Microsoft Solutions for Security

Securing Wireless LANs with Certificate Services

Build Guide

Release 1.6

Microsoft®

Build Guide Overview

The Build Guide provides IT professionals with step–by–step instructions to implement all of the components of the solution: a Public Key Infrastructure (PKI) based on Microsoft® Windows Server™ 2003 Certificate Services, a Remote Authentication Dial-In User Service (RADIUS) infrastructure based on Microsoft Internet Authentication Service (IAS), and the configuration of wireless access points (AP) and clients. Each chapter contains detailed procedures on installing and securing the operating system, configuring the software components, and then integrating them into the solution. All major steps are linked to verification procedures to help minimize errors.

The Build Guide contains the following chapters:

- Chapter 7: Implementing the Public Key Infrastructure
- Chapter 8: Implementing the RADIUS Infrastructure
- Chapter 9: Implementing Wireless LAN Security

Table of Contents

7

Implementing the Public Key Infrastructure

Introduction

This chapter provides detailed guidance for building a public key infrastructure (PKI) based on Microsoft® Windows Server™ 2003 Certificate Services. It includes the installation and configuration of the certification authorities (CA), the preparation of the Active Directory® directory service and Microsoft Internet Information Services (IIS), and the configuration of client certificate policy. This guidance is designed to help you create the certificate infrastructure that will be used in subsequent chapters to build a complete wireless LAN security solution.

The objective of this chapter is to give you implementation instructions for the PKI design described in Chapter 4, "Designing the Public Key Infrastructure." It does not attempt to explain any of the general concepts of PKI or the specifics of the Microsoft Certificate Services implementation.

The chapter is a companion to the PKI Planning and Operations chapters (Chapters 4 and 11, respectively). The Planning Guide chapter explains the rationale behind the implementation decisions used in this chapter. The Operations Guide chapter explains the necessary tasks and processes for successful maintenance of the PKI. If you have not already done so, you are strongly recommended to read the Planning Guide chapters before continuing with this chapter. You should also read and understand the implications of the support requirements in the Operations Guide before using the guidance in this chapter to implement your PKI.

Chapter Prerequisites

This section contains checklists that will help you establish your organization's readiness to implement the PKI. ("Readiness" is meant in a logistical sense rather than business sense−the business motivation for implementing this solution is discussed in the early chapters of the Planning Guide.)

Knowledge Prerequisites

You should be familiar with concepts of PKI and Microsoft Certificate Services in particular. Familiarity with Windows 2000 Server or Windows Server 2003 is also required in the following areas:

- Installation of the Microsoft Windows® operating system.
- Active Directory concepts (including Active Directory structure and tools; manipulating users, groups, and other Active Directory objects; and use of Group Policy).
- Windows system security; security concepts such as users, groups, and auditing, access control lists (ACLs); the use of security templates; and the application of security templates using Group Policy or command line tools.
- Administration of IIS.
- An understanding of Windows Scripting Host and knowledge of the Microsoft Visual Basic® Scripting Edition (VBScript) language will be helpful for you to get the most out of the supplied scripts, but this is not essential.

Before proceeding with this chapter, you should also have read the Planning Guide and have a thorough understanding of the architecture and design of the solution.

Organizational Prerequisites

You should consult with other members of your organization who may need to be involved in the implementation of this solution, such as:

- Business sponsors.
- Security and audit personnel.
- Active Directory engineering, administration, and operations personnel.
- DNS (Domain Name System), Web server, and network engineering personnel
- Administration and operations personnel.

IT Infrastructure Prerequisites

This chapter makes the following assumptions about the existing IT infrastructure:

- A deployed Windows 2000 or Windows Server 2003 Active Directory domain infrastructure exists. All users of Certificate Services in this solution should be members of a domain within the same Active Directory forest.

Notes:

Although the use of Windows Server 2003 Certificate Services and Internet Authentication Service (IAS–Microsoft's RADIUS implementation) with Windows 2000 Active Directory is fully supported, this solution has not been tested in such a configuration; it has only been tested with Windows 2003 Active Directory. Instructions for using Windows 2000 Active Directory are included in the guidance, however.

Although it is possible to deploy this solution for multiple forests with minor modifications, doing so is outside the scope of this guidance. For more information about multiple forest deployments, see the note in the "More Information" section at the end of the chapter.

This solution includes no guidance for integration into an existing PKI. However, the solution does not preclude deployment alongside an existing PKI.

- Server hardware adequate to run Windows Server 2003 Certificate Services is available. A suggested configuration is provided as part of the guidance.
- This solution is not to be integrated into an existing PKI. However, the solution does not preclude deployment alongside an existing PKI.
- Windows Server 2003 Standard Edition and Enterprise Edition licenses, installation media, and product keys are available.

Chapter Overview

The following figure shows the process of building the PKI described in this chapter.

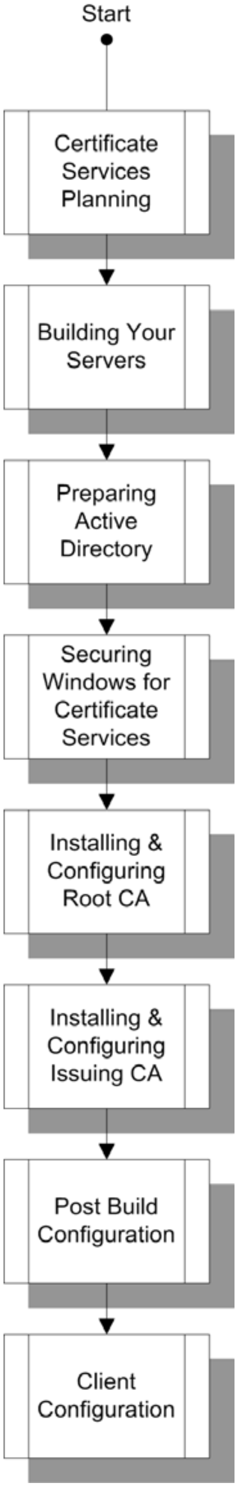
Start
Certificate Services Planning
Building Your Servers
Preparing Active Directory
Securing Windows for Certificate Services
Installing & Configuring Root CA
Installing & Configuring Issuing CA
Post Build Configuration
Client Configuration

Figure 7.1
Diagram of the process of building the PKI

These steps are mirrored in the organization of the chapter, and are described in the following list. Each consists of installation or configuration tasks. Each step also has verification procedures so that you can check that everything is working before continuing with the next step.

- **Certificate Services Planning Worksheet**. Lists the configuration information used in this chapter to install and configure Certificate Services. It includes a table of information that you must provide before commencing implementation.
- **Building Your Servers**. Describes the selection and configuration of hardware, the installation of Windows Server 2003, and the installation of optional components such as IIS.
- **Preparing Active Directory for Your PKI**. Explains prerequisites for the Active Directory forest and domain into which the PKI will be deployed together with essential preparation steps. It also explains the creation of management security groups and users and setting the correct permissions for delegating management tasks.
- **Securing Windows Server 2003 for Certificate Services**. Discusses the implementation of operating system-level security by applying security templates. The templates used are taken from the *Windows Server 2003 Security Guide*. See the "More Information" section at the end of this chapter for details on how to obtain this guide.
- **Other Windows Configuration Tasks**. Lists a few common tasks to complete the base installation of the servers.
- **Installing and Configuring the Root CA**. Describes the preparation steps, software installation, and configuration of Certificate Services, including defining administrative roles for the server. The final step is publishing the offline root CA's certificate and certificate revocation list (CRL) to the Active Directory and Web server.
- **Installing and Configuring the Issuing CA**. Similar to the root CA guidance except that it also includes obtaining a CA certificate from the root CA. The final verification step confirms that you can enroll certificates from the issuing CA.
- **Post-Build Configuration**. Explains configuring the default certificate types issued by the issuing CA, setting permissions for a multi-domain forest, and completing a backup before the CAs are ready to introduce into a production environment.
- **Client Configuration**. Describes how to enable autoenrollment for all users and computers in the domain and how to configure root certificate trust policies.

Certificate Services Planning Worksheet

The tables in this section list all the PKI configuration parameters used in the solution. You should use these as a checklist for your planning decisions.

Some of the parameters in these tables are entered manually as part of the procedures documented in this chapter. Others are either set by a script run as part of one of the procedures, or the parameter is in some way referenced by a script in order to complete a configuration or operational task. Where this is the case, the name of the related script is included in the table.

Note: The scripts used in this chapter are described in more detail in Appendix A and in the ToolsReadme.txt file that accompanies the scripts.

User-Defined Configuration Items

The following table lists organization-specific parameters taken from the fictitious Woodgrove Bank. You should ensure that you have collected or decided on the equivalent settings for your own organization for all of these items before beginning the setup procedure. Throughout the chapter, the fictitious values shown in this table are used in the sample commands. You should substitute values appropriate for your own organization in place of these values. The places in the text where you need to substitute your own values are shown in italics.

Table 7.1: User-Defined Configuration Items

Configuration item	Setting	Script reference
DNS name of Active Directory forest root domain	woodgrovebank.com	
Distinguished Name (DN) of forest root	DC=woodgrovebank,DC=com	Pkiparams.vbs
NetBIOS (network basic input/output system) name of domain	WOODGROVEBANK	
NetBIOS name of root CA workgroup	WGB-Root	
Server name of root CA	HQ-CA-01	
Server name of issuing CA	HQ-CA-02	
X.500 Common Name (CN) of root CA	WoodGrove Bank Root CA	
X.500 CN of issuing CA	WoodGrove Bank Issuing CA 1	
Fully-qualified host name of Web server used to publish CA certificate and revocation information	www.woodgrovebank.com	Pkiparams.vbs

Solution-Prescribed Configuration Items

The settings specified in this table do not need to be changed for your installation unless you need to use a setting that is different from the solution design. Changing the design parameters given here is perfectly acceptable as long as you understand that you are departing from the tested solution by doing this. Ensure that you fully understand the implications of changing a setting and the dependencies that the setting might have before altering any values here and in the configuration procedures and supplied scripts.

Table 7.2: Solution-Prescribed Configuration Items

Configuration item	Setting	Script reference
Administration Role Security Groups		
Administrators of Public Key Services configuration container.	Enterprise PKI Admins	ca_setup.wsf
Administrative group that is allowed to publish certificate revocation lists (CRLs) and CA certificates to Enterprise configuration container.	Enterprise PKI Publishers	ca_setup.wsf
Administrative group that configures and maintains the CAs; also controls the ability to assign all other CA roles and renew the CA certificate.	CA Admins	ca_setup.wsf
Administrative group that approves certificate enrollment and revocation requests. This is a CA Officer role.	Certificate Managers	ca_setup.wsf
Administrative group that manages CA audit and security logs.	CA Auditors	ca_setup.wsf
Administrative group that manages CA backups.	CA Backup Operators	ca_setup.wsf
IIS Configuration		
Name of Internet Information Services (IIS) virtual directory used to publish CA certificate and CRL information.	pki	Pkiparams.vbs
Physical path on issuing CA that maps to IIS virtual directory.	C:\CAWWWPub	Pkiparams.vbs
Common CA Parameters		
Drive and path to store Certificate Services request files.	C:\CAConfig	Pkiparams.vbs
Drive and path to store Certificate Services database logs.	%windir%\System32\CertLog	
Root CA Configuration		
Length of root CA key (see the note following this table).	4096	
Validity period of root CA certificate.	16	Pkiparams.vbs

(continued)

Units for previous value.	Years	Pkiparams.vbs
Maximum validity period of certificates issued by root CA.	8	Pkiparams.vbs
Units for previous value.	Years	Pkiparams.vbs
CRL publishing interval for root CA.	6	Pkiparams.vbs
Units for previous value.	months	Pkiparams.vbs
CRL overlap period (time between new CRL being published and old CRL expiring).	10	Pkiparams.vbs
Units for previous value.	Days	Pkiparams.vbs
Delta–CRL publishing period for root CA—0 = disable delta–CRLs.	0	Pkiparams.vbs
Units for previous value.	Hours	
Issuing CA Parameters		
Drive and path to store Certificate Services database.	D:\CertLog	
Length of issuing CA key.	2048	
Validity period of issuing CA certificate.	8	Pkiparams.vbs
Units for previous value.	Years	Pkiparams.vbs
Maximum validity period of certificates issued by issuing CA.	4	Pkiparams.vbs
Units for previous value.	Years	Pkiparams.vbs
CRL publishing interval for issuing CA.	7	Pkiparams.vbs
Units for above value.	Days	Pkiparams.vbs
CRL overlap period (time between new CRL being published and old CRL expiring).	4	Pkiparams.vbs
Units for above value.	Days	Pkiparams.vbs
Delta–CRL publishing period for issuing CA—0 = disable delta–CRLs.	1	Pkiparams.vbs
Units for previous value.	Days	Pkiparams.vbs
Delta–CRL overlap period (time between new delta CRL being published and old delta CRL expiring).	1	Pkiparams.vbs
Units for previous value.	Days	Pkiparams.vbs
Miscellaneous		
Path for installation scripts.	C:\MSSScripts	

Important: The use of key lengths of 4096 bits may cause compatibility problems if the certificates are to be issued to, or used by, some devices (for example, some routers) or some older software from other vendors that cannot process keys over a certain size. You should test your applications using certificates with a root CA certificate key of this size before deploying your PKI. If key lengths are a concern, reduce the size of the root CA key to 2048 bits. (You must specify this in the CAPolicy.inf file during the installation of the root CA−see the "Installing and Configuring the Root CA" section.)

Building Your Servers

This section discusses the basic tasks of preparing server hardware and installing the operating system. Two servers are required: one for the root CA, and one for the issuing CA.

Important: Before starting to build your CAs, you should read "Security Management of the CAs" in Chapter 4, "Designing the Public Key Infrastructure." This may affect the security environment used to build your servers.

Selecting and Configuring Server Hardware

The following subsections outline the basic server specification for both CA roles. Chapter 4, "Designing the Public Key Infrastructure," examines some of the key criteria for hardware selection in more detail.

Root CA Server Hardware

The following table shows a recommended hardware specification for the root CA, which is based on generic Windows Server 2003 hardware recommendations. However, you may not need to purchase new hardware if you have a server that fits the criteria outlined in Chapter 4 but is being retired because of performance reasons.

Table 7.3: Suggested Hardware Specification for Root CA Server

Item	Requirement
CPU	Single CPU 733 MHz or higher
Memory	256 MB
Network interfaces	None (or disabled)
Disk storage	IDE (integrated device electronics) or SCSI (small computer system interface) RAID (redundant array of independent disks) controller 2 x 18 GB (SCSI) or 2 x 20 GB (IDE) configured as RAID 1 volume (drive C) Local removable media storage (CD-RW or tape for backup) 1.44-MB disk drive for data transfer

Issuing CA Server Hardware

Although there are performance requirements for the issuing CA, they are relatively low because the issuing CA normally does very little work compared with many other types of servers. The same quality and reliability criteria for selecting hardware for the root CA server also apply here. There are some minor differences from the root CA specification in the networking and storage, as shown in the following table:

Table 7.4: Suggested Hardware Specification for Issuing CA Server

Item	Requirement
CPU	Single CPU 733 MHz or higher
Memory	256 MB
Network interfaces	2 x single network interface card (NIC) teamed for resilience
Disk storage	IDE or SCSI RAID controller 2 x 18 GB (SCSI) or 2 x 20-GB (IDE) configured as RAID 1 volumes (drives C and D) Local removable media storage (CD-RW or tape for backup) if no network backup facility 1.44-MB disk drive for data transfer

Important: The server specification in this table is sized for a user population of approximately 5,000 users. If you have more users you should at least double the disk capacity for the second drive (allow approximately 2 GB per 1000 users) and double the installed memory. For guidelines on disk usage, see "Determining Storage and Backup Requirements for an Issuing CA" in Chapter 11, "Managing the Public Key Infrastructure."

Preparing Hardware

Complete all hardware configurations as recommended by the hardware vendor. These recommendations may include applying the latest BIOS and firmware updates.

Use the disk controller management software supplied with your hardware to create the RAID 1 volumes as outlined in the preceding table (one disk volume for the root CA, two disk volumes for the issuing CA).

Preparing the Root CA Server

The tasks in this section describe the installation of Windows on the server that will be used for the root CA.

Installing Windows Server 2003 Standard Edition

Many organizations already have an automated server installation process. If the parameters used in this section can be included in the automated build process, it is acceptable to use this for the server builds.

One exception is if the build is dependent on a network connection. If so, you should strongly consider performing a manual build, at least for the root CA. Much of the security assurance for an offline CA depends on the fact that it is not and has never been connected to a network. This significantly reduces the possibility that the computer may have been compromised by an external attack (because the attacker would need physical access to the server in some way).

▶ **To install Windows Server 2003**

1. Start the system with the Windows Server 2003 Standard Edition CD in the CD-ROM drive. Ensure that the CD-ROM has been set as a bootable device in the server BIOS settings.
2. Create a partition on the primary volume, format it as NTFS, and select the option to install Windows on that partition.

3. Select the appropriate regional settings.
4. Type the name and company information against which Windows will be registered.
5. Enter a strong password for the local administrator account (at least 10 characters and a mixture of uppercase and lowercase alpha, numeric, and punctuation characters).
6. Type the computer name when prompted, such as ***HQ-CA-01*** (replace this value with the name of your computer).

   Important: Even though the root CA will be offline, it is essential for its name to be unique in the organization.

7. When prompted, select to join a workgroup. Type the workgroup name, such as ***WGB-Root*** (replace this value with your own choice of workgroup name).
8. Do not install any optional components when prompted.

   The server will restart at the end of the main setup process. Continue with the following steps.
9. Install the current Windows service packs (at the time of writing, Windows Server 2003 had only just released to manufacturing, so no service packs were available) and any recommended security updates (use a tool such as Microsoft Baseline Security Analyzer to determine the recommended updates). You should also install any other critical functional updates (not security-related) or updates that are required as a result of your own testing.
10. Activate this copy of Windows. Activation must be done offline so that the server does not connect to a network at any time.

Network Settings

The root CA is not connected to the network. You should disable any network interfaces on the system through **Network Connections** in Control Panel to prevent the root CA being accessible over the network in the event that it is connected to the network by mistake.

Verifying the Installation

You should verify that the operating system installation was correctly completed and that the configured parameters are consistent with what you expected.

▶ **To view the current system configuration**

1. Run the `systeminfo` program at a command prompt.

2. Verify the following elements of the systeminfo output; some detail from the output has been omitted for brevity and is indicated by "…" (ellipses):

```
Host Name:                 HQ-CA-01
OS Name:                   Microsoft® Windows® Server 2003,
                           Standard Edition
...
OS Configuration:          Standalone Server

Registered Owner:          YourOwnerName
Registered Organization:   YourOwnerOrganization
...
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\System32
Boot Device:               \Device\HarddiskVolume1
System Locale:             YourSystemLocale
Input Locale:              YourInputLocale
Time Zone:                 YourTimeZone
...
Domain:                    WGB-Root
Logon Server:              \\HQ-CA-01
Hotfix(s):                 X Hotfix(s) Installed.
                           [01]: Qxxxxxx
...
                           [nn]: Qnnnnnn
NetWork Card(s):           N/A
```

3. If these settings do not match what you expected, you will need to reconfigure the server through the Control Panel or re-run the installation.

Preparing the Issuing CA Server

The tasks in this section describe the installation of Windows on the server that will be used for the issuing CA.

Installing Windows Server 2003 Enterprise Edition

Follow the process for building the root CA server with the following exceptions.

Unlike the root CA, you can build the issuing CA server using a network-based build method if required. However, you should take reasonable precautions to ensure that the CA is not exposed to any security threats. For example, you should install it in an isolated network with no routable path to either the Internet or the main network of your organization. Remember that before the latest security updates are installed, the system may be vulnerable to network-borne threats.

▶ To install Windows Server 2003 Enterprise Edition

1. Follow steps 1-5 for installing the Windows operating system on the root CA server, except use the Enterprise Edition of Windows Server 2003 instead of Standard Edition.
2. Type the computer name when prompted, such as ***HQ-CA-02*** (replace this value with the name of your computer).
3. When prompted, select the option to join a domain. Enter the name of the Active Directory domain into which the servers will be joined, such as *WOODGROVEBANK* (replace this value with domain name into which you are installing the CA). When prompted, enter credentials of a user that is authorized to join computers to this domain.

   Note: For a multi-domain forest, the certificate servers would typically be installed in the forest root domain; although not essential, this is assumed in this solution.

4. Do not install any optional components.

   The server will restart at the end of the main setup process. Continue with the following steps.
5. Install any current service packs and required hotfixes as for the root CA.
6. Create a partition on the second hard drive volume, assign this partition drive letter D, and format it with NTFS.
7. Create a folder on drive D: named D:\CertLog.
8. Activate this copy of Windows. Activation must be done offline so that the server is not exposed to the Internet in any way.

Network Settings

The issuing CA has a single network interface (although this may be implemented by teaming two physical network interface cards for added resiliency). The network interface should be configured with a fixed Internet Protocol (IP) address and other IP configuration parameters (default gateway, DNS settings, and so on) as appropriate for your network.

For security reasons, you should block any inbound or outbound connectivity between the issuing CA and the Internet. Even granting outbound-only access can make viruses and other malicious software to be much more dangerous. It will, for example, allow them to download additional code from the Internet or steal and transport your CA private key material outside of your organization.

Verifying the Installation

You should verify that the operating system installation was correctly completed and that the configured parameters are consistent with what you expected.

▶ To view the Current System configuration

1. Run the `systeminfo` program at a command prompt.
2. Verify the following elements of the systeminfo output (some detail from the output has been omitted for brevity):

```
Host Name:                 HQ-CA-02
OS Name:                   Microsoft® Windows® Server 2003,
                           Enterprise Edition
...
OS Configuration:          Member Server

Registered Owner:          YourOwnerName
Registered Organization:   YourOwnerOrganization
...
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\System32
Boot Device:               \Device\HarddiskVolume1
System Locale:             YourSystemLocale
Input Locale:              YourInputLocale
Time Zone:                 YourTimeZone
...
Domain:                    woodgrovebank.com
Logon Server:              \\DomainControllerName
Hotfix(s):                 X Hotfix(s) Installed.
                           [01]: Qxxxxxx
...
                           [nn]: Qnnnnnn
NetWork Card(s):           1 NIC(s) Installed.
[01]:                      ModelAndVendorofNetworkCard
                           Connection Name: Local Area Connection
                           DHCP Enabled:    No
                           IP address(es)
                           [01]: 10.1.1.11
```

3. If these settings do not match what you expected, you should reconfigure the server through the Control Panel or re-run the installation.

Installing Configuration Scripts onto the Servers

A number of support scripts and configuration files are supplied with this solution to help simplify some aspects of the configuration and operation of the solution. You must install these onto each of the CA servers. Some of these scripts will be needed to perform the operations described in the Operations Guide chapters, so you should not delete them after completing the CA installation.

▶ To install the setup scripts on each server

1. Create a folder called C:\MSSScripts.
2. Copy the scripts from the distribution medium to this folder.

Installing and Configuring Internet Information Services

This section describes the installation and configuration of Internet Information Services (IIS) on the issuing CA. IIS is used to provide CA certificate and CRL download points for non-Windows clients. It is recommended that you do not install IIS on the root CA. Although you can install IIS on the issuing CA, a more secure approach is to host the Web download points for CA certificate and CRL on a different server than the CA itself. There might be many users of the certificates (internal and external) who need to retrieve CRLs or CA chain information but who should not necessarily be permitted access to the CA. Preventing such access is impossible to achieve if the download points are hosted on the CA itself.

Important: To simplify the guidance in this solution, the issuing CA server is used to host the Web server and the CA certificate and CRL download points. However, it is recommended that you use a separate Web server in your own environment to improve the security of your CAs. The steps described here can be used to install and configure IIS on either the issuing CA or on a separate server.

IIS can also host the Certificate Services Web enrollment pages, although these are not used in this solution. If you install the Web enrollment pages on a server other than the CA, you must mark this server as "Trusted for Delegation" by setting this property on the server's computer object in Active Directory.

Installing Internet Information Services on the Issuing CA

IIS is installed with the Windows Optional Components Manager (accessed through **Add-Remove Components** in Control Panel). The following table lists the components to be installed. The indentation reflects the hierarchical relationship between the components as you would see them in the Optional Components Manager Wizard (**Enable network COM+ access** is a sub-component of **Application Server**, for example). Components that are not selected are not shown in the table.

Table 7.5: Optional Components to Be Installed

Component	Install state
Application Server	Selected
Enable network COM+ access	Selected
Internet Information Services	Selected
Common Files	Selected
Internet Information Services Manager	Selected
World Wide Web Service	Selected

▶ To install IIS

1. Run the following at a command prompt:

   ```
   sysocmgr /i:sysoc.inf /u:C:\MSSScripts\OC_AddIIS.txt
   ```

   This command tells the Optional Components Manager to use the component configurations specified in the following unattended installation file C:\MSSScripts\OC_AddIIS.txt:

   ```
   [Components]
   complusnetwork = On
   iis_common = On
   iis_asp = On
   iis_inetmgr = On
   iis_www = On
   ```

   Note: Active Server Pages (ASP) are enabled in this configuration in the line iis_asp = on. This option is needed to support the Certificate Services Web enrollment pages solution extension but not for the core solution. You should consider disabling ASP (deleting the line iis_asp = on before running sysocmgr.exe) if you do not need the Web enrollment pages. You can enable this setting later if needed.

   ---

2. Run the Optional Components Manager again as follows and verify that the installed components match the ones listed in the previous table.

   ```
   sysocmgr /i:sysoc.inf
   ```

   No other subcomponents of **Application Server** are required and thus do not need to be selected.

Configuring IIS for Authority Information Access (AIA) and CRL Distribution Point (CDP) Publishing on the Issuing CA

You must create a virtual directory on IIS to use as the Hypertext Transfer Protocol (HTTP) location for CA Certificate and CRL publishing points (referred to as the AIA and CDP, respectively).

▶ To create a virtual directory on IIS

1. Log on to the IIS server (issuing CA) with local administrator privileges.
2. Create the folder C:\CAWWWPub that will contain CA certificates and CRLs.
3. Set security on the folder using Windows Explorer; the following table shows which permissions to apply. The first four should be already be present.

Table 7.6: Virtual Directory Permissions

User/Group	Permission	Allow/Deny
Administrators	Full Control	Allow
System	Full Control	Allow
Creator Owners	Full Control (subfolders and files only)	Allow
Users	Read List folder contents	Allow
IIS_WPG	Read List folder contents	Allow
Internet Guest Account	Write	Deny

4. In the Internet Information Services management console, create a new virtual directory under the default Web site:
   - Name the virtual directory *pki*
   - Specify *C:\CAWWWPub* as the path.
5. Clear the **Run scripts (such as ASP)** option at the virtual directory access permissions.
6. Ensure that anonymous authentication is enabled for the virtual directory.

Choosing a DNS Alias for the HTTP Publishing Point

You should create a generic DNS alias (CNAME) that resolves to the IIS server hosting the CDP and AIA, for example, www.woodgrovebank.com. This DNS alias should be used when configuring the CDP and AIA paths for the CAs in subsequent sections. Use of this alias allows you to easily move the CA publishing points to a different server or network location in the future without having to reissue the CA certificates.

Verifying IIS Installation

You should verify the basic operation of IIS before proceeding. If any of the following tests fail, you should re-check the IIS installation and configuration against the previous steps in this section.

▶ **To verify correct operation of the IIS virtual directory**

1. Log on to the IIS server (issuing CA) as a member of local Administrators, and then create a file using a text editor such as Notepad. Enter some recognizable text (it is not important what the text is, and it requires no HTML tags). For example:

```
Hello World
```

2. Save the file as **test.htm** in the folder that you created for publishing the CDP and AIA information in the previous steps – C:\CAWWWPub. Save the same file as **test.asp** in the same folder.

3. Open a browser and type in the Uniform Resource Locator (URL) to try to retrieve the pages:

   http://*www.woodgrovebank.com*/pki/test.htm

Note: If you have not yet set up this alias in DNS you can temporarily enter it in the local hosts file (%systemroot%\system32\drivers\etc\hosts) against the IP address of the IIS server. Alternatively, you can use the real host name of the IIS server in place of the alias. However, note that you will need to check the correct working of the DNS alias at a later stage.

---

4. You should see the text "Hello world" (or whatever you entered in Step 1) displayed in the browser.

▶ **To verify that Execute permission has been disabled**

1. Open a browser and type in the following URL to try to retrieve the pages:

   http://*www.woodgrovebank.com*/pki/test.asp

2. The following error message (or a similar message) should display in the browser:

```
The page cannot be displayed

You have attempted to execute a CGI, ISAPI, or other executable
program from a directory that does not allow programs to be
executed.
```

   The following error code should also display:

```
HTTP Error 403.1 - Forbidden: Execute access is denied.

Internet Information Services (IIS)
```

You need to ensure that anonymous access to the site has been enabled. Because Microsoft Internet Explorer will automatically and silently attempt to authenticate a user to a Web site, it is sometimes difficult to determine whether anonymous access has been used instead of authenticated access. One method is to change your Internet Explorer zone security settings to force the use of anonymous logon and repeat the previous tests. As an alternative, you can perform the following procedure, which uses telnet.exe to force unauthenticated access. This procedure assumes that you are testing the Web site from the IIS server itself; it will not work across a proxy server.

▶ **To verify that anonymous access has been enabled**

1. Run the `telnet` program at a command prompt.
2. At the telnet prompt, type the following command to turn on local display of typed characters:

```
set localecho
```

3. Type the command to connect to IIS using the DNS alias that you defined earlier:

   open *www.woodgrovebank.com* 80

4. Type the following text (exactly as shown, including case) to retrieve the test.htm page:

```
GET /pki/test.htm
```

Note: The cursor will have returned to the top of the screen, meaning that the typed text is overwriting existing text on the screen, which results in a slightly garbled display. You can safely ignore it.

If you make a mistake typing, press RETURN, and then type the **open** command (as in step 3) again to reconnect and retry the **GET** command.

---

5. You should see the following output:

```
Hello world
Connection to host lost.
Press any key to continue...
```

6. Type **`quit`** to exit telnet.

If all three tests in this section completed correctly, delete the test.htm and test.asp files from the Web server folder.

Installing and Configuring Additional Operating System Components

This section describes the installation and configuration of other components required on the servers. You should follow these procedures for both the root CA and issuing CA servers.

Removing Update Root Certificates Service

You should remove the Update Root Certificates service. This is an optional component that is installed by default. It is not desirable to have the root trust of your CAs automatically updated. In any case, the service will not work if it cannot access the Internet and will log errors to the event log. Obviously, the offline CA will have no network access, but you should also block any inbound or outbound connectivity between the issuing CA and the Internet, as discussed earlier.

▶ **To remove the Update Root Certificates service**

- Run the following at a command prompt:

```
sysocmgr /i:sysoc.inf /u:C:\MSSScripts\OC_RemoveRootUpdate.txt
```

This command configures the Optional Components Manager to use the component configurations specified in the following C:\MSSScripts\OC_ RemoveRootUpdate.txt file:

```
[Components]
rootautoupdate = Off
```

Checking Service Packs and Security Updates

You should re-check the service pack and update list installed at this point (since additional components such as IIS may have been installed). Use a tool such as Microsoft Baseline Security Analyzer (MBSA) to perform the check; obtain any required updates; and, after suitable testing, install them on the server(s).

For instructions on using MBSA, see the link provided in the "More Information" section at the end of the chapter.

Note: You will need to separately download the current Microsoft security update list, mssecure.xml, so that you can run MBSA offline. This is described in the MBSA documentation at the MBSA link.

Installing Additional Software

This section describes the installation of additional software required on the CAs.

CAPICOM

CAPICOM 2.0 (the current version is actually 2.0.0.3) is required on the root CA and the issuing CA for some of the setup and management scripts supplied with this solution. Information about where to find the latest version of CAPICOM is in the "More Information" section at the end of this chapter.

Follow the instructions in the self-extracting executable to install and register the CAPICOM dynamic-link library (DLL) library.

Windows Server 2003 Support Tools

Although not strictly necessary, it is helpful to have the Windows 2000 Support Tools installed on the issuing CA server. Several of the tools are useful for certain CA operations, and others can help with troubleshooting. You can install the Support Tools from the Windows installation CD (Suptools.msi in Support\Tools).

Preparing Active Directory for the PKI

This section describes how to prepare Active Directory for the installation of Windows Server 2003 Certificate Services.

Active Directory Schema Preparation

There are a few fundamental requirements on the Active Directory domain infrastructure for this solution. These requirements vary depending on whether the solution is being installed in a Windows 2000 Active Directory environment or one that has been upgraded to (or natively installed as) Windows Server 2003 Active Directory.

Requirements for All Versions of Active Directory

This solution has a minimum domain functional level requirement of Windows 2000 Native Mode, at least for the domain into which the certificate authority servers are installed. This requirement is necessary because the solution uses Active Directory Universal groups, which are first available in Windows 2000 Native Mode. If the domain does not meet this requirement, you need to change it following the instructions in the product documentation (see the "More Information" section at the end of this chapter).

Note: The default domain functional level of Active Directory is always Mixed mode, even if you have installed it using only Windows 2003 Active Directory domain controllers. You need to raise it from this level before continuing. If you cannot raise the domain level from Mixed mode because you need to support Microsoft Windows NT® version 4.0 domain controllers, you will need to manually create domain global groups in place of universal groups.

The solution assumes an Active Directory forest with the default Windows 2000 forest functionality level, at a minimum. You do not need to change this. For further information about these concepts, see the reference at the end of this chapter.

Installing in a Windows 2000 Domain

Important: Although Microsoft supports the installation and use of Windows Server 2003 Certificate Services in a domain using Windows 2000 domain controllers, this solution has not been fully tested with such a combination.

If the solution is to be installed into a Windows 2000 Active Directory forest, you must update the directory schema for the Windows 2003 Certificate Services installation to work correctly. You must also ensure that all Windows 2000 domain controllers have Service Pack 3 (or later) applied. The service pack is required for the schema update tool to work correctly and so that the domain controllers support LDAP (Lightweight Directory Access Protocol) signing. LDAP signing is a security enhancement required by Windows Server 2003 CAs and Windows XP clients using certificate autoenrollment.

Many of the features of Windows 2003 Certificate Services (such as user autoenrollment and editable templates) require a Windows Server 2003 version of the Active Directory schema. However, this requirement does not mean that any or all of the domain controllers need to be running Windows Server 2003. It is simply that Windows Server 2003 Certificate Services requires particular schema extensions that are not present in the Windows 2000 Active Directory schema. You can update the directory schema by using the ADPrep.exe tool, which is available in the i386 folder of the Windows Server 2003 distribution media.

To use Adprep, you must have applied Service Pack 3 to your Windows 2000 domain controllers (Adprep will work with Service Pack 1 plus some post-SP1 updates, although since SP3 is needed anyway this is not especially relevant). Do not attempt to use this tool without ensuring that all domain controllers are at the correct patch level.

Warning: Use of this tool causes an irreversible change to your directory schema. Although the procedure is safe, make sure to read the related documentation thoroughly before commencing.

On the forest Schema Master domain controller, run the following command:

```
ADPrep /ForestPrep
```

You must be a member of Schema Admins to perform this task or request that an administrator who has the correct permissions make this change for you.

For more information about the ADPrep tool, see the reference at the end of this chapter.

Verifying Active Directory Readiness

You can verify the domain functional level and schema version with the following steps.

▶ **To verify the domain functional level**

1. Open Active Directory Users and Computers.
2. View the properties of the Domain object.
3. On the **General** tab, you should see the **Domain Functional Level** listed as one of the following:
   - Windows 2000 native
   - Windows Server 2003

▶ **To verify the correct schema version**

1. At a command prompt, type the following (be sure to substitute the DN of your forest root domain):

   ```
   dsquery * "cn=schema,cn=configuration,
           DC=woodgrovebank,DC=com" -scope base -attr
           objectversion
   ```

   (This command is displayed on more than one line; enter it as a single line.)

   Note: You will need to run this command from a Windows 2003 server. Dsquery.exe is not available by default on Windows XP or Windows 2000.

   ---

2. The output should show the schema version of 30 (or higher) as follows:

   ```
   objectversion
   30
   ```

Active Directory Groups and Users

This section describes the creation of the Active Directory security groups and user accounts that the CAs use.

Creating PKI and CA Administration Groups

Administrative roles and capabilities are defined using domain user accounts and security groups.

Note: This solution defines multiple security groups corresponding to separate administrative roles. This approach provides a lot of control over how you can delegate responsibilities over the CA administration. However, you should not feel that you *have* to use all or any of these roles if they do not correspond to your administration model. In the extreme, if you only have a single PKI administrator who looks after all aspects of the service, you can add this account to all role groups on the CA. In practice, most organizations use some role separation, but very few will use all of the role separation capabilities of Certificate Services.

▶ To create CA administration groups in the domain

1. Log on to a domain member computer with an account that has sufficient permissions to create user and group objects in the Users container.
2. Run the following command to create the domain CA management groups:

```
Cscript //job:CertDomainGroups C:\MSSScripts\ca_setup.wsf
```

This script creates the security groups listed in the following table. The groups are created as Universal groups in the domain Users container and should then be moved to a more appropriate organizational unit (OU). (An illustration of a suitable OU structure is shown in later section.)

Caution: This script creates security groups that will be assigned a great deal of power within the Active Directory forest. You should be very careful who is made a member of these groups. Specifically:

Enterprise PKI Admins. This is an extremely powerful group. It will have complete control over the PKI throughout the Active Directory forest, including the ability to install and replace root and enterprise CAs, change root trusts, and install cross certificates. Treat it with the same caution used for the Enterprise Admins group.

Enterprise PKI Publishers. Although this sounds innocuous, this group also has powerful capabilities. It will have the ability to install and remove trusted root CAs and cross certificates for the entire forest. Although not as powerful as Enterprise Admins, you must still treat it with caution.

Table 7.7: Group Names and Purposes

Group name	Purpose
Enterprise PKI Admins	Administrators of Public Key Services configuration container.
Enterprise PKI Publishers	Allowed to publish CRLs and CA certificates to Enterprise configuration container
CA Admins	Have full administrative capability over the CA, including determining the membership of other roles
Certificate Managers	Manage certificate issuance and revocation
CA Auditors	Manage audit data for CA
CA Backup Operators	Have permissions to back up and restore CA keys and data

---

Notes:

If you require separate CA administrators, certificate managers, auditors, and backup operators for each enterprise CA, you should create separate domain groups for each CA instead of single enterprise-wide groups as shown here. Name them *CAName* CA Admins or something similar.

Most of these domain groups have equivalent local groups created on offline CAs.

The CA server local Administrators group also serves an important role in the management of a CA. This group exists on Windows servers by default.

For a multi-domain forest, you should create these groups in the same domain as the certificate servers; this is the approach assumed in the remainder of this guidance. (Because these are Universal groups, you can use them to administer CAs installed in any forest domain.)

Creating PKI and CA Administration Test Users

For the purposes of testing and illustration, the script in this section creates generic user accounts corresponding to each of the roles defined by the administration groups created earlier. However, if the actual accounts to be used already exist at this point, or they have been defined and you are able to create them, you should ignore this step and use those accounts instead.

▶ **To create test CA Administration user accounts**

1. Log on to a domain member computer with an account that has sufficient permissions to create user and group objects in the Users container.
2. Create test domain user accounts for individuals who will administer the CA by running the following script:

   ```
   Cscript //job:CertDomainTestAccts C:\MSSScripts\ca_setup.wsf
   ```

   The script sets random passwords on all of the accounts (rather than leaving them with blank passwords). Make a note of these from the script output, or reset the auto-assigned passwords to ones of your own choosing.

Caution: Using generic accounts such as these with passwords shared among administrators makes auditing virtually impossible. In anything other than a test environment, you should always use accounts that you can trace to unique individuals.

The script creates the domain accounts described in the following table. The script creates users in the Users container, and you should move them to a more appropriate OU. (An illustration is provided in a subsequent section.)

Table 7.8: Account Names and Purposes

User account	Purpose of account
EntPKIAdmin	Administrator of Public Key Services configuration container
EntPKIPub	Allowed to publish CRLs and CA certificates to Enterprise configuration container
CAAdmin	Has full administrative capability over the CA, including determining the membership of other roles
CertManager	Manages certificate issuance and revocation
CAAuditor	Manages audit data for CA
CABackup	Has permissions to back up and restore CA keys and data

Note: The test accounts illustrate the most complex administration role configuration–where each CA role corresponds to a separate individual (user account). However, there is usually little benefit in having separate accounts for each role unless you actually have separate individuals performing those roles. It is acceptable to have single user accounts in multiple role groups–or even in all role groups–if this more accurately reflects your administrative structure. See the subsequent section, "Creating a Simplified Administration Model for the Enterprise CAs."

Populating CA Administration Groups

You should populate the CA Administration groups with the accounts of the appropriate administration personnel of your organization. For a full description of how these groups map to the administrative roles of the Certificate Services infrastructure, see the "Management Roles" section in Chapter 4, "Designing the Public Key Infrastructure." For a fuller discussion of Windows Server 2003 Certificate Services administrative roles, see the "Role-based Administration" topic on online Help or see the reference at the end of this chapter.

Note: If you have created the test domain accounts, you must still manually add them as members of their corresponding security groups. As a security precaution, the script does not perform this step by default.

The setup procedures in the remainder of this document require that you perform some of the setup actions using accounts that are members of Enterprise PKI Admins, Enterprise PKI Publishers, and CA Admins. This approach avoids the need to use Enterprise Admins or Domain Admins privileges any more than absolutely necessary.

Note: It is possible to enforce strict role separation in Windows Server 2003 Certificate Services (Enterprise Edition only). This means that any account that is assigned more than one role (either directly or through group membership) is barred from all administrative roles on the CA. This option is not enabled in the product by default or in this solution, so it is acceptable to have the same user account assigned to multiple administrative roles if that is appropriate for your organization.

Creating a Simplified Administration Model for the Enterprise CAs

The test accounts and administrative groups illustrate the most complex administration role configuration–where each CA role corresponds to a separate individual (user account). However, it is quite legitimate to have single accounts in multiple role groups–or even in all role groups–if this more accurately reflects your administrative structure.

Many organizations will use just three roles: CA administrator, auditor, and backup operator. These roles are shown in the following table (using a subset of the test accounts created earlier for illustration).

Table 7.9: Simplified Administration Model Group Assignment

Simplified administration role user account	Group memberships of the user account
CAAdmin	Enterprise PKI Admins CA Admins Certificate Managers Administrators (local administrators of CA)
CAAuditor	CA Auditors Administrators (local administrators of CA)
CABackup	CA Backup Operators

Using this arrangement, the CAAdmin account would be able to perform all administrative tasks on enterprise CAs (including certificate approval and revocation) and would have administrative control of all enterprise PKI configuration information in the Active Directory (permissions for all of these are set later in the document).

Suggested Domain OU Structure for CA and Certificate Template Management

There are a number of groups and user accounts associated with the management and operation of a PKI. You should organize these groups and user accounts into OUs to allow for easier management. The following table shows a suggested OU structure and describes the purpose of each OU (the indented items are child OUs of the Certificate Services OU).

You must grant the Enterprise PKI Admins group permissions to create and delete groups and users in the Certificate Services OU and all child containers.

Table 7.10: Example OU Structure

OU	Purpose
Certificate Services	Parent OU.
\—Certificate Services Administration	Contains administrative groups for managing CAs and Enterprise PKI configuration.
\—Certificate Template Management	Contains groups for managing individual certificate templates.
\—Certificate Template Enrollment	Contains groups that are granted Enroll or Autoenroll permissions on templates of the same name. Control of these groups can then be delegated to appropriate personnel to allow flexible enrollment regime without touching the templates themselves.
\—Certificate Services Test Users	Contains temporary test accounts.

For more discussion of the uses of these OUs and the groups contained in them, see the relevant sections of Chapter 11, "Managing the Public Key Infrastructure."

▶ To create the Certificate Services OU administration hierarchy

1. Log on using an account with permissions to create OUs and to delegate permissions within those OUs. (As creator of the new OUs, you will always be able to grant yourself permission to delegate control of those OUs.)
2. Create the OU structure shown in the previous table at an appropriate location in your domain. (It is assumed, but not essential, that this is the forest root domain.)
3. Grant permissions to the Enterprise PKI Admins group to create and delete groups in the Certificate Services OU and all child containers.

Note: This OU structure is given only as an example. There is no requirement to adopt this structure.

Active Directory Public Key Services Security

This section describes how to delegate control over the Public Key Services container to the PKI administration security groups.

Granting Permissions to the Public Key Services Container

The forest–wide PKI configuration information is stored in the Active Directory Configuration container. Permissions to change this container and all its sub-containers and objects are limited by default to the Enterprise Administrators security group.

You must alter the security on the Public Key Services container for the following reasons:

- To enable Enterprise PKI Admins to install Enterprise CAs and to configure certificate templates without needing to be a member of the Enterprise Admins security group.
- To enable Enterprise PKI Publishers to publish certificate revocation lists and CA certificates without needing to be a member of Enterprise Admins.

You will need to request that a member of the Active Directory Enterprise Admins group perform the first procedure for you unless you are a member of this group.

Caution: This procedure delegates a very sensitive portion of the Active Directory, one that affects users and computers throughout the forest. You should be extremely careful to whom control over the Public Key Services container is granted. Accounts with permissions to control this container can, among other things, add and remove trusted root CAs, add and remove Enterprise CAs, and create valid credentials for any user in the forest.

▶ To grant permissions to Enterprise PKI Admins

1. Log on as a member of the Enterprise Admins security group.
2. In the Active Directory Sites and Services Microsoft Management Console (MMC) snap-in, display the **Services** node (from the **View** menu). Navigate to the Public Key Services subcontainer and open its properties.
3. On the **Security** tab, add the Enterprise PKI Admins security group and grant **Full Control** to this group.
4. In **Advanced** view, edit the permissions of this group to ensure that **Full Control** applies to **This object and all child objects**.
5. Select the Services container and open its properties.

6. On the **Security** tab, add the Enterprise PKI Admins security group and grant **Full Control** to this group.
7. In **Advanced** view, edit the permissions of this group to ensure that **Full Control** applies to **This object** only.

▶ **To grant permissions to Enterprise PKI Publishers**

1. Log on as a member of the Enterprise PKI Admins (or Enterprise Admins) security group.
2. In the Active Directory Sites and Services MMC snap-in, display the **Services** node and open the properties of the Public Key Services\AIA container.
3. On the **Security** tab, add the Enterprise PKI Publishers security group and grant the following permissions to this group:
   - Read
   - Write
   - Create All Child Objects
   - Delete All Child Objects
4. In **Advanced** view, edit the permissions of this group to ensure that the permissions are applied to **This object and all child objects**.
5. Repeat steps 2-4 for the following containers:
   - Public Key Services\CDP
   - Public Key Services\Certification Authorities

Note: After permissions have been granted to Enterprise PKI Admins in the previous procedure, a member of this group can grant permissions to Enterprise PKI Publishers.

Granting Permissions to the Cert Publishers Group

The Cert Publishers security group contains the computer accounts of all Enterprise CAs in the domain. This group is used to apply permissions to user and computer objects and to the objects in the CDP container mentioned in the previous procedure. When a CA is installed, its computer account needs to be added to this group. By default, only Domain Admins, Enterprise Admins or the built-in domain Administrators groups have permissions to modify the membership of Cert Publishers. To enable members of Enterprise PKI Admins to install enterprise CAs you must change the permissions on this security group.

▶ **To grant the modify membership permission on Cert Publishers**

1. Log on as a member of Domain Admins (of the domain in which the issuing CA is to be installed).
2. Open the Active Directory Users and Computers MMC snap-in.
3. From the **View** menu of the MMC ensure that **Advanced Features** is enabled.
4. Locate the Cert Publishers group (by default in the Users container) and view the properties of the group.
5. From the **Security** tab, **Add** the group **Enterprise PKI Admins** and click the **Advanced** button.
6. Select the group **Enterprise PKI Admins** from the list and click the **Edit** button.

7. Select the **Properties** tab, ensure **This Object Only** is selected in the **Apply onto**: box.
8. Scroll down and click the **Write Members** box in the **Allow** column.
9. Close all of the dialogs, saving the changes by clicking **OK** for each one.
10. You will need to restart the issuing CA server before installing the Certificate Services component. Restarting the computer allows the server to pick up the new group membership in its access token.

Granting Restore Permissions to Enterprise PKI Admins

To install Enterprise CAs you need to have the right to Restore Files and Directories in the domain in which you are installing the CA. The Certificate Services installation process requires this user right in order to install certificate templates into the domain. More specifically, this right is required to allow security descriptors on the templates and other directory objects to be merged, thus granting the correct permissions to domain PKI objects. The built-in domain groups Administrators, Server Operators and Backup Operators have this right by default.

Because you will be using the group Enterprise PKI Admins to perform the CA installation you must grant the user right Restore Files and Directories to this group.

▶ **To grant the Restore rights to Enterprise PKI Admins:**

1. Log on as a member of Domain Admins (of the domain in which the issuing CA is to be installed).
2. Open the Active Directory Users and Computers MMC snap-in.
3. Select the Domain Controllers OU and open the properties of that OU.
4. On the Group Policy tab, select the **Default Domain Controllers Policy** GPO and click **Edit**.
5. Navigate to Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment and double-click the item **Restore Files and Directories**.
6. Add the group Enterprise PKI Admins to the list shown.
7. Close the dialog box and the GPO editing MMC.

Important: If you have any other GPOs that set the **Restore Files and Directories** user right on the domain controllers, you must carry out the above procedure on the GPO with the highest priority instead of the **Default Domain Controllers Policy**. User rights settings are not cumulative, and only the last applied GPO (that is, the one with the highest priority) that has this right set will be effective.

Verification

You can verify creation of the groups, users, and OUs using the Active Directory Users and Computers MMC and browsing to the users and groups. The users should be members of the appropriate groups (whether you are using the test users or the real PKI administration user accounts).

You can verify the correct application of permissions to the Public Key Services container by performing the following steps. You will need a copy of the Windows Server 2003 Support Tools installed on the system on which you carry out this procedure. This procedure does not have to be performed on a CA.

Note: In the following procedures, instead of logging on with different user accounts, you can use Runas or the **Run As** context menu option in Windows Explorer to run the ADSIEdit MMC in the context of the required users.

▶ **To verify Public Key Services permissions**

1. Log on to a domain member server (such as, the issuing CA server) as a member of Enterprise PKI Admins.
2. Run mmc.exe and load the ADSI Edit snap-in.
3. Right-click the ADSI Edit folder, select **Connect to**, and then select **Configuration** from the **Select a Well Known Naming Context** drop-down list.
4. Navigate to the Public Key Services container and right-click this container. Then select **New**, and **Object**.
5. Select **Container** from the list and give it a name such as **Test**.
   The container object should be created successfully in the Public Key Services container.
6. Delete the container object that you just created.
7. You should be unable to create a container object anywhere in the Configuration container apart from the Services container and its child containers.
8. Log on as a member of Enterprise PKI Publishers.
9. Load ADSIEdit and connect to the **Configuration** naming context (NC).
10. Try to create a container object in the Public Key Services container. Your attempt should fail.
11. Create a test object (a container object) in each of the AIA, CDP, and Certification Authorities subcontainers.
12. Remove these test objects after verifying that they have been created successfully.

Caution: Be extremely careful to delete only the test objects that you have created. Members of Enterprise PKI Admins, in particular, now have sufficient permissions to delete the entire Public Key Services container.

Note: If you chose not to install the Windows Server 2003 support tools, ADSIEdit will not be available. You can perform these verification steps from the command line by using the built-in utilities dsadd.exe and dsrm.exe. However, you should be very careful to use the correct syntax and directory object paths when using these utilities. Test the commands carefully on a test system before using them in a production Active Directory forest.

Securing Windows Server 2003 for Certificate Services

This section describes how to apply security policies and other security measures to Windows Server prior to installing Certificate Services. You should also read the section on Physical Security in Chapter 4, "Designing the Public Key Infrastructure."

Implementing Security on the Root CA Server

The following sections describe the configuration of local groups and user accounts and the application of security policy to the CA server.

Creating Local User Accounts and Security Groups on the Root CA

Because the root CA is not part of a domain, administrative roles and capabilities are defined using local user accounts and security groups.

▶ **To create local user accounts and groups on the root CA server**

1. On the root CA, run the following script to create local CA management groups:

   ```
   Cscript //job:CertLocalGroups C:\MSSScripts\ca_setup.wsf
   ```

   The script creates the local groups described in the following table.

   Table 7.11: Group Names and Purposes

Group name	Purpose
CA Admins	Have full administrative capability over the CA, including determining the membership of other roles.
Certificate Managers	Manage certificate issuance and revocation.
CA Auditors	Manage audit data for CA.
CA Backup Operators	Have permissions to back up and restore CA keys and data.

2. Create local user accounts for the people who will administer the CA. For the purposes of testing and illustration, generic local accounts corresponding to each of the roles defined by the previous groups are created by the following script. However, you should skip this step if you are able to create the actual accounts at this time. Create those accounts instead.

   ```
   Cscript //job:CertLocalTestAccts C:\MSSScripts\ca_setup.wsf
   ```

   The script uses CAPICOM to generate pseudo-random passwords on all of the accounts (instead of leaving them with blank passwords). Make a note of these from the script output or reset the passwords to ones of your own choosing.

   Note: Using generic accounts with passwords shared among administrators makes audit trails virtually meaningless. In a high-security production environment you should always use accounts that you can trace to unique individuals.

   The script creates the local accounts listed in the following table.

Table 7.12: Account Names and Purposes

Account name	Purpose
CAAdmin	Has full administrative capability over the CA, including determining the membership of other roles.
CertManager	Manages certificate issuance and revocation.
CAAuditor	Manages audit data for CA.
CABackup	Has permissions to back up and restore CA keys and data.

Note: The test accounts illustrate the most complex administration role configuration; where each CA role corresponds to a separate individual (user account). However, there is little benefit in having separate accounts for each role unless you actually have separate individuals performing those roles. It is acceptable to have single accounts in multiple role groups–or even in all role groups–if this more accurately reflects your administrative structure.

3. Add these user accounts to the administration security groups as appropriate. Use the following table for the test accounts, or use your own accounts according to your organization's defined IT roles and security policy.

Table 7.13: Account Names and Group Memberships

Account name	Group membership
CAAdmin	CA Admins
CertManager	Certificate Managers
CAAuditor	–CA Auditors –Administrators
CABackup	CA Backup Operators

Note: You can also make members of the CA Admins group members of the local administrators group. There are certain tasks that require local administrative privileges, and you may want to combine these with the CA Admins role.

Creating a Simplified Administration Model for the Root CA

Most organizations will not require an administration structure as complex as the one shown in the previous procedure. Some organizations may not need any role separation; many will use three roles: CA administrator, auditor, and backup operator. These roles are shown in the following table (using a subset of the test accounts created earlier)

Table 7.14: Simplified Administration Model Group Assignment

Simplified administration role	Group membership
CAAdmin	CA Admins Certificate Managers Administrators
CA Auditor	CA Auditors Administrators
CABackup	CA Backup Operators

Verifying Groups and Accounts

Verify the creation of groups, users, and group memberships by looking at the Users & Groups node of the Computer Management MMC.

Applying System Security Settings on the Root CA Server

The CA servers are secured by using the Enterprise Client Certificate Services role defined in the guidance in the *Windows Server 2003 Security Guide* (see the reference in the "More Information" section at the end of this chapter).

The root CA is not a member of a domain and cannot use domain Group Policy, so the security templates and procedures must be applied manually. Obtain the following security templates from the *Windows Server 2003 Security Guide* and copy them to the C:\MSSScripts folder on the root CA server:

- Enterprise Client–Domain.inf
- Enterprise Client–Member Server Baseline.inf
- Enterprise Client–Certificate Services.inf

Customize the security templates and apply them to the server according to the following procedure.

▶ **To customize security templates**

1. Log on as a member of local Administrators and load Enterprise Client–Certificate Services.inf into the Security Templates MMC.
2. In Local Policies\Security Options, change the following items in accordance with your organization's security standards:
   - Accounts: Rename administrator account: *NewAdminName*
   - Accounts: Rename guest account: *NewGuestName*
   - Interactive logon: Message text for users attempting to log on: *LegalNoticeText*
   - Interactive logon: Message title for users attempting to log on: *LegalNoticeTitle*

   Note: You should determine the value of these items based on your organization's current policies. You do not have to configure these values, although it is recommended that you do so.

3. In Local Policies\User Rights Assignment, add local group CA Auditors to the **Manage Auditing and Security Log** user right.
4. In Local Policies\User Rights Assignment, add local group CA Backup Operators to the following user rights:
   - Back up files and directories
   - Restore files and directories

5. In Local Policies\User Rights Assignment, add the following local groups to the **Allow Log on Locally** right:
   - Administrators
   - Backup Operators
   - CA Admins
   - Certificate Managers
   - CA Auditors
   - CA Backup Operators
6. Open the properties of the following services in the System Services folder, and click **Define this policy setting in the template**. Accept the default permissions by clicking **OK**. Set the value of **Set service startup mode** to **Automatic**.
   - Removable Storage
   - Volume Shadow Copy
   - MS Software Shadow Copy Provider

   Note: These services are disabled in the member server baseline security template but are required by NTBackup.exe.

7. With the template selected, save the template changes (by clicking **Save** on the **File** menu), and then close the MMC.
8. Run the following commands in the specified order to apply the required security templates. The Secedit tool may indicate that some warnings were generated– these messages can safely be ignored (errors should be investigated, though):

```
secedit /configure /db %temp%\casec.db /cfg
        "C:\MSSScripts\Enterprise Client - Domain.inf" /overwrite
        /log "%temp%\Enterprise Client - Domain.log"
secedit /configure /db %temp%\casec.db /cfg
        "C:\MSSScripts\Enterprise Client–Member Server
        Baseline.inf" /log "%temp%\Enterprise Client–Member Server
        Baseline.log"
secedit /configure /db %temp%\casec.db /cfg
        "C:\MSSScripts\Enterprise Client - Certificate Services.inf"
        /log "%temp%\Enterprise Client - Certificate Services.log"
```

   (These commands display on more than one line; enter them as single lines.)

Note: The *Windows Server 2003 Security Guide* contains a more detailed discussion of these security settings.

Verifying Security Settings

To verify the correct application of security settings, perform the following procedure.

▶ **To verify the root CA security settings**

1. View the secedit logs produced in the previous section and verify that no major errors were logged. (It is normal to see a number of warnings and minor errors but nothing that should cause the application of the security template to fail.)
2. Restart the server and verify that all expected services start and that no errors are logged to the system event log.
3. Attempt to log on with the test accounts (or real accounts) that you have created. You should see the legal notice text, and you should be able to log on.

Implementing Security on the Issuing CA Server

The following sections describe application of security policy to the CA server.

Applying System Security Settings on the Issuing CA Server

The CA servers are secured by using the Certificate Services role defined in the *Windows Server 2003 Security Guide*. Since the issuing CA is a member of a domain, the security policy settings are applied by using domain-based Group Policy.

You will need to create a suitable OU structure that will hold the CA server computer objects and a GPO structure to apply the security settings. You must create three GPOs:

- Enterprise Client–Member Server Baseline
- Enterprise Client–Certificate Services
- Enterprise Client–Certificate Services IIS (only needed if IIS installed on the CA)

Note: The *Windows Server 2003 Security Guide* also includes recommended settings for the Domain Policy (password and account lockout policies). These settings are inherited by all computers in the domain. If you do not want to modify your domain-level policy but want to use the recommended settings for the issuing CA, you should also create a fourth GPO linked to the CA OU:

Enterprise Client–Certificate Services Account Policies

You should follow the following procedure to import the Domain Policy template into this GPO. These settings will only affect local accounts on the CA itself.

The following procedure outlines how you might create the OUs and GPOs for your organization. The GPO and OU names are only examples; you should adapt the procedure to your own domain OU and GPO standards.

▶ To create the CA server OUs and GPOs

1. Obtain the following security templates from the *Windows Server 2003 Security Guide*:
   - Enterprise Client–Domain
   - Enterprise Client–Member Server Baseline
   - Enterprise Client–Certificate Services
   - Enterprise Client–IIS Server (only required if IIS is installed on the CA)
2. Log on as a member of Domain Administrators or a user who has rights to create the OUs described in step 4. You will also need to be a member of Group Policy Creator Owners.
3. Open the Active Directory Users and Computers MMC snap-in.
4. Create the following OU structure:

```
woodgrovebank.com (domain)
    Member Servers
        CA
```

5. Open the properties of the domain container, and from the **Group Policy** tab click **New** to create a new GPO. Name it **Domain Policy**
6. Edit the GPO and navigate to Computer Configuration\Windows Settings\Security Settings. Right-click the Security Settings folder and then select **Import**. Browse to the Enterprise Client - Domain.inf file and select that as the template to import.
7. Close the GPO.
8. Repeat the previous three steps for the combination of OUs, GPOs, and security templates shown in the following table.

Table 7.15: Mapping of GPOs to Security Templates and OUs

OU	GPO	Security template
Member Servers	Enterprise Client—Member Server Baseline	Enterprise Client—Member Server Baseline.inf
CA	Enterprise Client—Certificate Services	Enterprise Client—Certificate Services.inf
CA	(Optional—see note above) Enterprise Client—Certificate Services Account Policies	Enterprise Client—Domain.inf
CA	(Optional—if IIS on CA) Enterprise Client—Certificate Services IIS	Enterprise Client—IIS Server.inf

Note: If you have opted to install IIS on the issuing CA (as described in this chapter), you will need to create a separate IIS GPO just for the CAs. Although you might also have an IIS GPO for your intranet IIS servers, it is strongly recommended that you create a separate GPO for use exclusively by the CAs. This approach ensures that any changes to the IIS GPO will not affect the security of the CAs, and the CA security settings remain entirely under the control of the CA GPO administrators.

After you have created the GPOs and imported the templates, you must customize the settings in the GPOs and apply them to the Certificate Services computers according to the following procedure.

▶ To customize and apply the Certificate Services GPO

1. From Active Directory Users and Computers, edit the Enterprise Client–Certificate Services GPO. In Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options, change the following items in accordance with your organization's security standards:
   - Accounts: Rename administrator account: *NewAdminName*
   - Accounts: Rename guest account: *NewGuestName*
   - Interactive logon: Message text for users attempting to log on: *LegalNoticeText*
   - Interactive logon: Message title for users attempting to log on: *LegalNoticeTitle*
2. In Local Policies\User Rights Assignment, add the CA Auditors domain group to the **Manage Auditing and Security Log** user right.
3. In Local Policies\User Rights Assignment, add the CA Backup Operators to the following user rights:
   - Back up files and directories
   - Restore files and directories
4. In Local Policies\User Rights Assignment, add the following local and domain groups to the **Allow Log on Locally** right:
   - (local) Administrators
   - (local) Backup Operators
   - (domain) Enterprise PKI Admins
   - (domain) Enterprise PKI Publishers
   - (domain) CA Admins
   - (domain) Certificate Managers
   - (domain) CA Auditors
   - (domain) CA Backup Operators
5. In **File System**, add the folder D:\CertLog. Ensure that the permissions are as shown in the following table.

Table 7.16: CA Database Folder Permissions

User/Group	Permission	Allow/Deny
Administrators	Full Control	Allow
System	Full Control	Allow
Backup Operators	Full Control	Allow
CREATOR OWNER	Full Control	Allow

6. For the same folder, add the audit entries shown in the following table for the Everyone group (click the **Advanced** button in the **Security** dialog box, and then click the **Auditing** tab). Type **Everyone** when prompted for a user or group name. Adding the Everyone group will display a dialog box entitled **Auditing entry for D:\CertLog** into which you can enter the detailed auditing settings. Ensure that **This Folder, subfolders and files** is selected in the **Apply onto** field. Select all of the items where Yes is shown in the table.

Table 7.17: CA Database Folder Auditing

Permission	Successful	Failed
Full Control		Yes
Traverse Folder/Execute File		Yes
List folder/read data		Yes
Read attributes		Yes
Read extended attributes		Yes
Create files/write data	Yes	Yes
Create folders/append data	Yes	Yes
Write attributes	Yes	Yes
Write extended attributes	Yes	Yes
Delete subfolders and files	Yes	Yes
Delete	Yes	Yes
Read permissions		Yes
Change permissions	Yes	Yes
Take Ownership	Yes	Yes

7. Open the properties of the following services in the System Services folder, and then click **Define this policy setting in the template**. Accept the default permissions by clicking **OK**. Set the value of **Set service startup mode** to **Automatic**.
   - Removable Storage
   - Volume Shadow Copy
   - MS Software Shadow Copy Provider
   - Task Scheduler

   Note: These services are disabled in the member server baseline security template, but the first three are required by NTBackup.exe. The Task Scheduler service is required by some of the operational scripts.

8. Move the issuing CA computer account into the Certificate Services OU.
9. On the issuing CA (the server onto which the CA will be installed), run the following command to apply the GPO settings to the computer:

```
gpupdate
```

Note: The *Windows Server 2003 Security Guide* contains more detailed discussion of these security settings.

Verifying Security Settings

To verify the correct application of security settings, perform the steps in the following procedure.

▶ **To verify the root CA security settings**

1. Check the Application Event log for events from the SceCli source. There should be an event ID 1704 following the execution of the **gpupdate** command. The text of the event should read as follows:

   ```
   Security policy in the Group policy objects has been applied
   successfully.
   ```

2. Restart the server and verify that all expected services start up and that no errors are logged to the system event log.
3. Attempt to log on with the test accounts (or real accounts) that you have created. You should see the legal notice text, and you should be able to log on.

Configuring Terminal Services Security on the Issuing CA

You should disable Terminal Services on the issuing CA because it provides an additional means for an intruder to attack the CA and significantly reduces the effect of any physical security measures that are protecting the server. If you must leave it enabled (for remote administration purposes), you should configure the settings described in the following table.

Note: The state of Terminal Services on the root CA is irrelevant because it is not connected to the network.

These settings should be configured in the Certificate Services Security GPO or another GPO that applies to the online CA(s).

Table 7.18: Settings to Configure in Computer Configuration\Administrative Templates\Windows Components\Terminal Services

Settings path	Policy	Setting
	Deny log off of an administrator logged in to the console session	Enabled
	Do not allow local administrators to customize permissions	Enabled
	Sets rules for remote control of Terminal Services user sessions	No remote control allowed
Client\Server data redirection	Allow Time Zone Redirection	Disabled
	Do not allow clipboard redirection	Enabled
	Allow audio redirection	Disabled
	Do not allow COM port redirection	Enabled
	Do not allow client printer redirection	Enabled
	Do not allow LPT port redirection	Enabled
	Do not allow drive redirection	Enabled
	Do not set default client printer to be default printer in a session	Enabled
Encryption and Security	Always prompt client for a password on connection	Enabled

(continued)

	Set Client Connection Encryption Level	High
Encryption and Security\RPC Security	Secure Server (Require Security)	Enabled
Sessions	Set time for disconnected sessions	10 minutes
	Allow reconnection from original client only	Enabled

Any domain account or security group requiring Terminal Service access to the CA must be added to the local Remote Desktop Users group (unless it is already a member of the local Administrators group).

Other Windows Configuration Tasks

There will almost certainly be other configuration tasks that you will need to perform on both the issuing and root CAs, depending on the infrastructure and standards in your organization. These tasks may include:

- Enabling backups (described in Chapter 11) or installing backup agents.
- Configuring Simple Network Management Protocol (SNMP) or Windows Management Instrumentation (WMI) options.
- Installing management agents such as Microsoft Operations Manager (MOM) or Microsoft Systems Management Server (SMS) client components.
- Installing antivirus software.
- Installing intrusion detection agents.

You should verify these items as they are installed according to the instructions supplied with the product.

Installing and Configuring the Root CA

This section describes how Certificate Services is installed and configured on the root CA.

Preparing the Capolicy.inf File for the Root CA

The Capolicy.inf file must be created before you set up a Windows 2003 root certificate authority. This file specifies characteristics of the self-signed root CA certificate, such as the key length, certificate validity period, the CRL and AIA publishing locations, certificate policies, and a certificate practices statement (CPS) if you have created one.

Note: See the "Creating a Certificate Practices Statement" section in Chapter 4, "Designing the Public Key Infrastructure," for further discussion of the CPS and whether you should consider creating one. A CPS is a legal document, not a technical item, so you should be sure that you need one before configuring one in your CA.

CRL and AIA information is not required for a root CA certificate itself, so the CRLDistributionPoint and AuthorityInformationAccess parameters are set to **Empty** in the Capolicy.inf file.

▶ **To create the CAPolicy.inf file**

1. In a text editor such as Notepad, enter the following text:

```
[Version]
Signature= "$Windows NT$"

[Certsrv_Server]
RenewalKeyLength=4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=16

[CRLDistributionPoint]
Empty=true

[AuthorityInformationAccess]
Empty=true
```

Caution: Configuring a key length of 4096 bits may cause compatibility problems. Certain devices (for example, some routers) and some older software from other vendors cannot process keys over a certain size.

2. If you have a CPS defined for this CA, include the following in your Capolicy.inf file (you must substitute your own values for all items in Italics):

```
[CAPolicy]
Policies=WoodGrove Bank Root CA CPS

[WoodGrove Bank Root CA CPS]
OID=your.Orgs.OID
URL = "http://www.woodgrovebank.com/YourCPSPage.htm"
```

3. Save the file as %windir%\Capolicy.inf (replace %windir% with the absolute path of the folder in which Windows is installed, such as C:\Windows). You must be a local administrator or have permissions to write to the Windows folder to complete this step.

Installing the Certificate Services Software Components

Use the Windows Components Wizard to install the CA software components. Note that the Windows Server 2003 installation CD or network path is required to complete the installation.

▶ **To install Certificate Services**

1. Log on as a member of the local Administrators group, and run the Optional Components Manager (or, via Control Panel, click **Add/Remove Programs/Windows Components**):

   ```
   sysocmgr /i:sysoc.inf.
   ```

2. Select the **Certificate Services** component (click **Yes** to dismiss the rename warning message box).
3. Select the CA type as **Stand-alone Root CA**, ensuring that you have selected the **Use custom settings** check box.
4. In the **Public and Private Key Pair** dialog box, leave the settings at their default values except the key length, which should be set to 4096. **CSP Type** should be **Microsoft Strong Cryptographic Provider**.

5. Enter Certificate Authority identifying information as follows:
   - CA Common Name: *WoodGrove Bank Root CA*
   - Distinguished Name suffix: *DC=woodgrovebank,DC=com* (the organization's Active Directory forest root name)
   - Validity Period: **8 Years**

Note: If a CA was previously installed on this computer, a warning dialog box will prompt you about overwriting the private key of the previous installation. You should verify that the key will never be needed again before proceeding. If in doubt, cancel the installation procedure and back up the existing key information. (Use either a system backup or backup of the existing CA certificate and private key−see the procedures documenting this in Chapter 11, "Managing the Public Key Infrastructure.")

The CSP generates the key pair, and it is written to the local computer key store.

6. Leave the locations of the certificate database, database logs, and configuration folder at their default values.

Notes:

Setup may display a warning about not being able to create a shared folder, because all network interfaces were earlier disabled. It is safe to ignore this warning and move on.

You must place the certificate database and the Certificate database log on local NTFS drives.

The Optional Component Manager then installs the Certificate Services components. This part of the process will require Windows Server 2003 installation medium (CD).

7. Click **OK** to dismiss the warning about IIS and continue the installation to completion.

Verifying Root CA Installation

You can verify the successful completion of the Certificate Services installation as follows:

▶ To verify the correct installation of the root CA

1. Open the Certificate Authority management console (from **All Programs**, **Administrative Tools**). Verify that Certificate Services has started and that you can view the properties of the CA.
2. On the **General** tab, select the CA certificate (or **Certificate #0** from the list if there is more than one certificate), and then click **View Certificate**.
3. Look at the **Details** tab of the CA Certificate and verify that the displayed values match those in the following table.

Table 7.19: Root CA Certificate Properties and Extensions

Certificate attribute	Required setting
Issuer and Subject fields	Both fields should be identical and should show the full CA Common name plus DN suffix that you supplied during installation.
Not Before - Not After	16 years.
Public Key Length	RSA (4096 bits).
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86).
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=None

The presence of the Basic Constraints subject type is very important because this value distinguishes a CA certificate from an end-entity certificate. In addition, there should be no CDP or AIA extensions listed.

If any of the values are not what you expected, you should re-start the installation of Certificate Services.

Note: If you re-run the installation of Certificate Services, you will see a warning about the private key already existing. If you know that you have not issued any certificates using this key, you can safely ignore this warning and generate a new key. If the CA has already issued certificates (other than test certificates), you should not reinstall Certificate Services until you have safely backed up the previous key and certificate (this procedure is described in Chapter 11, “Managing the Public Key Infrastructure").

4. You can view the Certificate Services setup log (%systemroot%\certocm.log) for further verification or to help troubleshoot any errors that might occur.

Configuring the Root CA Properties

The CA configuration procedure applies a number of parameters that are specific to the environment. The values of these parameters are documented in the "Certificate Services Planning Worksheet" section earlier in the chapter. This procedure configures the CA properties as listed in the following table.

Table 7.20: CA Properties to Be Configured

CA property	Description of setting
CRL Distribution Point URLs	Specifies HTTP, LDAP and FILE locations from which a current CRL can be obtained. The FILE location is a local folder and is only used by the CA to store the CRLs that it issues; only the LDAP and HTTP locations are included in the issued certificates. The HTTP URL is listed sequentially before LDAP, so clients using the root CA certificates are not dependent on Active Directory to obtain CRLs.
AIA URLs	Locations where CA certificates can be obtained. As with the CDPs, the file location is only used to publish the CA certificate, and the HTTP URL has priority over the LDAP URL.
Validity Period	Maximum validity period for issued certificates (different than the Validity Period of the CA certificate itself, which is set in the CAPolicy.inf or by the parent CA).
CRL Period	Frequency of CRL publication.
CRL Overlap time	Overlap time between when a new CRL is issued and when the previous CRL expires.
Delta–CRL Period	Frequency of delta-CRL publication (on the root CA, delta-CRLs are disabled).
CA Auditing	CA Auditing settings. All auditing is enabled by default.

Note: The properties shown in this table affect the certificates issued by the root CA, not the root CA certificate itself.

▶ To configure the root CA properties

1. Log on to the CA Server as a member of the local Administrators group.
2. Customize the following script (C:\MSSScripts\pkiparams.vbs) to include the correct DN of your Active Directory forest root and the HTTP URL that points to your CDP and AIA publishing Web server. Change the value of the **AD_ROOT_DN** setting to match your Active Directory forest root domain DN. Change the **HTTP_PKI_VROOT** setting to match the HTTP path to the IIS virtual directory that you set up earlier.

Note: Only part of the pkiparams.vbs file is shown here. Do not edit or remove other items in the file unless you understand the implications of doing so.

```
'************************************************************************
'   USER SETTABLE CONSTANTS
'
' These values MUST be set to reflect actual values used
' by the organization.
'************************************************************************

' This is the URL where CRL and CA certs are to be published.
CONST CA_HTTP_PKI_VROOT          = " http://www.woodgrovebank.com/pki"

' This needs to be set only if non Active directory clients need to query
' the ldap URL for CRLs. Normally they are OK with HTTP. If you do set this
' (to a specific DC FQDN) ALL clients will use this DC to query. Left blank
' AD clients use their default LDAP server (local DC) to query.
CONST CA_LDAP_SERVER             = ""

' This needs to be set to the DN of the Active Directory Forest root domain
' This is used to set the Root CA CDP and AIA paths so that clients can
' obtain CRL and CA Certificate information from the Active Directory
CONST AD_ROOT_DN                 = "DC=woodgrovebank,DC=com"
```

3. Then run the following script:

```
Cscript //job:RootCAConfig C:\MSSScripts\ca_setup.wsf
```

Configuring Administrative Roles

To make use of administrative roles on the CA (such as auditor and certificate manager), you need to map security groups created earlier to those roles.

Note: This solution uses the groups created earlier to define multiple separate roles. This approach gives you maximum flexibility to delegate responsibilities over CA management. However, if you do not require this level of delegation, you should consider using the simplified administration group model specified earlier in the chapter. The simplified model will allow you to use a smaller number of accounts to perform the CA administrative functions.

▶ **To configure administrative roles on the root CA**

1. From the Certificate Authority management console, click **Properties** to edit the properties of the CA.
2. Click the **Security** tab and add the local security groups listed in the following table. For each group, add the permissions shown.

Table 7.21: CA Permission Entries to Add

Group name	Permission	Allow/Deny
CA Admins	Manage CA	Allow
Certificate Managers	Issue and Manage Certificates	Allow

Note: If you want to have greater role separation, you should also remove Manage CA permissions from the local Administrators group. (Since the root CA is installed on the Standard Edition of Windows Server, you cannot enforce role separation– this option is only available on the Enterprise Edition.)

3. Other CA security roles for this CA have already been defined through the security policy applied earlier to the server:
   - CA Auditors have been granted Manage Security and Audit Logs user rights.
   - Backup Operators have the necessary rights to back up and restore the CA.

Transferring the Root CA Certificate and CRL to Disk

You must copy the root CA Certificate and CRL from the CA so that they can be published to the Active Directory and to the IIS Certificate and CRL publishing server.

▶ **To copy the root CA certificate and CRL to disk**

1. Log on to the root CA as a member of the local CA Admins group, and then place a disk to be used for transfer into the drive.
2. Run the following script to copy the CA certificate to disk:

```
Cscript //job:GetCACerts C:\MSSScripts\CA_Operations.wsf
```

3. Run the following script to copy the CA CRL to disk:

```
Cscript //job:GetCRLs C:\MSSScripts\CA_Operations.wsf
```

4. Label this disk **Transfer-[***HQ-CA-01***]**, date it, and retain it for later in the procedure.

Note: The disk does not contain any security sensitive information (such as CA private key material), so you do not need to handle it with any special security precautions.

Publishing the Root CA Information

Before you can install the issuing CA, you must publish the root CA's certificate to the Active Directory trusted root store, and publish the root CA's CRL to the Active Directory CDP container. This will cause all domain members (including the issuing CA) to import the root CA's certificate into their own root stores and enable them to verify the revocation status of any certificates issued by the root CA. (The issuing CA must be able to verify the revocation status of its own certificate before Certificate Services will start.)

Note: You can carry out the following procedure from any domain member, although it requires Certutil.exe and supporting certadm.dll and certcli.dll libraries to be installed on that system— certutil.exe (plus required DLLs) are installed as part of Windows Server 2003. You can use the unconfigured issuing CA server to do perform the procedure.

▶ **To publish the root CA certificate and CRL to Active Directory**

1. Log on to a domain member computer as a member of the Enterprise PKI Admins group, and insert the disk used earlier to store the root CA certificate and CRL (labeled **Transfer-[***HQ-CA-01***]**).
2. Run the following script to publish the CA certificate to Active Directory:
   ```
   Cscript //job:PublishCertstoAD C:\MSSScripts\CA_Operations.wsf
   ```
3. Run the following script to publish the CA CRL(s) to Active Directory:
   ```
   Cscript //job:PublishCRLstoAD C:\MSSScripts\CA_Operations.wsf
   ```

Publishing the Root CA Certificate and CRL to the Web Server

This task is needed since HTTP versions of the CDP and AIA URLs are specified in the extensions of certificates issued by this CA. If these extensions are present, they must be honored by publishing CRLs and certificates to the URLs configured in the certificates.

Note: This procedure is the same whether the CDP and AIA publishing Web server is on the issuing CA or on another server. It does assume that the Virtual directory matches the one set up in the earlier procedure to configure IIS–C:\CAWWWPub. If you chose to use a different path, you will need to update the value WWW_LOCAL_PUB_PATH in the file C:\MSSScripts\PKIParams.vbs.

▶ **To publish the root CA certificate and CRL to the Web URL**

1. Log on to the Web server as a local administrator or with an account that has permissions to write to the C:\CAWWWPub folder.
2. Ensure that the disk (labeled **Transfer-[***HQ-CA-01***]**) containing the CA certificates and CRLs is in the drive.
3. Run the following script to publish the CA certificate to the Web server folder:
   ```
   Cscript //job:PublishRootCertstoIIS
           C:\MSSScripts\CA_Operations.wsf
   ```
   (This command is displayed on more than one line; enter it as a single line.)
4. Run the following script to publish the CA CRL(s) to the Web server folder:
   ```
   Cscript //job:PublishRootCRLstoIIS
           C:\MSSScripts\CA_Operations.wsf
   ```
   (This command is displayed on more than one line; enter it as a single line.)

Verifying the Publication of Root CA Information

You should verify that the publication of the root CA information has happened correctly. You need to perform these steps while logged on to a domain member computer connected to the network and using a valid domain user account.

Note: You may need to wait for Active Directory replication to happen. Use the certutil -pulse command to force root CA certificate download prior to verifying root CA information publication.

▶ **To verify root CA information publication**

1. To verify publication of the CA certificate to the trusted root store, run the following command:

```
certutil -viewstore -enterprise Root
```

2. You should see a certificate displayed. Verify that the **Issuer** and **Subject** values match what you configured for the root CA name and that the **Valid from** date is today's date.
3. To verify the publication of the root CA CRL to the directory, run the following command, replacing the items in italics with the values used in your own installation (CA Common name, CA short hostname and DN of your Active Directory forest root):

```
certutil -store -enterprise "ldap:///cn=WoodGrove Bank Root
        CA,cn=HQ-CA-01,cn=CDP,CN=Public Key
        Services,CN=Services,CN=Configuration,DC=woodgrovebank,DC
        =com?certificateRevocationList?base?objectClass=crlDistribution
        Point"
```

(This command is displayed on more than one line; enter it as a single line.)

4. You should see output similar to the following. Verify that the **Issuer** value matches the name that you configured for the root CA:

```
================ CRL 0 ================
Issuer:    CN=WoodGrove Bank Root CA,DC=woodgrovebank,DC=com
CA Version: V1.0
CRL Number: CRL Number=1
CRL Hash(sha1): 73 03 a1 c7 5f a3 c3 f9 8a 09 d0 3c b5 09 00 9c b5 a3
de fe
CertUtil: -store command completed successfully.
```

5. To verify the publication of the CA certificate to the Web server, enter the following URL into a browser, replacing the items in italics with the values used in your own environment:

   http://*www.woodgrovebank.com*/pki/*HQ-CA-01_WoodGrove Bank Root CA*.crt

---

Note: You may need to use the fully qualified DNS name of the CA server in the certificate file name (that is, *HQ-CA-01.woodgrovebank.com_WoodGrove Bank Root CA*.crt instead of the name shown above).

---

6. You should be prompted to open or save the file. Open it and verify that the root CA certificate is displayed.

7. To verify the publication of the root CA CRL to the Web server, enter the following URL into a browser, replacing the items in italics with the values used in your own environment:

   `http://`*`www.woodgrovebank.com`*`/pki/`*`WoodGrove Bank Root CA`*`.crl`

8. You should be prompted to open or save the file. Open it and verify that the root CA CRL is displayed.

Note: If you have renewed the CA certificate or issued more than one CRL, you may see different version numbers displayed in the output from these commands.

Installing and Configuring the Issuing CA

This section describes how Certificate Services is installed and configured on the issuing CA server. During the installation process there is a complex set of interactions between this CA, the root CA, Active Directory, and the Web Server. These interactions are illustrated in the following diagram. It may help you to refer to this diagram as you work your way through this section.

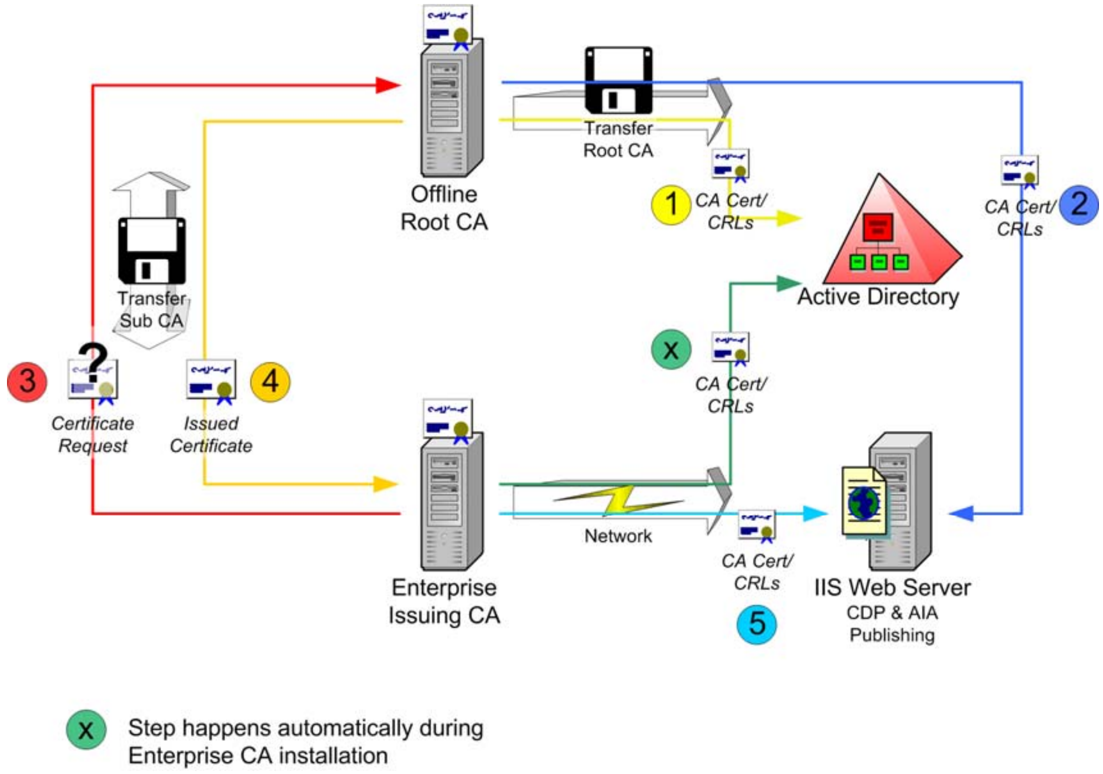

Figure 7.2

Interaction between CAs, Active Directory, and Web server during issuing CA installation

The main interactions between different systems during the issuing CA installation are shown on the diagram. These interactions are:

1. Publishing the root CA certificate and CRL to Active Directory.
2. Publishing the root CA certificate and CRL to the Web server.
3. Installing the Certificate Services software, which generates a certificate request that you need to take to the root CA on disk. At the root CA you issue the certificate for this request.
4. Installing the issuing CA certificate.
5. Publishing the issuing CA certificate and CRL to the Web server.

Note: Steps 1 and 2 were described in the earlier section, "Publishing Root CA Information." The Step labeled as X on the diagram happens automatically as part of configuring the CRL and AIA values on the issuing CA during the "Configuring the Issuing CA Properties" task. The other steps are described in this section.

Preparing the Capolicy.inf File for the Issuing CA

A CAPolicy.inf is not strictly required for the issuing CA. However, you will need one if you need to change the key size used by the CA. You should create the Capolicy.inf file before you set up the issuing CA (although you can add one later and renew the CA certificate). This file specifies some of the characteristics of the CA certificate, such as the key length and the CPS (if you have created one).

▶ To create the CAPolicy.inf file

1. In a text editor such as Notepad, enter the following text.

```
[Version]
Signature= "$Windows NT$"

[Certsrv_Server]
RenewalKeyLength=2048
```

2. If you have a CPS defined for this CA, include the following in your Capolicy.inf file (you must substitute your own values for all items in Italics):

```
[CAPolicy]
Policies=WoodGrove Bank Issuing CA 1 CPS

[WoodGrove Bank Issuing CA 1 CPS]
OID=your.Orgs.OID
URL = "http://www.woodgrovebank.com/YourCPSPage.htm"
```

Note: See the "Creating a Certificate Practices Statement" section in Chapter 4, "Designing the Public Key Infrastructure," for further discussion of the CPS and whether you should consider creating one. A CPS is a legal document, not a technical item, so you should be sure that you need one before configuring one in your CA.

3. Save the file as %windir%\Capolicy.inf (or replace %windir% with the absolute path of the folder in which Windows is installed, such as C:\Windows). You must be a local administrator or have permissions to write to the Windows folder to complete this step.

Installing the Certificate Services Software Components

Use the Windows Components Wizard to install the CA software components. Note that the Windows Server 2003 installation medium (CD) will be required to complete the installation.

▶ **To install Certificate Services**

1. Log on to the server as a member of the local Administrators group and run the Optional Components Manager (or click **Add/Remove Programs**/**Windows Components** in Control Panel):

   ```
   sysocmgr /i:sysoc.inf
   ```

   Note: You need to be a member only of the local Administrators group to complete the first part of the installation. In the following procedure, you must also be a member of Enterprise PKI Admins (or Enterprise Administrators) to install the CA certificate.

   ---

2. Select the Certificate Services component (click **OK** to dismiss the rename warning message box).
3. Select the CA type as **Enterprise Subordinate CA**, ensuring that you have selected the **Use custom setting** check box.
4. In the **Public and Private Key Pair** dialog box, leave the settings at their default values except the key length, which should be set to **2048** bits. CSP Type should be **Microsoft Strong Cryptographic Provider**.
5. Enter Certificate Authority identifying information as follows:
   - CA Common Name: *WoodGrove Bank Issuing CA 1*
   - Distinguished Name suffix: *DC=woodgrovebank,DC=com* (your organization's Active Directory forest root name)
   - Validity Period: Determined by parent CA

   Note: If a CA was previously installed on this computer, a warning dialog box will prompt you about overwriting the private key of the previous installation. You should ensure that the key will never be required again before proceeding. If in doubt, cancel the installation procedure and back up the existing key information. (Use either a system backup or backup of the existing CA certificate and private key–see the procedures that document this in Chapter 11, "Managing the Public Key Infrastructure.")

   ---

6. The CSP will generate the key pair and write it to the local computer key store.
7. Enter the locations of the certificate database, database logs, and configuration folder as follows:
   - Certificate Database: **D:\CertLog**
   - Certificate Database Log: **%windir%\System32\CertLog**
   - Shared Folder: Disabled

   You should always store the CA database and logs on physically separate volumes if possible, for performance and resiliency reasons. (If the database is damaged for any reason, you can use the last backup and the logs to restore the CA to the point where the failure occurred.) The certificate database and the Certificate database logs must both be on local, NTFS-formatted drives.

8. Copy the certificate request file to disk. The certificate request is generated and is stored in the Shared Folder path. Copy the *HQ-CA-02.woodgrovebank.com_WoodGrove Bank Issuing CA 1.req* file to the disk and label the disk **Transfer-[***HQ-CA-02***]**.

   The Optional Component Manager will then install the Certificate Services components. This installation will require Windows Server 2003 installation medium (CD).
9. Click **OK** to dismiss the warning about IIS and continue the installation until completion. The setup wizard will display a notice that you need to obtain the certificate from the parent CA before continuing.

Notes:

You will see a warning during the latter stages of the installation that the CA could not be added to the **Pre Windows 2000 Compatible Access Group**. This is only relevant if you need to use the Certificate Manager Restriction feature of Certificate Services. If you do require this feature, you should ask your domain administrator to add the computer account of the CA to this group.

Certificate Services will not start until the certificate request is processed by the root CA and the certificate is returned and installed in the CA.

Submitting the Certificate Request to the Root CA

Next, you must take the issuing CA certificate request to the root CA for the request to be signed and a certificate issued to the issuing CA.

▶ **To submit the certificate request to the root CA**

1. Log on to the root CA as a member of the local Certificate Managers group.
2. From the Certification Authority management console, on the CA **Tasks** menu, select **Submit new request** and then submit the request transferred from the issuing CA (on the **Transfer-[***HQ-CA-02***]** disk).

Note: If a previous CA setup has failed and you repeat the setup, never re-use the request file of the earlier CA setup; it is associated with the previous key material and not with the current CA being installed.

---

3. The root CA requires that all requests be manually approved. Locate the request in the Pending Requests container of the Certification Authority MMC, verify that the **Common Name** field has the name of the issuing CA, and then approve the request by right-clicking the request and clicking **Issue**.
4. Locate the newly issued certificate in the Issued Certificates container and open it.
5. Verify that the Certificate details are correct, and then export the certificate to a file by clicking **Copy to File**, saving it as a PKCS#7 file (select the option to include all possible certificates in the chain) on the disk labeled **Transfer-[***HQ-CA-02***]** (for transfer back to the issuing CA).

Installing the Issuing CA Certificate

The tasks in this section ensure that the root CA information published earlier to Active Directory can be downloaded to the issuing CA. Then the issuing CA certificate can be installed on the CA.

Refreshing the Certificate Information on the Issuing CA

The root CA certificate was published earlier to the trusted root store of Active Directory. Now you should ensure that the issuing CA has downloaded this information and placed the certificate into its own root store.

▶ **To refresh the certificate trust information on the Issuing CA**

1. Log on to the issuing CA as a local administrator.
2. Run the following at a command prompt:

```
certutil –pulse
```

This command will force the CA to download the new trusted root information from the directory and place the root CA certificate into its own local trusted root store.

Note: This procedure is not absolutely necessary, because the last step of installing the certificate into the CA will automatically place the root CA certificate into its local trusted root store. However, this step enables you to verify that the earlier publishing steps to Active Directory completed successfully. It is vital that this publishing happens correctly, because all domain clients will receive their trust information about the root and issuing CAs from Active Directory.

▶ **To verify the successful download of root CA trust from Active Directory**

1. Run mmc.exe and add the **Certificates** snap-in.
2. Select **Computer Account** as the certificate store to manage.
3. Ensure that the root CA certificate is in the Trusted Root Certificate Authorities folder (the certificates are listed by the friendly form of the CA subject name–the CN element).

Installing the Certificate

The signed response (the PKCS#7 package containing the certificate) from the root CA can now be installed into the issuing CA. In order to successfully publish the CA certificate to the Active Directory NTAuth store (which identifies the CA as an Enterprise CA), you must install the CA certificate using an account that is *both* a member of Enterprise PKI Admins and local Administrators on the CA. The former group has rights to publish the certificate to the directory, and the latter has rights to install the CA certificate on the CA server. If you are using the simple administration model suggested earlier, the CAAdmin role is a member of both of these groups.

▶ **To install the issuing CA certificate**

1. Log on to the issuing CA using an account that is a member of both Enterprise PKI Admins and the local Administrators group.
2. Insert the disk (**Transfer-[***HQ-CA-02***]**) with the saved certificate issued by the root CA.
3. From the CA **Tasks** menu in the Certification Authority management console, select **Install Certificate** and install the issuing CA certificate from the disk.

The CA should now start.

Verifying the Issuing CA Installation

You can verify the successful completion of the Certificate Services installation as follows:

▶ **To verify the issuing CA installation**

1. Open the Certification Authority management console. Verify that Certificate Services has started and that you can view the properties of the CA.
2. On the **General** tab, select the CA certificate (or **Certificate #0** if more than one certificate is shown) and then click **View Certificate**.
3. On at the **Details** tab of the CA Certificate, verify that the displayed values match those in the following table.

Table 7.22: Issuing CA Certificate Properties and Extensions

Certificate attribute	Required setting
Issuer	Root CA Common name (plus DN suffix)
Subject	Issuing CA Common name (plus DN suffix)
Not Before - Not After	8 years
Public Key Length	2048 bits
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=None
CRL Distribution Points	2 entries—HTTP and LDAP URLs
Authority Information Access	2 entries—HTTP and LDAP URLs

The presence of the Basic Constraints subject type is very important because this value distinguishes a CA certificate from an end-entity certificate. In addition, there will be another extension listed, **Authority Key Identifier**, which does not appear in the root CA certificate. This value should match the **Subject Key Identifier** of the root CA certificate.

If any of the previous values are not what you expected, you should re-start the installation of Certificate Services.

Note: If you re-run the installation of Certificate Services, you will see a warning about the private key already existing. If you know that you have not issued any certificates using this key, you can safely ignore this warning and generate a new key. If the CA has already issued certificates (other than test certificates), you should not reinstall Certificate Services until you have safely backed up the previous key and certificate (this procedure is described in Chapter 11, "Managing the Public Key Infrastructure").

---

4. Look at the **Certification Path** tab and verify that the issuing CA certificate chains properly to the root CA.
5. You can view the Certificate Services setup log (%systemroot%\certocm.log) for further verification or to help troubleshoot any setup errors that occur.

Configuring the Issuing CA Properties

The CA configuration procedure applies a number of parameters that are specific to your environment. The values of these parameters are documented in the "Certificate Services Planning Worksheet" section earlier in the chapter. This procedure configures the CA properties described in the following table.

Table 7.23: CA Properties to Be Configured

CA property	Description of setting
CRL Distribution Point URLs	Specifies HTTP, LDAP and FILE locations from which a current CRL can be obtained. The FILE location is a local folder and is only used by the CA to store the CRLs that it issues; only the LDAP and HTTP locations are included in the issued certificates. The LDAP URL is listed sequentially before the HTTP so that local domain controllers will be the preferred target for CRL downloads but see the note following the table.
AIA URLs	Locations where CA certificates can be obtained. As with the CDPs, the file location is only used to publish the CA certificate, and the LDAP URL has priority over the HTTP URL but see the note following the table.
Validity Period	Maximum validity period for issued certificates (this is different than the Validity Period of the CA certificate itself, which is set in the CAPolicy.inf or by the parent CA).
CRL Period	Frequency of CRL publication.
CRL Overlap time	Overlap time between when a new CRL is issued and when the previous CRL expires.
Delta–CRL Period	Frequency of delta-CRL publication.
Delta–CRL Overlap	Overlap time between when a new CRL is issued and when the previous CRL expires.
CA Auditing	CA Auditing settings. All auditing is enabled by default.

Important: If you need to support non-domain clients (as discussed in Chapter 4, "Designing the Public Key Infrastructure"), you must change the order of the CDP and AIA entries so that the HTTP entry has higher priority. To change this order you will need to edit the CA configuration script (ca_setup.vbs) or use the CA MMC to manually change the CDP and AIA entries. Because LDAP URLs only work reliably for domain clients, you may decide only to use HTTP URLs. If you do, you must ensure that the Web server(s) hosting the HTTP AIA and CDP publishing points are resilient.

▶ **To configure the issuing CA properties**

1. Log on to the CA Server as a member of the local Administrators group.
2. You should have customized the script C:\MSSScripts\pkiparams.vbs to your organization-specific settings when you set up the root CA. You need to replicate these changes in the copy of C:\MSSScripts\pkiparams.vbs that you have installed on the issuing CA.
3. Then run the following script:

```
Cscript //job:IssCAConfig C:\MSSScripts\ca_setup.wsf
```

Configuring Administrative Roles

To make use of administrative roles on the CA (such as auditor and certificate manager), you must map security groups to those roles.

Note: This solution uses the groups created earlier to define multiple separate roles. This approach provides maximum flexibility to delegate responsibilities over CA management. However, if you do not require this level of delegation, you should consider using the simplified administration group model specified earlier in the chapter. The simplified model will allow you to use a smaller number of accounts to perform the CA administrative functions.

▶ **To configure administrative roles on the issuing CA**

1. From the Certification Authority management console, click **Properties** to edit the properties of the CA.
2. Click the **Security** tab and add the domain security groups listed in the following table. For each group, add the permissions shown.

Table 7.24: CA Permission Entries to Add

Group name	Permission	Allow/Deny
CA Admins	Manage CA	Allow
Certificate Managers	Issue and Manage Certificates	Allow

Note: If you want to enforce full role separation, you should also remove Manage CA permissions from the local Administrators group.

---

3. Other CA security roles require some additional configuration (although they have already been partly defined through the security policy applied earlier to the server):
   - CA Auditors was granted Manage Security and Audit Logs user rights. Add this group to the local Administrators group.
   - CA Backup Operators was granted Backup and Restore rights on the CA. No further configuration needs to be done for this group.

Publishing the Issuing CA Information

Certificates and CRLs are automatically published from the issuing CA to Active Directory. However, publication of the CA certificate and CRLs to the HTTP CDP and AIA paths is not automatic; you must set up a scheduled job to perform these tasks.

Publishing the Issuing CA Certificate and CRLs to the Web Server

The issuing CA certificate(s) and CRL(s) must be published to the HTTP AIA and CDP locations, respectively. It is technically possible to configure the CA to publish directly to the Web server folder; having the Web server hosted on the issuing CA makes this very easy. However, this method is not always possible for reasons of security and network connectivity. The following method uses a simple file copy technique that you can extend to suit most configurations.

Note: This procedure is not suitable for directly publishing to an Internet-facing Web server because it requires direct network connectivity and uses Windows network file sharing which is usually blocked by Internet firewalls . To publish to an Internet server, use the following procedure to publish to an intermediate location and then use your standard method of securely publishing content to your Web server. You must take into account the effect that this extra step might have on the freshness of your CRLs.

The CA certificate is updated very rarely, so you can publish to the AIA manually whenever the CA certificate is renewed.

▶ **To publish the issuing CA's certificate**

1. Log on to the issuing CA with an account that has permissions to write to the published Web server folder.
2. If the Web server is on a remote server, ensure that the Web server folder is shared. Record the UNC path to the shared folder.
3. If the Web server is on the same server as the CA, record the local path to the folder.
4. Update the WWW_REMOTE_PUB_PATH parameter in C:\MSSScripts\PKIParams.vbs to match the destination path of the Web server folder (default is local path C:\CAWWWPub).
5. Run the following command to publish the CA certificate to the Web server:

   ```
   Cscript //job:PublishIssCertsToIIS
           C:\MSSScripts\CA_Operations.wsf
   ```

   (This command is displayed on more than one line; enter it as a single line.)

CRLs are published from the issuing CA much more regularly (daily or hourly in the case of delta-CRLs) than the CA certificate, so an automated method of replicating the CRLs to the Web server is required.

▶ **To automate the publication of CRLs**

1. Log on to the issuing CA with an account that is a member of local Administrators.
2. Ensure that the Web server folder is accessible (as a remote share or local path) from this server.
3. If the Web server is remote, grant the issuing CA write access to the file system folder (by allowing **Modify** access) and to the share (by allowing **Change** access). If the Web server is a member of the forest, you can use the domain Cert Publishers group to grant access. This will ensure that any Enterprise CA in the domain has the required permissions to publish certificates and CRLs to this folder. You do not need to change the Web server permissions (see the previous section on configuring IIS for AIA and CDP publishing).
4. Create a scheduled job to copy the CRLs by running the following command:

   ```
   schtasks /create /tn "Publish CRLs" /tr "cscript.exe
          //job:PublishIssCRLsToIIS C:\MSSScripts\CA_Operations.wsf"
          /sc Hourly /ru "System"
   ```

   (This command is displayed on more than one line; enter it as a single line.)

Note: This procedure creates an hourly scheduled job to publish the CRLs from the CA to the Web server. This frequency is sufficient to cope with a daily or even half-daily delta CRL publication schedule. If your CRL schedule is more frequent than this, you should make the scheduled job run more frequently. A good guideline is that the job schedule should be approximately 5-10 percent of the delta CRL schedule.

Verifying the Publication of Issuing CA Information

You should verify that the publication of the issuing CA Information has occurred successfully. You need to perform these steps logged on to a domain member computer connected to the network and using a valid domain account.

▶ To verify issuing CA information publication

1. To verify publication of the CA certificate to the intermediate CA store, run the following command:

   ```
   certutil -viewstore -enterprise CA
   ```

2. You should see two certificates displayed–one for the root CA, and one for the issuing CA. Double-click the issuing CA certificate and verify that the **Subject** name matches what you configured for the issuing CA and that the **Valid from** date is the current date.
3. To verify publication of the CA certificate to the NTAuth CA store (where all Enterprise CAs are published), run the following command:

   ```
   certutil -viewstore -enterprise NTAuth
   ```

   You should see the same certificate displayed for the issuing CA.
4. To verify the publication of the issuing CA CRL to the directory, run the following command, replacing the items in Italics with the values used in your own installation (CA Common name, CA short hostname, and DN of your Active Directory forest root):

   ```
   certutil -store -enterprise "ldap:///cn=Woodgrove Bank Issuing CA
           1,cn=HQ-CA-02,cn=CDP,CN=Public Key Services,
           CN=Services,CN=Configuration,DC=woodgrovebank,DC=com
           ?certificateRevocationList?base?objectClass=
           cRlDistributionPoint"
   ```

   (This command is displayed on more than one line; enter it as a single line.)
5. You should see output similar to the following. Verify that the **Issuer** value matches the name that you configured for the issuing CA:

   ```
   ================ CRL 0 ================

   Issuer: CN= WoodGrove Bank Issuing CA,DC=woodgrovebank,DC=com

   CA Version: V1.0

   CRL Number: CRL Number=1

   CRL Hash(sha1): 73 03 a1 c7 5f a3 c3 f9 8a 09 d0 3c b5 09 00 9c b5 a3
   de fe

   CertUtil: -store command completed successfully.
   ```

6. To verify publication of the CA certificate to the Web server, enter the following URL into a browser, replacing the items in Italics with the values used in your own installation:

   `http://`*`www.woodgrovebank.com`*`/pki/`*`HQ-CA-02_WoodGrove Bank Issuing CA 1`*`.crt`
7. You should be prompted to open or save the file. Open it and verify that the issuing CA certificate is displayed.
8. To verify publication of the issuing CA CRL to the Web server, enter the following URL into a browser, replacing the items in Italics with the values used in your own installation:

   `http://`*`www.woodgrovebank.com`*`/pki/`*`WoodGrove Bank Issuing CA 1`*`.crl`
9. You should be prompted to open or save the file. Open it and verify that the root CA CRL is displayed.

Note: If you have renewed the CA certificate or issued more than one CRL, you may see different version numbers displayed in the output from these commands.

Verifying Certificate Enrollment

You should verify that you can enroll certificates from the issuing CA.

▶ **To verify certificate enrollment**

1. Log on to a computer in the same domain as the issuing CA. Use a domain account.
2. Open the Certificates MMC snap-in for the current user. (You will need to add this snap-in to a blank MMC with **Add/Remove Snap in** because there is no predefined one.)
3. Right-click the Personal folder and select **Request a New Certificate** from the **All Tasks** sub-menu.
4. You should be prompted with a list of certificate types to choose from – select the **User** type. Do not select the **Advanced options** check box.
5. Name the certificate with a recognizable friendly name, such as **Issuing CA Verification**.
6. Click **Finish** to enroll the certificate.
7. Navigate to the Certificates subfolder of the Personal Folder. You should see the **Issuing CA Verification** certificate there. (You may need to refresh the store first by right–clicking the **Certificates–Current User** root object in the left pane of the MMC and then clicking **Refresh**.)

If this verification test fails, you should retrace the steps in this chapter and rectify any problems identified. If you still have a problem, see the "Troubleshooting" section of Chapter 11, "Managing the Public Key Infrastructure."

Post-Build Configuration

Even though you have built the root and issuing CAs for your organization, there are still a few outstanding configuration tasks to complete. This section describes those tasks.

Configuring Certificate Templates

Most of the tasks are associated with configuring the types of certificates that the CAs can issue, who controls that issuance, and to whom or what the certificates are issued.

Removing Unwanted Templates From the Issuing CA

Until you need a certificate type, it is good practice to remove the corresponding template from the CA configuration so that certificates cannot be issued accidentally. The templates are always available in the directory however, and can be re-added if needed.

▶ **To remove unwanted templates from the issuing CA**

1. Log on as a member of the CA Admins domain group.
2. From the Certification Authority management console, select the Certificate Templates container.
3. Remove the following template types:
   - EFS Recovery Agent
   - Basic EFS
   - Web Server
   - Computer
   - User
   - Subordinate Certification Authority
   - Administrator

Note: This procedure removes all templates from the issuing CA except those for Domain Controller, Domain Controller Authentication, and Directory Email Replication. Windows 2000 domain controllers use Domain Controller certificates to enable smart card logon and Simple Mail Transfer Protocol (SMTP) Active Directory replication. Windows Server 2003 domain controllers use Domain Controller Authentication certificates to support smart card logon and secure LDAP and use the Directory Email Replication certificate for SMTP Active Directory replication.

All of the removed templates can be re-added in the future if needed. In the meantime, it is good practice to allow only the certificate types that you have deliberately chosen to be issued.

Creating and Managing Certificate Templates

Enterprise certificate templates can be effectively managed and used with security groups. These groups can control which users can modify the properties of each template and which users can enroll certificates of that type.

Note: Template administration groups are useful when there is a possibility that control over templates will be delegated to different administrators. If your PKI administration structure is not large or complex, this capability is probably not required. In this case, only members of the Enterprise Admins built-in group and Enterprise PKI Admins (created as part of this solution) will be able to administer certificate templates.

For instructions on creating and maintaining certificate template administration groups, see the operational procedures documented in Chapter 11, "Managing the Public Key Infrastructure."

For instructions on creating the specific certificate templates for this solution, see the "Configuring and Deploying Wireless Authentication Certificates" section in Chapter 9, "Implementing the Wireless LAN Security Infrastructure."

For general instructions on creating and modifying certificate templates, see the "Managing Certificate Templates" product documentation section and the technical paper, *Implementing and Administering Certificate Templates in Windows Server 2003*. (See reference at the end of this chapter.)

Managing Certificate Enrollment

Template enrollment groups make it easy to manage who can enroll or is autoenrolled for a given certificate type. Users can simply be added to or removed from a security group. Control over the membership of the template enrollment group can also be granted to administrative staff that you might not want to directly edit the properties of certificate templates.

For instructions on creating and maintaining certificate template enrollment groups, see Chapter 11, "Managing the Public Key Infrastructure."

Setting Permissions for Multi-Domain Deployment

If you are deploying this solution into a multi-domain forest, you may need to issue certificates to users and computers in domains other than the CA's domain. If this is the case, you will need to change the permissions from the default to allow the CAs to correctly publish certificates to other domains in the Active Directory forest.

When setting enrollment permissions for users on CAs and on certificate templates, you must explicitly include users and computers from all domains where you want those users and computers to be able to enroll certificates.

▶ **To allow publication of certificates to users and computers in other domains**

1. Log on to a domain member in the domain where you want to enable certificate publishing. You must be a member of domain administrators for this domain or a member of group with sufficient rights to change permissions on the domain object.
2. Open the Active Directory Users and Computers MMC snap-in and right-click the domain node.

Note: You can perform this operation from another domain as long as your account has the correct permissions in the target domain. You need to connect to the target domain from Active Directory Users and Computers.

---

3. Click **Delegate Control** to start the Delegation Wizard.
4. In the wizard, click **Next** and add the Cert Publishers group from the domain in where you installed the issuing CA. Then click **Next**.
5. Select **Create a custom task to delegate**, and then click **Next**.
6. Select **Only the following objects in the folder**.
7. Select the **User objects**, and then click **Next**.
8. Select the **Property-specific** option.
9. Select the **Read userCertificate** and **Write userCertificate** options.
10. Click **Next**, and then click **Finished**.
11. Repeat steps 3 to 10, but at step 7, select **Computer objects** instead of **User objects.**

This procedure ensures that the Enterprise CAs have permission to correctly publish certificates for users and computers in this domain.

Backing Up the CA Keys and CA Servers

Now that you have built the root and issuing CAs, you should back them up as soon as possible so that their keys and certificate databases are protected against server failure or data corruption.

Complete the following procedures as documented in Chapter 11, "Managing the Public Key Infrastructure":

- "Configuring the Issuing CA Backup"
- "Configuring and Executing the Root CA Backup"
- "Backing Up the CA Keys and Certificates" (This task needs to be performed for each CA.)

Client Configuration

This section describes a few important client configuration tasks. There are only a few because most of the client-related settings are specific to the application or service using the certificate services, such as WLAN or virtual private networking (VPN), rather than tasks common to all certificate applications.

Enabling User and Computer Certificate Autoenrollment

The measures described in the earlier section "Managing Certificate Enrollement" allow you to use security groups and template permissions to control autoenrollment at a very precise level. The autoenrollment capability of Windows XP clients is disabled by default, however. To enable it you must configure the correct setting in Group Policy. If you are using security groups to control autoenrollment, you can enable autoenrollment capability for all users and computers in the domain and use the enrollment security groups to determine who receives certificates of each type.

Caution: This procedure enables autoenrollment for *all* computers and users in the domain. Please ensure that you have removed the default templates from the issuing CA before starting this procedure to prevent the default Computer and User certificates being enrolled to every computer and user in the domain. This procedure assumes that you will be controlling autoenrollment using security groups as described in Chapter 11, "Managing the Public Key Infrastructure."

▶ **To enable autoenrollment for all users and computers in the domain**

1. Log on with an account that has permissions to create GPOs (a member of Group Policy Creator Owners) and has permission to link GPOs to the domain. Alternatively, request that a domain administrator create and link the GPO for you, and then grant read and write permissions for you on the GPO.
2. In Active Directory Users and Computers, select the domain object, right-click it, and then click **Properties**.
3. On the **Group Policy** tab, click **New** and then type a name for the GPO (for example, *Domain PKI Policies*).
4. Click **Edit** to edit the GPO and navigate to Public Key Policies under Computer Configuration\Windows Settings\Security Settings.
5. In the details pane, double-click **Autoenrollment Settings**.
6. Ensure that the following items are selected:
    - **Enroll certificates automatically**
    - **Renew expired certificates, update pending certificates, and remove revoked certificates**
    - **Update certificates that use certificate templates**
7. Repeat steps 5 and 6 for the user Autoenrollment Settings at User Configuration\Windows Settings\Security Settings\Public Key Policies.
8. Close the GPO.
9. Make sure that the GPO has a higher priority than the Default Domain Policy GPO.

Notes:
If you have a multi-domain Active Directory forest, you must carry out this procedure for each domain in the forest in which you want to enable certificate autoenrollment.

If you do not want to enable autoenrollment for all users or computers in the domain, you can create GPOs linked to OUs that contain the subset of users and/or computers for which you want to enable autoenrollment.

If your users do not use roaming profiles and you allow autoenrollment universally, certificates will be enrolled for users at every computer to which they log on. You may want to prevent administrators and operators autoenrolling certificates when they log on to servers. You can do this by creating a GPO that applies to these servers (for example, by linking it to the Servers OU). In that GPO, disable autoenrollment for users by selecting **Do not enroll certificates automatically**. In the same GPO, enable GPO loopback processing by enabling the **Computer Configuration\Administrative Templates\System\Group Policy\User Group Policy loopback processing mode** setting and selecting the **Replace** option.

Enabling certificate autoenrollment is also described in detail in documents listed in the "More Information" section at the end of this chapter.

Only Windows XP clients and later support autoenrollment of both user and computer certificates. Windows 2000 clients only support automatic enrollment of computer certificates (although some applications such as EFS have their own automatic enrollment mechanisms for user certificates).

If you are deploying this solution in a Windows 2000 Active Directory environment, you must edit the autoenrollment settings in the GPOs from a computer running Windows Server 2003 or Windows XP Professional with the Windows Server 2003 Administration Tools installed (Windows XP requires a specific service pack and hotfix level before it will support the Windows Server 2003 Administration Tools).

Configuring Root Certificate Authority Domain Policies

This section describes how to manage which commercial root CAs are trusted by clients in your organization and how much control you want over whether individual users can change which root CAs they trust.

Managing Third Party Trusts

By default, Windows clients are configured to trust a large number of commercial root CAs (known as baked-in-roots). If you want to prevent your users from automatically trusting these third-party root CAs, there is a procedure in the "To prevent users from trusting third-party root certification authorities with a Group Policy" online Help section. There is also a link to an article on this topic in the "More Information" section.

Note: Disabling third-party roots may cause errors or failures in client applications, so you should not do this without properly testing the consequences. For example, client connections to most public secure Web sites will cause a trust error to be produced.

You can alleviate some of the problems of removing all third-party trusts in several ways:

- You can selectively re-add individual roots by adding them to the Trusted Root Certification Authorities policy setting in Group Policy.
- You can add the root certificates to Certificate Trust Lists and deploy these via the Enterprise Trust setting of Group Policy. This method also allows you to control the usages for which you will trust certificates that the roots issue. However, because it has limited client support it is only recommended if you have no other alternatives.
- You can cross-certify (or create a qualified subordination trust relationship with) other certification authorities. This method provides you with even more control over the usages and certificate parameters that you will allow to be trusted in your organization.

The use of either certificate trust lists or qualified subordination is the most secure way to deploy third-party trusted roots in your organization. This topic is discussed in more detail in Chapter 4, "Designing the Public Key Infrastructure."

Managing User Control over Trusted Roots

You can also use Group Policy to prevent users from opting to trust new root CAs. This is particularly important if you have created your own qualified subordination trusts or Certificate Trust Lists in order to control the use of third-party certificates in your organization. You can find the procedure for using Group Policy to manage user control over trusted roots in the "To prevent users from selecting new root certification authorities with a Group Policy" online Help section, or from the link listed in the "More Information" section.

Summary

If you performed all the procedures in this chapter you have completed the following tasks:

- Installed and configured an offline root CA.
- Installed and configured an online issuing CA.
- Installed and configured a Web server to publish CRLs and CA certificates.
- Configured administrative groups and users to manage the CAs and Active Directory PKI configuration information.
- Configured Active Directory and Group Policy to support your PKI.

You are now ready to configure applications to use the PKI. This is described in the next two chapters of this guide: Chapter 8, "Implementing the RADIUS Infrastructure," and Chapter 9, "Implementing the Wireless LAN Security Infrastructure."

You should also now read the relevant parts of Chapter 11, "Managing the Public Key Infrastructure" and ensure that the relevant operations personnel are acquainted with it. This chapter contains essential information about how to keep your PKI running in a secure and reliable manner.

More Information

General Background Information on PKI and Windows Certificate Services

- For a good introduction to PKI concepts and the features of Windows 2000 certificate services, see *An Introduction to the Windows 2000 Public-Key Infrastructure* at www.microsoft.com/technet/archive/windows2000serv/evaluate/featfunc/pkiintro.mspx
- For a description of the enhanced PKI functionality in Windows Server 2003 and Windows XP, see *PKI Enhancements in Windows XP Professional and Windows Server 2003* at www.microsoft.com/technet/prodtechnol/winxppro/plan/pkienh.mspx
- For background product documentation that discusses key concepts and administration tasks, see the "Certificate Services" section of online Help or the Public Key Infrastructure section of the Windows Server 2003 product documentation at www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/SE_PKI.asp

Information on Specific Topics

- For more information about deploying a PKI in a multi-forest Active Directory environment, see "To publish certificates in a foreign Active Directory forest" in the Windows Server 2003 product documentation at www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_CS_procs_xforest_cert_pub.asp.
- CAPICOM can be downloaded from the Microsoft Download Center at www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=860EE43A-A843-462F-ABB5-FF88EA5896F6. However, you may want to search for "CAPICOM" on the Download Center site to ensure that you are getting the latest version.

- For instructions on how to use the Microsoft Baseline Security Analyzer (MBSA), see the Microsoft Baseline Security Analyzer v1.2 page at www.microsoft.com/technet/security/tools/mbsahome.mspx.
- For information about Active Directory domain functional levels and instructions on how to change between them, see the following sections of the Windows Server 2003 product documentation.
  - The Domain and forest functionality section at www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_levels.asp describes the different domain and forest levels.
  - The page titled "To raise the domain functional level" at www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_changedomlevel.asp describes how to change the domain and forest level.
- For more information about the ADPrep tool, see Microsoft Knowledge Base article Q325379, "How to upgrade Windows 2000 domain controllers to Windows Server 2003" at http://support.microsoft.com/?kbid=325379
  and the ADPrep page at www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/adprep.asp.
- For more information about ADPrep patch level requirements, see Microsoft Knowledge Base article Q331161, "Hotfixes to install on Windows 2000 domain controllers before running Adprep /Forestprep" at http://support.microsoft.com/?kbid=331161.
- For a fuller discussion of Certificate Services administrative roles, see "Managing role-based administration" in the Windows Server 2003 product documentation at www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_CS_Manage_Role_based_admin_topnode.asp.
- For more information about the server security settings and server roles used in this guide, see the *Windows Server 2003 Security Guide* at http://go.microsoft.com/fwlink/?LinkId=14845.
- For instructions on creating and modifying certificate templates, see the technical paper *Implementing and Administering Certificate Templates in Windows Server 2003* at www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspx
  and the Manage certificate templates for an enterprise certification authority section of the product documentation at www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_CS_procs_temps.asp.
- For information about how to disable automatic trust for third-party CAs, see "To prevent users from trusting third-party root certification authorities with a Group Policy" at www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/sag_pkpprocsconfig3rdpartyrootca.asp.
- For information about how to manage user control over trusted roots, see "To prevent users from selecting new root certification authorities with a Group Policy" at www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/sag_pkpprocsconfigtrustedrootca.asp.

- For more information about certificate autoenrollment, see *Certificate Autoenrollment in Windows XP* at www.microsoft.com/WindowsXP/pro/techinfo/administration/autoenroll/default.asp
  and "Checklist: Configuring certificate autoenrollment" at www.microsoft.com/resources/documentation/WindowsServ/2003/datacenter/proddocs/en-us/certsrv_checklist_autoenroll.asp.
- For more information about advanced certificate enrollment, see Advanced Certificate Enrollment and Management at www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/advcert.mspx.
- For more information about web enrollment, see Configuring and Troubleshooting Windows 2000 and Windows Server 2003 Certificate Services Web Enrollment at www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/webenroll.mspx.
- For more information about managing a Windows PKI (in addition to the information in Chapter 11, "Managing the PKI"), see the *Windows Server 2003 PKI Operations Guide* at www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03pkog.mspx.

8

Implementing the RADIUS Infrastructure

Introduction

This chapter provides detailed guidance for building a RADIUS (Remote Authentication Dial-In User Service) infrastructure for wireless LAN (WLAN) security based on Microsoft® Windows Server™ 2003 Internet Authentication Service (IAS). This guidance includes the installation and configuration of the RADIUS servers, the preparation of the Active Directory® directory service, and the configuration of IAS server settings. The RADIUS infrastructure will be used in the next chapter to build a complete wireless LAN solution.

This chapter's objective is to provide implementation guidance for the RADIUS design described in Chapter 5, "Designing the RADIUS Infrastructure for Wireless LAN Security." The chapter does not try to explain any of the general concepts of RADIUS or any of the specifics of how IAS implements the RADIUS protocol.

The chapter is a companion to the RADIUS and WLAN Planning Guide and Operations Guide chapters. The Planning Guide chapters explain the rationale behind the implementation decisions used in this chapter, and the Operations Guide chapter explains the tasks and processes needed to successfully maintain the RADIUS infrastructure. If you have not already done so, it is strongly recommended that you read the planning chapters before you continue with this chapter. You should also read and understand the implications of the support requirements in the operations chapter before you use the guidance in this chapter to implement your RADIUS infrastructure.

Chapter Prerequisites

This section contains checklists that will help you establish your organization's readiness to implement the RADIUS infrastructure. ("Readiness" here is meant in a logistical sense rather than business sense – the business motivation for implementing this solution is discussed in the early Planning Guide chapters.)

Knowledge Prerequisites

You should be familiar with concepts of RADIUS and IAS in particular. Familiarity with Windows 2000 Server or Windows Server 2003 is also required in the following areas:

- Installation of the Microsoft Windows® operating system.
- Active Directory concepts (including Active Directory structure and tools; manipulating users, groups, and other Active Directory objects; and use of Group Policy).
- Windows system security; security concepts such as users, groups, and auditing; access control lists (ACL); the use of security templates; and the application of security templates using Group Policy or command line tools.
- An understanding of batch file scripting. Knowledge of Windows Scripting Host and the Microsoft Visual Basic® Scripting Edition (VBScript) language will help you get the most out of the supplied scripts, but is not essential.

Before you read this chapter, you should also read Chapter 5, "Designing the RADIUS Infrastructure for Wireless LAN Security" and have a thorough understanding of the architecture and design of the solution.

Organizational Prerequisites

You should consult with other members of your organization who may need to be involved in the implementation of this solution, such as:

- Business sponsors.
- Security and audit personnel.
- Active Directory engineering, administration, and operations personnel.
- DNS (Domain Name System) and network engineering, administration, and operations personnel.

IT Infrastructure Prerequisites

The chapter makes the following assumptions about the existing IT infrastructure:

- A deployed Windows Server 2003 Active Directory domain infrastructure exists. All users of the RADIUS infrastructure in this solution should be members of domains within the same Active Directory forest.

Note: For more information about compatibility with earlier versions of Microsoft Windows, please see Appendix A, "Windows Version Support Matrix."

- This solution does not include guidance for integration into an existing RADIUS infrastructure, however this does not preclude deployment alongside an existing RADIUS infrastructure.
- Server hardware capable of running Windows Server 2003 IAS is available. A suggested configuration is provided as part of the guidance.
- Windows Server 2003 Standard Edition and Enterprise Edition licenses, installation media, and product keys are available.

Chapter Overview

The following figure shows the process of building the RADIUS infrastructure as detailed in this chapter.

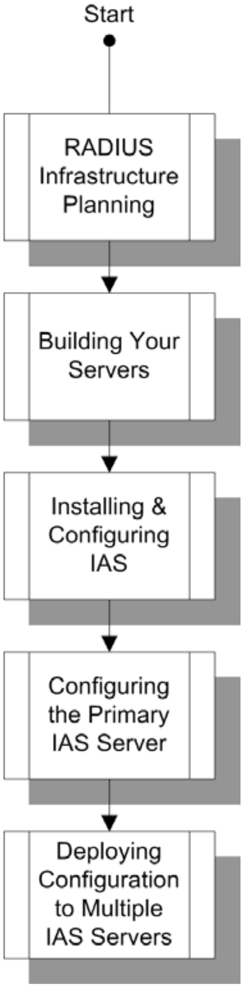
Start
RADIUS Infrastructure Planning
Building Your Servers
Installing & Configuring IAS
Configuring the Primary IAS Server
Deploying Configuration to Multiple IAS Servers

Figure 8.1
Diagram of the process of building the RADIUS infrastructure

These steps are mirrored in the organization of the chapter, and are described in the following list. Each consists of installation or configuration tasks and one or more verification procedures so that you can check what you have just completed before continuing with the next step.

- **IAS Planning Worksheet**. Lists the configuration information used in this chapter to install and configure IAS. It includes a table of information that you must provide before beginning implementation.
- **Building Your Servers**. Describes the selection and configuration of hardware, installation of Windows Server 2003, and the installation of optional components. It also describes the creation of Active Directory management security groups, how to set the correct permissions for delegating management tasks, and the implementation of operating system level security by applying security templates. The templates that are used are from the *Windows Server 2003 Security Guide*. Information about how to obtain this guide can be found at the end of this chapter. This section also lists a few common tasks that complete the base installation of the servers.
- **Installing and Configuring IAS**. Discusses the preparation steps, software installation, and configuration of IAS, including creating and securing IAS data directories.
- **Configuring the Primary IAS Server** Describes configuration of the primary IAS server that will be used as the configuration template for additional IAS servers of similar roles in the environment. It also discusses export of IAS configuration for use on other IAS servers. This procedure will be used again in subsequent chapters after more extensive configuration has been performed.
- **Configuring the Secondary IAS Server**. Describes configuration of the secondary IAS server that will join the primary IAS server in a RADIUS server pair for fault resilience and load balancing. It also describes how to import the primary IAS configuration for automated deployment. This procedure will be used again in subsequent chapters after more extensive configuration has been performed.
- **Configuring Branch Office IAS Servers**. Describes configuration of an optional branch office IAS server that can be used as an example for distributed environments, and how to import the primary IAS configuration for automated deployment. This procedure will be used again in subsequent chapters after more extensive configuration has been performed.

RADIUS Infrastructure Planning Worksheet

The following tables list the configuration parameters used in this solution. You should use these as a checklist for your planning decisions.

Many of the parameters in these tables are set manually as part of the documented procedures in this chapter. Others are either set by a script that is run as part of one of the procedures or referenced by a script in order to complete some other configuration or operational task.

Note: The scripts used in the Build Guide are described in more detail in the ToolsReadme.txt file that accompanies the scripts.

User-Defined Configuration Items

The following table lists organization-specific parameters taken from the fictitious Woodgrove Bank. You should ensure that you have collected or decided on the equivalent settings for your own organization for all of these items before you begin the setup procedure. Throughout the chapter, the fictitious values shown here are used in the sample commands given. You should substitute values appropriate for your own organization in place of these values. The places where you need to substitute your own values are shown in Italics.

Table 8.1: User-Defined Configuration Items

Configuration item	Setting
DNS name of Active Directory forest root domain	*woodgrovebank.com*
NetBIOS (network basic input/output system) name of domain	*WOODGROVEBANK*
Server name of primary IAS server	*HQ-IAS-01*
Server name of secondary IAS server	*HQ-IAS-02*
Server name of secondary IAS server	*BO-IAS-03*

Solution-Prescribed Configuration Items

The settings specified in this table do not need to be changed for a specific installation unless you have a specific need to use a setting that is different from the solution design. Changing the design parameters given here is acceptable if you understand that you are departing from the tested solution guidance. Ensure that you fully understand the implications of changing a setting and the dependencies that the setting might have before altering any values in the configuration procedures or supplied scripts.

Table 8.2: Solution-Prescribed Configuration Items

Configuration item	Setting
[Accounts] Full name of the administrative group that controls the configuration of IAS	IAS Admins
[Accounts] Pre-Windows 2000 name of the administrative group that controls the configuration of IAS	IAS Admins
[Accounts] Full name of the group that reviews IAS authentication and accounting request logs for security purposes	IAS Security Auditors
[Accounts] Pre-Windows 2000 name of group that reviews IAS authentication and accounting request logs for security purposes	IAS Security Auditors
[Scripts] Path for installation scripts	C:\MSSScripts
[Scripts] IAS configuration export batch file	IASExport.bat
[Scripts] IAS configuration import batch file	IASImport.bat
[Scripts] IAS RADIUS client configuration export batch file	IASClientExport.bat
[Scripts] IAS RADIUS client configuration import batch file	IASClientImport.bat
[Config] Path for configuration backup files	D:\IASConfig
[Request Logs] Location of IAS authentication and auditing request logs	D:\IASLogs
[Request Logs] Share name of RADIUS request logs	IASLogs

Preparing for IAS

The solution includes two centrally located IAS servers configured as RADIUS servers for WLAN access control. The solution also includes an optional branch office IAS server configured as a RADIUS server for environments that require distributed infrastructure. For more information about IAS server placement, see Chapter 5, "Designing the RADIUS Infrastructure for Wireless LAN Security."

You must complete a number of preparation tasks prior to the installation of IAS, such as:

- Configuring server hardware.
- Installing server operating system software.
- Preparing Active Directory.
- Performing server security hardening tasks.

Building Your Servers

The following sections describe the steps for building your servers. Although building each server can occur independently, it is important that all steps be completed on each of the servers.

Specifying Server Hardware

Server hardware for IAS should be selected from the Windows Server 2003 Hardware Compatibility List (HCL). Selecting server hardware from the Windows Server 2003 HCL helps to avoid reliability and compatibility issues that may arise with untested hardware or poorly written device drivers. You can find more information about the Windows Server 2003 HCL in the "More Information" section at the end of this chapter.

Tested Server Hardware Specifications

The following hardware specifications were used when testing this solution in a lab environment. These hardware specifications are for reference only and are not mandatory. For further discussion of IAS server hardware requirements, see Chapter 5, "Designing the RADIUS Infrastructure for Wireless LAN Security."

Table 8.3: Tested Server Hardware Specifications

Resource	Requirement
CPU	Dual CPU 850–MHz or better.
Memory	512 MB.
Network interfaces	2 x single network interface card (NIC) teamed for resilience.
Disk storage	IDE (integrated device electronics) or SCSI (small computer system interface) RAID (redundant array of independent disks) controller. 2 x 9 GB (SCSI or IDE) configured as RAID 1 volume (drive C). 2 x 18 GB (SCSI or IDE) configured as RAID 1 volume (drive D). Local removable media storage (CD-RW or tape for backup) if no network backup facility. 1.44-MB disk drive for data transfer.

Preparing Hardware

Complete all hardware configurations as recommended by the hardware vendor. These configurations may include applying the latest BIOS (basic input/output system) and firmware updates from your vendor.

Use the disk controller management software supplied with your hardware to create the RAID 1 volumes as outlined in the preceding table.

Installing Windows Server 2003

This section details the installation of Windows Server 2003 on the IAS servers. Many organizations already have an automated server installation process. You can use this for the server builds providing that the parameters used in the following procedure can be included in the build. For information about whether to use Windows Server 2003 Standard Edition or Windows Server 2003 Enterprise Edition, see Chapter 5, "Designing the RADIUS Infrastructure for Wireless LAN Security."

Perform the following steps to install Windows Server 2003 on one of the IAS servers.

▶ **To install Windows Server 2003**

1. Ensure that the CD-ROM has been set as a bootable device in the server BIOS settings. Restart the computer with the Windows Server 2003 CD in the CD-ROM drive.
2. Create a partition on the primary volume, format it as NTFS file system (NTFS), and select the option to install Windows on that partition.
3. Select the appropriate regional settings.
4. Type name and company information against which Windows will be registered.
5. Type a strong password for the local administrator account (at least 10 characters and a mixture of uppercase and lowercase alpha, numeric, and punctuation characters).
6. Type the computer name when prompted (replace this value with the name of your computer):
    - Primary IAS: *HQ-IAS-01*
    - Secondary IAS: *HQ-IAS-02*
    - Branch office IAS: BO-IAS-03
7. When prompted, select the option to join a domain. Enter the name of the Active Directory domain into which the servers will be joined: ***WOODGROVEBANK*** (replace this value with domain name into which you are installing the RADIUS server). When prompted, enter the credentials of a user who is authorized to join computers to this domain.

    Note: For a multi-forest domain, the IAS servers would typically be installed in the forest root domain to optimize Kerberos operations. Although this configuration is not essential, it is assumed in this solution.

8. Do not install any optional components.

    The computer will restart at the end of the main setup process. Continue with the following steps.
9. Install any current services packs, critical updates and any other required updates.
10. Reassign the CD-ROM/DVD drive the letter R.
11. Create a partition on the second hard drive volume, assign this partition drive letter D, and format it with NTFS.
12. Activate this copy of Windows.

Network Settings

The IAS servers have a single network interface (although this configuration may be implemented by teaming two physical NICs for added resiliency). The network interface should be configured with a fixed Internet Protocol (IP) address and other IP configuration parameters (such as default gateway and DNS settings) as appropriate for your network.

Verifying the Installation

You should verify that the operating system installation has completed correctly and that the configured parameters are consistent with what you expected.

▶ **To view the Current System configuration**

1. Run the `systeminfo` program at a command prompt.
2. Verify the following elements of the systeminfo output (some detail from the output has been omitted for brevity):

```
Host Name:                   HQ-IAS-01
    OS Name:                 Microsoft® Windows® Server 2003,
                                 Enterprise Edition
...
OS Configuration:            Member Server

Registered Owner:            YourOwnerName
Registered Organization:     YourOwnerOrganization
...
Windows Directory:           C:\WINDOWS
System Directory:            C:\WINDOWS\System32
Boot Device:                 \Device\HarddiskVolume1
System Locale:               YourSystemLocale
Input Locale:                YourInputLocale
Time Zone:                   YourTimeZone
...
Domain:                      woodgrovebank.com
Logon Server:                \\DomainControllerName
Hotfix(s):                   X Hotfix(s) Installed.
                             [01]: Qxxxxxx
...
                             [nn]: Qnnnnnn
NetWork Card(s):             1 NIC(s) Installed.
                             [01]: ModelAndVendorofNetworkCard
                             Connection Name: Local Area Connection
                             DHCP Enabled:    No
                             IP address(es)
                             [01]: xxx.xxx.xxx.xxx
```

3. If these settings do not match what you expected, you should reconfigure the server through Control Panel or rerun the installation.

Installing Configuration Scripts onto Servers

A number of support scripts and configuration files are supplied with this solution to help simplify some aspects of the configuration and operation of the solution. You must install these onto each of the servers. Some of these scripts will be required by the operations described in Chapter 12, "Managing the RADIUS and WLAN Security Infrastructure," so you should not delete them following completion of the RADIUS server installation.

▶ **To install the setup scripts on each server**

1. Create a folder called **C:\MSSScripts**.
2. Copy the scripts from the distribution media to this folder.

Checking Service Packs and Security Updates

You should recheck the list of service packs and security updates installed at this point. Use a tool such as the Microsoft Baseline Security Analyzer (MBSA) to perform the check and obtain any required updates. After suitable testing, install them on the server(s).

For more information about MBSA, see the "More Information" section at the end of this chapter.

Installing Additional Software

This section describes the installation of any additional software required on the IAS servers.

CAPICOM

CAPICOM 2.0 is required on the RADIUS servers for some of the setup and management scripts supplied with this solution. Information about where to find the latest version of CAPICOM is in the "More Information" section at the end of this chapter.

Follow the instructions in the self-extracting executable to install and register the CAPICOM dynamic-link library (DLL) library before proceeding with this guidance.

Validating Network and Active Directory Connectivity

IAS is heavily dependent on correct network configuration and connectivity to Active Directory. Therefore, consider running network diagnostics on the server prior to deployment of IAS.

You can perform network diagnostics with the Netdiag.exe utility from the Windows Server 2003 Support Tools, which can be found on the Windows Server 2003 CD. Netdiag.exe can be extracted by executing the following command:

```
expand r:\support\tools\support.cab –f:netdiag.exe c:\mssscripts
```

Upon completion, type the following command to run the utility:

```
C:\mssscripts\netdiag.exe
```

Be sure to investigate any errors or warnings that are displayed.

Verifying Domain Functionality Level

The preferred model for controlling network access is to leverage the **Control access through Remote Access Policy** setting on user accounts within Active Directory. The **Control access through Remote Access Policy** setting is only available when Active Directory is running in Windows 2000 native mode or higher. Therefore, you should check the domain functionality level prior to deployment of Remote Access Policy (RAP) on IAS.

You can check the domain functionality level by viewing the properties of the domain within the Active Directory Domains and Trusts tool. If the destination domain for IAS is configured in Windows 2000 mixed mode, contact appropriate Active Directory administrators to plan migration to native mode.

For more information about this topic, see the "More Information" section at the end of this chapter.

Configuring Active Directory Security Groups

IAS is part of your network security infrastructure. Accordingly, access to IAS configuration and log files should be strictly controlled. A combination of Active Directory global groups and Windows Server 2003 local groups are used to implement the required access controls.

Creating IAS Administration Groups

Run the following script as a domain administrator to create IAS Administration security groups:

```
Cscript //job:CreateIASGroups C:\MSSScripts\IAS_Tools.wsf
```

This script creates the following security groups as domain global groups:

- IAS Admins
- IAS Security Auditors

For a multi-domain forest, these groups should be created in the same domain as the IAS servers.

Note: Organizations with administrators located in multiple domains should consider using universal groups instead of the global groups created here. The script that creates the security groups may be easily modified by using the syntax used to create the group Remote Access Policy – Wireless Access in the next chapter (see "Creating Active Directory Groups Required for WLAN Access" in chapter 9).

Configuring IAS Administrators Group

IAS is a core component of the Windows Server 2003 operating system, and membership in the local Administrators security group is required to perform IAS configuration tasks.

You must add the IAS Admins domain global group into the local Administrators group on each IAS server. If IAS is installed on a domain controller, you must add the IAS Admins to the Administrators group for the domain using the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in.

Warning: Adding groups to the built–in Administrators domain group has serious security consequences. For more information, please see the discussion on co-locating IAS on domain controllers in Chapter 5, "Designing the RADIUS Infrastructure for Wireless LAN Security."

You should populate the IAS Admins and IAS Security Auditors groups with the accounts of the appropriate administration personnel. For a full description of how these groups map to administrative roles of IAS, see the discussion on administrative permission planning in Chapter 5, "Designing the RADIUS Infrastructure for Wireless LAN Security."

The setup procedures in the remainder of this document require you to use accounts that are members of the IAS Admins group.

Securing Windows Server 2003 for IAS

You should take whatever additional steps are necessary to secure the IAS servers from unauthorized access. IAS servers are a core part of your security infrastructure, and you should treat them with the same consideration given to firewalls and other security access infrastructure.

Physical Security

You should house the IAS servers in a location where physical access is strictly controlled. These servers need to be continuously online and so should be stored in a location with typical computer server room facilities such as temperature control, air filtering, and fire extinguishing capabilities.

The location for the servers should be chosen to be as free as possible from external risks that might damage the server, such as fire and floods.

It is equally important to control physical access to, and ensure the physical safety of, backups, documentation, and other configuration data. This information should be stored at a different location than the servers themselves.

Applying System Security Settings on the Servers

The IAS servers are secured through use of the IAS server role defined in the *Windows Server 2003 Security Guide*. More information about this guide and the location for downloading the security templates is available in the "More Information" section at the end of this chapter.

Because the IAS servers are members of a domain, the security policy settings are applied using domain-based Group Policy. You must create a suitable organizational unit (OU) structure to hold the IAS server computer objects and a Group Policy object (GPO) structure to apply the security settings. You must create two GPOs for IAS servers running on dedicated servers (that is, not installed on domain controllers):

- Enterprise Client–Member Server Baseline
- Enterprise Client–Internet Authentication Service

After reviewing Chapter 5, "Designing the RADIUS Infrastructure for Wireless LAN Security," you may decide to run some or all of your IAS services on domain controllers. Due to the complexity of hardening domain controllers, this document does not provide instruction on how to apply domain controller security templates. The *Windows Server 2003 Security Guide* includes a template for domain controllers, which performs a lockdown similar to that of the Member Server Baseline policy. You should apply the Domain Controllers security template to existing domain controllers only after reading the *Windows Server 2003 Security Guide* carefully and assessing any potential impact on your domain clients and applications.

If you use the Enterprise Client–Domain Controller security template on your combined IAS and domain controller servers, you will also need to apply the Enterprise Client–IAS Server security template to those computers. This template applies additional settings that enable the IAS service. (The IAS service is disabled in the Enterprise Client–Domain Controller template.) To apply this template, you should create one additional GPO to be applied in a new child OU located below the Domain Controllers OU:

- Enterprise Client–IAS on Domain Controllers

You should perform the following procedure to import the Enterprise Client–IAS Servers template into this GPO. This procedure describes how you to create the OUs and GPOs. The GPO and OU names are only examples; you should adapt the procedure to your own domain OU and GPO standards.

▶ To create the IAS servers OUs and GPOs

1. Obtain the following security templates from the *Windows Server 2003 Security Guide*:
   - Enterprise Client–Domain
   - Enterprise Client–Member Server Baseline
   - Enterprise Client–IAS Server
   - Enterprise Client–Domain Controller
2. Log on as a member of Domain Admins or a user who has rights to create the OUs described in step 4. You will need to be a member of Domain Admins or the Group Policy Creator Owners group to create GPOs.
3. Open the Active Directory Users and Computers MMC snap-in.
4. Create the following OU structure:

```
woodgrovebank.com
 -  Member Servers
     - IAS
 -  Domain Controllers
     - Domain Controllers with IAS
```

Warning: Steps 5 through 7 apply domain policies that configure local account policies on all computers in the domain. You should examine the settings in the Enterprise Client – Domain security template. Instead of applying it to the whole domain you may want to create this GPO linked to the IAS OU so that its scope is restricted to just the IAS servers.

---

5. Open the properties of the domain container. From the **Group Policy** tab, click **New** to create a new GPO and name it **Domain Policy**.
6. Edit the GPO, and navigate to Computer Configuration\Windows Settings\Security Settings. Right-click the **Security Settings** folder, and then click **Import**. Browse to the file Enterprise Client–Domain.inf, and select it as the template to import.
7. Close the GPO.
8. Repeat the previous three steps for the combination of OUs, GPOs, and security templates shown in the following table. (These three GPOs only affect the IAS servers, so the previous warning does not apply here.)

Table 8.4: Group Policy Objects and Location

OU	GPO	Security template
Member Servers	Enterprise Client–Member Server Baseline	Enterprise Client–Member Server Baseline.inf
IAS	Enterprise Client–Internet Authentication Service	Enterprise Client–IAS Server.inf
Domain Controllers with IAS	Enterprise Client–IAS on Domain Controllers (optional if IAS is on a domain controller)	Enterprise Client–IAS Server.inf

After you create the GPOs and import the templates, you must customize the settings in the GPOs and apply them to the IAS server computers according to the following procedure.

▶ To customize and apply the Enterprise Client–Internet Authentication Service GPO

1. From Active Directory Users and Computers, edit the Enterprise Client–Internet Authentication Service GPO. In Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options, change the following items in accordance with your organization's security standards:
    - Accounts: Rename administrator account: *NewAdminName*
    - Accounts: Rename guest account: *NewGuestName*
    - Interactive logon: Message text for users attempting to log on: *LegalNoticeText*
    - Interactive logon: Message title for users attempting to log on: *LegalNoticeTitle*
2. In Local Policies\User Rights Assignment, add the following local and domain groups to the **Allow Log on Locally** right:
    - (local) *Administrators*
    - (local) *Backup Operators*
    - (domain) IAS Security Auditors
3. Open the properties of the following services in the System Services folder and click **Define this policy setting in the template**. Accept the default permissions by clicking **OK**. Set the value of **Set service startup mode** to **Automatic**
    - Removable Storage
    - Volume Shadow Copy
    - MS Software Shadow Copy Provider
    - Task Scheduler

    Note: These services are disabled in the member server baseline security template, but the first three are required by NTBackup.exe. The Task Scheduler service is required by some of the operational scripts.

4. Move the IAS server computer account into the IAS OU.
5. On the IAS server, execute the `gpupdate` command to apply the GPO settings to the computer.

    Note: The *Windows Server 2003 Security Guide* contains a more detailed discussion of these security settings. See the "More Information" section at the end of this chapter for information about obtaining this guide.

▶ To customize and apply the Enterprise Client–IAS on Domain Controllers GPO

1. From Active Directory Users and Computers, edit the Enterprise Client–IAS on Domain Controllers GPO. In Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options, change the following items in accordance with your organization's security standards:
   - Accounts: Rename administrator account: *NewAdminName*
   - Accounts: Rename guest account: *NewGuestName*
   - Interactive logon: Message text for users attempting to log on: *LegalNoticeText*
   - Interactive logon: Message title for users attempting to log on: *LegalNoticeTitle*
2. In Local Policies\User Rights Assignment, add the following local and domain groups to the **Allow Log on Locally** right:
   - (Builtin) *Administrators*
   - (Builtin) *Backup Operators*
   - (domain) IAS Security Auditors
3. Open the properties of the following services in the System Services folder and click **Define this policy setting in the template**. Accept the default permissions by clicking **OK**. Set the value of **Set service startup mode** to **Automatic**.
   - Removable Storage
   - Volume Shadow Copy
   - MS Software Shadow Copy Provider
   - Task Scheduler

   Note: These services are disabled in the member server baseline security template, but the first three are required to allow NTBackup.exe to run. The Task Scheduler service is required by some of the operational scripts.

4. Move the IAS server computer account into the Domain Controllers with IAS OU.
5. On the IAS server, execute the `gpupdate` command to apply the GPO settings to the computer.

   Note: The *Windows Server 2003 Security Guide* contains a more detailed discussion of these security settings. See the "More Information" section at the end of this chapter for information about obtaining this guide.

Verifying Security Settings

To verify the correct application of security settings, perform the steps in the following procedure.

▶ **To verify the IAS server security settings**

1. Check the Application Event log for events from the SceCli source. There should be an event ID 1704 following the **gpupdate** command. The text of the event should read as follows:

   ```
   Security policy in the Group Policy objects has been applied
   successfully.
   ```

2. Restart the server, and verify that all expected services start and that no errors are logged to the system event log.
3. You should be able to log on and you should see the legal notice text.

Configuring Terminal Services Security

You should use Terminal Services for scheduled changing of the passwords (RADIUS secrets) used by RADIUS clients. Terminal Services traffic encryption protects the RADIUS secrets as they pass across the network.

Important: If another method is used to set or change RADIUS client secrets over the network (such as using telnet or other simple remote execution tool), ensure that Internet Protocol Security (IPsec) or another appropriate technology is used to protect the information in transit.

The following Terminal Services settings should be configured in the Enterprise Client–IAS on Domain Controllers GPO and the Enterprise Client–Internet Authentication Service GPO that apply to the IAS servers.

Table 8.5: Settings to Configure in Computer Configuration\Administrative Templates\Windows Components\Terminal Services

Path	Policy	Setting
	Deny log off of an administrator logged in to the console session	Enabled
	Do not allow local administrators to customize permissions	Enabled
	Sets rules for remote control of Terminal Services user sessions	No remote control allowed
Client\Server data redirection	Allow Time Zone Redirection	Disabled
	Do not allow clipboard redirection	Enabled
	Allow audio redirection	Disabled
	Do not allow COM port redirection	Enabled
	Do not allow client printer redirection	Enabled
	Do not allow LPT port redirection	Enabled
	Do not allow drive redirection	Enabled
	Do not set default client printer to be default printer in a session	Enabled
Encryption and Security	Set Client Connection Encryption Level	High
	Always prompt client for a password on connection	Enabled
Encryption and Security\RPC Security	Secure Server (Require Security)	Enabled
Sessions	Set time limit for disconnected sessions	10 minutes
	Allow reconnection from original client only	Enabled

Any domain account or security group requiring Terminal Service access to the IAS servers must be added to the local Remote Desktop Users group (unless it is already a member of the local Administrators group).

Remaining Windows Configuration Tasks

There will be other configuration tasks, depending on the infrastructure and standards in your organization. For example:

- Enabling backups or installing backup agents.
- Configuring Simple Network Management Protocol (SNMP) or Windows Management Instrumentation (WMI) options.
- Installing management agents such as Microsoft Operations Manager (MOM) or Microsoft Systems Management Server (SMS) client components.
- Installing antivirus software.
- Installing intrusion detection agents.

You should verify these items as they are installed.

Installing and Configuring IAS

This solution includes two centrally located IAS servers that act as RADIUS servers for authenticating users and authorizing network access. The solution also includes an optional branch office IAS server for environments that require distributed authentication and authorization of network access. For more information about IAS server placement, see Chapter 5, "Designing the RADIUS Infrastructure for Wireless LAN Security."

The following section describes the tasks to install IAS onto your servers. It is important that you perform all installation and configuration steps on each of your IAS servers.

Installing the IAS Software Components

IAS is installed with the Windows Optional Components Manager (accessed through **Add-Remove Components** in Control Panel). The following table lists the components to be installed. The indentation reflects the hierarchical relationship between the components as you would see them in the Optional Components Manager wizard Components that are not selected are not shown in the table.

Table 8.6: IAS Components for Installation

Optional Component to Be Installed	Install State
Network Services	Selected
Internet Authentication Service	Selected

Note: The Windows Server 2003 installation medium will be required to complete the installation.

▶ **To install IAS components**

- Run the Optional Components Manager on each IAS server to automate the installation of IAS; the following command will accomplish this task:

```
sysocmgr /i:sysoc.inf /u:C:\MSSScripts\OC_AddIAS.txt
```

Registering IAS in Active Directory

IAS servers must be registered in each domain. This means making the computer account of the IAS server a member of the RAS and IAS Servers security group in each domain for which they will be required to perform authentication. Membership of this group ensures that IAS servers have permission to read the remote access properties of users and computer accounts in the domain.

The computer account objects of the IAS servers can be put into this group using the Active Directory Users and Computers MMC snap-in or the Netshell (**netsh**) command.

▶ **To register IAS on servers in the default domain with the netsh command**

1. Log on to each IAS server with an account that has the Domain Admins privilege for the domain.
2. Open a command prompt and type:

```
netsh ras add registeredserver
```

▶ **To register IAS in domains other than the default domain with the netsh command**

1. Log on to each IAS server with an account that has the Domain Admins privilege for the target domain.
2. Open a command prompt and type the following, replacing *DomainName* with the name of the domain in which to register the IAS server:

```
netsh ras add registeredserver domain = DomainName
```

Note: Alternatively, you can add the IAS Server computer object into the RAS and IAS Servers security group using the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in.

Creating and Securing IAS Data Directories

You must create data directories on the IAS servers' data drives to store IAS configuration and log file data. Perform the following procedures at a command prompt on each IAS server to create and secure the IAS data directories. Alternatively, you can use the provided batch script to automate this procedure.

▶ **To create and secure IAS data directories**

- Run the following commands, replacing WOODGROVEBANK with the NetBIOS name of your domain:
  - md D:\IASConfig
  - md D:\IASLogs
  - cacls D:\IASConfig /G system:F administrators:F "Backup Operators":C
  - cacls D:\IASLogs /G system:F administrators:F "Backup Operators":C "WOODGROVEBANK\IAS Security Auditors":C

You should also share the D:\IASLogs directory to IAS Security Auditors so that they may access the RADIUS request log data remotely.

▶ **To share the IAS log directory securely**

- Run the following command, replacing WOODGROVEBANK with the NetBIOS name of your domain:

```
net share IASLogs=D:\IASLogs /GRANT:"WOODGROVEBANK\IAS
Security Auditors",CHANGE
```

An optional batch file has been created that contains the preceding commands, but it must be edited to include the correct NetBIOS name of your domain.

▶ **To edit and execute the batch file to create, secure, and share the IAS data directories**

1. Use Notepad to edit the C:\MSSScripts\IAS_Data.BAT file, and replace WOODGROVEBANK with the NetBIOS name of your domain.
2. Execute the batch file by running the following command at a command prompt:

```
C:\MSSScripts\IAS_Data.BAT
```

Configuring the Primary IAS Server

You should select one of the IAS servers in your environment as your primary server. You will configure this server before the other IAS servers and it will serve as a template for configuring the settings on subsequent IAS servers.

Configuring Logging of Authentication and Accounting Requests

IAS does not log RADIUS authentication and accounting requests by default. If possible, both types of request logs should be enabled to ensure that security events are logged and can be investigated at a later date. In addition, your organization may have a requirement to use accounting data for billing purposes.

Note: RADIUS request logging has an impact on server performance and requires procedures to ensure that logs do not fill data disks. See Chapter 5, "Designing the RADIUS Infrastructure for Wireless LAN Security," for more information about capacity planning, and Chapter 3, "Managing the RADIUS and Wireless LAN Security Infrastructure," for information about how to archive and delete log files.

▶ **To configure authentication and accounting logging on IAS Servers**

1. Use the Internet Authentication Service MMC snap‑in to select **Remote Access Logging**, and then view the properties of the **Local File** logging method.
2. Select **Accounting** requests (for example, accounting start or stop) and **Authentication** requests (for example, access-accept or access reject).

   Note: This guidance does not enable periodic status request logging. However, you may require this to accurately track user network session information. For more information, see Chapter 5, "Designing the RADIUS Infrastructure for Wireless LAN Security."

3. Ensure that the log file directory is set to D:\IASLogs and that **Database-compatible** format is selected.

Using the **Database-compatible** format allows you to import the request logs directly into databases such as Microsoft Access and Microsoft SQL Server™ 2000, which facilitates querying and reporting on the data.

Configuring IAS for Wireless LAN Access and Other Network Applications

You have now configured the base settings for IAS. The remainder of the chapter describes how to replicate the settings from the first IAS server to subsequent servers. Before you replicate these settings you must configure the remote access policies and other settings specific to your application. Chapter 9, "Implementing Wireless LAN Security" describes how to configure IAS for wireless LANs. After you configure the first server you can return to this chapter and follow the procedures to replicate the IAS settings to other servers.

Deploying Configuration to Multiple IAS Servers

You can use the **netsh** command to export portions of IAS configuration to text files. The following configuration areas can be exported individually:

- Server settings
- Logging configuration
- Remote access policies
- Connection request policies
- RADIUS clients
- Full configuration

These text files can be used to transfer common configuration settings across multiple IAS servers to ensure consistent configuration and speed your deployment. The following configuration sections can be common to servers of a similar role:

- Server configuration
- Logging settings
- Remote access policy
- Connection request polices

You should configure the preceding items only on the primary IAS server, then use the **netsh** command to export these items to text files. The text files can then be imported to additional IAS servers of a similar role. This process ensures that configuration text files of common configuration settings will be synchronized across all servers.

Each IAS server contains configuration of RADIUS clients with shared secret information that is usually unique to each server. Therefore, this information must be configured and backed up separately on each server.

Warning: Using **netsh** to perform a full dump produces a configuration text file with potentially sensitive RADIUS shared secret information. This guidance shows you how to deploy settings and perform backup without using a full dump of IAS settings. If you decide to use full dump configuration text files, be sure to handle and store them with extreme sensitivity. The information in these files allow anyone to gain access to your network.

The following sections describe the procedure for transferring configuration from the primary IAS server to additional IAS servers of a similar role. You can replicate the settings at this stage but only minimal configuration changes have so far been made to the IAS servers. You should perform this replication procedure again after more extensive IAS configuration changes have occurred in the following chapter, such as creation of network access policy and addition of RADIUS clients.

Exporting the Primary IAS Server Configuration

Export of the primary IAS server configuration is required to transfer settings to additional IAS servers used in this solution.

Batch files can automate the export of the common IAS configuration areas for backup and to aid in deployment of IAS settings across multiple IAS servers with the same role. When creating batch files for settings deployment, only include the following types of settings that are portable across IAS servers:

- Server configuration
- Logging settings
- Remote access policy
- Connection request polices

▶ **To export the common configuration on the primary IAS server**

- Type the following command at a command prompt:

```
C:\MSSScripts\IASExport.bat
```

This batch file contains a series of **netsh** commands that export the common configuration information to configuration text files in the D:\IASConfig directory.

Loading the Backup Configuration from the Primary Server

IAS uses the **netsh** command to transfer configuration state from one server to another. This process speeds deployment and reduces the chance of error during multi-server deployments. Primary IAS server configuration state text files that were created earlier can now be used to load configuration onto both the secondary IAS server and any branch office IAS servers.

Load the exported configuration text files from the primary IAS server to the other IAS server(s) by performing the following steps.

▶ **To load the common configuration from the primary IAS server to the other IAS server(s)**

1. Copy all configuration files from the D:\IASConfig directory on the primary IAS server to the D:\IASConfig directory on the other IAS server(s).
2. Use the following batch file to load the configuration from the configuration text files of the primary IAS server:

```
C:\MSSScripts\IASImport.bat
```

Summary

If you performed all the procedures in this chapter you should have completed the following tasks:

- Installed and configured the basic settings for a primary IAS server.
- Installed and configured a secondary IAS server.
- Installed and configured an optional branch office IAS server.
- Configured administrative groups used to manage the IAS servers.

You are now ready to configure WLAN specific settings, which is described in Chapter 9, "Implementing the Wireless LAN Security." You may then need to return to the final part of this chapter to replicate the IAS settings that will be configured in the next chapter.

You should also now read the relevant parts of Chapter 12, "Managing the RADIUS and Wireless LAN Security Infrastructure," which contains essential information about keeping your RADIUS infrastructure running in a secure and reliable manner.

More Information

- CAPICOM can be downloaded from the Microsoft Download Center at www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=860EE43A-A843-462F-ABB5-FF88EA5896F6. However, you may want to search for "CAPICOM" on the Download Center site to ensure that you are getting the latest version.
- The article "Managing Remote Access on a Per-Group Basis Using Windows 2000 Remote Access Policies" is available at www.microsoft.com/windows2000/techinfo/administration/management/pgremote.asp.
- The *Windows Server 2003 Security Guide* is available for download at http://go.microsoft.com/fwlink/?LinkId=14846.
- The "Internet Authentication Service" chapter of the *Windows Server 2003 Technical Reference*. This guidance can be found at http://go.microsoft.com/fwlink/?LinkId=4630.
- The "Deploying IAS" chapter of the *Windows Server 2003 Deployment Kit* can be found at: http://go.microsoft.com/fwlink/?LinkId=4716.
- Hardware qualifications for the Windows logo program are described in the "FAQ for Windows Logo Program for Hardware" at www.microsoft.com/whdc/winlogo/logofaq.mspx.
- The article "Microsoft Baseline Security Analyzer V1.2" is available at www.microsoft.com/technet/security/tools/mbsahome.mspx.
- 802.1X WLAN technologies are described in the article "Windows XP Wireless Deployment Technology and Component Overview" at www.microsoft.com/technet/prodtechnol/winxppro/maintain/wificomp.mspx

9

Implementing Wireless LAN Security

Introduction

This chapter provides detailed guidance for implementing wireless LAN (WLAN) security with the 802.1X protocol that is based on Microsoft® Windows Server™ 2003 and Microsoft Windows® XP Service Pack 1 (SP1). The guidance in this chapter includes the configuration of Active Directory® directory service security groups, the deployment of X.509 certificates for WLAN authentication, the modification of Microsoft Internet Authentication Service (IAS) server settings, the deployment of WLAN Group Policy, and tips for configuring wireless access points (APs). This chapter includes all of the settings required to implement WLAN security using 802.1X and EAP-TLS (Extensible Authentication Protocol-Transport Layer Security).

This chapter's objective is to provide implementation guidance for the secure WLAN design described in Chapter 6, “Designing the Wireless LAN Security Using 802.1X.“ The chapter does not try to explain any of the general concepts of 802.1X, EAP, RADIUS (Remote Authentication Dial-In User Service), or any of the specifics of an 802.1X-based secure WLAN implementation. For an overview of many of these technologies, see the article "Windows XP Wireless Deployment Technology and Component Overview," which is listed in the “More Information” section at the end of this chapter.

This chapter is a companion to the public key infrastructure (PKI), RADIUS, and WLAN Planning Guide and Operations Guide chapters. The Planning Guide chapters explain the rationale behind the implementation decisions used here. The Operations Guide chapter explains the tasks and processes needed to successfully maintain the 802.1X infrastructure. If you have not already done so, you should read the planning chapters before you continue with this chapter. You should also read and understand the implications of the support requirements in the operations chapter before you implement this guidance in a production environment.

Chapter Prerequisites

This section contains checklists that will help you decide on your organization's readiness to implement the 802.1X-based WLAN. (“Readiness” here is meant in a logistical sense rather than business sense–the business motivation for implementing this solution is discussed in the early Planning Guide chapters.)

Knowledge Prerequisites

You should be familiar with concepts of 802.1X and the implementation of this standard across the relevant Microsoft products, such as Windows Server 2003 and Windows XP Service Pack 1. Familiarity with Windows Server 2003 or Windows 2000 is also required in the following areas:

- Active Directory concepts (including Active Directory structure and tools; manipulating users, groups, and other Active Directory objects; and use of Group Policy).
- Windows system security; security concepts such as users, groups, and access control lists (ACLs); and the use of command line tools.
- An understanding of batch file scripting. Knowledge of Windows Scripting Host and the Microsoft Visual Basic® Scripting Edition (VBScript) language will help you get the most out of the supplied scripts, but is not essential.

Before proceeding with this chapter, you should also read the planning chapters and have a thorough understanding of the architecture and design of the solution.

Organizational Prerequisites

You should consult with other members of your organization who may need to be involved in the implementation of this solution, such as:

- Business sponsors
- Security and audit personnel
- Active Directory engineering, administration, and operations personnel
- Desktop engineering, administration, and operations personnel
- DNS (Domain Name System) and network engineering, administration, and operations personnel

IT Infrastructure Prerequisites

The chapter also assumes the following:

- A deployed Windows Server 2003 Active Directory domain infrastructure already exists. All users of the 802.1X solution should be members of domains within the same Active Directory forest.

Note: For more information about compatibility with earlier versions of Microsoft Windows, see Appendix A, “Windows Version Support Matrix.”

- That you have no existing 802.1X-based WLAN solution. Although this solution does not preclude deployment alongside an existing 802.1X WLAN solution, it includes no guidance for integration into an existing 802.1X infrastructure.
- A PKI has been deployed as described in Chapter 7, "Implementing the Public Key Infrastructure" and be ready to perform certificate autoenrollment.

- Supporting infrastructure such as DNS and Dynamic Host Configuration Protocol (DHCP) must be deployed and be ready to service WLAN client computers.
- Two or more servers running IAS as RADIUS servers as described in chapter 8, "Implementing the RADIUS Infrastructure." Further configuration of these servers will be performed during this chapter.
- A WLAN with 802.1X-compliant wireless APs and Windows XP Professional Service Pack 1 clients with 128-bit Wired Equivalent Privacy (WEP) or WPA and 802.1X-capable WLAN network interface cards (NICs). Further configuration of these components will be performed during this chapter.

Chapter Overview

This figure diagram shows the process of implementing the WLAN security using 802.1X as described in this chapter.

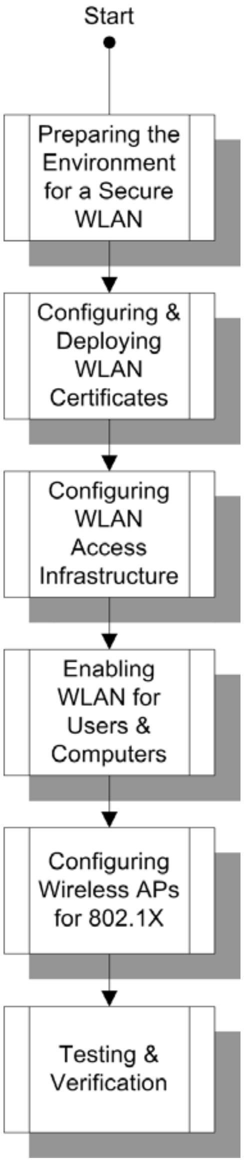
Start
Preparing the Environment for a Secure WLAN
Configuring & Deploying WLAN Certificates
Configuring WLAN Access Infrastructure
Enabling WLAN for Users & Computers
Configuring Wireless APs for 802.1X
Testing & Verification

Figure 9.1

Diagram of the process of implementing the 802.1X infrastructure

These steps are mirrored in the organization of the chapter, and are described in the following list. Each consists of installation or configuration tasks. Each step also has verification procedures so that you can check that everything is working before continuing with the next step.

- **802.1X WLAN Planning Worksheet**. Lists the configuration information used in this chapter to configure the various components of the 802.1X WLAN. It includes a table describing information that you must provide before commencing implementation of the guidance in this chapter.
- **Preparing the Environment for a Secure WLAN**. Describes the preparation of Active Directory security groups required to configure and manage the 802.1X WLAN over a period of time. In addition, high-level recommendations are provided for DHCP.
- **Configuring and Deploying WLAN Authentication Certificates**. Details the creation and deployment of X.509 certificate templates required for 802.1 X WLAN authentications. Deployment verification is also included.
- **Configuring WLAN Access Infrastructure**. Details the creation and configuration of IAS remote access policy for 802.1X and EAP-TLS networking. The addition of wireless APs as RADIUS clients to the IAS servers is also included.
- **Enabling WLAN Access for Users and Computers**. Describes the configuration of user and computer permissions through Active Directory to enable access to the secure WLAN. In addition, this section includes steps to create and deploy Active Directory Group Policy to configure WLAN clients with appropriate 802.1X and 802.11 settings.
- **Configuring Wireless APs for 802.1X Networking**. Lists topics that must be considered to configure wireless APs for 802.1X-based networking.
- **Testing and Verification**. Provides a procedure to allow you to test the functionality of your 802.1X-based WLAN.

802.1X WLAN Planning Worksheet

The tables in this section list the configuration parameters used in the solution. You should use these as a checklist for your planning decisions.

Many of the parameters in these tables are set manually as part of the documented procedures in this chapter. Many are either set by a script that is run as part of one of the procedures or referenced by a script in order to complete some other configuration or operational task.

Note: The scripts used in the Build Guide are described in more detail in the ToolsReadme.txt file that accompanies the scripts.

User-Defined Configuration Items

The following table lists organization-specific parameters taken from the fictitious Woodgrove Bank. You should ensure that you have collected or decided on the equivalent settings for your organization for all of these items before beginning the setup procedure. Throughout the chapter, the fictitious values shown here are used in the sample commands given. You should substitute values appropriate for your own organization in place of these. The places where you need to substitute your own values are shown in Italics.

Table 9.1: User-Defined Configuration Items

Configuration item	Setting
DNS name of Active Directory forest root domain	*woodgrovebank.com*
Network basic input/output system (NetBIOS) name of domain	*WOODGROVEBANK*
Server name of primary IAS server	*HQ-IAS-01*
Server name of secondary IAS server	*HQ-IAS-02*
Server name of optional branch office IAS server	*BO-IAS-03*

Solution-Prescribed Configuration Items

The settings specified in this table do not need to be changed for your installation unless you need to use a setting that is different from the solution design. Changing the provided design parameters is perfectly acceptable if you understand that you are departing from the tested solution by doing so. Ensure that you fully understand the implications of changing a setting and the dependencies that the setting might have before altering any of the values in the configuration procedures and supplied scripts.

Table 9.2: Solution-Prescribed Configuration Items

Configuration item	Setting
[Accounts] Active Directory global group controlling deployment of 802.1X user authentication certificates	AutoEnroll Client Authentication - User Certificate
[Accounts] Pre-Windows 2000 name for the Active Directory global group controlling deployment of 802.1X user authentication certificates	AutoEnroll Client Authentication - User Certificate
[Accounts] Active Directory global group controlling deployment of 802.1X computer authentication certificates	AutoEnroll Client Authentication - Computer Certificate
[Accounts] Pre-Windows 2000 name for the Active Directory global group controlling deployment of 802.1X computer authentication certificates	AutoEnroll Client Authentication - Computer Certificate
[Accounts] Active Directory global group containing IAS servers requiring 802.1X authentication certificates	AutoEnroll RAS and IAS Server Authentication Certificate
[Accounts] Pre-Windows 2000 name for the Active Directory global group containing IAS servers requiring 802.1X authentication certificates	AutoEnroll RAS and IAS Server Authentication Certificate
[Accounts] Active Directory global group that contains users allowed access to the wireless network	Remote Access Policy - Wireless Users
[Accounts] Pre-Windows 2000 name for the Active Directory global group that contains users allowed access to the wireless network	Remote Access Policy - Wireless Users
[Accounts] Active Directory global group that contains computers allowed access to the wireless network	Remote Access Policy - Wireless Computers
[Accounts] Active Directory global group that contains computers allowed access to the wireless network	Remote Access Policy - Wireless Computers
[Accounts] Active Directory universal group that contains both the Wireless Users group and the Wireless Computers group	Remote Access Policy - Wireless Access
[Accounts] Active Directory universal group that contains both the Wireless Users group and the Wireless Computers group	Remote Access Policy - Wireless Access
[Accounts] Active Directory global group that contains computers requiring configuration of wireless network properties	Wireless Network Policy - Computer
[Accounts] Active Directory global group that contains computers requiring configuration of wireless network properties	Wireless Network Policy - Computer
[Certificates] Certificate template used to generate certificates for user client authentication	Client Authentication - User

(continued)

[Certificates] Certificate template used to generate certificates for computer client authentication	Client Authentication - Computer
[Certificates] Certificate template used to generate server authentication certificates for use by IAS	RAS and IAS Server Authentication
[Scripts] Path for installation scripts	C:\MSSScripts
[Config] Path for configuration backup files	D:\IASConfig
[Request Logs] Location of IAS authentication and auditing text logs	D:\IASLogs
[Remote Access Policy] Policy name	Allow Wireless Access
[Group Policy] Active Directory Group Policy Object (GPO) name	Wireless Network Policy
[Group Policy] Wireless Network policy within the GPO	Client Computer Wireless Configuration

Preparing the Environment for a Secure WLAN

You must prepare the supporting infrastructure in your environment prior to implementing 802.1X-based secure wireless networking. Supporting infrastructure includes Active Directory and DHCP servers. For thorough WLAN planning guidance, see the "Deploying a Wireless LAN" chapter of the *Windows Server 2003 Deployment Kit* and other resources listed in the "More Information" section at the end of this chapter.

Creating Active Directory Groups Required for WLAN Access

You must run the following script as a user with permission to create Active Directory security groups. This script creates the required groups for wireless authentication certificate enrollment, remote access policy, and wireless network Group Policy:

```
Cscript //job:CreateWirelessGroups C:\MSSScripts\wl_tools.wsf
```

This script creates the following Active Directory-based security groups that are used throughout the rest of this guidance:

- AutoEnroll Client Authentication-User Certificate
- AutoEnroll Client Authentication-Computer Certificate
- AutoEnroll RAS and IAS Server Authentication Certificate
- Remote Access Policy-Wireless Users
- Remote Access Policy-Wireless Computers
- Remote Access Policy-Wireless Access
- Wireless Network Policy-Computer

For a multi-domain forest, these groups should be created in the same domain as the wireless users.

Note: Most groups created here are global groups but could be substituted for universal groups if required. The script that creates the security groups can be easily modified; copy the syntax used to create the Remote Access Policy - Wireless Access universal group.

Verifying DHCP Settings

To accommodate wireless networking, you should configure DHCP servers with wireless-specific scopes and Internet Protocol (IP) address lease times that are shorter than those of wired clients. Check with DHCP server administrators to ensure that you have configured your DHCP servers adequately to support a wireless solution.

For thorough DHCP planning guidance for wireless networking, see the "Deploying a Wireless LAN" chapter of the *Windows Server 2003 Deployment Kit.*

Configuring and Deploying WLAN Authentication Certificates

The secure WLAN solution detailed in this guidance uses X.509 certificates to perform computer and user authentication with EAP-TLS. The following section details the creation and deployment of the following certificates:

- Client Authentication - Computer
- Client Authentication - User
- RAS and IAS Server Authentication

Note: See Chapter 11, “Managing the Public Key Infrastructure,” for detailed information about these tasks and the roles required to perform them.

Creating a Certificate Template for Server Authentication

A server certificate is required on the IAS server to authenticate the computer to clients during the EAP-TLS protocol handshake. Have your Certificate Services administrator perform the following steps using the Certificate Templates Microsoft Management Console (MMC) snap-in on the Certificate Services server to create a server authentication certificate template for use with IAS servers.

▶ **To create a certificate template for server authentication**

1. Create a duplicate of the RAS and IAS Server certificate template. Type **RAS and IAS Server Authentication** into the **Template display name field** on the **General** tab of the new template’s properties.
2. On the **Extensions** tab, ensure that the application policies only include **Server Authentication** (OID 1.3.6.1.5.5.7.3.1).
3. Also on the **Extensions** tab, edit the Issuance policies and add the **Medium Assurance** policy.
4. On the **Subject Name** tab, select **Build from this Active Directory information**. Also, ensure that **Subject name format** is set to **Common name** and that only **DNS name** is selected under **Include this information in subject alternative name**.
5. On the **Request Handling** tab, click the **CSPs** button, ensure that **Requests must use one of the following CSPs** is selected, and that only **the Microsoft RSA SChannel Cryptographic Provider** is selected.
6. On the **Security** tab, add the AutoEnroll RAS and IAS Server Authentication Certificate security group with **Read**, **Enroll**, and **Autoenroll** permissions.

Important: You should remove any other groups that have permissions to enroll and/or autoenroll this certificate template. Any users or groups that need to enroll these certificates should be added to the relevant certificate template enroll (or autoenroll) group. This configuration prevents users or groups from being able to inadvertently enroll certificates that they should not be able to enroll. See the section "Creating Certificate Template Enrollment Groups" in chapter 11, "Managing the Public Key Infrastructure" for more details.

Chapter 4, “Designing the Public Key Infrastructure,” discusses setting this certificate type to require Certificate Manager approval. Because this certificate is considered to have a relatively high value, you should consider enabling this option to provide an additional check against someone enrolling a rogue IAS server. This approach will mean that manual approval is required to issue the certificate (although the request will still be automatically sent by the IAS server and the certificate automatically retrieved once approved).

Creating a Certificate Template for User Authentication

User certificates are required by end users to authenticate to the IAS server during EAP-TLS authentication. Have your Certificate Services administrator perform the following steps using the Certificate Templates MMC snap-in on the Certificate Services server to create a user authentication certificate template.

▶ **To create a user authentication certificate template**

1. Create a duplicate of the Authenticated Session template. Type **Client Authentication-User** in the **Template display name** field on the **General** tab of the new template.
2. On the **Request Handling** tab, select **CSPs** and clear the **Microsoft Base DSS Cryptographic Provider** check boxes.
3. On the **Subject Name** tab, ensure that you select **Build from this Active Directory Information**. Under **Subject name format**, select **Common name**. Ensure that **User principal name (UPN**) is the only option selected under **Include this information in subject alternate name**.
4. On the **Extensions** tab, ensure that only **Client Authentication (OID 1.3.6.1.5.5.7.3.2)** is included in **Application Policies**.
5. Also on the **Extensions** tab, edit the Issuance policies and add the **Low Assurance** policy.
6. On the **Security** tab, add the AutoEnroll Client Authentication-User Certificate security group with **Read**, **Enroll**, and **Autoenroll** permissions.

Important: You should remove any other groups that have permissions to enroll and/or autoenroll this certificate template. Any users or groups that need to enroll these certificates should be added to the relevant Certificate Template enroll (or autoenroll) group. See the previous note.

Creating a Certificate Template for Computer Authentication

A certificate is required to authenticate computers to the IAS server during EAP-TLS authentication. Have your Certificate Services administrator perform the following steps using the Certificate Templates MMC snap-in on the Certificate Services server to create a computer authentication certificate template.

▶ To create a computer authentication certificate template

1. Create a duplicate of the Workstation Authentication template. Type **Client Authentication-Computer** in the **Template display name** field on the new template's **General** tab.
2. On the **Subject Name** tab, ensure that you select **Build from this Active Directory Information**. Under **Subject name format** select **Common name.** Ensure that **DNS name** is the only option selected under **Include this information in subject alternate name**.
3. On the **Extensions** tab, edit the application policies and ensure that only **Client Authentication (OID 1.3.6.1.5.5.7.3.2)** is included.
4. Also on the **Extensions** tab, edit the Issuance policies and add the **Low Assurance** policy.
5. On the **Security** tab, add the AutoEnroll Client Authentication-Computer Certificate (WOODGROVEBANK\AutoEnroll Client Authentication - Computer Certificate) security group with **Read**, **Enroll**, and **Autoenroll** permissions.

Important: You should remove any other groups that have permissions to enroll and/or autoenroll this certificate template. Any users or groups that need to enroll these certificates should be added to the relevant Certificate Template enroll (or autoenroll) group. See the previous note.

Adding the WLAN Authentication Certificates to the Certification Authority

Once WLAN authentication certificate templates have been configured, you must add them to the certification authority (CA) to enable enrollment. Have your Certificate Services administrator perform the following steps to add certificate templates to the CA.

▶ Add certificate templates to the CA

From the Certification Authority MMC snap-in, right-click the **Certificate Templates** folder, select **New** and then **Certificate Template to Issue**. Select the following certificates, and then click **OK**:

- Client Authentication - Computer
- Client Authentication - User
- RAS and IAS Server Authentication

Enrolling for the IAS Server Certificate

Deployment of server authentication certificates to IAS servers is relatively straightforward and automated. Complete the steps in the following section to perform this task.

▶ **To enroll an IAS server authentication certificate from the CA**

1. Use the Active Directory Users and Computers MMC snap-in to add the IAS computer accounts to the AutoEnroll RAS and IAS Server Authentication Certificate security group.

   Important: You will need to restart the server so that it receives this new group membership.

2. Log on to the IAS as a member of the local Administrators group and run `GPUPDATE /force` at a command prompt.
3. Open the MMC, and then add the **Certificates** snap-in. When prompted, select the **Computer account** option, and then select **Local Computer**.
4. Select **Certificates (Local Computer)** from the console tree, select **All Tasks** from the **Action** menu, and then click **Automatically Enroll Certificates**.

Note: If the option to require Certificate Manager approval was selected for this certificate type, you will need to contact the CA administrator to verify that this is a legitimate request from an IAS server. Once verified, the CA administrator will issue the certificate.

Verifying IAS Server Certificate Deployment

The speed at which an enrolled IAS server certificate will be issued and deployed to the server certificate store is dependent upon certificate approval settings on the certificate template. Delays can also occur because the server only polls the CA every few hours.

▶ To verify that the IAS server authentication certificate has been deployed

1. Log on as a member of the local Administrators group on the local computer, open the Certificates MMC snap-in, and then add the **Certificates** snap-in. When prompted, select the **Computer account** option and then select **Local Computer**.
2. Open the **Certificates (Local Computer)**, **Personal**, **Certificates** store, and look for a certificate issued to the local computer name from the RAS and IAS Server Authentication certificate template. You can see the template name in the right pane. You may have to scroll horizontally to see the appropriate column.
3. If the required certificate does not appear in the Certificates MMC snap-in, select **Certificates (Local Computer)** from the console tree, select **All Tasks** from the **Action** menu, and then select **Automatically Enroll Certificates**. Wait a few moments for this action to perform, and then refresh the view of the Personal, Certificates folder.

Note: Certificate autoenrollment success can also be identified by an event in the Application Event Log that has a source of AutoEnrollment and an Event ID of 19.

Adding Users and Computers to Autoenrollment Groups

Deployment of WLAN authentication certificates to users and computers is normally transparent to end users. The process requires a local area network (LAN) connection, a domain-based user account, and a computer that has been joined to an Active Directory domain.

Users and computers that will require access to the new WLAN must have certificates deployed in advance to ensure they can perform EAP-TLS authentication. On computers running Windows XP and Windows Server 2003, both computer and user certificates can be automatically enrolled and renewed without end-user input. Certificate enrollment and renewal is controlled via Active Directory security groups.

Note: This solution uses custom security groups (AutoEnroll Client Authentication - User Certificate and AutoEnroll Client Authentication - Computer Certificate) to restrict which users and computers will automatically enroll WLAN certificates. If you want all of your domain users and computers to receive WLAN certificates, you can add Domain Users to the AutoEnroll Client Authentication - User Certificate group and Domain Computers to the AutoEnroll Client Authentication - Computer Certificate group.

▶ To add users and computers to security groups for autoenrollment

1. Open the Active Directory Users and Computers MMC snap-in.
2. Add users to the AutoEnroll Client Authentication-User Certificate group.
3. Add computers to the AutoEnroll Client Authentication-Computer Certificate group.

Important: The users will not receive this new group membership in their access tokens until they log off and log back on again. The computers will not receive this new group membership in their access tokens until they are restarted. Ensure that both of these things happen before continuing with the verification steps.

Verifying User Certificate Deployment

Perform the following steps when logged on as a user who has been added into the AutoEnroll Client Authentication-User Certificate group.

▶ **To verify user authentication certificate deployment**

1. If you have not done so, log off and log back on as the selected user. Open the MMC and add the **Certificates** snap-in to it. If prompted, select the **My user account** option.
2. Open the **Certificates–Current User**, **Personal**, **Certificates** store and look for a certificate issued to the user from the Client Authentication - User certificate template. You should see the template name in the right pane. You may have to scroll horizontally to see the appropriate column.
3. If the required certificate does not appear in the **Certificates** snap-in, run `GPUPDATE /force` at a command prompt, wait a few minutes, and then refresh the view of the Personal, Certificates folder.

Verifying Computer Certificate Deployment

Perform the following steps from a client computer that has been added to the AutoEnroll Client Authentication-Computer Certificate group.

▶ **To verify computer authentication certificate deployment**

1. If you have not restarted the computer after adding it to the certificate Autoenrollment group, restart it now.
2. Log on as a member of the local Administrators group on the local computer, open the MMC, and then add the **Certificates** snap-in. When prompted, select the **Computer account** option and then select **Local Computer**.
3. Open the **Certificates (Local Computer)**, **Personal**, **Certificates** store, and look for a certificate issued to the local computer name from the Client Authentication - Computer certificate template. You should see the template name in the right pane. You may have to scroll horizontally to see the appropriate column.
4. If the required certificate does not appear in the **Certificates** snap-in, run `GPUPDATE /force` at a command prompt, wait a few minutes, and then refresh the view of the Personal, Certificates folder.

Tip: You can reboot the computer to force certificate autoenrollment to retry. Certificate autoenrollment success can also be identified by an event in the Application Event Log that has a source of AutoEnrollment and an Event ID of 19.

Configuring WLAN Access Infrastructure

You must configure your primary IAS server with remote access policy and connection request settings that determine authentication and authorization of wireless users and computers to the WLAN. These settings must then be replicated to your other IAS servers; use the procedure detailed in the “Deploying Configuration to Multiple IAS Servers” section of Chapter 8, “Implementing the RADIUS Infrastructure” to do this. Following this, each IAS server must be uniquely configured to accept connections from RADIUS clients such as wireless APs. Wireless APs must then be configured to use IAS servers as the source of authentication and accounting for 802.1X networking.

Creating an IAS Remote Access Policy for WLANs

Use the Internet Authentication Service MMC snap-in to perform the following steps to configure IAS with a remote access policy for wireless networking.

▶ **To create a remote access policy in IAS**

1. Right-click the Remote Access Policies folder and select **Create New Remote Access Policy**.
2. Name the policy **Allow Wireless Access** and instruct the wizard to set up **A typical policy for a common scenario**.
3. Select **Wireless** for the access method.
4. Grant access based on group, and use the Remote Access Policy - Wireless Access security group.
5. Choose **Smart Card or Other Certificate** for the Extensible Authentication Protocol (EAP) type, and then select the server authentication certificate installed for IAS. Finish and exit the wizard.

Note: The new Allow Wireless Access policy can coexist with other user-created remote access policies or the default remote access policies. However, ensure that any default remote access policies are either deleted or listed after the Allow Wireless Access policy in the Remote Access Policies folder.

Modifying the WLAN Access Policy Profile Settings

The default settings of the remote access policy created previously should be changed to ignore user dial-in settings from Active Directory that can potentially cause issues with some wireless APs. In addition, RADIUS attributes should be set for client reauthentication at timed intervals to ensure that WEP session keys are refreshed. For more information about remote access policy settings, see Chapter 6, “Designing the Wireless LAN Security Using 802.1X.”

▶ **To modify the wireless access policy profile settings**

1. Open the properties of the Allow Wireless Access policy, and then click **Edit Profile**.
2. On the **Dial-in Contraints** tab, select the **Minutes clients can be connected (Session-Timeout)** option and enter **10 minutes** for a value.

Note: You can use a longer timeout value of up to 60 minutes without significant loss of security. This will give you an installation that is more resilient to temporary network outages and imposes less load on your IAS servers.

3. On the **Advanced** tab, add the **Ignore-User-Dialin-Properties** attribute, set it to **True**, and then add the **Termination-Action** attribute and set it to **RADIUS Request**.

Verifying the Connection Request Policy for WLAN

The default IAS connection request policy is configured to instruct IAS to authenticate users and computers directly against Active Directory. Perform the following steps to verify the configuration of the default connection request policy.

▶ **To verify configuration of the default connection request policy**

1. Open the Internet Authentication Service MMC snap-in and view the properties of the **Use Windows authentication for all users** connection request policy.
2. Verify that the policy conditions list contains **Date-And-Time-Restrictions matches "Sun 00:00-24:00; Mon 00:00-24:00; Tue 00:00-24:00; Wed 00:00-24:00; Thu 00:00-24:00; Fri 00:00-24:00; Sat 00:00-24:00"**
3. Click the **Edit Profile** button. On the **Authentication** tab, ensure that **Authenticate requests on this server** is selected.
4. Ensure that no rules exist on the **Attribute** tab.

Note: No additional connection request policy settings are required for this solution. However, your organization may have additional settings configured for various scenarios.

After configuring WLAN access, any configuration changes made on the primary IAS server should be replicated to the other IAS servers. Use the procedure detailed in the "Deploying Configuration to Multiple IAS Servers" section of Chapter 8, "Implementing the RADIUS Infrastructure" to do this.

Adding RADIUS Clients to IAS

You must add wireless APs and RADIUS Proxies as RADIUS clients to IAS before they are allowed to use authentication and accounting services via the RADIUS protocol. To add wireless APs to IAS, perform the following steps in the Internet Authentication Server MMC snap-in.

▶ **To add RADIUS clients to IAS**

1. Right-click the RADIUS Clients folder and select **New RADIUS Client**.
2. Enter a friendly name and the IP address of the wireless AP.
3. Select **RADIUS Standard** as the client-vendor attribute, and then enter the shared secret for this particular wireless AP. (You can use the GenPwd script, described in the next procedure, to generate a strong secret.) Then select the **Request must contain the Message Authenticator** attribute.

Note: Some RADIUS clients may require you to configure vendor-specific attributes (VSA) to function correctly. Consult your AP documentation for information regarding VSA requirements.

You can use the GenPwd script included with this guidance to generate random, strong 23–character secrets for individual use by each wireless AP configured as a RADIUS client. GenPwd will generate a cryptographically random secret and store the secret along with a friendly name for each RADIUS client in a Clients.txt file. GenPwd automatically appends the information to a Clients.txt file in the current directory in the form of comma-separated values.

Do *not* copy this file to the hard disk of the server. Keep the file on a floppy disk or other writable, removable media labeled “RADIUS Clients for Server ***HQ-IAS-01***“ (use your server name instead of *HQ-IAS-01*), and store it securely. This same server-specific disk is used to perform export and import of RADIUS clients in Chapter 12, “Managing the RADIUS and Wireless LAN Security Infrastructure.”

▶ **To use GenPwd to generate RADIUS secrets in a Clients.txt file**

1. Open a command prompt and make drive A: your current directory. (If you are using a media type other than floppy disk, use the appropriate drive letter.) Your file system directory location is important, because the Clients.txt file in the default directory will automatically be appended with the new information. If no Clients.txt file exists, one will be created.
2. Execute the following command. Be sure to substitute *ClientName* for the friendly name of the wireless AP. This name can be a DNS name or other string:

```
Cscript //job:GenPWD C:\MSSScripts\wl_tools.wsf /client:Client
Name
```

Important: You should store the RADIUS client storage disk in a secure location that is accessible in the event that emergency restoration is required. Once created, the comma-separated file can easily be imported into a spreadsheet or database application for reference and editing.

Enabling WLAN Access for Users and Computers

The final steps to enable users and computers for secure WLAN access include actions that you must perform on Active Directory objects. These actions include verifying account permissions, modifying group membership, and implementing WLAN Group Policy settings. You can perform these actions in a controlled manner to suit a phased deployment schedule and reduce the risk of significant change in the environment.

Verifying Active Directory Remote Access Permissions

Active Directory user and computer accounts must have the correct remote access permissions in order to use remote access policy. By default, the remote access permission on accounts in a native mode Active Directory domain are set to **Control access through Remote Access Policy**; therefore, no modification is typically required.

However, you can verify that the target users and computers are configured correctly with the Active Directory Users and Computers MMC snap-in. Check that **Control access through Remote Access Policy** is selected for the **Remote Access Permission (Dial-in or VPN)** setting on the **Dial-in** tab of the account properties.

Adding Users to Remote Access Policy Groups

IAS remote access policy uses Active Directory-based security groups to determine whether users and computers are authorized to connect to the WLAN. Security groups created earlier in this chapter include the ones described in the following table.

Table 9.3: Active Directory Security Groups

Security group	Description
Remote Access Policy - Wireless Users	Global group for users who require access to the WLAN.
Remote Access Policy - Wireless Computers	Global group for computers that require access to the WLAN.
Remote Access Policy - Wireless Access	Universal group that should contain the previous two global groups.

Use the Active Directory Users and Computers MMC snap-in to add the Remote Access Policy-Wireless Users group and the Remote Access Policy-Wireless Computers to the Remote Access Policy-Wireless Access group.

Important: This solution uses custom security groups (Remote Access Policy-Wireless Users and Remote Access Policy-Wireless Computers) to restrict which users and computers will be allowed access to the WLAN. If you want all of your domain users and computers to access the WLAN, you can add the Domain Users and Domain Computers groups to these custom security groups to simplify administration.

The group structure is now ready to be populated with users and computers that will be authorized to access the WLAN.

▶ **To add users and computers to the WLAN access groups**

1. Open the Active Directory Users and Computers MMC snap-in.
2. Add users permitted to access the WLAN to the Remote Access Policy - Wireless Users (WOODGROVEBANK\Remote Access Policy - Wireless Users) group.
3. Add computers permitted to access the WLAN to the Remote Access Policy - Wireless Computers (WOODGROVEBANK\Remote Access Policy - Wireless Computers) group.

Note: For more discussion on why you should enable both user and computer authentication to the WLAN, see Chapter 6, “Designing the Wireless LAN Security Using 802.1X.”

Creating Active Directory WLAN Group Policy

You can automate and enforce client computer WLAN configuration by leveraging Windows Group Policy. The Group Policy MMC in Windows Server 2003 exposes **Wireless Network Policy** settings, including those settings related to 802.1X-based security and 802.11 WLAN behaviors.

To create a Wireless Network Group Policy profile for the new 802.1X-enabled WLAN for client computers, perform the following steps using the Active Directory Users and Computers MMC snap-in.

Notes:
Creation of GPOs at the domain level may not be suitable for all organizations. Review your organization's Group Policy strategy to determine the best location for GPOs.

The wireless GPO settings will not be shown in the GPO MMC if you are editing the GPO from a Windows 2000 or Windows XP system. You must edit these from a Windows Server 2003 system or a system with the Windows Server 2003 Administration tools installed. You can use these GPO settings in either Windows 2000 or Windows Server 2003 Active Directory.

▶ **To create a Wireless Network Group Policy**

1. Select the properties of your domain object (such as woodgrovebank.com), and on the **Group Policy** tab click **New** and name the GPO **Wireless Network Policy**.
2. Click the **Properties** button, and on the **Security** tab grant the Wireless Network Policy - Computer security group **Read** and **Apply Group Policy** permissions. Also, remove **Apply Group Policy** permission from Authenticated Users on the GPO.
3. On the **General** tab, select **Disable User Configuration settings** on the policy object and select **Yes** to any warning messages which appear. Apply the changes, and close the GPO **Properties** window.
4. Click the **Edit** button to edit the policy, and navigate to \Computer Configuration\Windows Settings\Security Settings\Wireless Network (IEEE 802.11) Policies.
5. Select the **Wireless Network (IEEE 802.11) Policies** object from the navigation pane, and then select **Create Wireless Network Policy** from the **Action** menu. Use the wizard to name the policy **Client Computer Wireless Configuration**. Leave the **Edit properties** option selected and then click **Finish** to close the wizard.

6. Select **Add** from the **Preferred Networks** tab of the Client Computer Wireless Configuration policy, and then enter the Network Name or Service Set ID (SSID) of your wireless network.

Note: If clients are using an existing WLAN, you must choose a different SSID for the new 802.1X wireless LAN. This SSID is the one that should then be entered into the 802.1X wireless network profile.

7. Click the **IEEE 802.1x** tab and then open the settings for the **Smartcard or other certificate** EAP type. Under **Trusted Root Certificate Authorities**, select the root CA certificate for the PKI that issued the IAS server certificates (that is, the PKI installed in Chapter 7, "Implementing the Public Key Infrastructure").
8. Close the properties for **Client Computer Wireless Configuration** and the Group Policy Object Editor.

Adding Computers to Security Groups for WLAN Group Policy

Active Directory-based security groups are used to determine which computers have Wireless Network policies applied to automatically configure 802.11 and 802.1X settings.

You should deploy Wireless Network Group Policy settings for the new 802.1X-based network well in advance of configuring 802.1X settings on your wireless APs and activating the new WLAN. This approach ensures that client computers have an adequate chance to download and apply the computer-based Group Policy, even if they only rarely connect to the wired LAN.

The Group Policy settings can be applied to the computer before a WLAN network interface card (NIC) is installed and configured by Windows. Once a wireless LAN NIC is installed, it will automatically retrieve and apply the correct Wireless Network Group Policy settings.

Important: This solution uses a custom security group (Wireless Network Policy-Computer) to determine which computers receive configuration for the WLAN. If you want to allow all computers to receive the WLAN configuration settings, you can add the Domain Computers or Authenticated Users group to this group to simplify administration. You should be aware that this will cause the policy settings to be applied to all servers as well as client computers in the domain (if you use Domain Computers) or forest (if you use Authenticated Users).

▶ **To add computers to groups for Wireless Network Group Policy**

1. Use the Active Directory Users and Computers MMC snap-in to add computers to the Wireless Network Policy-Computer group.
2. Ensure that the systems are restarted before they try to use the WLAN. (This step is necessary to allow the computer to receive the new group membership configured in the previous step.)

Note: The Wireless Network GPO settings will update on client computers during the next computer Group Policy refresh interval. Alternatively, you can use the command `GPUPDATE /force` at a command prompt to force a refresh of computer policy.

Verifying Application of WLAN Group Policy

Perform the following steps from a client computer that has been added to the **Client Computer Wireless Configuration** security group in Active Directory.

Note: Computers must have a wireless network adapter installed and recognized by Windows before Wireless Network policy is visible.

▶ **To verify wireless networking configuration deployment**

1. Log on as an Administrator on the local computer, click **Start**, **Run**, and type the following command to open the Network Connections folder:

   ```
   ncpa.cpl
   ```

2. View the properties of the **Wireless Network Connection** icon that corresponds to your wireless card. On the **Wireless Networks** tab, you should see the new wireless network SSID name under **Preferred networks**. Select the new wireless network configuration and click **Properties** to explore the settings and verify that they match those chosen in the Wireless Networking Group Policy.
3. If the SSID name does not appear under **Preferred networks**, or network settings do not match settings configured in the Wireless Networking Group Policy, close all Wireless Networks dialog boxes and run GPUPDATE `/force` at a command prompt. After a few minutes, inspect the settings again.

Configuring Wireless APs for 802.1X Networking

The procedure for configuring wireless APs varies significantly, depending on the make and model of the device. However, wireless AP vendors will generally provide instruction for configuring the device with:

- 802.1X networking settings.
- IP address of the primary RADIUS authentication server.
- IP address of the primary RADIUS accounting server.
- RADIUS secret shared with the primary RADIUS server.
- IP address of the secondary RADIUS authentication server.
- IP address of the secondary RADIUS accounting server.
- RADIUS secret shared with the secondary RADIUS server.

See the vendor's documentation for information about configuring your wireless APs for 802.1X.

If users in your environment are currently using wireless APs that are configured with no security or only static WEP security, you will need to develop a migration plan. For more information about migration from an existing wireless network, see Chapter 6, “Designing Wireless LAN Security Using 802.1X.” Although providing instruction for configuring various vendors' wireless APs is outside the scope of this guidance, discussion of security topics related to wireless APs can also be found in Chapter 6.

Testing and Verification

You should test the functionality of the 802.1X-based WLAN by leveraging a client computer that is configured with a computer certificate, a user certificate, Wireless Network group policy, and a WLAN NIC.

▶ **To test wireless network functionality**

1. Restart the client computer that is a member of the Remote Access Policy - Wireless Computers security group.
2. Log on to the computer as a user who is a member of the Remote Access Policy - Wireless Users group.
3. From a command prompt, use the **ping** command to test network connectivity to another computer on the network.

For more detailed testing procedures, see Chapter 13, “Testing the Solution.”

Summary

If you performed all the procedures in this chapter, you should have completed the following tasks:

- Created and configured Active Directory security groups used to manage WLAN security components.
- Created required certificate templates and deployed wireless certificates to your IAS servers, selected computers, and selected end users.
- Created and configured IAS–based remote access policy and connection request policy for wireless networking.
- Configured wireless APs for 802.1X.
- Created and deployed Wireless Network Group Policy to selected client computers.

After completing these tasks, your 802.1X-based WLAN security infrastructure should be fully working and ready to enhance your organization's network security.

More Information

- The article "Managing Remote Access on a Per-group Basis Using Windows 2000 Remote Access Policies" is available at www.microsoft.com/windows2000/techinfo/administration/management/pgremote.asp
- The Windows Server 2003 product documentation is available at www.microsoft.com/windowsserver2003/proddoc/default.mspx. Product documentation provides an overview of IAS features, basic instructions for configuration, and best practices for deployment.
- The IAS Technical Reference provides technical details about IAS that may be used as a reference when more information is required. It is available at: http://www.microsoft.com/resources/documentation/windowsServ/2003/all/techref/en-us/W2K3TR_ias_intro.asp.
- The "Deploying a Wireless LAN" chapter of the *Microsoft Windows Server 2003 Deployment Kit* is available at www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/DNSBM_WIR_OVERVIEW.asp. This Deployment Kit chapter contains deployment guidance for using IAS in a number of scenarios that fall outside the scope of this secure wireless networking guidance but that affect design decisions.
- For extensive coverage of 802.1X WLAN, WLAN security issues and related standards, see The Unofficial 802.11 Security Web Page at www.drizzle.com/~aboba/IEEE/.
- For information about WLAN solutions and industry information, visit the WiFi Alliance Web site at www.wi-fialliance.org.
- For information about WLAN technology, including background information, market research, white papers, and training programs, visit the Wireless LAN Association (WLANA) Learning Center at www.wlana.org/learning_center.html.
- For information about EAP-TLS, EAP over LAN (EAPOL), EAP-RADIUS, RADIUS, and other Internet standards used with 802.1X, see the Internet Engineering Task Force (IETF) Web site at www.ietf.org/.

- Relevant WLAN standards include: 802.11, 802.11b, 802.11a, 802.11g, 802.1X, 802.11i, among others. Information about these standards can be found on the IEEE Wireless Standards Zone at http://standards.ieee.org/wireless/.
- For more information about 802.1X WLAN technologies, see the article "Windows XP Wireless Deployment Technology and Component Overview" at www.microsoft.com/technet/prodtechnol/winxppro/maintain/wificomp.mspx.