Windows 2008 R2 NPS (RADIUS) Server for Wi-Fi Protected Access Enterprise

- Active Directory Domain Service Installation
- Dcpromo procedure
- Installing the Active Directory Certificate Services
- NPS (Network Policy and Access Services) Installation
- Creating User account for authenticating via NPS(RADIUS)
- Creating NPS Rules
- WAP/WPA2-enterprise configuration on Access Point/Wireless client
- 802.1x Authentication configuration on Access Point/Wireless client

| | Activate Windows | Product ID: | Not activated | |
|----------------|--|--|---|---|
| | Set time <u>z</u> one | Time Zone: | (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi | |
| | Configure networking | Local Area Connection: | 192.168.0.201, IPv6 enabled | |
| | Novide computer name and domain | Full Computer Name: Domain: | aaron-win2k8R2.aaron2k8.com aaron2k8.com | |
| 2 | Update This Server | | Updating your Windows server | |
| | Enable automatic updating and feedback | Updates: Feedback: | Not configured Windows Error Reporting off Not participating in Customer Experience Improvement Program | |
| | Pownload and install updates | Checked for Updates: Installed Updates: | Never Never | |
| 3 | Customize This Server | | Customizing your server | |
| | Add roles | Roles: | DNS Server, Active Directory Domain Services | |
| | Add features | Features: | Group Policy Management, Remote Server Administration Tools, .NET Framework 3.5.1 Features | |
| | Enable Remote Des <u>k</u> top | Remote Desktop: | Disabled | |
| | Configure Windows Firewall | Firewall: | Domain: On | |
| Prir | nt, e-mail, or <u>s</u> ave this information | | | - |
| | Do not show this window at logon | | Qose | |
| A Start | y 🔁 📜 🚺 | | | |

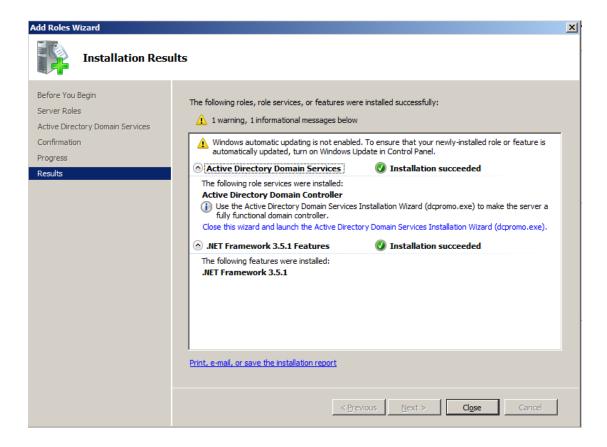
| Add Roles Wizard | X |
|---|---|
| Before You Begin | |
| Before You Begin Server Roles Confirmation Progress Results | <text><text><list-item><list-item><text></text></list-item></list-item></text></text> |
| | |

• Active Directory Domain Service Installation

| Add Roles Wizard | | × |
|---|--|--|
| Selec | ct Server Roles | |
| Before You Begin Server Roles Confirmation Progress Results | Select one or more roles to install on this server. Roles: Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services | Description: <u>Active Directory Domain Services (AD</u> <u>DS</u>) stores information about objects on the network and makes this information available to users and |
| | .NET Framework 3.5.1 the power of with new te applications interfaces, identity info | ures are also installed. |
| | Add F (i) Why are these features required? | Required Features Cancel |
| | < Previous Nex | t > Install Cancel |

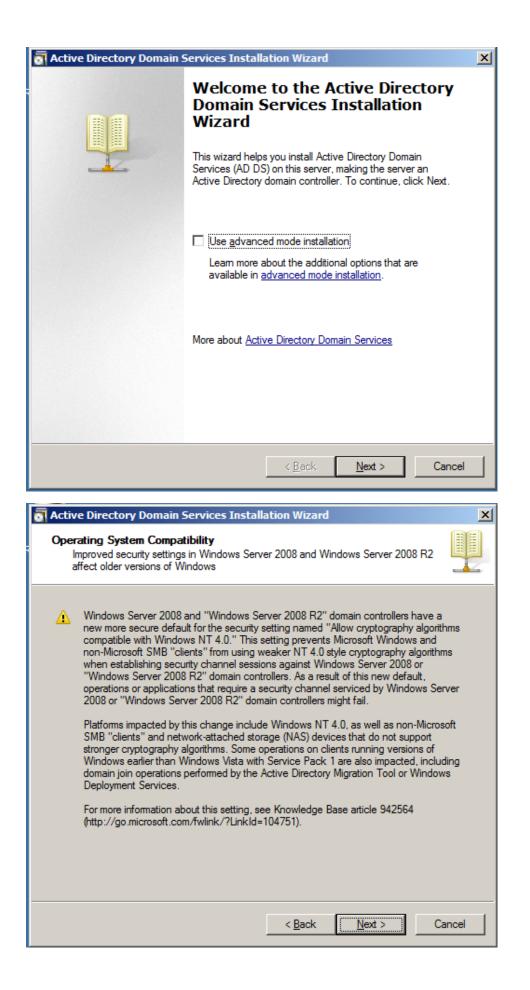
| Add Roles Wizard | | × |
|---|---|---|
| Active Directory | Domain Services | |
| Before You Begin Server Roles Active Directory Domain Services Confirmation Progress Results | Introduction to Active Directory Domain Services Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy. Things to Note To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain. AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this server. After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller. Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by Directory Service. Additional Information Overview of AD DS Installing AD DS Common Configurations for AD DS | F |
| | < Previous Next > Install Cancel | |

| Add Roles Wizard | | × |
|---|--|---|
| Confirm Installat | ion Selections | |
| Before You Begin Server Roles Active Directory Domain Services Confirmation Progress Results | To install the following roles, role services, or features, click Install. | - |
| | Print, e-mail, or save this information | |
| | < Previous Next > Install Cancel | |
| Add Roles Wizard | | |
| Installation Prog | ress | |
| Before You Begin | The following roles, role services, or features are being installed: | |
| Server Roles | Active Directory Domain Services | |
| Active Directory Domain Services Confirmation | .NET Framework 3.5.1 Features | |
| Progress Results | Installing | |
| | < Previous Next > Install Cancel | |



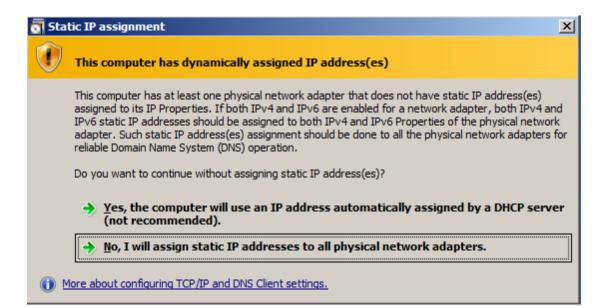
• Dcpromo procedure

| | | aninnna innin | | | puice |
|--------------|---------|---------------|---|-----------|-----------|
| Programs (1) | | | | | up: |
| | | | | | |
| 👼 dcprom | 0 | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | for |
| | | | | | Upo |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | Desl |
| | | | | | |
| 0.0 | | | | | |
| See more | results | | | | |
| ₽ See more | | | | | |
| dcpromo | | | | Log off 🕨 | |
| 1 . | | | _ | | |
| Start | | | | | |
| Start : | | | | | |



| Acti | ve Directory Domain Services Installation Wizard |
|------|---|
| | Pose a Deployment Configuration You can create a domain controller for an existing forest or for a new forest. |
| | O Existing forest |
| | $igcap_{	riangledd}$ $ ightarrow$ domain controller to an existing domain |
| | C <u>C</u> reate 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 |
| | |
| | |
| | |
| | |
| | < <u>B</u> ack <u>N</u> ext > Cancel |
| -, | |
| Nan | we Directory Domain Services Installation Wizard X ne 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. |
| | EQDN of the forest root domain: |
| | tsd.test.com |
| | Example: corp.contoso.com |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | < Back Next > Cancel |

| | Functional Level e forest functional level. | | | |
|--|---|---|---|--------|
| | nctional level: | | | |
| | s Server 2008 R2 | | | |
| <u>D</u> etails: | | | | |
| are availa additiona - Any new | dows Server 2008 R2 forest fund able in the Windows Server 2008 I feature: Recycle Bin, which, when it is deleted objects in their entirety Services is running. domains that are created in this s Server 2008 R2 domain function | 3 forest functional le enabled, provides th while Active Directo forest will operate b | evel, plus the follo ne ability to restore ory Domain | wing |
| Δ | You will be able to add only d Windows Server 2008 R2 or I | | at are running | |
| More abo | ut <u>domain and forest functional l</u> | <u>evels</u> | | |
| | | | | |
| | | < <u>B</u> ack | <u>N</u> ext > | Cancel |
| ve Direc | tory Domain Services Inst | | <u>N</u> ext > | Cancel |
| | tory Domain Services Inst Comain Controller Options | | <u>N</u> ext > | Cancel |
| itional [| | allation Wizard | <u>N</u> ext > | Cancel |
| Select ad | Domain Controller Options | allation Wizard | <u>N</u> ext > | Cancel |
| itional [Select ad | Domain Controller Options Iditional options for this domain c | allation Wizard | <u>N</u> ext > | Cancel |
| Select ad | Domain Controller Options Iditional options for this domain c S server pal catalog | allation Wizard | <u>N</u> ext > | Cancel |
| Select ad | Domain Controller Options Iditional options for this domain c | allation Wizard | <u>N</u> ext > | Cancel |
| Select ad Select ad Select ad Select ad Select Select Select Select Select Select ad Select ad Select ad S | Domain Controller Options Iditional options for this domain of Server Dat catalog Id-only domain controller (RODC) | allation Wizard | | Cancel |
| Select ad Select ad DNS Glot Eea Addition The first cannot | Domain Controller Options Iditional options for this domain of Server bal catalog id-only domain controller (RODC) al information: t domain controller in a forest mu be an RODC. ommend that you install the DNS | allation Wizard ontroller. | og server and | Cance |
| Select ad Select ad DNS Glot Eea Addition The first cannot We rec controll | Domain Controller Options Iditional options for this domain of Server bal catalog id-only domain controller (RODC) al information: t domain controller in a forest mu be an RODC. ommend that you install the DNS | allation Wizard ontroller. | og server and | Cance |



Configuring your server with a static IP address

| Active | Directory Domain Services Installation Wizard | × |
|----------|--|---|
| <u>^</u> | A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "tsd.test.com". Otherwise, no action is required. Do you want to continue? | |
| | <u>Y</u> es | |

Click Yes

| Active Directory Domain Services Installation Wizard | × |
|---|-----------------|
| Location for Database, Log Files, and SYSVOL Specify the folders that will contain the Active Directory domain controlle database, log files, and SYSVOL. | er 📕 |
| For better performance and recoverability, store the database and log file volumes. | es on separate |
| Database folder: | |
| C:\Windows\NTDS | Browse |
| , Log files folder: | |
| C:\Windows\NTDS | Browse |
| , SYSVOL folder: | |
| C:\Windows\SYSVOL | Browse |
| < Back Next > | Cancel |
| | |
| Active Directory Domain Services Installation Wizard | X |
| Directory Services Restore Mode Administrator Password | |
| The Directory Services Restore Mode Administrator account is different Administrator account. | from the domain |
| Assign a password for the Administrator account that will be used when controller is started in Directory Services Restore Mode. We recommend choose a strong password. | |

| Di | irectory Services Restore Mo | ode Admini | strator Passwo | ord | |
|----|--|----------------|---------------------|------------------|--------|
| | The Directory Services Restore Administrator account. Assign a password for the Admin controller is started in Directory choose a strong password. | nistrator acco | ount that will be u | used when this d | lomain |
| | <u>P</u> assword: | ••••• | | | |
| | <u>C</u> onfirm password: | ••••• | | | |
| | More about <u>Directory Services</u> | Restore Mod | e password | | |
| | | | < <u>B</u> ack | <u>N</u> ext > | Cancel |

| | | 100 (cc.) |
|---|--|-----------------------------------|
| mary | | |
| Review your selections: | | |
| Configure this server as the first Active D | Directory domain controller in a new forest. | |
| The new domain name is "tsd.test.com" | . This is also the name of the new forest. | |
| The NetBIOS name of the domain is "TS | SD". | |
| Forest Functional Level: Windows Serve | er 2008 R2 | |
| Domain Functional Level: Windows Serv | ver 2008 R2 | |
| Site: Default-First-Site-Name | | |
| Additional Options: | | |
| | | • |
| o change an option, click Back. To be | gin the operation, click Next. | |
| | | |
| | < <u>B</u> ack <u>N</u> ext > | Cancel |
| re Directory Domain Services Installation | | Cancel |
| nary | | Cancel |
| mary | Wizard | Cancel |
| nary leview your selections: Configure this server as the first Active Directory d | Wizard | Cancel |
| mary Review your selections: Configure this server as the first Active Directory d The new domain name is "tsd.test.com". This is al The NetBIOS name of the domain is "TSD". | Wizard | Cancel |
| mary <u>Review your selections:</u> Configure this server as the first Active Directory d The new domain name is "tsd.test.com". This is al The NetBIOS name of the domain is "TSD". Forest Functional Level: Windows Server 2008 F | Wizard | |
| mary Seview your selections: Configure this server as the first Active Directory d The new domain name is "tsd.test.com". This is al The NetBIOS name of the domain is "TSD". Forest Functional Level: Windows Server 2008 F Domain Functional Level: Windows Server 2008 | Wizard Wizard Mizard Mizard | tion Wizard n Services. This p |
| eview your selections: onfigure this server as the first Active Directory d he new domain name is "tsd.test.com". This is al he NetBIOS name of the domain is "TSD". orest Functional Level: Windows Server 2008 F lomain Functional Level: Windows Server 2008 ite: Default-First-Site-Name | Wizard | tion Wizard n Services. This p |
| nary eview your selections: configure this server as the first Active Directory d he new domain name is "tsd.test.com". This is al he NetBIOS name of the domain is "TSD". orest Functional Level: Windows Server 2008 F Domain Functional Level: Windows Server 2008 ite: Default-First-Site-Name | Wizard | tion Wizard n Services. This p |
| mary <u>Review your selections:</u> Configure this server as the first Active Directory d The new domain name is "tsd.test.com". This is al The NetBIOS name of the domain is "TSD". Forest Functional Level: Windows Server 2008 F | Wizard | tion Wizard n Services. This p |

These settings can be exported to an answer file other unattended operations. More about <u>using an answer file</u>

Ì

Installing Group Policy Management Console...

Reboot on completion

Cancel

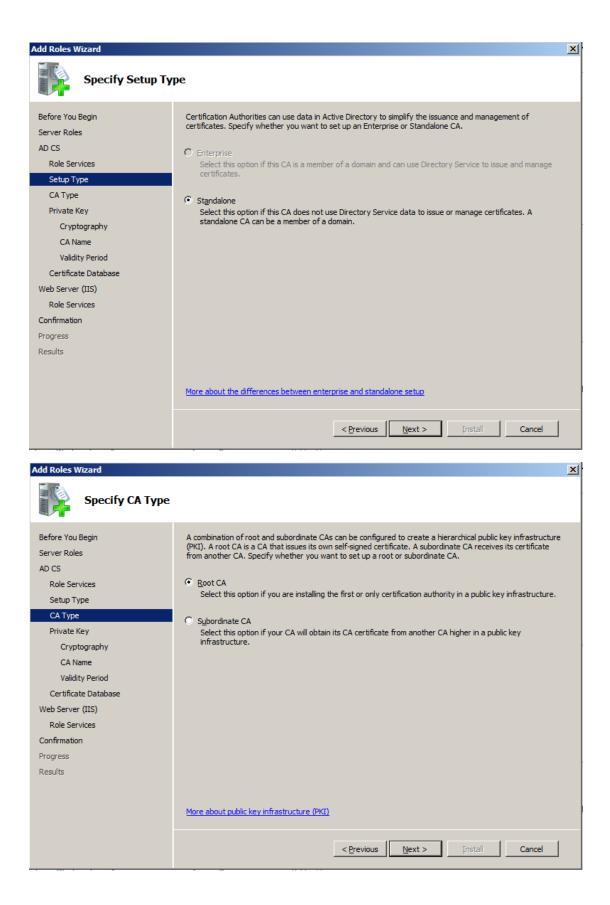
• Installing the Active Directory Certificate Services

| Add Roles Wizard | | 2 | × |
|--|---|---|---|
| Select Server Ro | les | | |
| Select Server Rol 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 one or more roles to install on this server. Roles: Active Directory Certificate Services Active Directory Domain Services (Installed) Active Directory Cederation Services Active Directory Lightweight Directory Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services DHCP Server DHCP Server DHCP Server DHCP Server File Services Hyper-V Network Policy and Access Services Print and Document Services Web Server (IIS) Windows Deployment Services Windows Server Update Services | Description: <u>Active Directory Certificate Services</u> (<u>AD CS</u>) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications. | |
| Add Roles Wizard | More about server roles < | | × |
| Introduction to A | ctive Directory Certificate Services | | |
| Before You Begin Server Roles AD CS Role Services Setup Type CA Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress | Active Directory Certificate Services (AD CS) Active Directory Certificate Services (AD CS) provides the certificate in secure wireless networks, virtual private networks, Internet Protocol Services (NAP), encrypting file system (EFS) and smart card logon. Things to Note Things to Note The name and domain settings of this computer cannot be change been installed. If you want to change the computer name, join a component complete, complete these changes before installing the Computer naming. Additional Information Active Directory Certificate Services Overview Managing a Certification Authority Certification Authority Naming | Security (IPSec), Network Access ed after a certificate authority (CA) has domain, or promote this server to a | |
| Results | | | |

| Add Roles Wizard | | | × |
|---|--|--|---|
| Sel | ect Role Serv | vices | |
| Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptograph | Enr | role services and features require | t Description: <u>Certification Authority (CA)</u> is used to issue and manage certificates. Multiple CAs can be linked to form a |
| CA Name Validity Peric Certificate Data Confirmation Progress Results | install <u>R</u> ole : [[[] F | | Description: <u>Web Server (IIS)</u> provides a reliable, manageable, and scalable Web application infrastructure. |
| | Why are the | ese role services and features required? More about role services | Add Required Role Services Cancel |

Continue by adding required role services

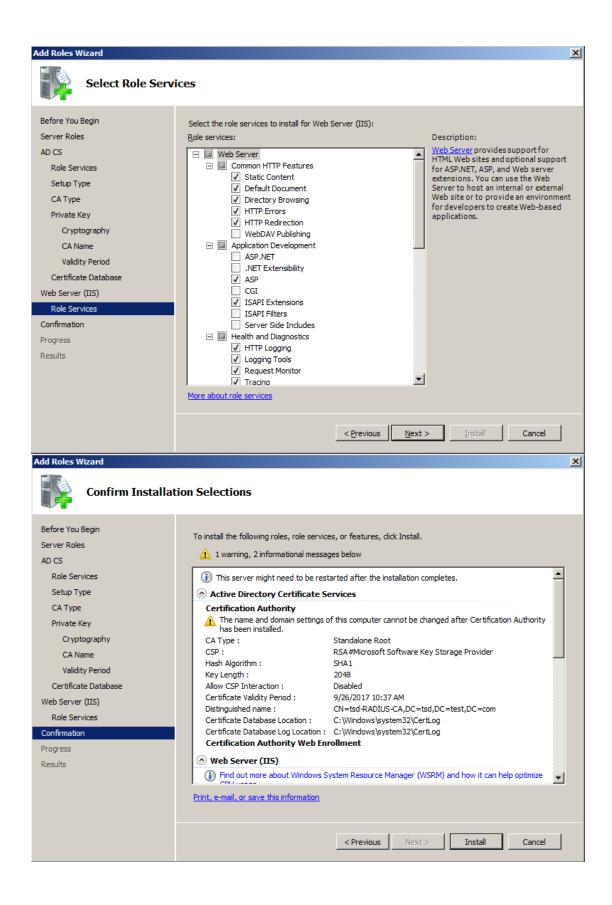
| Add Roles Wizard | | × |
|--|---|---|
| Select Role Servic | es | |
| Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results | Select the role services to install for Active Directory Certificate Service Certification Authority Certification Authority Web Enrolment Online Responder Network Device Enrolment Service Certificate Enrolment Web Service Certificate Enrolment Policy Web Service More about role services < | Description: Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates. |



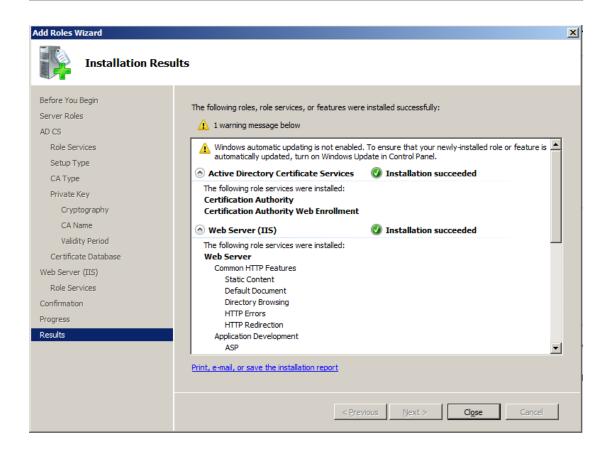
| | <u>×</u> |
|---|---|
| Set Up Private Ke | ŷ |
| Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key | To generate and issue certificates to dients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one. Create a new 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 this option to ensure continuity with previously issued certificates when reinstalling a CA. |
| Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results | Selegt 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 gyisting 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 Install Cancel |
| | |
| Add Roles Wizard | x |
| Configure Crypto | graphy for CA |
| Configure Crypto Before You Begin Server Roles AD CS Role Services Setup Type CA Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results | graphy for CA To reacte a new private key, you must first select a cryptographic service provider, hash algorithm, and give for key length will result in stronger security, but increase the time needed to complete signing service provider (CSP): Ret cryptographic service provider (CSP): Ret wey hash algorithm for signing certificates issued by this CA: Setect the hash algorithm for signing certificates issued by this CA: SHA256 SHA384 SHA512 SHA384 Sha38 |
| 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 | To create a new private key, you must first select a <u>cryptographic service provider</u> , <u>hash algorithm</u> , 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. Select a cryptographic service provider (CSP): RSA #Microsoft Software Key Storage Provider Select the hash algorithm for signing certificates issued by this CA: SHA256 SHA384 SHA512 VA 1 |

| Add Roles Wizard | X |
|----------------------|--|
| Configure CA Nat | me |
| Before You Begin | Type in a common name to identify this CA. This name is added to all certificates issued by the CA. |
| Server Roles | Distinguished name suffix values are automatically generated but can be modified. |
| AD CS | Common name for this CA: |
| Role Services | tsd-RADIUS-CA |
| Setup Type | , Distantial anno a ffur |
| CA Type | Distinguished name suffix: DC=tsd,DC=test,DC=com |
| Private Key | |
| Cryptography | |
| CA Name | Pre <u>v</u> iew of distinguished name: |
| Validity Period | CN=tsd-RADIUS-CA,DC=tsd,DC=test,DC=com |
| Certificate Database | |
| Web Server (IIS) | |
| Role Services | |
| Confirmation | |
| Progress | |
| Results | |
| | |
| | |
| | More about configuring a CA name |
| | < Previous Next > Install Cancel |
| | |
| Add Roles Wizard | X |
| Set Validity Perio | od |
| Before You Begin | A certificate will be issued to this CA to secure communications with other CAs and with clients requesting |
| Server Roles | certificates. The validity period of a CA certificate can be based on a number of factors, including the intended purpose of the CA and security measures that you have taken to secure the CA. |
| AD CS | ישר איז |
| Role Services | Select validity period for the certificate generated for this CA: |
| Setup Type | 5 Years |
| СА Туре | CA expiration Date: 9/26/2017 10:37 AM |
| Private Key | Note that CA will issue certificates valid only until its expiration date. |
| Cryptography | |
| CA Name | |
| Validity Period | |
| Certificate Database | |
| Web Server (IIS) | |
| Role Services | |
| Confirmation | |
| Progress | |
| Results | |
| | |
| | More about setting the certificate validity period |
| | |
| | < Previous Next > Install Cancel |

| Add Roles Wizard | × |
|--|--|
| Configure Certific | cate Database |
| 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 | The certificate database records all certificate requests, issued certificates, and revoked or expired certificates. The database log can be used to monitor management activity for a CA. Certificate database location: Brgwse C:\Windows\system32\CertLog Brgwse Use existing certificate database log location: Certificate database log location: C:\Windows\system32\CertLog Brgwse |
| Add Roles Wizard | <previous next=""> Install Cancel X</previous> |
| 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 | Introduction to Web Server (IIS) Web servers are computers that have specific software that allows them to accept requests from dient computers and extran responses to those requests. Web servers let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 7.0, a unified web platform that integrates IIS 7.0, ASP.NET, and Windows Communication Foundation. IIS 7.0 also features endnece security, simplified diagnostics, and delegated administration. Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server affic, especially when there are multiple roles on this computer. The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression. Deterview of Web Server (IIS) Overview of Available Role Services in IIS 7.0 Using Checklisti Common Administrative Tasks in IIS Overview of WSRM Overview of WSRM |
| | < Previous Next > Install Cancel |



| Add Roles Wizard | |
|----------------------|--|
| Installation Progre | 255 |
| Before You Begin | The following roles, role services, or features are being installed: |
| Server Roles | Active Directory Certificate Services |
| AD CS | Web Server (IIS) |
| Role Services | Remote Server Administration Tools |
| Setup Type | |
| CA Type | |
| Private Key | |
| Cryptography | |
| CA Name | |
| Validity Period | |
| Certificate Database | |
| Web Server (IIS) | |
| Role Services | |
| Confirmation | |
| Progress | |
| Results | |
| | |
| | Tinstalling |
| | < <u>Previous</u> <u>Next</u> > <u>I</u> nstall Cancel |



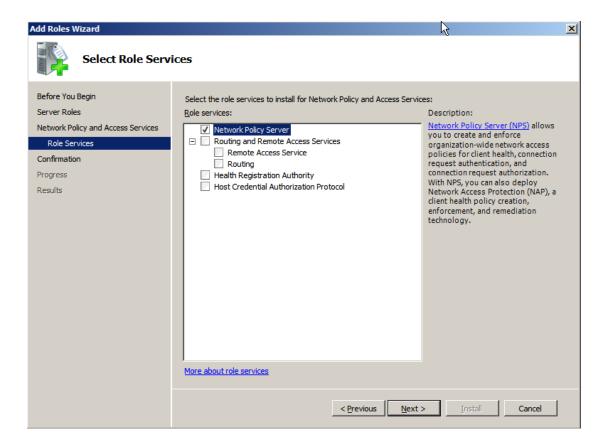
• NPS (Network Policy and Access Services) Installation



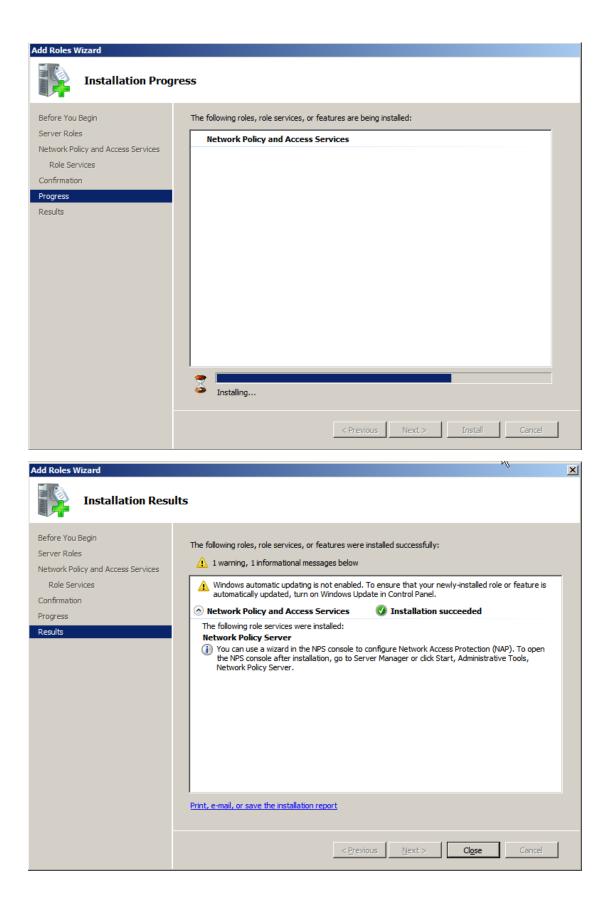
More about server roles

< Previous Next > Install

Cancel



| Add Roles Wizard | | x |
|--|---|---|
| Confirm Installat | ion 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, dick Install. | |
| | Print, e-mail, or save this information | |
| | < Previous Next > Install Cancel | |



| e ci cating est | | | | | |
|---------------------------------------|---------------------------|-----------------------|-------------------|--------------------|-------------------------------|
| 🗢 🔿 🖄 🚾 🛛 🐇 🗈 | 1 🗶 🗐 🧕 🗟 🛛 | 2 | | | |
| Server Manager (RADIUS | 5) | | Users 19 objects | [Filter Activated] | |
| E 🖗 Roles | | | Name | Type | Description |
| | Certificate Services | | & Administrator | User | Built-in account for admini |
| 🖃 🞇 Active Directory [| | DADTUC had been and 1 | Allowed ROD | Security Group | Members in this group can. |
| Active Director E iii tsd.test.org | ory Users and Computers [| RADIUS.tsd.test.com j | & Cert Publishers | Security Group | Members of this group are. |
| 🖃 📑 tsa.test.o | | | & Denied ROD | Security Group | Members in this group can. |
| | outers | | & DnsAdmins | Security Group | DNS Administrators Group |
| | ain Controllers | | & DnsUpdatePr | | DNS dients who are permi |
| | gnSecurityPrincipals | | & Domain Admins | Security Group | Designated administrators. |
| | ged Service Accounts | | & Domain Com | Security Group | All workstations and serve. |
| Users | | | & Domain Cont | Security Group | All domain controllers in th. |
| 🕀 🔡 Active Direct | Delegate Control | | & Domain Guests | Security Group | All domain quests |
| 🛨 🚊 DNS Server | Find | | & Domain Users | Security Group | All domain users |
| 🕀 🗳 Web Server (IIS | New 🕨 | Computer | Renterprise A | Security Group | Designated administrators. |
| 🕀 🗃 Features | All Tasks | Contact | Enterprise R | Security Group | Members of this group are. |
| 🛨 🚋 Diagnostics | All TOSKS | Group | Group Policy | | Members in this group can. |
| 🕀 🁬 Configuration | View 🕨 | InetOrgPerson | Guest | User | Built-in account for quest |
| 🕀 🔚 Storage | Refresh | msImaging-PSPs | | Security Group | Servers in this group can |
| | Export List | MSMQ Queue Alias | Read-only D | Security Group | Members of this group are. |
| | Export List | Printer | | Security Group | Designated administrators. |
| | Properties | User | TSD | User | besignated daministrators. |
| | | Shared Folder | - 100 | 000 | |
| | Help | Shareu Folder | | | |
| | | | | | |
| New Object Course | | | | | |
| New Object - Group | , | | | × | |
| | | | | | |
| (a) | | | | | |
| Create | in: tsd.test.com/ | Users | | | |

• Creating User account for authenticating via NPS(RADIUS)

| Create in: tsd.test | com/Users |
|--|------------------------|
| Group n <u>a</u> me: Wireless Users | |
| Group name (pre- <u>W</u> indows 2000 |): |
| Wireless Users | |
| Group scope | Group type |
| C Domain local | © Security |
| C <u>G</u> lobal C <u>Universal</u> | C <u>D</u> istribution |
| | |
| | OK Cancel |

| 🚡 Server Manager (RADIU | IS) | | Users 20 objects | [Filter Activated] |
|---|-----------------------------|-----------------------|------------------|--------------------|
| 🖃 🖥 Roles | | | Name | Туре |
| E Active Directory | | | & Administrator | User |
| Plant - | Domain Services | | | Security Group |
| | tory Users and Computers [| RADIUS.tsd.test.com J | | Security Group |
| E 👬 tsd.test | | | & Denied ROD | |
| E Built | | | & DnsAdmins | Security Group |
| | iputers iain Controllers | | | Security Group |
| | eignSecurityPrincipals | | | Security Group |
| | aged Service Accounts | | Domain Com | |
| User | | | & Domain Cont | |
| 🕀 🏢 Active Direc | Delegate Control | | & Domain Guests | |
| 🛨 🚊 DNS Server | Find | | & Domain Users | Security Group |
| 🕀 🍓 Web Server (IIS | New 🕨 | Computer | Enterprise A | |
| 🕀 🚮 Features | All Tasks 🕨 | Contact | Enterprise R | |
| Diagnostics | | Group | Group Policy | |
| Configuration | View • | InetOrgPerson | 🖁 Guest | User |
| 🕀 📇 Storage | Refresh | msImaging-PSPs | | Security Group |
| | Export List | MSMQ Queue Alias | Read-only D | |
| | | Printer | | Security Group |
| | Properties | User | 👗 TSD | User |
| | Help | Shared Folder | & Wireless Users | Security Group |
| New Object - User Image: Eirst name: Last name: Full name: User logon name: aaron User logon name (pre TSD\ | aaron aaron @tsd.tes | st.com | | |
| | < <u>B</u> ack | <u>N</u> ext > | Cancel | |

| Remo | operties | | | | ? × |
|------------|---|---|---|---|--|
| nemo | te Deskto | p Services Prof | ile 🛛 Person | al Virtual Deskto | p COM+ |
| Dial | | | Profile Telepho | | emote control |
| | | s Account i | Profile Telepho | ones Organiza | |
| Memb | | A D | | | |
| Dom | ie iain Users | | irectory Domain :om/Users | Services Folder | |
| Wire | less Users | tsd.test.c | om/Users | | |
| | | | | | |
| A | k <u>d</u> d | <u>R</u> emove | | | |
| Primar | y group: | Domain Use | ers | | |
| | | 1 There | e is no need to c | hance Primarv c | roup unless |
| <u>5</u> e | t Primary G | roup you h | ave Macintosh (ations. | | |
| | | appire | | | |
| | | | | | |
| | | | | | |
| | Г | | | | |
| | | OK I | Cancel | Apply | Help |
| | | ОК | Cancel | Apply | Help |
| TSD P | Properties | ОК | Cancel | Apply | |
| | roperties | | | | <u>?</u> × |
| R | emote Desk | top Services Pro | | al Virtual Desktop | COM+ Member Of |
| Re | emote Desk | top Services Pro | file Persona Profile Telepho | Il Virtual Desktop nes Organization | ?× |
| Gen | emote Desk eral Addre Dial-in | top Services Pro | file Persona Profile Telepho | Il Virtual Desktop nes Organization | COM+ in. COM+ in. Member Of re. ote control in. |
| Gen | emote Desk eral Addre Dial-in | top Services Pro ess Account Environmen ess Permission | file Persona Profile Telepho | Il Virtual Desktop nes Organization | ? × Image: COM+ n Member Of re, ote control |
| Gen Gen | emote Desk eral Addre Dial-in letwork Acc | top Services Pro ess Account Environmen ess Permission - | file Persona Profile Telepho | Il Virtual Desktop nes Organization | COM+ Member Of note control ni. re. note control ni. rs. /e. |
| | emote Desk eral Addre Dial-in letwork Acc Allow acc | top Services Pro ess Account Environmen ess Permission - ess ess | file Persona Profile Telepho | I Virtual Desktop nes Organizatio ns Rem | COM+ Member Of ote control ni. re. ni. re. re. re. re. re. re. re. re |
| Ren Gen | emote Desk eral Addre Dial-in letwork Acc Allow acc | top Services Pro ess Account Environmen ess Permission - ess ess eccess through NF | file Persona Profile Telepho t Sessio | I Virtual Desktop nes Organizatio ns Rem | ? × I COM+ in. in. in Member Of in in. |
| Ringen | emote Desk eral Addre Dial-in letwork Acc Allow acc Deny acc Control ac | top Services Pro ess Account Environmen ess Permission ess ess eccess through NF er-ID: | file Persona Profile Telepho t Sessio | I Virtual Desktop nes Organizatio ns Rem | COM+ Member Of note control ni. re. note control ni. rs. /e. |
| | emote Desk eral Addre Dial-in letwork Acc Allow acc Deny acc Control ac Verify Call | top Services Pro ess Account Environmen ess Permission ess ess ccess through NF er-ID: ions | file Persona Profile Telepho t Sessio | I Virtual Desktop nes Organizatio ns Rem | ? × In. COM+ In. In. < |
| | emote Desk eral Addra Dial-in letwork Acc ? [Allow acc ? [Allow acc ? [Ontrol ac ? Control ac ? [Verify Call allback Opt ? No Qallba | top Services Pro ess Account Environmen ess Permission ess ess ccess through NF er-ID: ions | file Persona Profile Telepho t Sessio | al Virtual Desktop nes Organization ns Rem | ? × In COM+ an. m Member Of ote control an. p mi. rs. re. rs. |
| | emote Desk eral Addra Dial-in letwork Acc ? [Allow acc ? [Allow acc ? [Ontrol ac ? Control ac ? [Verify Call allback Opt ? No Qallba | top Services Pro ess Account Environmen ess Permission ess ess ccess through NF er-ID: ions ack aller (Routing and | file Personz Profile Telepho t Sessic | al Virtual Desktop nes Organization ns Rem | ? × In. COM+ In. In. < |
| | emote Desk eral Addra Dial-in letwork Acc) Deny acc) Deny acc) Deny acc) Deny acc) Control ac) Deny acc) Control ac) Deny acc) Control ac) Deny acc) Control ac) Deny acc) D | top Services Pro ess Account Environmen ess Permission ess ess ccess through NF er-ID: ions ack aller (Routing and allback to: | file Personz Profile Telepho t Sessio 2'S Network <u>Policy</u> Remote Access | al Virtual Desktop nes Organization ns Rem | ? × In. COM+ an. n Member Of re. ote control an. rs. re. rs. re. rs. re. r. rs. re. rs. re. r. re. re |
| | emote Desk eral Addra Dial-in letwork Acc <u>Deny acc</u> <u>Deny acc</u> <u>Control ac</u> <u>Control ac</u> <u>Verify Call</u> allback Opt <u>No Callback</u> <u>Set by Ca</u> <u>Always C</u> Assign St | top Services Pro ess Account Environmen ess Permission ess ess eccess through NF er-ID: ions eck aller (Routing and allback to: atic <u>IP</u> Addresses | file Persona Profile Telepho t Sessio 25 Network <u>P</u> olicy | al Virtual Desktop nes Organization ns Rem | ? × Image: COM+ n Member Of ote control ni. rs. /e. th. rs. re. rs. re. |
| | emote Desk eral Addra Dial-in letwork Acc <u>Deny acc</u> <u>Deny acc</u> <u>Control ac</u> <u>Control ac</u> <u>Verify Call</u> allback Opt <u>No Callback</u> <u>Set by Ca</u> <u>Always C</u> Assign St | top Services Pro ess Account Environmen ess Pemission ess ccess through NF er-ID: ions ack aller (Routing and allback to: atic [P Addresses Idresses to enabl | file Persona Profile Telepho t Sessio 2S Network <u>P</u> olicy Remote Access | al Virtual Desktop nes Organization ns Rem | ? × Image: COM+ in. |
| | emote Desk eral Addre Dial-in letwork Accc Allow acc Deny acc Deny acc Deny acc Control ac Deny acc Control ac Contro | top Services Pro ess Account Environmen ess Permission ess ess eccess through NF er-ID: ions ack aller (Routing and allback to: atic IP Addresses Idresses to enable | file Persona Profile Telepho t Sessio 2S Network <u>P</u> olicy Remote Access | al Virtual Desktop nes Organizatio ns Rem | ? × Image: COM+ in. |
| | emote Desk eral Addra Dial-in letwork Acc 2 [Allow acc 2 [Deny acc 2 Control ac 3 Deny acc 3 Control ac 3 Deny Call allback Opt 5 No Callback 3 Set by Ca 3 Always C 5 Always C 5 Always C 5 Define IP ac Dial-in connu 5 Apply Sta | top Services Pro ess Account Environmen ess Permission ess ess eccess through NF er-ID: ions ack aller (Routing and allback to: atic IP Addresses Idresses to enable | file Persona Profile Telepho t Sessio 2S Network <u>Policy</u> Remote Access s e for this | al Virtual Desktop nes Organizatio ns Rem | ? × COM+ m. m Member Of ote control m. rs. re. rb. rs. re. re. re. |
| | emote Desk eral Addre Dial-in letwork Accc Allow acc Deny acc Deny acc Control ac Co | top Services Pro ess Account Environmen ess Permission ess ess ccess through NF er-ID: ions | file Persona Profile Telepho t Sessio 2S Network <u>Policy</u> Remote Access s e for this | I Vitual Desktop nes Organization ns Rem Service only) | ? × COM+ m. m Member Of ote control m. rs. re. rb. rs. re. re. re. |

Add account from AD

Modifying remote access permission to Allow access (Deny access by default)

• Creating NPS Rules

Configuring NPS for the RADIUS, for the Standard Configuration option, select RADIUS server for 802.1X Wireless or Wired Connections

| Configure 802.1X Configuration Configuration Select 802.1X Connections Configuration Configuratio | Server Manager (RADIUS) | NPS (Local) |
|--|---|--|
| Arther Directory Duran Services Retwork Folicy and Neuros Access protection Retwork Folicy and Neuros Retwork Folicy and Neuro | Roles Active Directory Certificate Services | Getting Started |
| Standard Configuration Finder Standard Configuration Finder Standard Configuration Finder Select a configuration scenario from the lat and then click the link below to open the scenario watad. Finder Finder Finder Select a configuration scenario from the lat and then click the link below to open the scenario watad. Finder Finder Finder Select a configuration scenario from the lat and then click the link below to open the scenario watad. Finder Finder Finder Select a configuration Finder Schedicals and Schools (Weild Connections Schedicals and Schools (Weild Connections Finder Schedicals and Schools (Weild Connections) Finder | | Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client |
| Select 802.1X Connections Type Select 802.1X Connections Type Select 802.1X Connections Type Select 802.1X connections Type Select 802.1X connections Type Select 802.1X connections Type Select 802.1X connections Type Select 802.1X connections Type Select 802.1X connections Type Deposite Select 802.1X connections Type Select 802.1X connections Type Deposite Select 802.1X connections Type Select 802.1X connections Type Deposite Select 802.1X connections Type Select 802.1X connections Type Deposite Select 802.1X connections Type Select 802.1X connections Type Deposite Sele | | Standard Configuration |
| Particular and Remote Access Image: Particular and Remote Access Image: Particular and Remote Access Image: Particular and Automatication and Automaticati | Accounting | Select a configuration scenario from the list and then click the link below to open the scenario wizard. |
| Secure Wireless Connections: Secure Wireless connections through the access points. | Routing and Remote Access | |
| Configures Configures Configures Configure 802.1X C | | RADIUS server for Dial-Up of VPN Connections |
| Advanced Configuration Templates Configuration Memplates Configuration Memplates Configuration Memplates Configuration Memplates Configuration Memplates Configuration Memplates Connections Configure 802.1X connections Type Configure Vireless 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. Configure Wireless 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: Tis 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. | | authenticate and authorize connections from wireless access points and authenticating switches (also called RADIUS clients |
| Templates Configuration Configure 802.1X Select 802.1X Connections Type Select 802.1X Connections Type Type of 802.1X connections Secure Wireless Connections When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize connection requests made by wireless clients connecting through the access points. Secure Wirel (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet 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 . | | Configure 802.1X Learn more |
| Configure 802.1X Image: Configure 802.1X Select 802.1X Connections Type Image: Configure 802.1X Connections Type Select 802.1X Connections Type Image: Connections Connections Image: Connections Connection requests made by wireless clients connecting through the access points. Image: Connection requests made by wireless clients connecting through the access points. Connection requests made by wireless clients connecting through the sections points. Image: Connection requests made by Ethemet clients connecting through the switches. Connection requests made by Ethemet clients connecting through the switches. Image: Connection requests made by Ethemet clients connecting through the switches. Connection requests made by Ethemet clients connecting through the switches. Image: Connection requests made by Ethemet clients connecting through the switches. Connection requests made by Ethemet clients connecting through the switches. Image: Connection requests made by Ethemet for each of the policies created with this wizard. You can use the default text or modify it . | | Advanced Configuration |
| Select 802.1X Connections Type Secure Vireless 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 (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet clients connecting through the switches. Mame: 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 . | | Templates Configuration |
| Select 802.1X Connections Type Secure Vireless 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 (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet clients connecting through the switches. Mame: 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 . | | |
| Select 802.1X Connections Type Steps 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 Wirele (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet clients connecting through the switches. Mame: 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 . | | |
| 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 (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet clients connecting through the switches. Mame: 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 . | onfigure 802.1X | X |
| 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 (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet clients connecting through the switches. Mame: This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it . | | |
| Secure Wireless Connections 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 <u>Wired</u> (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet 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 . | Select 80 | 2.1X Connections Type |
| 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 <u>Wired</u> (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet clients connecting through the switches. Name: This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it . | | |
| Secure Wireless Connections 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 (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet clients connecting through the switches. Name: This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it . | | |
| Secure Wireless Connections 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 (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet clients connecting through the switches. Name: This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it . | | |
| Secure Wireless Connections 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 (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet 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 . | Type of 902 1X 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 (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet 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 . | | • |
| connection requests made by wireless clients connecting through the access points. Secure Wired (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet 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 . | | and a concern paints on your naturals. NPS and a therein and a therein |
| Secure Wired (Ethemet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet 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. | | |
| When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethemet 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 . | | |
| Connection requests made by Ethemet 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 . | C Secure Wired (Ethemet) Conn | ections |
| 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 . | | |
| 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 . | connection requests made by I | Ethemet clients connecting through the switches. |
| 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 . | | |
| default text or modify it . | | the same for each of the collector exceeded with this wiread. You each use the |
| | | the name for each of the policies created with this wizard. You can use the |
| | · · · · · · · · · · · · · · · · · · · | |
| | Secure Wireless Connections | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | Breaking Next Civit Correct |
| | | Previous <u>N</u> ext Einish Cancel |

| Settings Setect an existing template: Select an existing template: RADIU RADIU To spe DAP-2360 Address (IP or DNS): 192.168.0.50 Verify Shared Secret Select an existing Shared Secrets template: None |
|--|
| Select an existing template: RADIU RADIU To spe DAP-2360 RADIU DAP-2360 Shared Secret Select an existing Shared Secrets template: |
| RADIU RADIU To spe DAP-2360 RADIL DAP-2: Shared Secret Select an existing Shared Secrets template: |
| RADIU RADIU Name and Address point. To spe DAP-2360 |
| RADIU RADIU To spe DAP-2360 RADIU DAP-2: 192.168.0.50 Shared Secret Select an existing Shared Secrets template: |
| RADIU Friendly name: To spe DAP-2360 RADIU Address (IP or DNS): DAP-2: [192.168.0.50 Shared Secret Select an existing Shared Secrets template: |
| To spe DAP-2360 RADIL DAP-2 IShared Secret Select an existing Shared Secrets template: |
| RADIU Address (IP or DNS): DAP-2: 192.168.0.50 Shared Secret Select an existing Shared Secrets template: |
| DAP-2: Verify Shared Secret Select an existing Shared Secrets template: |
| Shared Secret Select an existing Shared Secrets template: |
| Select an existing Shared Secrets template: |
| Select an existing Shared Secrets template: |
| None |
| |
| |
| To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared |
| secret entered here. Shared secrets are case-sensitive. |
| |
| Manual O Generate |
| Shared secret: |
| |
| Confirm shared secret: |
| |
| |
| |
| OK Cancel Apply el |
| |
| Configure 802.1X |
| Configure an Authentication Method |
| |
| |
| |
| |
| |
| Select the EAP type for this policy. |
| |
| Select the EAP type for this policy. |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |
| Select the EAP type for this policy. Type (based on method of access and network configuration): |

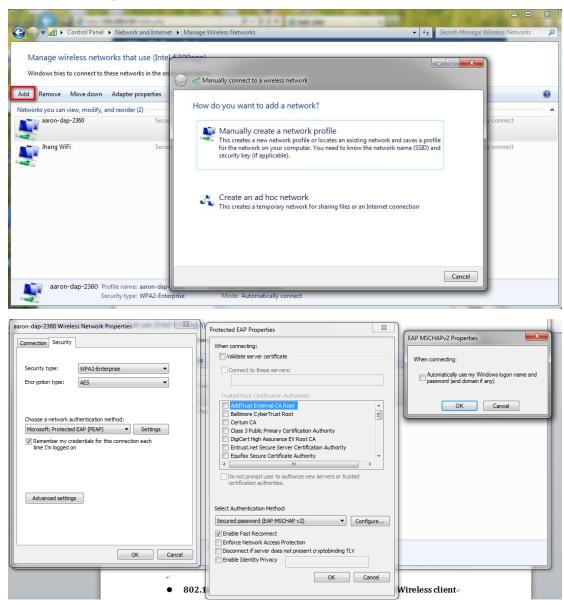
| Configure 802. | 1X X |
|--------------------------|--|
| | |
| | Specify User Groups |
| 5 | Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting. |
| To select <u>U</u> ser (| Groups, click Add. If no groups are selected, this policy applies to all users. |
| Groups | Add |
| TSD\Wireless | Users |
| | <u>R</u> emove |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | Previous Next Finish Cancel |
| | Previous Next Einish Cancel |
| | |
| | |
| Configure 802. | 1X X |
| | Configure Traffic Controls |
| | Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic. |
| If your RADIUS | clients (authenticating switches or wireless access points) support the assignment of traffic |
| controls using F | ADIUS tunnel attributes, you can configure these attributes here. If you configure these attributes, ADIUS clients to apply these settings for connection requests that are authenticated and |
| If you do not us | e traffic controls or you want to configure them later, click Next. |
| | |

| | Configure Traffic Controls | |
|-------------------|---|--|
| | Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic. | |
| controls using R | clients (authenticating switches or wireless access points) support the assignment of traffic ADIUS tunnel attributes, you can configure these attributes here. If you configure these attributes, ADIUS clients to apply these settings for connection requests that are authenticated and | |
| lf you do not use | e traffic controls or you want to configure them later, click Next. | |
| Traffic control | l configuration | |
| To configure t | traffic control attributes, click Configure. | |
| | <u>C</u> onfigure | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | Previous Next Finish Cancel | |
| | | |

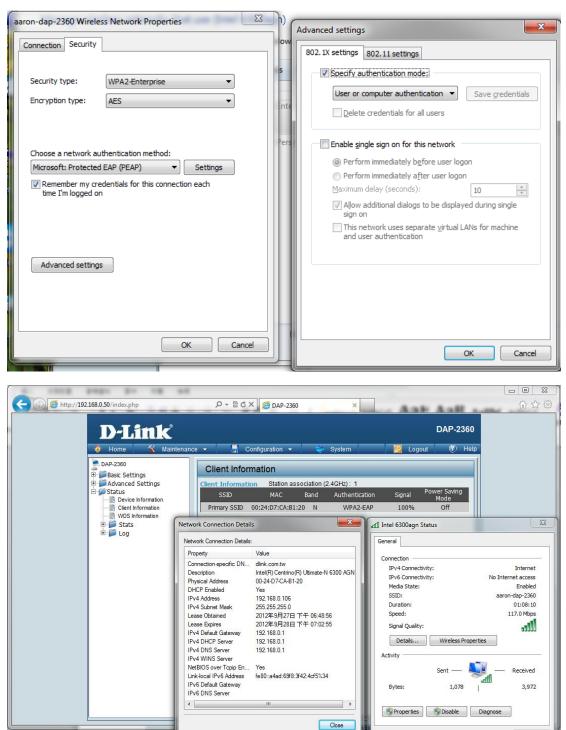
| Configure 802.1 | IX | | | | × |
|---|---|----------------------------|------|----------------|--------|
| | Completing New Wireless Conne | | | | nd |
| To view the co To change the | ssfully created the following onfiguration details in your de configuration, click Previou onfiguration and close this w | fault browser, click s. | | | s. |
| Connection R Secure Wireless Network Polic Secure Wireless | ies: | | | | |
| Configuration De | <u>tails</u> | | | | |
| | | Previous | Next | <u>F</u> inish | Cancel |

• WAP/WPA2-enterprise configuration on Access Point/Wireless client Access Point Authentication WPA-Enterprise

| D-Link | DAP-2360 |
|---------------------|--|
| 🔶 Home 🌋 Maintenan | ce 👻 🍶 Configuration 👻 💝 System 🛛 👰 Logout 📧 Help |
| DAP-2360 | Wireless Settings |
| Wireless LAN | Wireless Band 2.4GHz 💌 |
| E Advanced Settings | Mode Access Point 💌 |
| ⊞ 🃁 Status | Network Name (SSID) aaron-dap-2360 |
| | SSID Visibility Enable 💌 |
| | Auto Channel Selection Enable - |
| | Channel 1 - |
| | Channel Width 20 MHz 🔻 |
| | Authentication WPA-Enterprise 🔻 |
| | RADIUS Server Settings |
| | WPA Mode AUTO (WPA or WPA2) |
| | Cipher Type Auto Group Key Update Interval 1800 (Seconds) Network Access Protection |
| | Network Access Protection Protection Protection |
| | Primary RADIUS Server Setting |
| | RADIUS Server 192.168.0.204 RADIUS Port 1812 |
| | RADIUS Secret |
| | Save |
| | |



Wireless client / PEAP Authentication method



Close

字數: 112 | 🅉 中文 (台灣) | 插入 |

• 802.1x Authentication configuration on Access Point/Wireless client

Access Point Authentication 802.1x

| D-Link [®] | | | | DAP-2360 |
|-----------------------|------------------------|---------------------|-------------|----------|
| 🔅 Home 🏾 🌠 Maintenand | ce 👻 🚽 Configurati | on 👻 👙 System | 💋 Logout | 🕐 Help |
| DAP-2360 | Wireless Settings | | | |
| Wireless LAN | Wireless Band | 2.4GHz 🔻 | | |
| | Mode | Access Point 💌 | | |
| 🗄 🃁 🃁 Status | Network Name (SSID) | aaron-dap-2360 | | |
| | SSID Visibility | Enable 🔻 | | |
| | Auto Channel Selection | Enable 🔻 | | |
| | Channel | 1 - | | |
| | Channel Width | 20 MHz 💌 | | |
| | Authentication | 802.1X - | | |
| | RADIUS Server Settings | | | |
| | Key Update Interval | 300 (Seconds) | | |
| | Primary RADIUS Server | - | | |
| | RADIUS Server | 192.168.0.204 RADIU | S Port 1812 | |
| | RADIUS Secret | ••••• | | |
| | | | 6 | |
| | | | C | Save |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Wireless client / PEAP Authentication method

| aaron-dap-2360 Wireless Network Properties | Protected EAP Properties | EAP MSCHAPv2 Properties |
|---|---|---|
| Connection Security | When connecting: | When connecting: |
| Security type: 802.1X - | Connect to these servers: | Automatically use my Windows logon name and password (and domain if any). |
| Encryption type: WEP - | Trusted Root. Certification Authonities: | Cancel |
| Choose a network authentication method: Microsoft: Protected EAP (PEAP) ▼ Settings | Baltmore CyberTrust Root Certum CA Cartum CA Class 3 Public Primary Certification Authority DiglCert High Assurance EV Root CA Entrust.net Secure Servier Certification Authority Equifax Secure Certificate Authority O not prompt user to authorize new servers or trusted certification authorities. | |
| | Select Authentication Method: Secured password (EAP-MSCHAP v2) Configure Tenable Fast Reconnect Fnforce Network Access Protection | |
| OK Cancel | Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel | |

