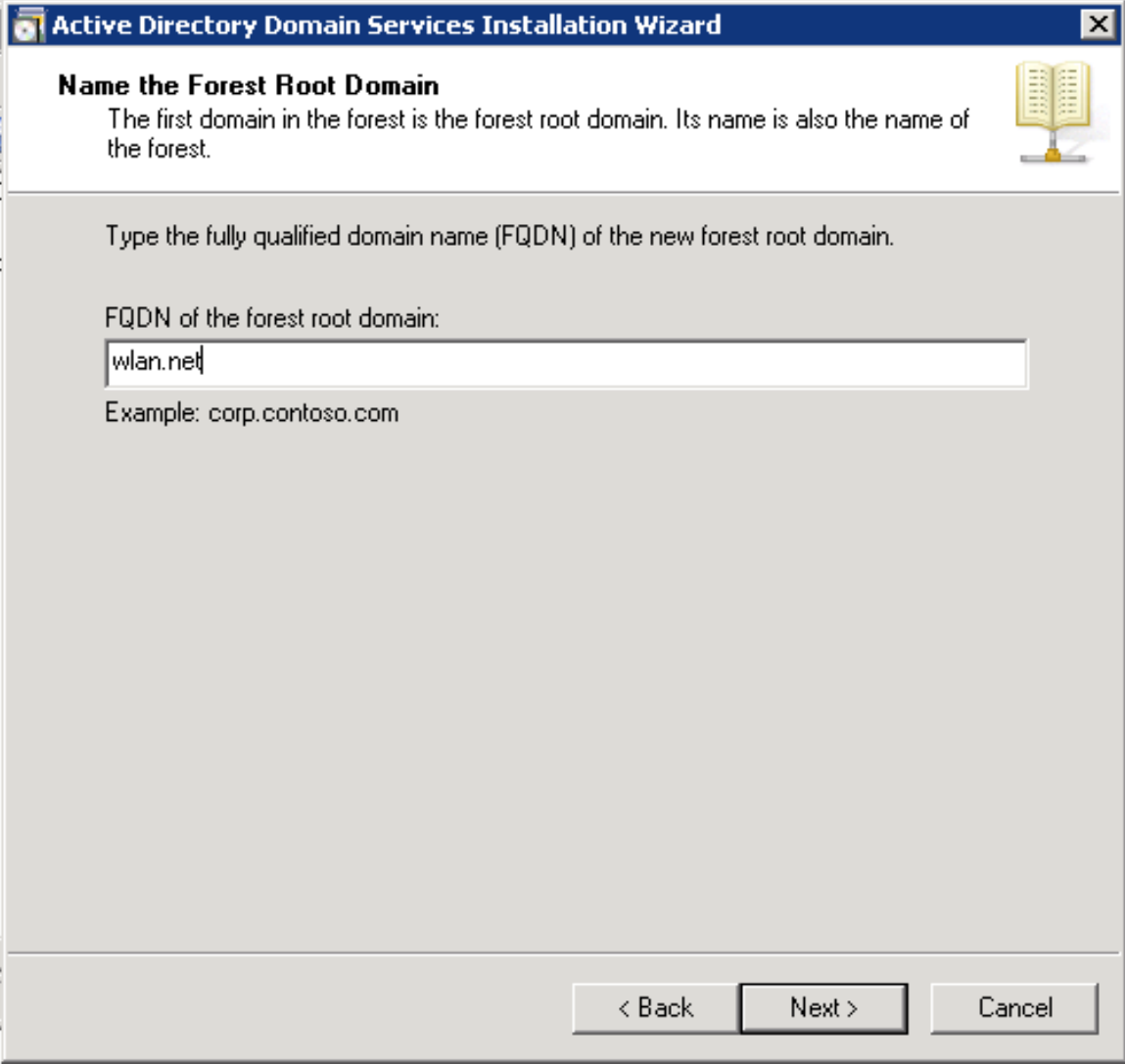
- ☐ Add a domain controller to an existing domain
- ☐ Create a new domain in an existing forest
This server will become the first domain controller in the new domain.

☒ Create a new domain in a new forest

More about [possible deployment configurations](#)

< Back Next > Cancel

For our example domain we'll use "wlan.net". Click "Next" and it will check to see if the name is already used on the network.



The image shows a screenshot of the 'Active Directory Domain Services Installation Wizard' window. The title bar is blue with the text 'Active Directory Domain Services Installation Wizard' and a close button. The main window has a white header area with the title 'Name the Forest Root Domain' and a sub-explanation: 'The first domain in the forest is the forest root domain. Its name is also the name of the forest.' To the right of the text is an icon of an open book. Below the header is a large gray area with the instruction 'Type the fully qualified domain name (FQDN) of the new forest root domain.' and 'FQDN of the forest root domain:'. A text input field contains 'wlan.net'. Below the input field is an example: 'Example: corp.contoso.com'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Active Directory Domain Services Installation Wizard

Name the Forest Root Domain

The first domain in the forest is the forest root domain. Its name is also the name of the forest.

Type the fully qualified domain name (FQDN) of the new forest root domain.

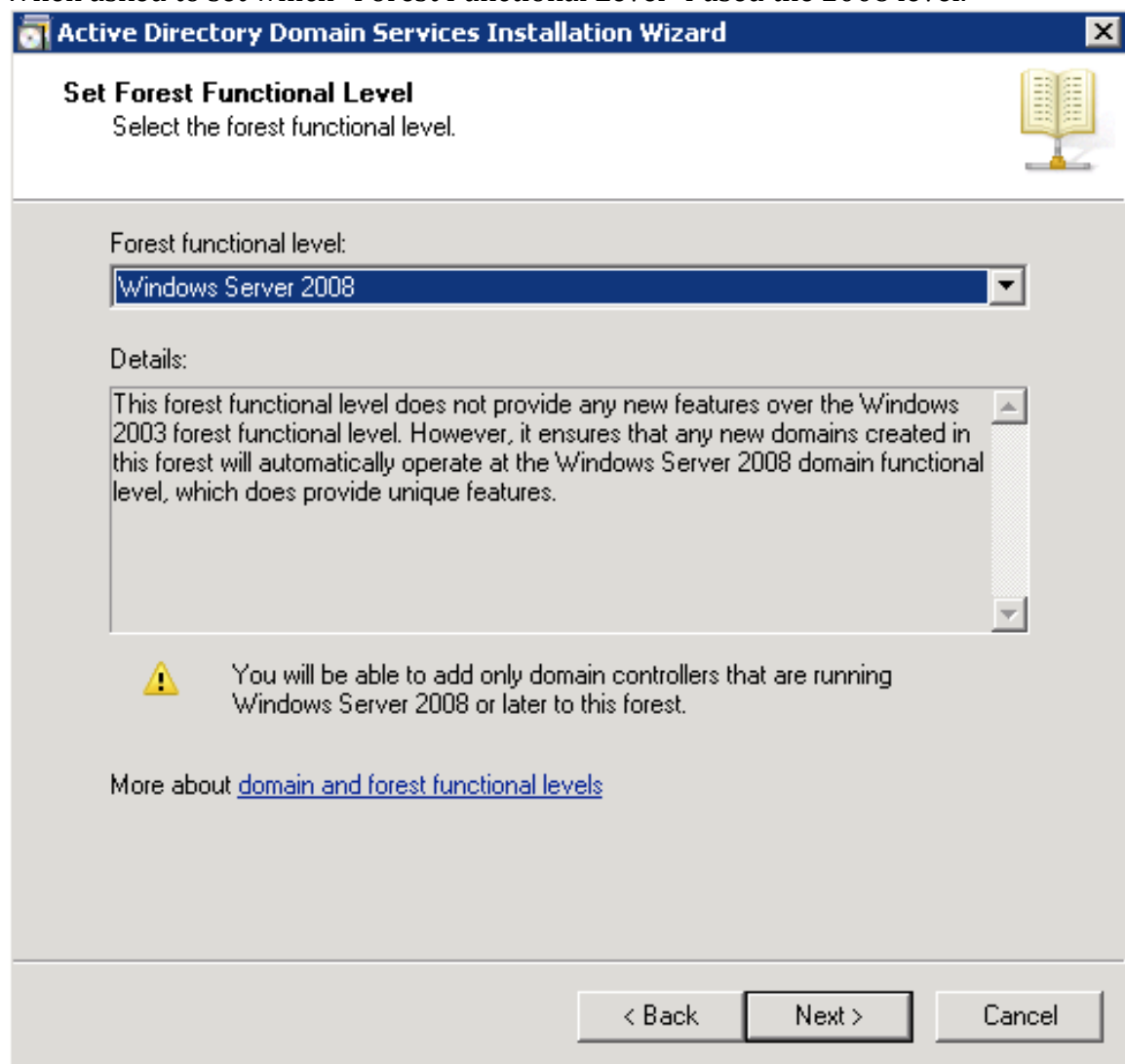
FQDN of the forest root domain:

wlan.net

Example: corp.contoso.com

< Back Next > Cancel

When asked to set which “Forest Functional Level” I used the 2008 level.



The image shows a screenshot of the 'Active Directory Domain Services Installation Wizard' window. The title bar reads 'Active Directory Domain Services Installation Wizard'. The main heading is 'Set Forest Functional Level', with the instruction 'Select the forest functional level.' below it. A dropdown menu for 'Forest functional level:' is set to 'Windows Server 2008'. A 'Details' section contains a text box explaining that this level does not provide new features over Windows Server 2003 but ensures new domains operate at the Windows Server 2008 level. A yellow warning icon is followed by the text: 'You will be able to add only domain controllers that are running Windows Server 2008 or later to this forest.' A link for 'More about domain and forest functional levels' is provided. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

Active Directory Domain Services Installation Wizard

Set Forest Functional Level
Select the forest functional level.

Forest functional level:
Windows Server 2008

Details:

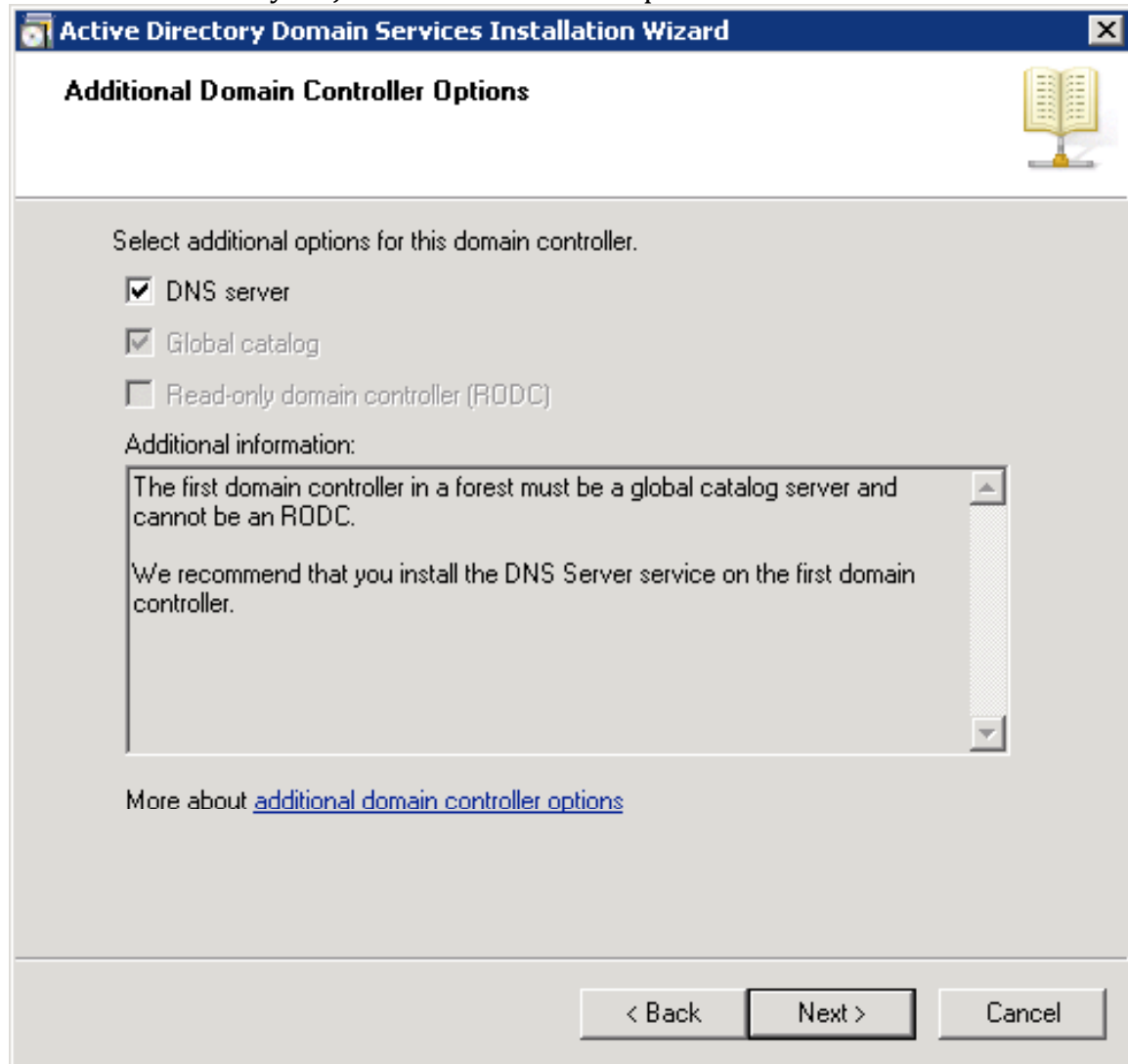
This forest functional level does not provide any new features over the Windows 2003 forest functional level. However, it ensures that any new domains created in this forest will automatically operate at the Windows Server 2008 domain functional level, which does provide unique features.

 You will be able to add only domain controllers that are running Windows Server 2008 or later to this forest.

More about [domain and forest functional levels](#)

< Back Next > Cancel

The next screen you'll see is a warning that the DNS service isn't install and will offer to install it for you. Just click "Next" to accept and install.



The screenshot shows the 'Active Directory Domain Services Installation Wizard' window. The title bar includes a help icon, the text 'Active Directory Domain Services Installation Wizard', and a close button. The main heading is 'Additional Domain Controller Options', accompanied by a book icon. Below this, a text prompt asks to 'Select additional options for this domain controller.' There are three checkboxes: 'DNS server' (checked), 'Global catalog' (checked), and 'Read-only domain controller (RODC)' (unchecked). An 'Additional information:' section contains a text box with two paragraphs: 'The first domain controller in a forest must be a global catalog server and cannot be an RODC.' and 'We recommend that you install the DNS Server service on the first domain controller.' At the bottom, there is a link 'More about [additional domain controller options](#)' and three buttons: '< Back', 'Next >', and 'Cancel'.

Active Directory Domain Services Installation Wizard

Additional Domain Controller Options

Select additional options for this domain controller.

- ☒ DNS server
- ☒ Global catalog
- ☐ Read-only domain controller (RODC)

Additional information:

The first domain controller in a forest must be a global catalog server and cannot be an RODC.

We recommend that you install the DNS Server service on the first domain controller.

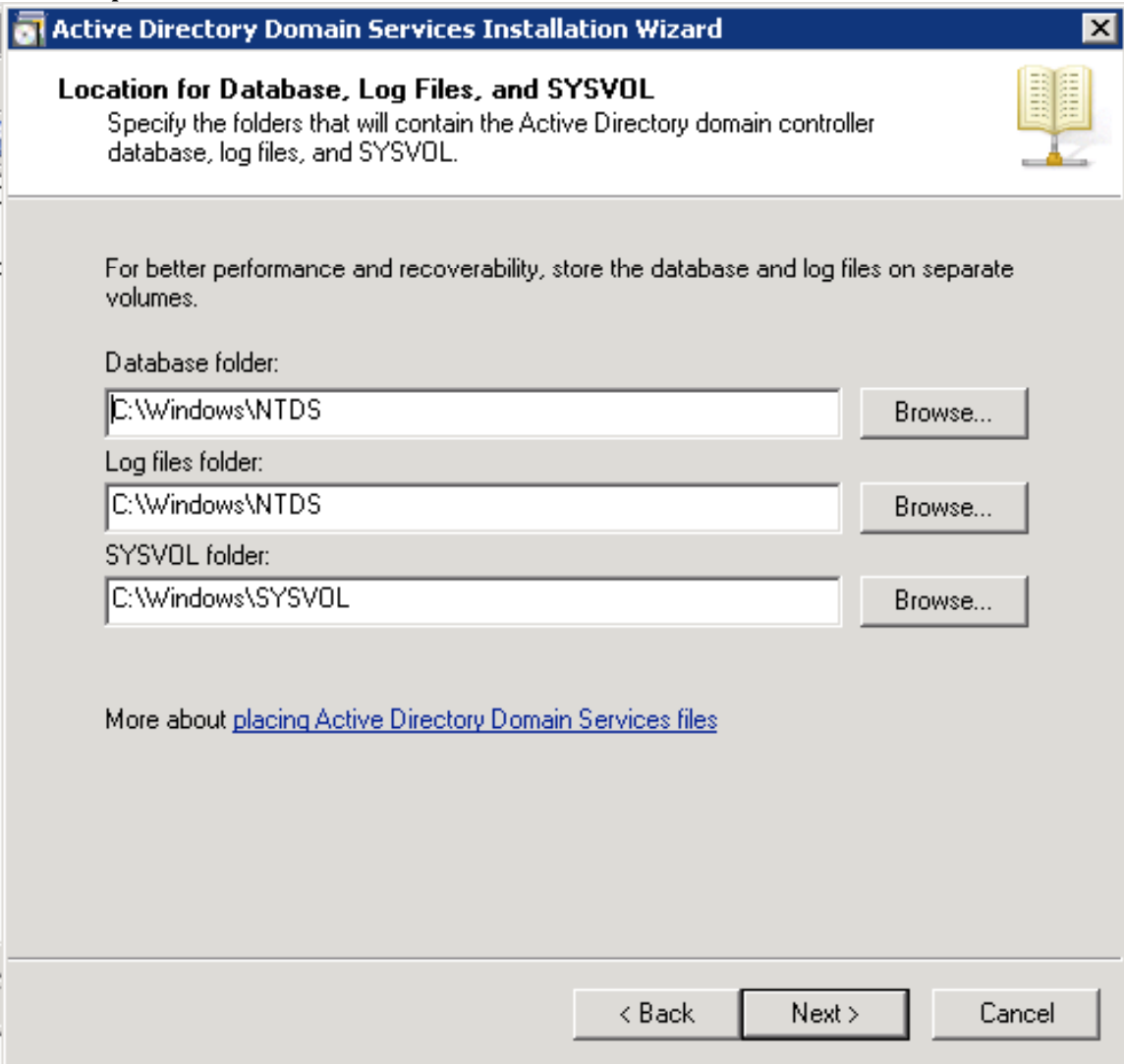
More about [additional domain controller options](#)

< Back Next > Cancel

It will display the following warning, just click "Yes" to continue.



Just accept the defaults and click “Next”.



The image shows a screenshot of the 'Active Directory Domain Services Installation Wizard' window. The title bar reads 'Active Directory Domain Services Installation Wizard'. The main heading is 'Location for Database, Log Files, and SYSVOL'. Below this, it says 'Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.' There is a small icon of an open book in the top right corner. The main area contains a note: 'For better performance and recoverability, store the database and log files on separate volumes.' Below this, there are three sections for folder selection: 'Database folder:' with a text box containing 'C:\Windows\NTDS' and a 'Browse...' button; 'Log files folder:' with a text box containing 'C:\Windows\NTDS' and a 'Browse...' button; and 'SYSVOL folder:' with a text box containing 'C:\Windows\SYSVOL' and a 'Browse...' button. At the bottom, there is a link: 'More about [placing Active Directory Domain Services files](#)'. The bottom of the window has three buttons: '< Back', 'Next >', and 'Cancel'.

Active Directory Domain Services Installation Wizard

Location for Database, Log Files, and SYSVOL
Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.

For better performance and recoverability, store the database and log files on separate volumes.

Database folder:
C:\Windows\NTDS Browse...

Log files folder:
C:\Windows\NTDS Browse...

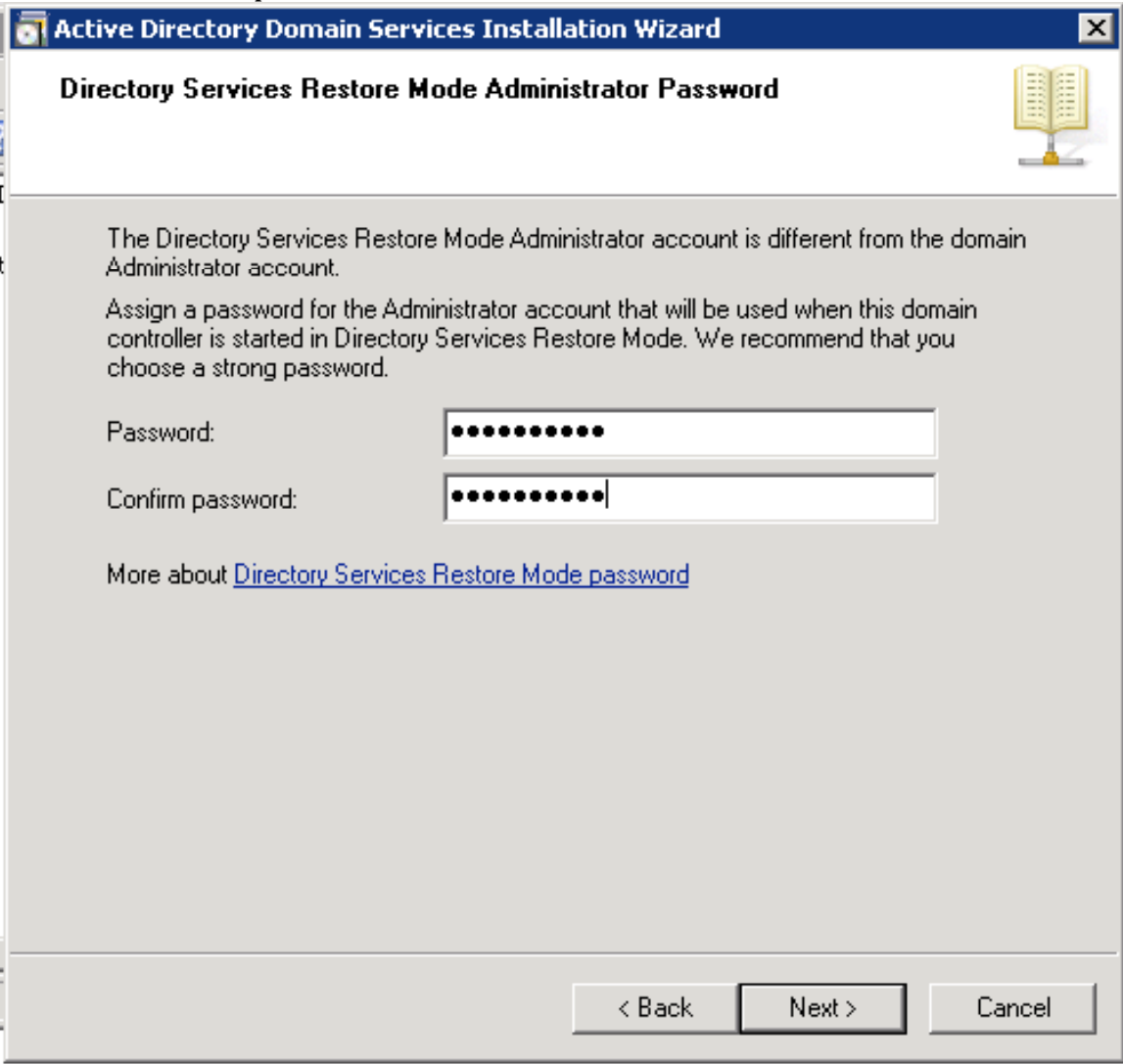
SYSVOL folder:
C:\Windows\SYSVOL Browse...

More about [placing Active Directory Domain Services files](#)

< Back Next > Cancel

Now you'll be prompted to enter a "Directory Services Restore Mode Administrator

Password". Enter a password and click "Next".



The screenshot shows a Windows XP-style window titled "Active Directory Domain Services Installation Wizard". The window has a blue title bar with a close button (X) in the top right corner. Below the title bar, the main heading is "Directory Services Restore Mode Administrator Password". To the right of this heading is a small icon of an open book. The main content area is light gray and contains the following text: "The Directory Services Restore Mode Administrator account is different from the domain Administrator account." followed by "Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password." Below this text are two input fields. The first is labeled "Password:" and the second is labeled "Confirm password:". Both fields contain ten black dots, indicating that the passwords are masked. Below the input fields is a blue hyperlink that reads "More about [Directory Services Restore Mode password](#)". At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted with a black border.

Active Directory Domain Services Installation Wizard

Directory Services Restore Mode Administrator Password

The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

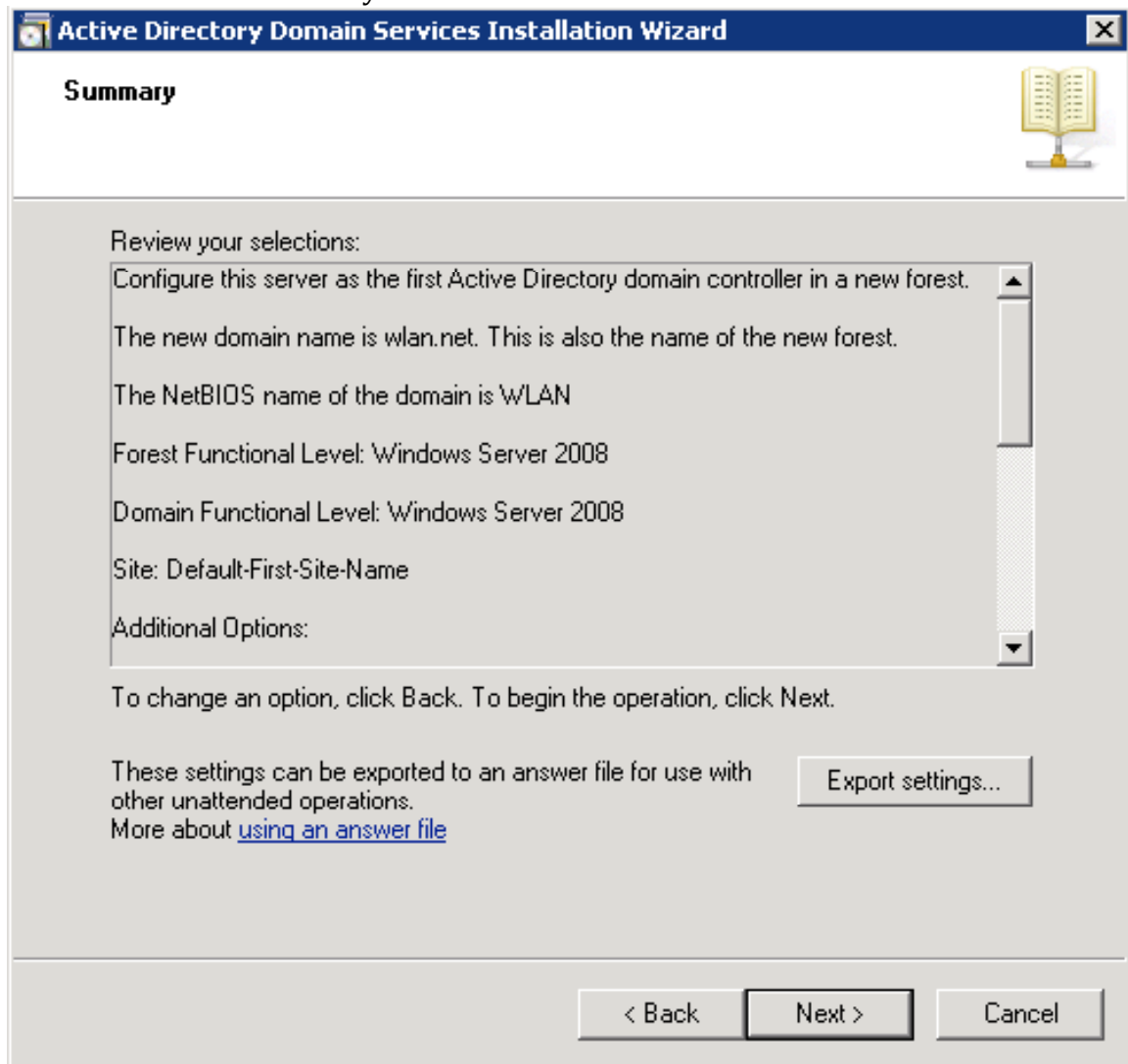
Password:

Confirm password:

More about [Directory Services Restore Mode password](#)

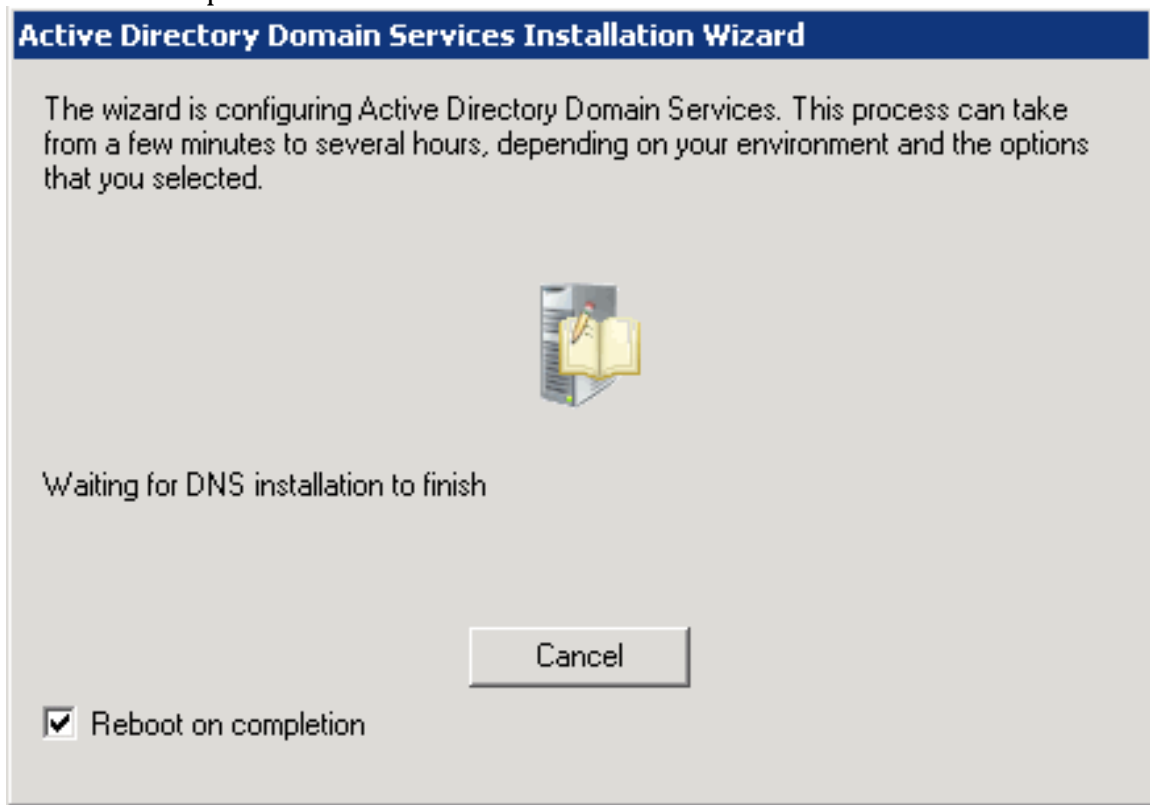
< Back Next > Cancel

Click "Next" at the Summary screen.



You'll now see the Installation Wizard install DNS and Active Directory. Check the "Reboot on completion" box and once the wizard finishes it'll reboot and be ready

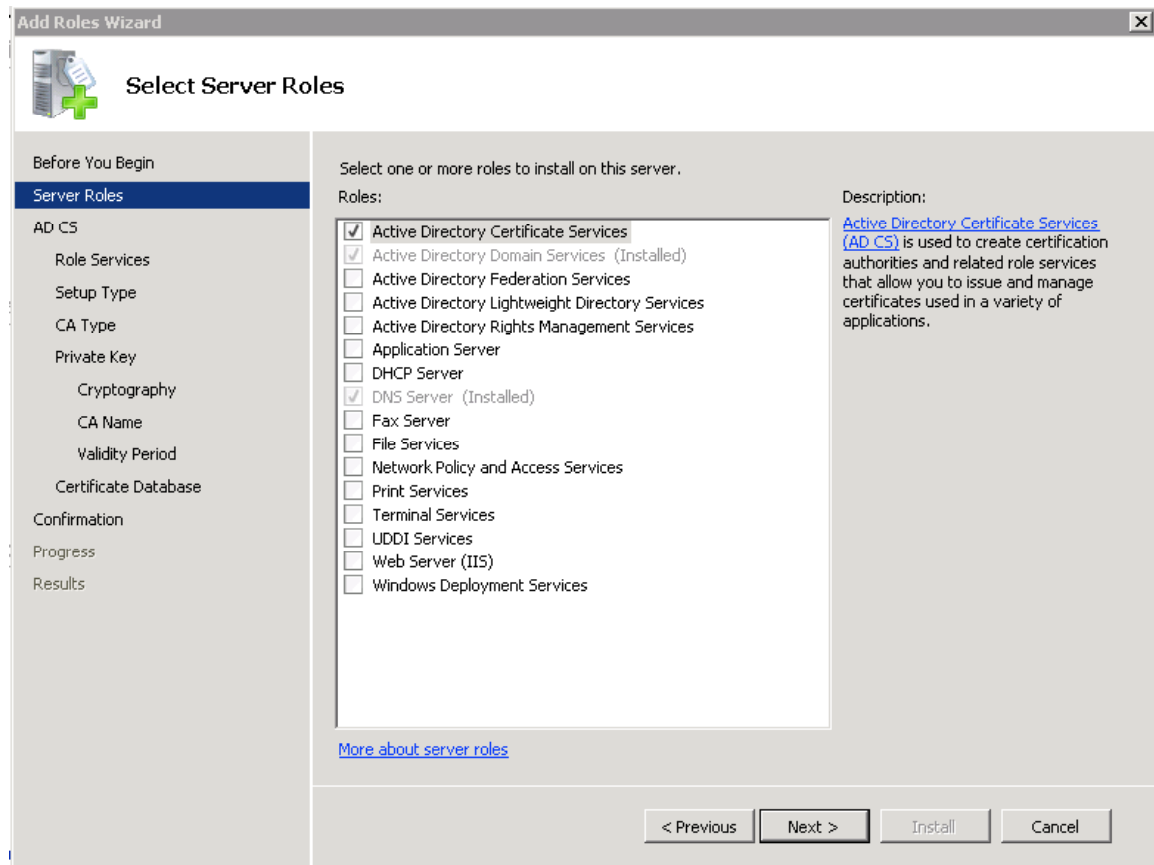
for the next step.



Installing Certificate Services

To enable PEAP or EAP-TLS we'll need to install Certificate Services to enable a Certificate Authority (CA) to generate and sign certificates for our domain. Again, add a Role via the Server Manager and select "Active Directory Certificate Services"

and click “Next”.



Click through the conformation screen and select “Certification Authority” and “Certificate Authority Web Enrollment” which will tell you that you’ll need IIS to be installed to use the “Certificate Authority Web Enrollment”. Click “Add Required

Role Services” and click “Next” to continue.

Add Roles Wizard

Select Role Services

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Select the role services to install for Active Directory Certificate Services:

Role services:

- ☒ Certification Authority
- ☐ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service

Description:
[Certification Authority \(CA\)](#) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

Add Roles Wizard

Add role services and features required for Certification Authority Web Enrollment?

You cannot install Certification Authority Web Enrollment unless the required role services and features are also installed.

Role Services:

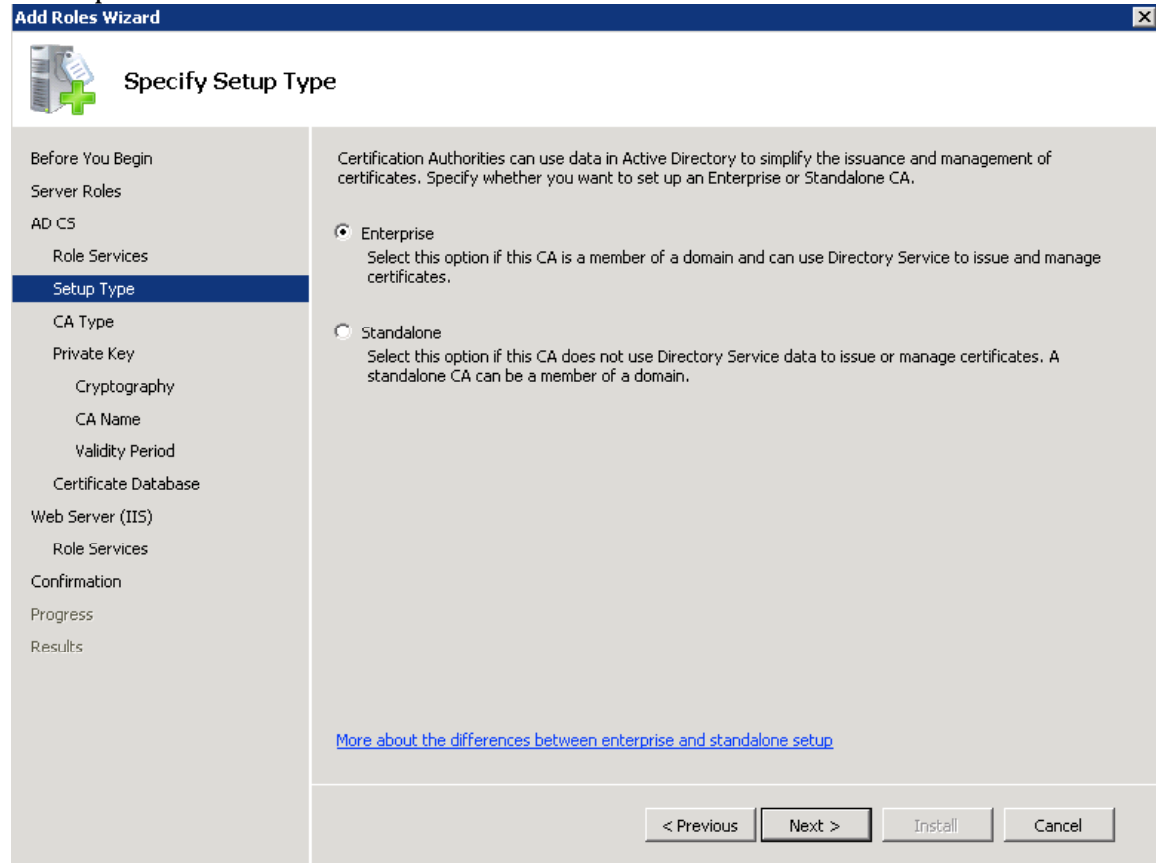
- ☒ **Web Server (IIS)**
 - ☒ Web Server
 - ☒ Management Tools
- ☒ **Windows Process Activation Service**
 - ☒ Process Model
 - ☒ Configuration APIs

Description:
[Web Server \(IIS\)](#) provides a reliable, manageable, and scalable Web application infrastructure.

Add Required Role Services **Cancel**

< Previous **Next >** **Install** **Cancel**

When prompted for which type of Certificate Authority to install, choose “Enterprise”.



The screenshot shows the 'Add Roles Wizard' window, specifically the 'Specify Setup Type' step. The window has a title bar with 'Add Roles Wizard' and a close button. Below the title bar is a navigation pane on the left with the following items: 'Before You Begin', 'Server Roles', 'AD CS', 'Role Services', 'Setup Type' (highlighted), 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Web Server (IIS)', 'Role Services', 'Confirmation', 'Progress', and 'Results'. The main content area is titled 'Specify Setup Type' and contains a green plus icon. Below the icon, there is a list of steps: 'Before You Begin', 'Server Roles', 'AD CS', 'Role Services', 'Setup Type' (highlighted), 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Web Server (IIS)', 'Role Services', 'Confirmation', 'Progress', and 'Results'. The main content area contains the following text: 'Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.' Below this text are two radio button options: 'Enterprise' (selected) and 'Standalone'. The 'Enterprise' option has a description: 'Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.' The 'Standalone' option has a description: 'Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.' At the bottom of the main content area is a link: 'More about the differences between enterprise and standalone setup'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Add Roles Wizard

Specify Setup Type

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Web Server (IIS)
Role Services
Confirmation
Progress
Results

Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

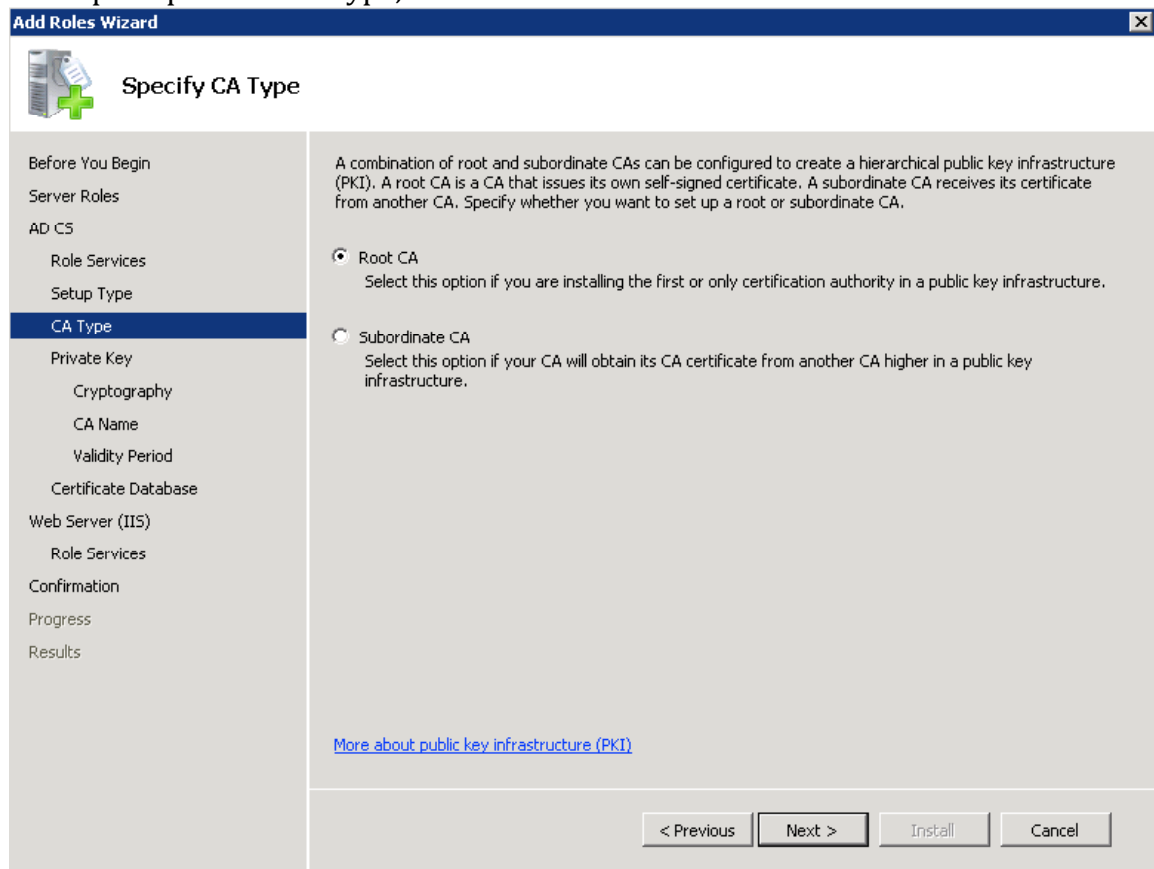
☒ Enterprise
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.

☐ Standalone
Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.

[More about the differences between enterprise and standalone setup](#)

< Previous Next > Install Cancel

When prompted for CA Type, select “Root CA” and click “Next”.



The image shows a screenshot of the "Add Roles Wizard" window, specifically the "Specify CA Type" step. The window has a title bar with the text "Add Roles Wizard" and a close button. Below the title bar is a navigation pane on the left with a tree view containing the following items: "Before You Begin", "Server Roles", "AD CS", "Role Services", "Setup Type", "CA Type" (which is highlighted with a blue background), "Private Key", "Cryptography", "CA Name", "Validity Period", "Certificate Database", "Web Server (IIS)", "Role Services", "Confirmation", "Progress", and "Results". The main content area on the right is titled "Specify CA Type" and contains a paragraph explaining that a combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). It defines a root CA as one that issues its own self-signed certificate and a subordinate CA as one that receives its certificate from another CA. Below this text are two radio button options: "Root CA" (which is selected) and "Subordinate CA". Each option has a descriptive sentence below it. At the bottom of the main content area is a blue hyperlink that reads "More about public key infrastructure (PKI)". At the very bottom of the window are four buttons: "< Previous", "Next >", "Install", and "Cancel".

Add Roles Wizard

Specify CA Type

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Web Server (IIS)
Role Services
Confirmation
Progress
Results

A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

☒ Root CA
Select this option if you are installing the first or only certification authority in a public key infrastructure.

☐ Subordinate CA
Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.

[More about public key infrastructure \(PKI\)](#)

< Previous Next > Install Cancel

When prompted to Set Up Private Key select “Create a new private key” and click “Next”.

The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard' and a close button. The main title is 'Set Up Private Key' next to a green plus icon. On the left is a navigation pane with the following items: 'Before You Begin', 'Server Roles', 'AD CS', 'Role Services', 'Setup Type', 'CA Type', 'Private Key' (highlighted), 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Web Server (IIS)', 'Role Services', 'Confirmation', 'Progress', and 'Results'. The main area contains the text: 'To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.' Below this are four radio button options: 1. 'Create a new private key' (selected), with subtext: 'Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.' 2. 'Use existing private key', with subtext: 'Use this option to ensure continuity with previously issued certificates when reinstalling a CA.' 3. 'Select a certificate and use its associated private key', with subtext: '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.' 4. 'Select an existing private key on this computer', with subtext: 'Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.' At the bottom left of the main area is a blue hyperlink: 'More about public and private keys'. At the bottom right are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Add Roles Wizard

Set Up Private Key

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Web Server (IIS)
Role Services
Confirmation
Progress
Results

To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.

- ☒ **Create a new private key**
Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.
- ☐ **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.

[More about public and private keys](#)

< Previous **Next >** Install Cancel

When prompted to Configure Cryptography for CA, accept the defaults and click “Next” for the rest of the conformation screens.

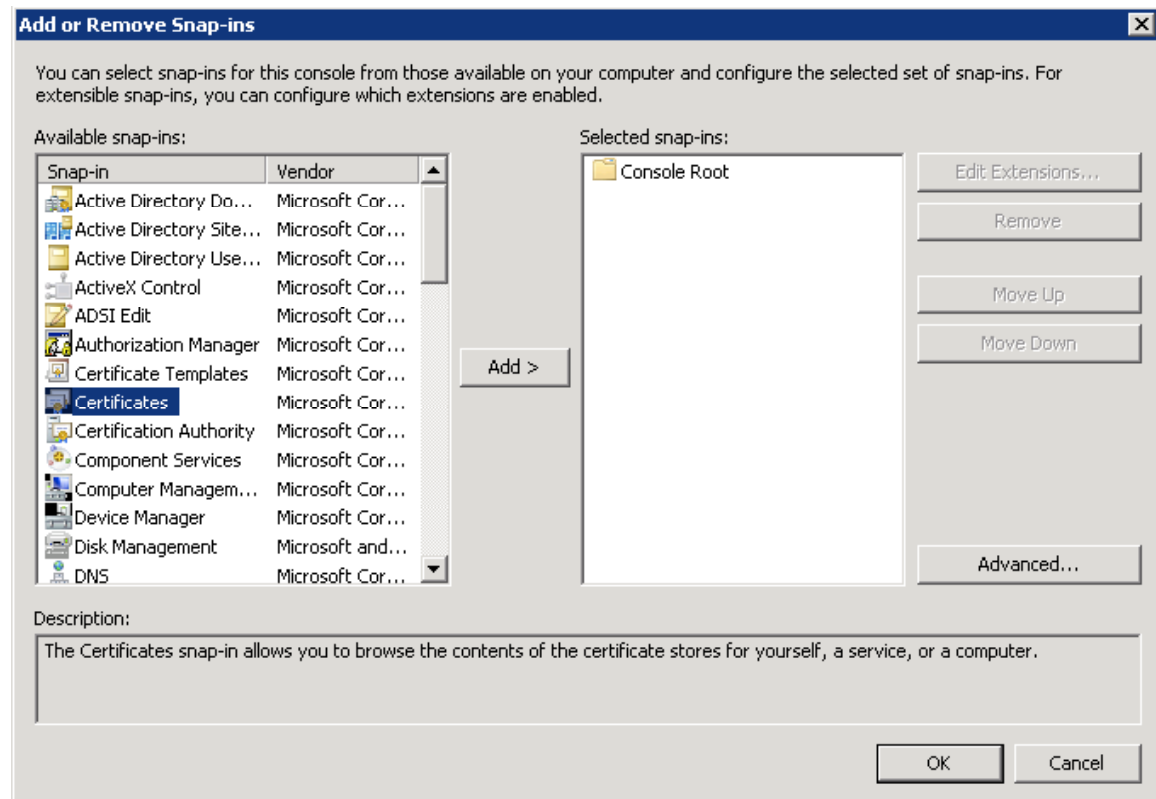
The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard'. The main window is titled 'Configure Cryptography for CA'. On the left is a navigation pane with the following items: 'Before You Begin', 'Server Roles', 'AD CS', 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography' (highlighted with a blue bar), 'CA Name', 'Validity Period', 'Certificate Database', 'Web Server (IIS)', 'Role Services', 'Confirmation', 'Progress', and 'Results'. The main area contains the following text: 'To create a new private key, you must first select a [cryptographic service provider](#), [hash algorithm](#), and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.' Below this text are two dropdown menus: 'Select a cryptographic service provider (CSP):' with 'RSA#Microsoft Software Key Storage Provider' selected, and 'Key character length:' with '2048' selected. Below these is another dropdown menu: 'Select the hash algorithm for signing certificates issued by this CA:' with 'sha1' selected. Below the dropdowns is a checkbox labeled 'Use strong private key protection features provided by the CSP (this may require administrator interaction every time the private key is accessed by the CA)'. At the bottom of the main area is a link: '[More about cryptographic options for a CA](#)'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Request Certificates (optional)

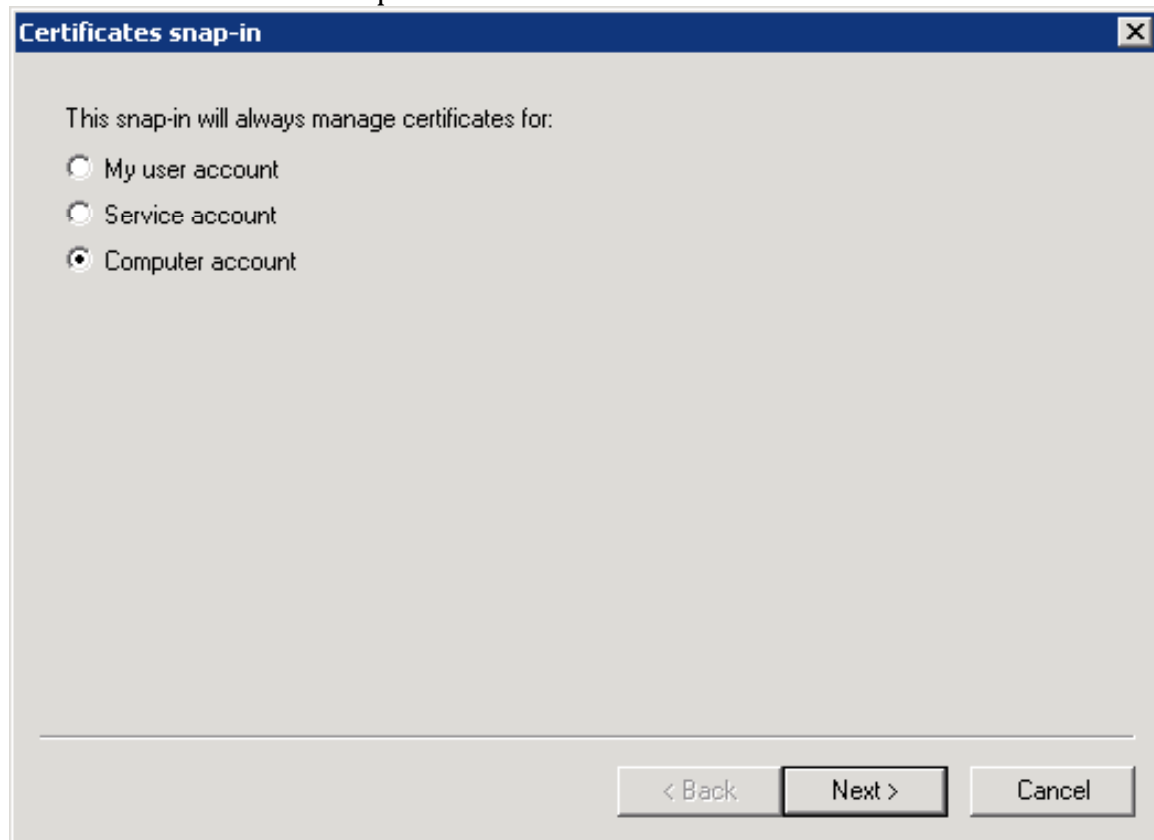
Now that we have our Certificate Authority (CA) up and running we may want to request a certificate for our Authentication Server.

We'll create a Microsoft Management Console (MMC) that will allow us to request and install the certificate for our server. Press the “Start” button and enter “MMC” in the command field to open the MMC. Next we'll add the Certificate (For Local Computer) snap-in by clicking “File” and choosing “Add/Remove Snap-in”. Select

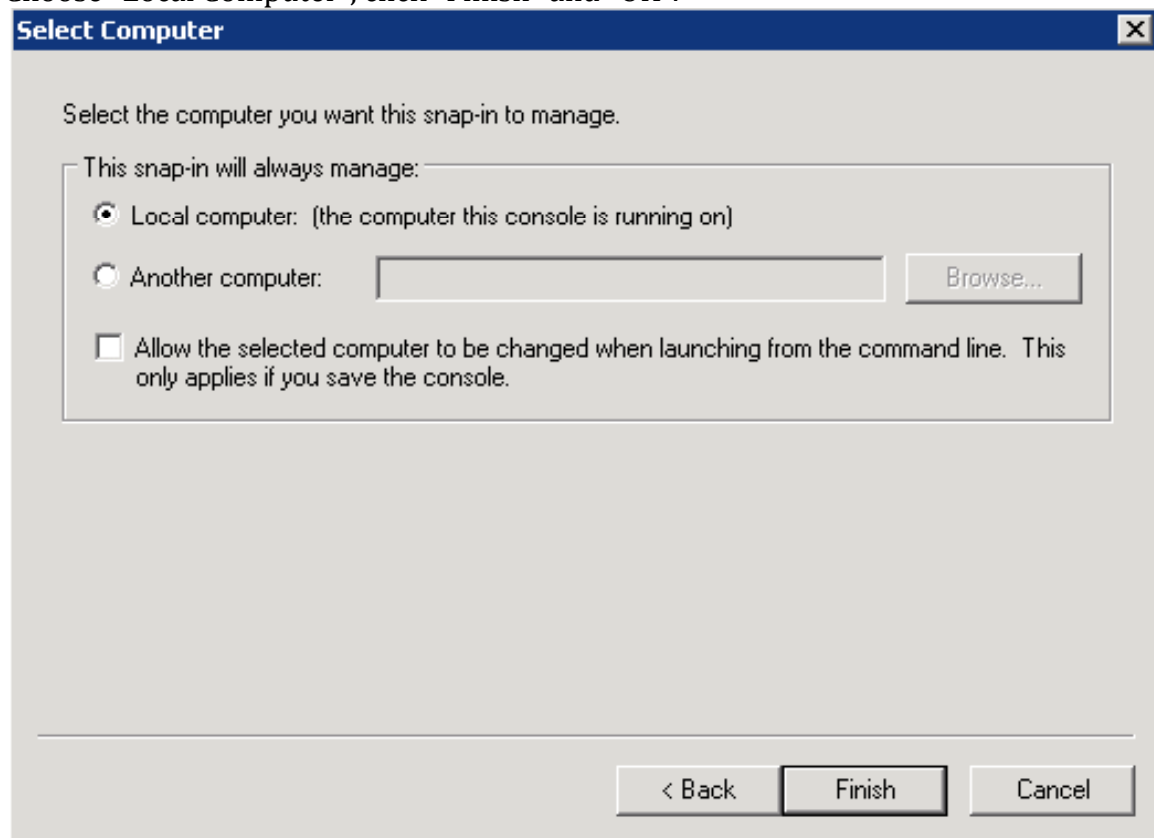
“Certificates” and click “Add”.



Now be sure to select "Computer Account" and click "Next".

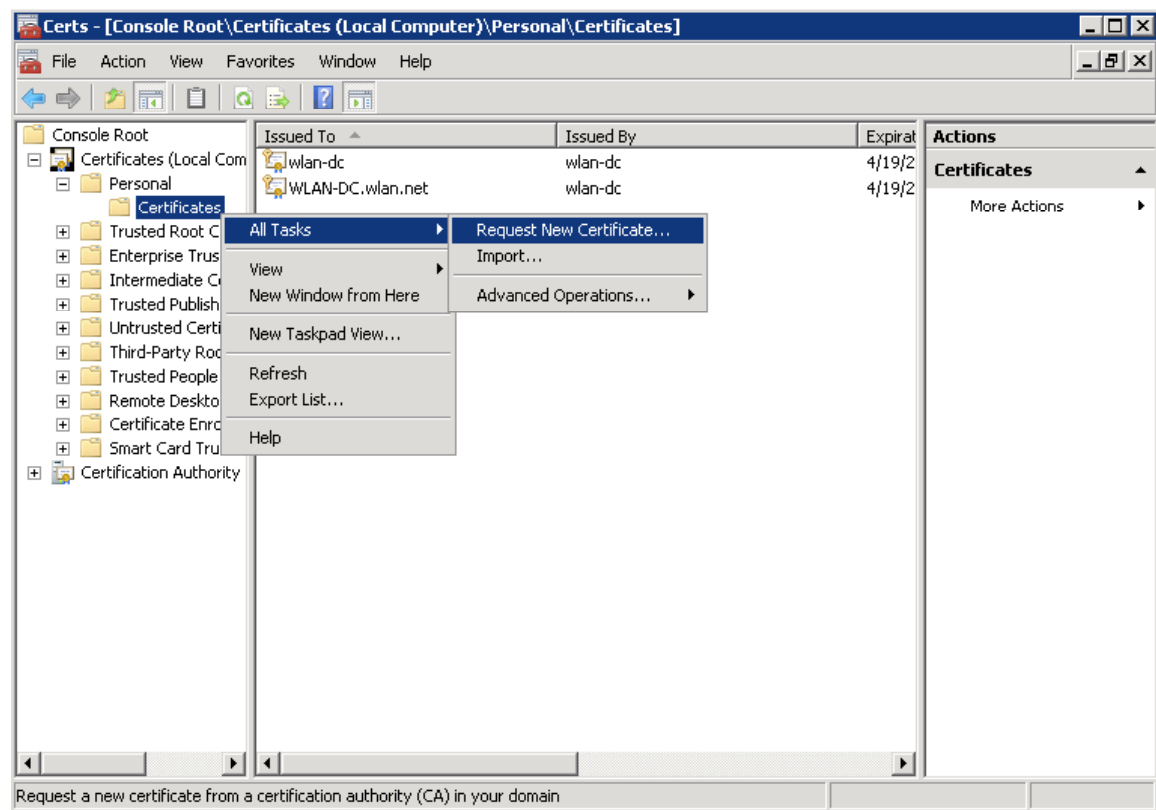


Choose “Local Computer”, click “Finish” and “OK”.

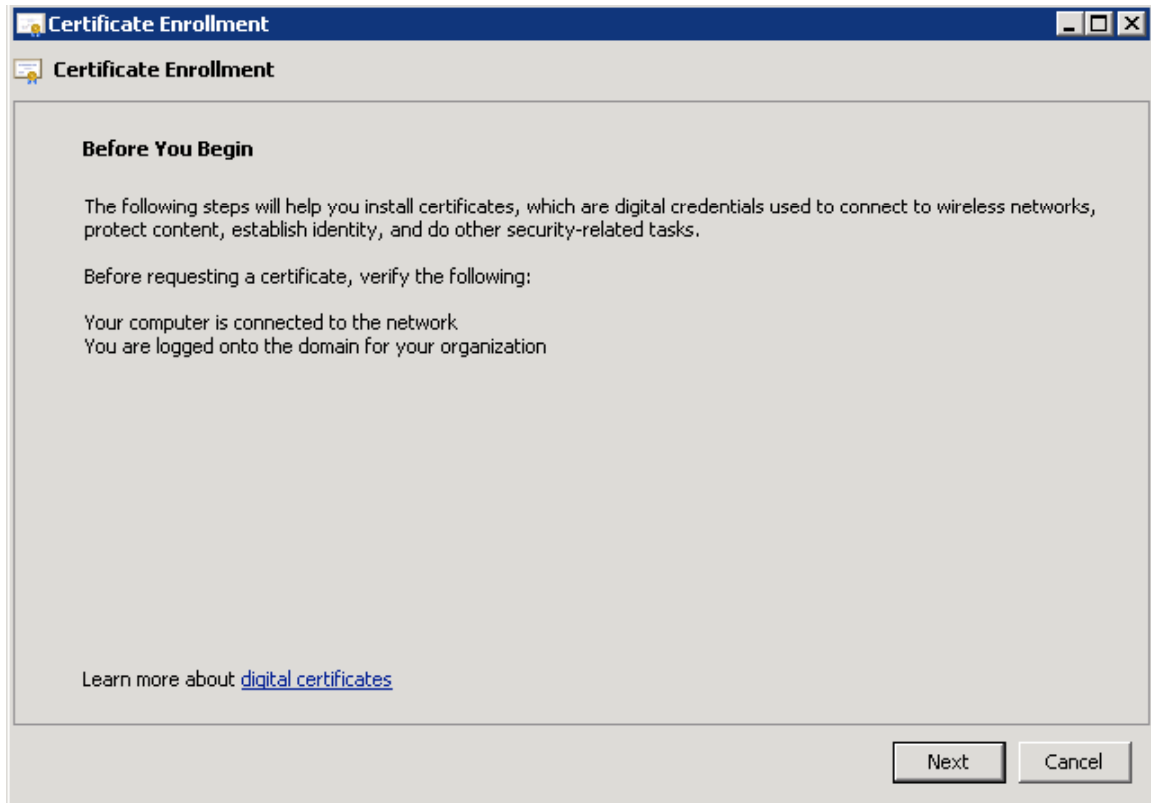


TIP: While you’re here you might as well add the “Certificate Authority” snap-in and save this MMC to your desktop because you’ll need it again in the future.

To request a certificate for your server (if you don’t want to use the default certificate) expand “Certificates (Local Computer Account)”, “Personal”, and right-click “Certificates” and select “All Tasks”, “Request New Certificate...”



Click through the Enrollment screens choosing the settings you desire for your certificate.



Installing Network Policy and Access Services

In Windows 2008 Server you can no longer just install the Internet Authentication Service (IAS) and have RADIUS functionality. You must now install Network Policy and Access Services, which now include everything from earlier versions of Windows server such as RRAS/IAS/etc,... but now includes NAP (think NAC for Windows). We will be installing and configuring just enough to enable PEAP and RADIUS functionality with our Aruba controller. So once again head to the Server Manager and "Add a Role" selecting "Network Policy and Access Services" and click through the confirmation screen.

Add Roles Wizard

 **Select Server Roles**

Before You Begin

Server Roles

Network Policy and Access Services

Role Services

Confirmation

Progress

Results

Select one or more roles to install on this server.

Roles:

- ☒ Active Directory Certificate Services (Installed)
- ☒ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☒ DNS Server (Installed)
- ☐ Fax Server
- ☐ File Services
- ☒ **Network Policy and Access Services**
- ☐ Print Services
- ☐ Terminal Services
- ☐ UDDI Services
- ☒ Web Server (IIS) (Installed)
- ☐ Windows Deployment Services

Description:

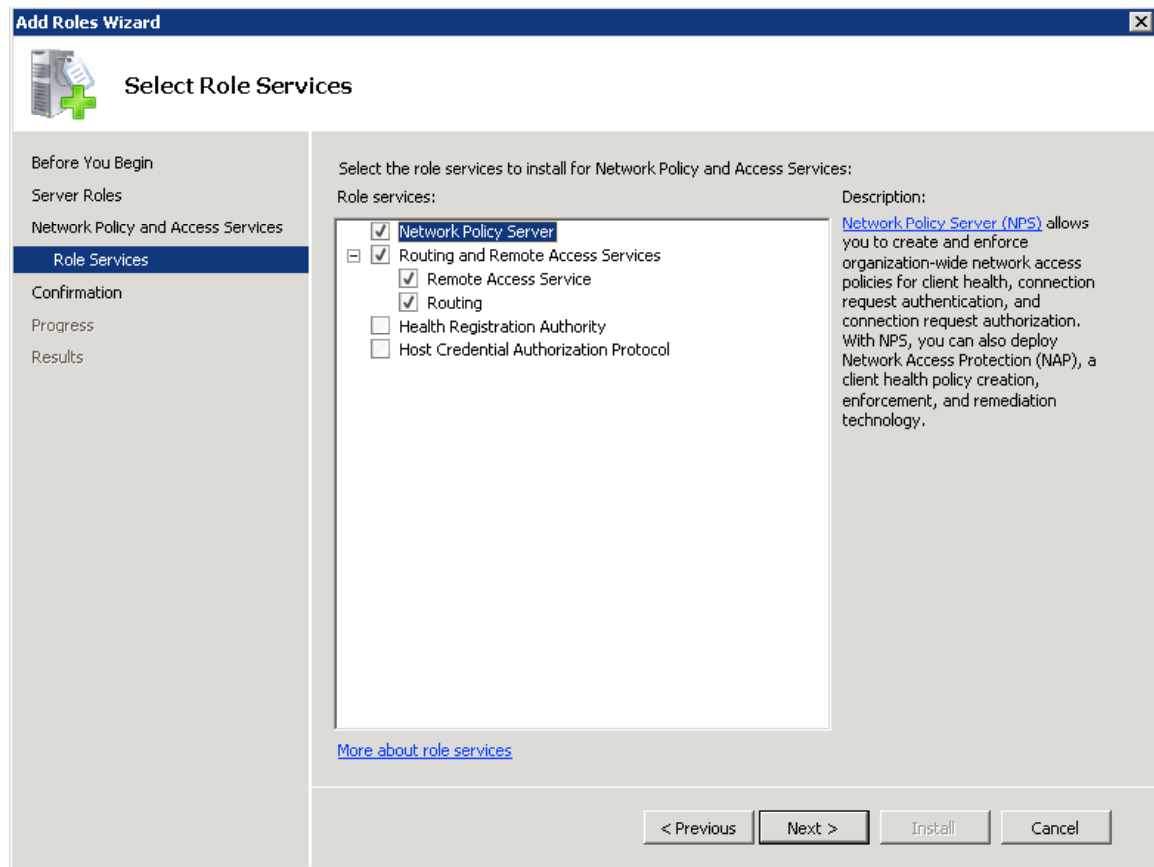
[Network Policy and Access Services](#) provides Network Policy Server (NPS), Routing and Remote Access, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.

[More about server roles](#)

< Previous Next > Install Cancel

Select “Network Policy Server”, “Routing and Remote Access Services”, “Remote Access Service” and “Routing”. Click “Next”, click through the confirmation screen

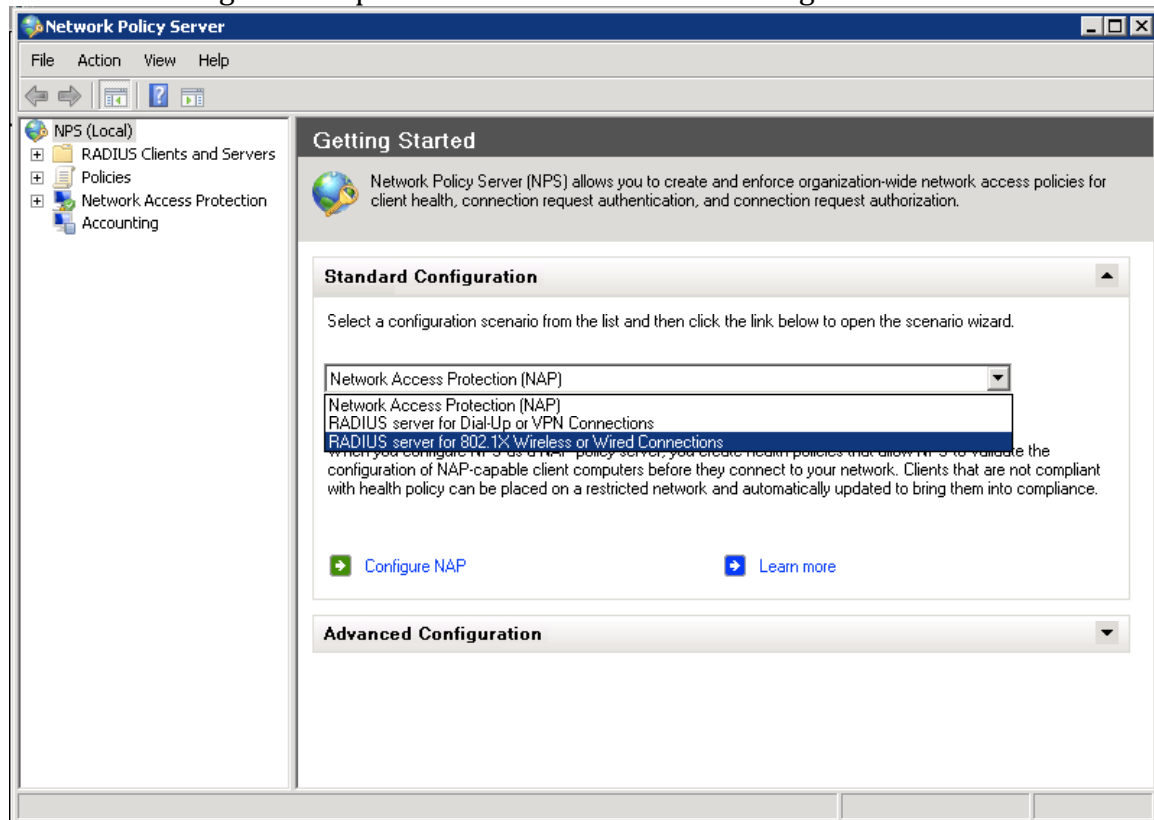
and click “Install”.



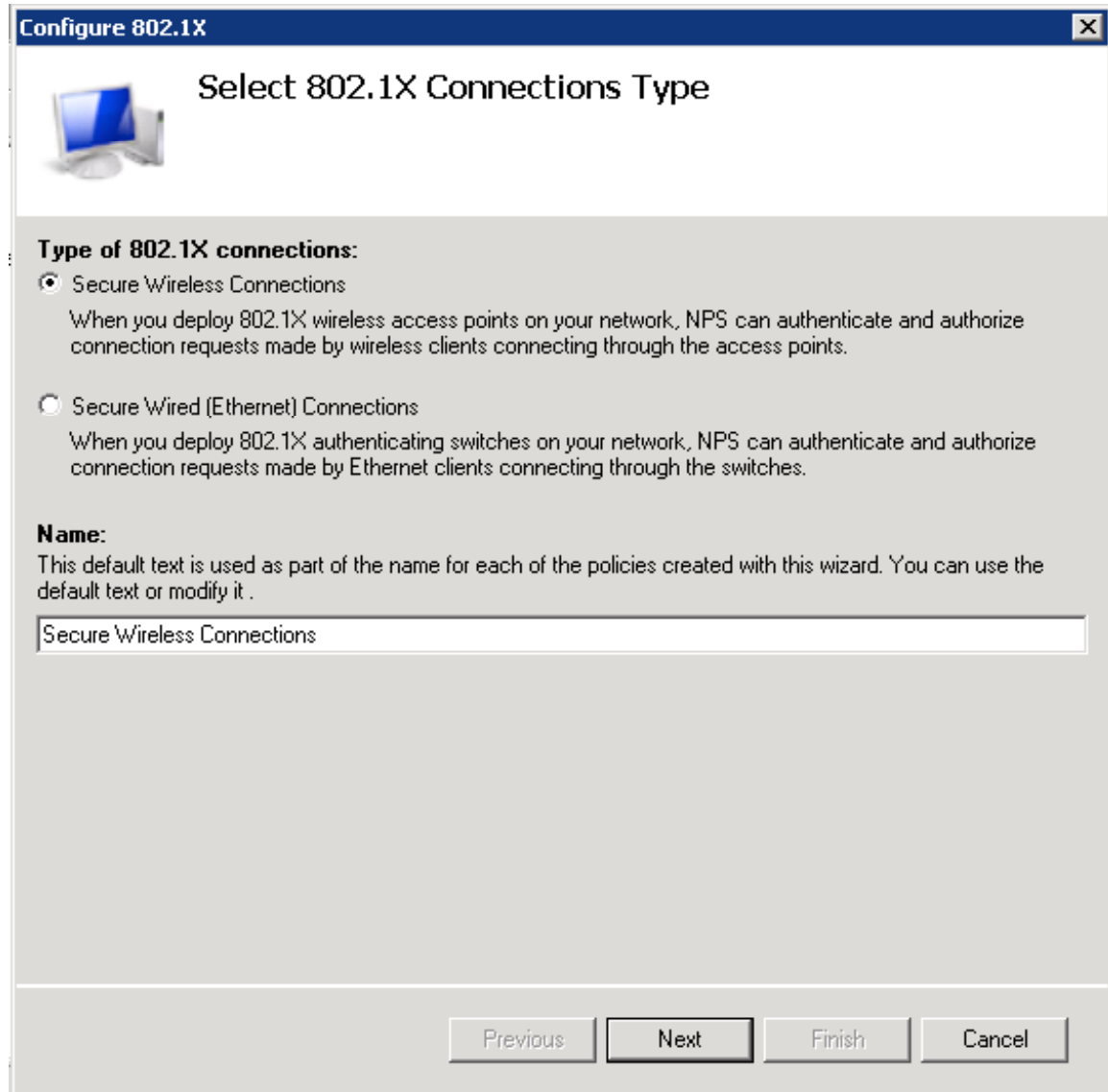
Installation will take a couple of minutes and present you with an install summery. Just click “Close”.

Now that NPS is installed, press the “Start” button and enter “nps.msc” in the command field. The NPS MMC should open up allowing you to select the “RADIUS server for 802.1X Wireless or Wired Connections” Installation Wizard from the

“Standard Configuration” pull-down menu and click “Configure 802.1X”.



From the “Select 802.1X Connections Type” page, select “Secure Wireless Connections” and click “Next”.



The screenshot shows a Windows-style dialog box titled "Configure 802.1X". The main heading is "Select 802.1X Connections Type". On the left, there is a small icon of a computer monitor. The content area has a light gray background and contains the following elements:

- 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 .
- A text input field containing the text "Secure Wireless Connections".

At the bottom of the dialog, there are four buttons: "Previous", "Next", "Finish", and "Cancel". The "Next" button is highlighted with a darker border.

From the “Specify 802.1X Switches” screen click “Add...” and enter the settings for your Aruba controller and press “OK”.

The screenshot shows a Windows-style dialog box titled "Configure 802.1X" with a sub-dialog titled "Specify 802.1X Switches". The sub-dialog has a title bar with a close button (X). Inside, there's a computer icon and the text "Specify 802.1X Switches" and "Please specify 802.1X switches or Wireless Access Points (RADIUS Clients)". Below this, a paragraph explains that RADIUS clients are network access servers, not client computers. It then says "To specify a RADIUS client, click Add." On the right side of the sub-dialog are three buttons: "Add...", "Edit...", and "Remove". The "Add..." button is highlighted. Overlaid on top of the sub-dialog is another dialog box titled "New RADIUS Client" with its own title bar and close button. This dialog has two sections. The first section, "Name and Address", contains a "Friendly name:" field with "Aruba-Master" and an "Address (IP or DNS):" field with "10.1.0.250", followed by a "Verify..." button. The second section, "Shared Secret", contains instructions on how to manually type or generate a shared secret. It has two radio buttons: "Manual" (selected) and "Generate". Below these are two text fields for "Shared secret:" and "Confirm shared secret:", both filled with dots. At the bottom of the "New RADIUS Client" dialog are "OK" and "Cancel" buttons. At the bottom of the "Specify 802.1X Switches" dialog is a "Cancel" button.

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.

New RADIUS Client

Name and Address

Friendly name:
Aruba-Master

Address (IP or DNS):
10.1.0.250 Verify...

Shared Secret

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

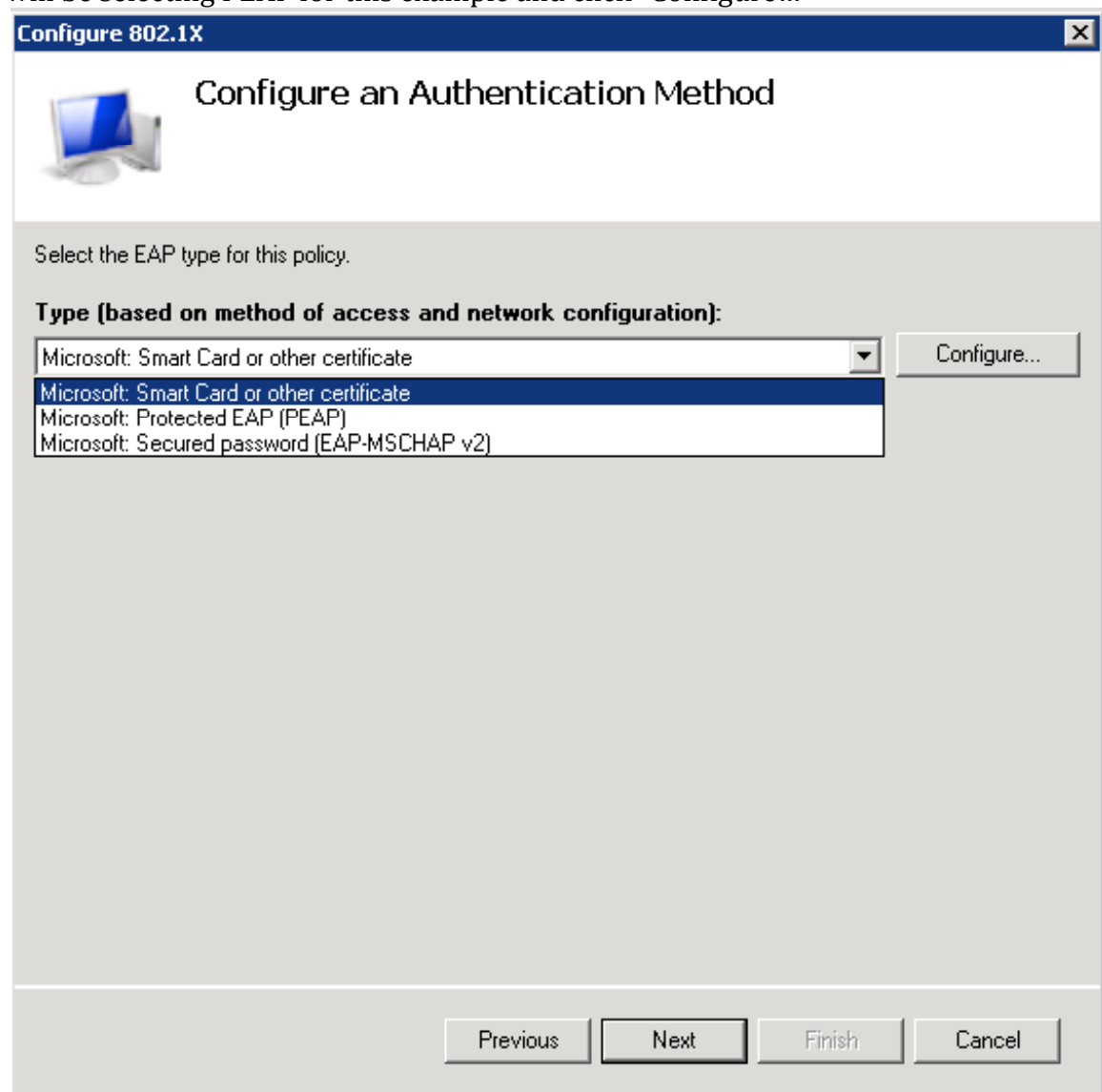
Shared secret:
.....

Confirm shared secret:
.....

OK Cancel Cancel

For the “Configure an Authentication Method” screen select “Microsoft Smart Card or other certificate” for EAP-TLS or “Microsoft Protected EAP (PEAP)” for PEAP. I

will be selecting PEAP for this example and click "Configure..."



Select the appropriate certificate to use for this server. In this case we'll use the "WLAN-DC.wlan.net" certificate and click "OK".

Edit Protected EAP Properties

Select the certificate the server should use to prove its identity to the client. A certificate that is configured for Protected EAP in Connection Request Policy will override this certificate.

Certificate issued: WLAN-DC.wlan.net

Friendly name:

Issuer: wlan-dc

Expiration date: 4/19/2009 8:44:55 AM

☒ Enable Fast Reconnect

☐ Disconnect Clients without Cryptobinding

Eap Types

Secured password (EAP-MSCHAP v2)

Move Up

Move Down

Add Edit Remove OK Cancel

For the "Specify User Groups" screen select the users and/or groups you would like to allow wireless access. For this example I am allowing all of my domain users by selecting the "Domain Users" group. If I want to enforce Machine Authentication I need to add the "Domain Computers" group as well as checking the "Enforce Machine Auth" option in the dot1x policy on my Aruba controller. Click "Next" to continue.

Note: Groups listed here are considered as an OR statement.



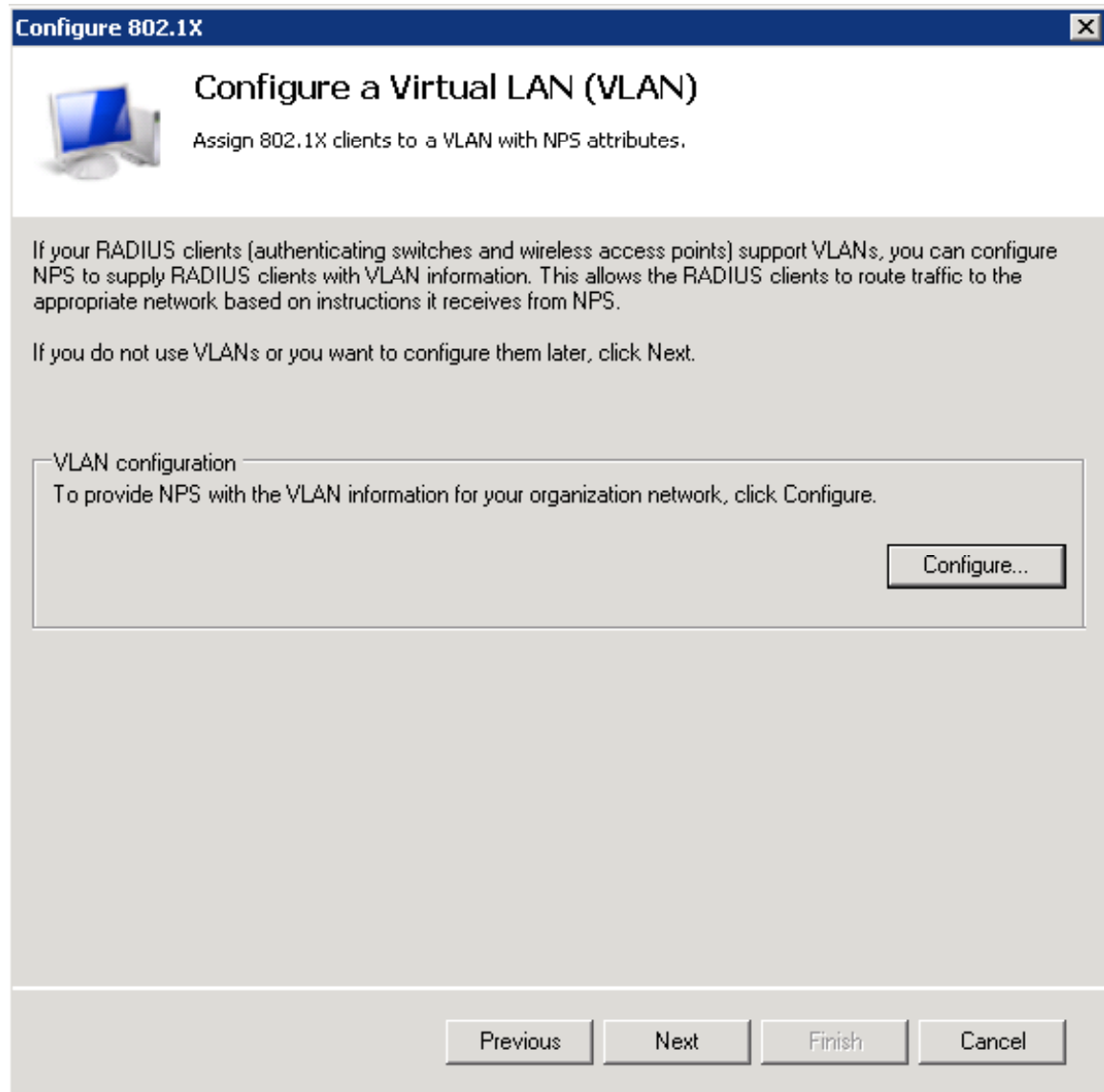
Specify User Groups

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	
WLAN\Domain Users	Add... Remove
WLAN\Domain Computers	

For the next screen you can click “Next” and “Finish” or click “Configure...” to add RADIUS attributes for Server Derivation rules.



The screenshot shows a Windows-style dialog box titled "Configure 802.1X". Inside, there's a section titled "Configure a Virtual LAN (VLAN)" with a sub-header "Assign 802.1X clients to a VLAN with NPS attributes." Below this, there's explanatory text about RADIUS clients and VLANs. A "VLAN configuration" box contains the instruction "To provide NPS with the VLAN information for your organization network, click Configure." and a "Configure..." button. At the bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

Configure 802.1X

Configure a Virtual LAN (VLAN)

Assign 802.1X clients to a VLAN with NPS attributes.

If your RADIUS clients (authenticating switches and wireless access points) support VLANs, you can configure NPS to supply RADIUS clients with VLAN information. This allows the RADIUS clients to route traffic to the appropriate network based on instructions it receives from NPS.

If you do not use VLANs or you want to configure them later, click Next.

VLAN configuration
To provide NPS with the VLAN information for your organization network, click Configure.

Configure...

Previous Next Finish Cancel

For example, you may want to map the “Domain Users” to the “employee_role” on your Aruba controller. You could do that here with the “Filter-Id” attribute.

Virtual LAN (VLAN) Configuration

RADIUS standard attributes | Vendor Specific attributes

To send VLAN properties 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	employee_role
Tunnel-Type	<not configured>
Tunnel-Medium-Type	<not configured>
Tunnel-Pvt-Group-ID	<not configured>
Tunnel-Assignment-ID	<not configured>

Description:
Specifies the name of filter list for the user requesting authentication.

Edit...

OK Cancel

Note: There seems to be a bug in Windows if you mess with these attributes too much the "Filter-Id" attribute vanishes. If this happens cancel out of the wizard and start over.

Press "Next" and "Finish" to complete the wizard. This should now allow you to authenticate users against your Windows 2008 Server. To test your configuration, ssh to your Aruba controller and configure it to use the new RADIUS server.

```
(MC800) >en
```

```
Password:*****
```

```
(MC800) #configure terminal
```

Enter Configuration commands, one per line. End with CNTL/Z

(MC800) (config) #aaa authentication-server radius nps

(MC800) (RADIUS Server "nps") #host 10.1.0.236

(MC800) (RADIUS Server "nps") #enable

(MC800) (RADIUS Server "nps") #key p@ssw0rd

(MC800) (RADIUS Server "nps") #nas-identifier Aruba-Master

(MC800) (RADIUS Server "nps") #nas-ip 10.1.0.250

Now test to see if everything is working properly.

(MC800) #aaa test-server mschapv2 nps tobias qwerty12!@

Authentication successful