Microsoft Solutions for Security

Securing Wireless LANs with Certificate Services

Operations Guide

Release 1.6

Microsoft

Operations Guide Overview

The Operations Guide outlines the procedures for long-term maintenance of the solution components. Based on Microsoft Solutions for Management (MSM), the guide gives a comprehensive set of tasks and instructions that you can use to operate, monitor, change, and support the components for Microsoft® Windows Server™ 2003 Certificate Services and Microsoft Internet Authentication Service (IAS). The guidance includes setup tasks to implement the management system, regular daily and weekly tasks, system-check and monitoring scripts, backup and recovery procedures, and troubleshooting techniques and tools.

The Operations Guide contains the following chapters:

- Chapter 10: Introduction to the Operations Guide
- Chapter 11: Managing the Public Key Infrastructure
- Chapter 12: Managing the RADIUS and Wireless LAN Security Infrastructure

Table of Contents

10

Introduction to the Operations Guide

How to Use This Guide

Unlike the earlier chapters, the Operations Guide is not meant to be read from beginning to end. Accordingly, it is structured in a slightly different way. Although the Build Guide chapters are usually only used once during deployment, the Operations Guide chapters will be referred to continually throughout the life of the solution. It is important to understand how the Operations Guide chapters are structured so you can maximize the information that is contained in them.

The chapters in this guide are based on the Solutions Operations Guide (SOG) template designed by the Microsoft Solutions for Management (MSM) team. Each SOG uses the Microsoft Operations Framework (MOF) to analyze and categorize all of the activities needed to maintain, support, and improve the operation of a solution during its lifetime. A brief introduction to MOF is included in the next section, but you should also consult the references included at the end of this chapter to gain a more thorough understanding of the framework.

Each chapter is divided into a “must-read” section and a much larger reference section. The "must-read" section consists of the following items:

- A list of the management “setup” tasks that you need to perform to put the operations into practice, such as how to configure backups and how to configure monitoring.
- A list of the regular operations that must be performed to keep the solution functioning. (This list includes things like renewing CA certificates.)
- Instructions on how to allocate operational roles to operations staff.

The remainder of each chapter is composed of the detailed steps of the operational and support tasks that you will need to refer to. The list of setup tasks and regular operations mentioned previously refers to tasks defined in this section.

The reference section of each chapter is organized according to MOF categories, which are discussed in the next section. Following this is a short section on the layout of each task. You should read this before you continue with chapters 11 and 12.

Introduction to the Microsoft Operations Framework

The Operations Guide chapters for this solution are based on Microsoft Solutions for Management (MSM). MSM provides a combination of best practices, best practice implementation services, and best practice automation to help customers achieve operational excellence, which is demonstrated by high quality service, industry reliability, availability, security, and low total cost of ownership (TCO).

The best practices are based on Microsoft Operations Framework (MOF), which includes guidelines on how to plan, deploy, and maintain IT operational processes in support of mission-critical service solutions.

MOF is a structured yet flexible approach based on the IT Infrastructure Library (ITIL), which describes the processes and best practices necessary for the delivering mission-critical service solutions. The following sections provide you with an introduction to MOF, and MSM.

To understand the structure of this guide and use it effectively, you should understand the MOF Process Model and the MOF Team Model.

The MOF Process Model

The MOF Process Model is divided into four quadrants. Each quadrant deals with one aspect of a system lifecycle: Operating, Supporting, Optimizing, and Changing. Each quadrant, in turn, is comprised of a number of service management functions (SMF). Each SMF deals with a particular area of activity such as storage management, incident management, or change management. The MOF Process Model is depicted graphically in the following figure.

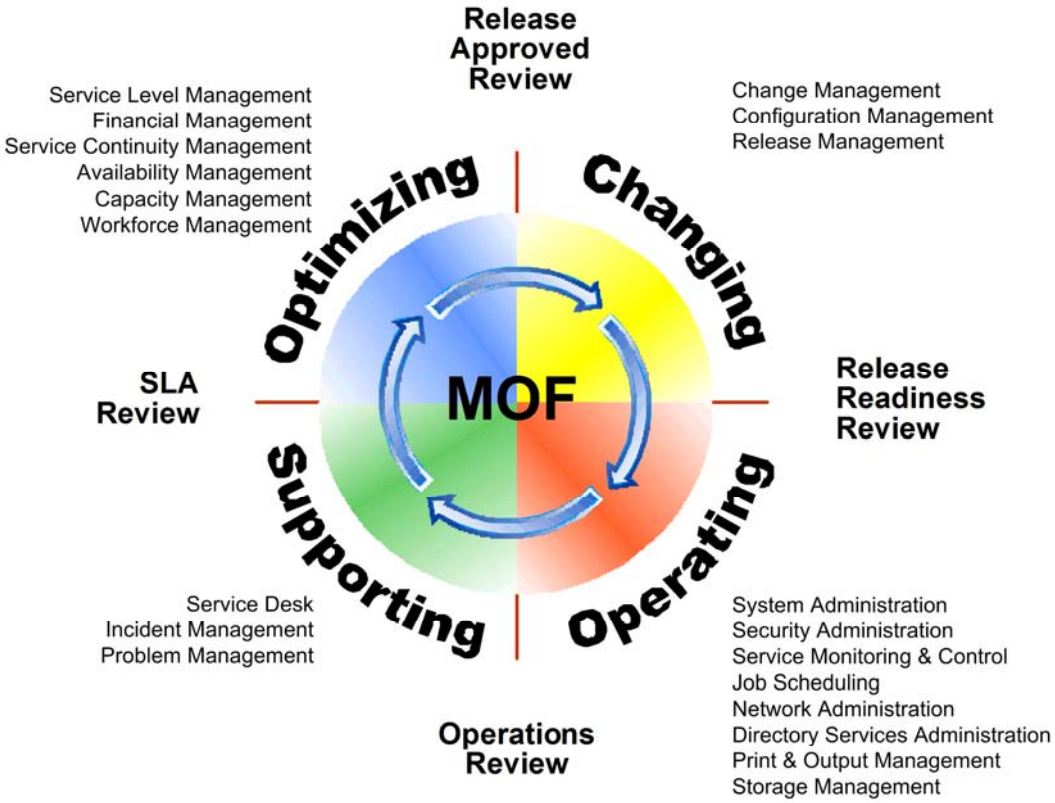

Figure 10.1
The MOF process model

Operating Quadrant

The operating quadrant includes all of the tasks that are needed to maintain a system in a properly working state, such as backing up data, monitoring service health, and directory and security management. In this section, you find all of the operating quadrant tasks that relate to the solution, including day-to-day operating tasks and monitoring and control recommendations. Both of these areas take advantage of the management scripts that are included with this solution.

Supporting Quadrant

The supporting quadrant is concerned with managing and recovering from problems with the system. It includes things like server and service recovery, help desk, problem analysis, and resolution. In the supporting quadrant, you can find support-related tasks for managing your secure wireless solution.

Optimizing Quadrant

The optimizing quadrant is concerned with how to improve the service that your system offers. In this section, you find key information about such functions as capacity planning, availability, and continuity management.

Changing Quadrant

The changing quadrant is concerned with planning and implementing changes in your environment. It includes change and release management, together with configuration management. This quadrant contains the most common subset of the changes that you might want to make to the solution infrastructure and a description of the change and release processes associated with these. The quadrant also describes the information that needs to be maintained in a configuration management system.

The MOF Team Model

The MOF Team Model and its associated role clusters offer guidance for ensuring the proper people are assigned to operational roles. Those roles and functional teams are shown in the following figure, and they are mapped to the MOF role cluster to which each would likely be assigned.

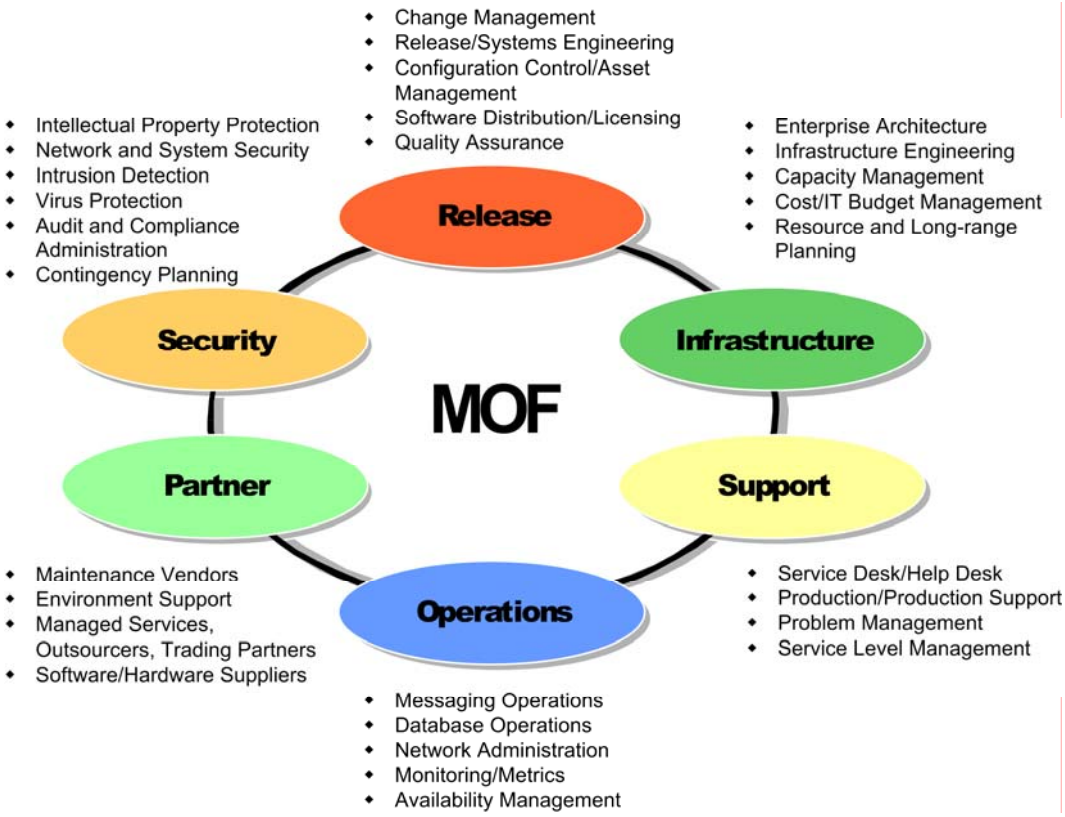

Figure 10.2

The MOF team model

You can use the MOF Team Model descriptions given previously to help you decide who in your organization will be responsible for each task and then produce a task and responsibilities breakdown for each individual involved in the management of your public key infrastructure (PKI).

Practical Implementation of Roles

The MOF Team Model defines roles that are clustered around management process responsibilities rather than technology or organizational divisions. In small organizations, one or two IT staff may take on the responsibilities for all of these roles. Even in larger organizations where there is much more specialization within the IT department, a clean mapping may not exist between the MOF process roles and individual IT staff roles.

In each of the following Operations Guide chapters, administrative roles and corresponding security groups have been defined. You will need to map these roles and security groups to the personnel in your organization. You should read through the operational procedures defined in the following chapters to evaluate who in your organization would be responsible for carrying out those tasks.

When performing this evaluation you need to keep in mind the following:

- Always try to avoid having only one individual responsible for a role, which is likely to cause problems if that individual ever leaves the organization.
- Avoid using generic accounts shared between several individuals, which makes auditing and accountability impossible.
- Most security professionals recommend that at least the auditor role be kept separate even if all of the other roles are combined.

Layout Conventions for the Tasks

All of the tasks documented in the Operations Guide chapters are categorized according to the MOF quadrant and SMF classification described earlier. At the highest level, the tasks are grouped by quadrant and then into different SMFs that make up the quadrant. The ordering of the tasks within each SMF and the ordering of the SMFs within each quadrant has no particular significance.

Note: Not all of the SMFs have tasks associated with them in the guide. Some SMFs, such as workforce management and financial management, need to be defined in the context of your own organization.

Each task is structured as follows:

- Task Name
- Task purpose and brief description
- Task attributes summary
- Task details

The task header and purpose are self-explanatory. The task attributes summary lists the security requirements (in terms of security group memberships), the frequency at which you need to perform the task, and any technology and tools required to complete the task. An example is shown here:

Summary Information

- **Security Requirements**: Account with rights to create OUs in the designated part of the Active Directory® directory service
- **Frequency**: Setup task
- **Technology Requirements**: Active Directory Users and Computers Management Console MMC snap-in

The task details section typically contains the step-by-step procedure required to complete the task. In some tasks (particularly setup tasks), task details may contain information (such as description of event log IDs) needed to carry out the task rather than procedural steps.

More Information

- For additional information about MSM, see the Improve Platform Manageability page at www.microsoft.com/solutions/msm.
- For general information about MOF, see the Microsoft Operations Framework page at www.microsoft.com/mof.
- For additional information about MOF, see the article "Team Model for Operations" at www.microsoft.com/technet/itsolutions/techguide/mof/moftml.mspx.
- For additional background on each of the MOF process model SMFs, see the individual chapters of the *SMF Operations Guide* at www.microsoft.com/technet/itsolutions/techguide/msm/smf/default.mspx.

11

Managing the Public Key Infrastructure

Introduction

This chapter describes the operational procedures required to manage the PKI (public key infrastructure) implemented as part of this *Securing Wireless LANs* solution. The structure is based on the Microsoft Operations Framework (MOF) categories and concepts discussed in the first chapter of the Operations Guide (Chapter 10).

The aim of this chapter is to enable you to implement a full management system for your PKI. Topics include all of the setup tasks needed to begin monitoring and maintaining the system and the regular operational tasks needed to keep it working properly. Procedures to help you deal with support incidents, manage changes to the environment, and optimize the performance of the system are also discussed.

There are two main parts to this chapter. The first part consists of two sections, "Essential Maintenance Tasks" and "Assigning Administrative Roles," which are brief and meant to be read in their entirety. These sections provide essential information about setting up a properly managed environment for the system. The remainder of the chapter is primarily a reference. There are some tasks in the reference sections that you will need to implement when the system is deployed, but they are clearly indicated in the "Essential Maintenance Tasks" section.

Although you do not need to absorb all of the details in the reference section, look through it to familiarize yourself with the contents so that you can quickly locate items that you need in the future.

Chapter Prerequisites

You should be familiar with the concepts used in MOF as described in Chapter 10, "Introduction to the Operations Guide." Detailed knowledge of MOF is not required.

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

- Basic operations and maintenance of Microsoft Windows Server™ 2003, including the use of tools such as Event Viewer, Computer Management, and NTBackup.
- The Active Directory® directory service, 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, auditing, access control lists; the use of security templates; the application of security templates using Group Policy or command line tools.
- Administration of Internet Information Services (IIS).
- An understanding of Windows Scripting Host and knowledge of the Microsoft Visual Basic® Scripting Editing (VBScript) language will be helpful for you to get the most out of the supplied scripts, but is not essential.

Before proceeding with this chapter, you should read the related Planning Guide and Build Guide chapters (chapters 4 and 6) and have a thorough understanding of the architecture and design of the solution.

Chapter Overview

The following list describes each of the major sections of this chapter.

- **Essential Maintenance Tasks.** Contains two tables listing the tasks you need to set up the management system and the regular list of tasks that need to be performed in order to maintain the system.
- **Administrative Roles**. Describes the administrative roles used in the solution, what the capabilities of each role are, and how these roles map to MOF role clusters and the administrative security groups defined for the solution.
- **Operating Quadrant Tasks**. Includes all of the tasks related to the normal maintenance of the PKI. These tasks include monitoring, backups, and directory and security operations.
- **Supporting Quadrant Tasks**. Includes all of the procedures related to recovering from system problems. These procedures include certificate and certification authority (CA) revocation, restoring from backup, and operations to deal with a failed CA.
- **Optimizing Quadrant Tasks**. Includes some capacity management planning procedures.
- **Changing Quadrant Tasks**. Includes common tasks relating to making changes to the CA configuration and releasing them into production in a controlled manner. Also included are procedures to help you gather and maintain essential configuration information about the PKI.
- **Troubleshooting**. Contains procedures for helping you troubleshoot common problems that you might encounter with your PKI. It also includes descriptions of useful troubleshooting tools and procedures to enable logging of different components.
- **Configuration Tables.** Contains a subset of the configuration parameters used in the build guide. These values are used as examples in the text of procedures.
- **More Information**. Lists a variety of extra information sources referred to in the text.

Essential Maintenance Tasks

This section lists the key tasks that you must perform to successfully operate the PKI. One-time setup tasks and ongoing operational tasks are listed in two tables. The tasks listed in the tables are described in detail later in the document. The tasks are grouped by MOF quadrant, and the MOF service management function (SMF) that the task belongs to is listed next to the task to help you find the required task easily.

Also included in this section is a list of tools and technologies used in the procedures in this chapter.

Initial Setup Tasks

This table lists the tasks that must be performed to put PKI operations into production. Depending on your operational standards and practices you may not need to perform all of these tasks, but you should review each task detail and decide whether it is necessary. Some of these tasks may also need to be performed again; for example, if a new CA is installed you will need to configure its backup and monitoring jobs.

Table 11.1: Initial Setup Tasks

Task name	Role cluster	SMF
Operating Quadrant		
Preparing a Domain Organizational Unit (OU) Structure for Certificate Services Management	Infrastructure	Directory Services Administration
Publishing the Issuing CA CRLs to the Web Server	Security	Security Administration
Configuring an Issuing CA Database Backup	Infrastructure	Storage Management
Configuring the Root CA Database Backup	Infrastructure	Storage Management
Testing CA Database Backups	Operations	Storage Management
Testing CA Keys Backups	Operations	Storage Management
Categorizing Monitoring Alerts	Infrastructure	Service Monitoring and Control
Monitoring Certificate Services Capacity Constraints	Infrastructure	Service Monitoring and Control
Monitoring Certificate Services Health and Availability	Infrastructure	Service Monitoring and Control
Setting up SMTP Alerts for Pending Certificate Requests	Infrastructure	Service Monitoring and Control
Scheduling Jobs on an Issuing CA	Infrastructure	Job Scheduling
Optimizing Quadrant		
Determining Maximum Load on the Issuing CA	Infrastructure	Capacity Management
Determining Storage and Backup Requirements for an Issuing CA	Infrastructure	Capacity Management
Changing Quadrant		
Managing Operating System Updates	Infrastructure	Change Management Release Management

Although there is not a documented task to set up a configuration management system for the PKI, review the procedures in the "Configuration Management" section. These procedures describe the types of information that should be collected and maintained in a configuration management system.

Maintenance Tasks

This table lists the tasks that must be performed on a regular basis to keep your PKI operating correctly. You can use this table to help plan the resources you will need and the operational schedule for administering the system.

There may be some tasks that you do not need to perform but you should review the task detail and make that decision. Some of these tasks might also need to be performed on an ad hoc basis as well as on a scheduled basis. For example, if a root CA certificate is renewed you will need to perform a backup of the root CA even if it is not scheduled. Where this is the case, it is noted in the Frequency column. Dependencies such as these are also noted in the task details themselves.

Table 11.2: Maintenance Tasks

Task name	Frequency	SMF
Operating Quadrant		
Checking Pending Requests	Daily	Security Administration
Renewing the Root CA Certificate	Every eight years	Security Administration
Renewing the Issuing CA Certificate	Every four years	Security Administration
Publishing an Offline CRL and CA Certificate	Every six months	Security Administration
Backing up the CA Keys and Certificates	Yearly, or every time CA certificate is renewed–whichever is sooner	Storage Management
Testing CA Database Backups	Monthly	Storage Management
Testing CA Keys Backups	Every six months	Storage Management
Archiving Security Audit Data from a CA	Monthly (Issuing CA)	Storage Management
Archiving Security Audit Data from a CA	Every six months (Root CA)	Storage Management

Technology Required in Operations Guide

The following table lists the tools or technologies used in the procedures that are described in this chapter.

Table 11.3: Required Technology

Item name	Source
Active Directory Users and Computers Management Console (MMC snap-in)	Microsoft Windows Server 2003
Certification Authority MMC snap-in	Windows Server 2003
Certificate Templates MMC snap-in	Windows Server 2003
Certutil.exe	Windows Server 2003
Certreq.exe	Windows Server 2003
MSS scripts	This solution
Text editor	Notepad—Windows Server 2003
Windows Task Scheduler Service	Windows Server 2003
SchTasks.exe	Windows Server 2003
Windows Backup	Windows Server 2003
Cipher.exe	Windows Server 2003
Event Viewer	Windows Server 2003
Performance Monitor	Windows Server 2003
Net.exe	Windows Server 2003
DSquery.exe	Windows Server 2003
Ldifde.exe	Windows Server 2003
DCDiag.exe	Windows Server 2003
Operational Alert Console	Microsoft Operations Manager (MOM)
Removable Media for backing up Root CA	CD–RW or Tape
Issuing CA server backup	Corporate backup service or Local backup device
Group Policy MMC snap-in	Web download from Microsoft.com
PKI Health	Windows Server 2003 Resource Kit

Table 11.4: Recommended Technology

Item name	Source
Operational Alert Console	Microsoft Operations Manager or other service monitoring system
E-mail infrastructure – for operational alerts (alternative to MOM)	SMTP/POP3/IMAP server and client, such as Microsoft Exchange Server and Microsoft Outlook®
Eventquery.vbs	Windows Server 2003
Capacity planning tools	Microsoft Operations Manager or other capacity planning tools
Security update distribution system	Microsoft Systems Management Server or Microsoft Software Update Services

Certificate Services Administrative Roles

Numerous different roles are involved in the management of a PKI. The following two sections divide them into core roles and supporting roles.

Core Certificate Services Roles

Core certificate services roles are central to the management of a public key infrastructure. Many of these roles correspond to the Common Criteria (CC) security roles defined for Certificate Services. Where this is the case, it is noted in parentheses following the role name.

Table 11.5: Core Certificate Services Roles

Role name	Scope	Description
Enterprise PKI Administrator	Enterprise	Responsible for overall PKI–defines certificate types, application policies, trusts paths, and so on, for enterprise
Enterprise PKI Publisher	Enterprise	Responsible for publishing trusted root certificates, sub-CA certificates, and CRLs to the directory.
CA Administrator (CC "Administrator" Role)	CA	CA administrator–responsible for CA configuration and allocation of roles on the CA. Often will be same individuals as Enterprise PKI Admins. There may be different CA administrators in charge of different CAs if the certificate usage dictates this.
Administrator (CC "Administrator" Role)	CA	Administrator of the CA server operating system–responsible for server wide configuration (such as CA installation). Often will be same individuals as CA Admins role. There may be different administrators in charge of different CAs if the certificate usage dictates this.
CA Auditor (CC "Auditor" Role)	CA	Manages audit events, policy, and similar types of auditable events from CAs.

(Continued)

Certificate Manager (CC "Officer" Role)	CA	Approves certificate requests that require manual approval and revokes certificates. There may be multiple Certificate Managers in charge of approvals on different CAs if the certificate usage dictates this.
Registration Authority	Certificate Profile	An extension of the role of Certificate Manager. Responsible for approving and signing certificate requests following ID verification of the certificate subject. Can be a person, an IT process, or a device (such as a fingerprint scanner and database). Different Registration Authorities can be specified for different certificate profiles (templates) and can span multiple CAs.
Key Recovery Agent	CA	Holds key to decrypt archived private keys in CA database.
CA Backup Operator (CC "Operator" Role)	CA	Responsible for backup and recovery of CA servers and secure storage of backup media.

Supporting Certificate Services Roles

The operational roles in the following table are not central to the management of the public key infrastructure, but they provide supporting functions to the core roles.

Table 11.6: Supporting Certificate Services Roles

Role name	Scope	Description
Monitor Operator	Enterprise	Responsible for monitoring events.
Capacity Planner	Enterprise	Responsible for analyzing performance and loading to predict future capacity requirements.
Active Directory Administrator	Enterprise	Responsible for configuration and support of Active Directory infrastructure.
Active Directory Operations	Enterprise	Responsible for day to day maintenance of the directory, such as security group maintenance, account creation, and so on.
Change Approvals Board	Enterprise	Business and technical representatives required to approve changes to infrastructure.

Mapping of Certificate Services Roles to Security Groups

The following table lists the security groups defined for this solution and briefly describes the capabilities or permissions of each group.

For offline CAs, there are only local security groups. In this case, you must create individual local accounts on the CA itself and use them to populate the local groups. You can make individual accounts members of multiple or even all local role groups if this configuration supports your organization's security and IT policies.

For online CAs, the domain security groups are used to apply permissions that are applicable to each role. Domain accounts are used to populate the role groups. Again, you make single accounts members of multiple role groups if this configuration supports your organization's security and IT policies.

Table 11.7: Mapping of Certificate Services Roles to Security Groups

Role name	Domain security group (Online CAs)	Local security group (Offline CAs)	Capabilities
Enterprise PKI Administrator	Enterprise PKI Admins	–	Control over Active Directory Public Key Services container. Therefore controls templates, trust publication, and other enterprise (forest)-wide configuration elements.

(Continued)

Enterprise PKI Publisher	Enterprise PKI Publishers	–	Can publish enterprise trusted root certificates, sub-CA certificates, and CRLs to the directory.
CA Administrator	CA Admins	CA Admins (root CA only)	Has "Manage CA" permissions on the CA. Controls assignment of roles on the CA. Also has permissions to change CA properties. Often will be combined with local administrator on the CA server, unless role separation is enforced.
Administrator		Administrators	Local administrator of CA server.
CA Auditor	CA Auditors	CA Auditors (root CA only) Administrators	Has "Manage Security and Audit logs" user right on a CA. Also a member of local Administrators group on CA (required to access audit logs).
Certificate Manager	Certificate Managers	Certificate Managers (root CA only)	Has "Issue and Manage Certificates" permission on the CA. Multiple Certificate Managers may be set up on each CA, and each can manage certificates for a subset of users or other end entities.
Registration Authority	–	–	Holds certificate and key required to sign certificate request prior to approval.
Key Recovery Agent	–	–	Holds certificate and key required to decrypt archived private keys stored in the certificate database.
CA Backup Operator	CA Backup Operators	CA Backup Operators (root CA only)	Has "Backup and Restore" rights on CA server.

Operating Quadrant Tasks

This section provides more detailed information about the maintenance tasks that belong to the MOF Operating Quadrant.

The MOF Operating Quadrant includes the IT operating standards, processes and procedures that are applied regularly to service solutions to achieve and maintain predetermined service levels. The goal of this quadrant is highly predictable execution of both manual and automated day-to-day tasks.

The Operating Quadrant contains the following SMFs:

- Directory Services Administration
- Security Administration
- Storage Management
- Service Monitoring and Control
- Job Schedule

There are no tasks that belong to the remaining SMFs:

- System Management
- Network Management
- Print and Output Management

Note: Each task description includes the following summary information: security requirements, frequency, and technology requirements.

Directory Services Administration

Directory services allow users and applications to find network resources such as users, servers, applications, tools, services and other information over the network. Directory services administration involves the day-to-day operations, maintenance and support of the enterprise directory. The goal of directory services administration is to ensure that information is accessible through the network to any authorized requester through a simple and organized process.

Preparing a Domain OU Structure for Certificate Services Management

The purpose of this task is to create a suitable OU structure to manage Certificate Services security groups and user accounts.

Summary Information

- **Security Requirements**: Account with rights to create OUs in the designated part of Active Directory
- **Frequency**: Setup task
- **Technology Requirements**: Active Directory Users and Computers MMC snap-in

Task Details

This task is not prescriptive because it depends primarily on your existing OU structure and on current management policies and procedures. The following table provides an example of a simple OU subtree that could be used to help organize the security groups created and referred to in this guide.

Table 11.8: Location of Security Groups Within the OU Structure

OU	Groups	Purpose
Certificate Services		
Certificate Services Administration	Enterprise PKI Admins Enterprise PKI Publishers CA Admins CA Auditors Certificate Managers CA Backup Operators	Contains administrative groups for managing CAs and enterprise PKI configuration.
Certificate Template Management	Examples: Manage User Template Manage Smartcard Logon Template	Contains groups granted Full Control of the template of the same name. Allows delegation of control by template type.
Certificate Template Enrollment	Examples: Enroll User Certificate Auto Enroll User Certificate Enroll Email Signing Certificate	Contains groups that are granted Enroll or AutoEnroll permissions on templates of the same name. Control of the groups can then be delegated to appropriate personnel to allow flexible enrollment regime without touching the actual templates.

Creating Certificate Template Management Groups

Template Management Groups are a useful way of delegating control over templates and template settings to different administrators. Only Enterprise Administrators and Enterprise PKI Admins have permission to modify templates. If your IT organization is not large, this kind of detailed delegation may not be required. In this case, only members of Enterprise Admins (the built-in group) and Enterprise PKI Admins (created as part of this solution) will be able to administer certificate templates.

Summary Information

- **Security Requirements**: Enterprise PKI Admins
- **Frequency**: As required
- **Technology Requirements**:
  - Active Directory Users and Computers MMC snap-in
  - Certificate Template MMC snap-in

Caution: Be extremely careful using this feature. Delegating control over a template type implies that you have complete trust in the person to whom you are delegating. Users with write permissions can change all of the parameters in a template to create any certificate type desired. You may prefer to create the template on their behalf, thereby keeping control over the certificate types solely within the Enterprise PKI Admins group.

Task Details

For each certificate template that you create or want to enable in your environment, perform the following procedures.

▶ **To create certificate template management groups**

1. Log on as a member of Enterprise PKI Admins.
2. In the Certificate Template Management OU, create a domain global security group named **Manage *CertTemplateName* Template** (where *CertTemplateName* is the name of the Certificate template to be managed).
3. Load the **Certificate Templates** snap-in into an MMC.
4. Open the properties of the required template and click the **Security** tab.
5. Add the Manage *CertTemplateName* Template group with **Write** permission.

Creating Certificate Template Enrollment Groups

Template Enrollment Groups make it easy to manage who can enroll or who is autoenrolled for a given certificate type; users or computers can simply be added to or removed from security groups. You can also grant control over the membership of these groups to administrative staff, who do not have permission to edit properties of certificate templates.

Summary Information

- **Security Requirements**: Enterprise PKI Admins
- **Frequency**: As required
- **Technology Requirements**:
  - Active Directory Users and Computers MMC snap-in
  - Certificate Template MMC snap-in

Task Details

Create an enrollment group for each certificate template type, or at least all of those where the certificate approval is automatic. (If you use a more complex or a manual registration process for a particular certificate type, using template enrollment groups may not be as useful.) If autoenrollment is appropriate for the certificate type, you can create a separate group that controls which users and devices autoenroll the certificate.

▶ **To create a certificate template enrollment group**

1. Log on as a member of Enterprise PKI Admins and open the Active Directory Users and Computers MMC snap-in.
2. In the Certificate Template Enrollment OU, create domain global security groups named as follows:
   - **Enroll *CertTemplateName* Certificate**
   - **Autoenroll *CertTemplateName* Certificate** (if required)
3. Load the Certificate Templates snap-in into an MMC.
4. Open the properties of the template to edit the security.
5. Add the Enroll *CertTemplateName* Certificate group and grant it **Read** and **Enroll** permissions.
6. Add the Autoenroll *CertTemplateName* Certificate group and grant it **Read**, **Enroll**, and **Autoenroll** permissions.

Note: You can optionally delegate control over these security groups to allow the certificate application owner to specify who can and cannot enroll for this certificate type.

Enabling Enrollment (or Autoenrollment) of a Certificate Type for a User or Computer

This task uses Enrollment groups to allow manual enrollment or initiate automatic enrollment of a certificate type for a user, computer, or security group containing users and/or computers.

Summary Information

- **Security Requirements**: Modify membership permissions for the certificate enrollment group
- **Frequency**: As required
- **Technology Requirements**: Active Directory Users and Computers MMC snap-in

---

Note: Autoenrollment must also be enabled in domain policy for the target users or computers. For details, see the section on configuring autoenrollment in Group Policy in Chapter 6, "Implementing the Public Key Infrastructure."

Task Details

▶ **To enable enrollment or autoenrollment for a user or computer**

1. In Active Directory Users and Computers, locate the Certificate Template Enrollment security group (or autoenrollment group for autoenrolling the certificate) corresponding to the certificate type to be enrolled. You must be logged on as a user with **Modify Membership** permissions for this group.

2. Add the user, computer, or security group to the selected template's security group.

Disabling Enrollment (or Autoenrollment) of a Certificate Type for a User or Computer

Issuing a certificate to a user or computer typically enables some functionality for the certificate holder; you may need to revoke this functionality at a later time.

Summary Information

- **Security Requirements**: Modify membership permissions for certificate enrollment group
- **Frequency**: As required
- **Technology Requirements**:
  - Active Directory Users and Computers MMC snap-in
  - Certification Authority MMC snap-in

Task Details

▶ **To disable enrollment or autoenrollment for a user or computer**

1. In Active Directory Users and Computers, locate the Certificate Template Enrollment (or Autoenrollment) security group corresponding to the certificate type to be disabled. You need to log on as a user that has **Modify Membership** permissions for this group.
2. Remove the user, computer, or security group from the template security group.

Note: For each certificate user that you want to disable, you will also need to revoke that user's certificate.

---

3. Log on as a member of Certificate Managers and locate the user's existing certificate(s) in the CA database (in the Certification Authority MMC). To locate the certificate(s) from the CA's Issued Certificates folder, click the **View** menu, and then click the **Filter** option.
4. Click the certificate to select it, and then, from the **Tasks** menu, click **Revoke**.
5. Select an appropriate reason code for the revocation. If the reason for revocation does not fall into one of the predefined reason codes, select **Unspecified**.

Important: Only the **Certificate Hold** reason allows later reinstating of the certificate. All other reasons result in the permanent disabling of the certificate. However, do not use **Certificate Hold** if there is a merely the possibility that the certificate may be reinstated. Only use this code when you genuinely need temporary suspension of the certificate.

Security Administration

Security administration is responsible for maintaining a safe computing environment. Security is an important part of an organization's infrastructure; an information system with a weak security foundation will eventually experience a security breach.

Checking Pending Requests

Certificate requests may be posted to the issuing CAs at any time. Most certificates will issue automatically, using either Active Directory as the registration authority (RA) or a predefined set of signatures from nominated RAs. If you have set up any certificate types to require manual approval by a Certificate Manager, these requests will queue until they are either approved or denied.

Summary Information

- **Security Requirements**: Certificate Managers
- **Frequency**: Daily
- **Technology Requirements**: Certification Authority MMC snap-in

Task Details

Check the requests folder daily for queued requests. Before issuing a certificate, check the request carefully to verify the requester and the contents of the request. Check that it contains the subject name, alternate subject name, key usages, policies, and extensions that are expected. If you are in doubt about any of these items, do not approve the request.

You can also set up the CA to send e-mail alerts for different events, including the arrival of a pending request. See the procedure "Setting up SMTP Alerts for Pending Certificate Requests."

▶ **To check pending requests**

1. Log on to the issuing CA as a member of Certificate Managers. (You can perform this task remotely by refocusing the Certification Authority MMC on the CA.)
2. Open the Certification Authority MMC and open the **Requests** folder.
3. To view the details of any request in the folder, right-click the request and click **View Attributes/Extensions** from the **View** submenu.

   Note: The **Attributes** tab shows request attributes received as part of the request and the **Extensions** tab shows the certificate extensions that will be used in the certificate. Each extension entry indicates whether it was there because it was included in the request, because it is a server supplied value, or because it is defined by the CA Policy module. (This latter origin usually indicates that it is an extension defined in the certificate template.)

   Depending on your organization's policies, you may also expect some other information concerning the request. This information may be provided in person, by telephone, e-mail, or other method.
4. After you are satisfied that the request is valid, you can approve it by right-clicking the request and clicking **Issue** from the **Tasks** submenu. If you are not satisfied, you can deny the request by clicking **Deny** from the same menu.

Renewing the Root CA Certificate

You must renew the CA certificate regularly to allow subordinate CAs and end entities to enroll certificates with this CA. Certificates issued by this CA and its subordinates cannot have an expiration date later than the expiration date of this CA certificate. Other reasons to renew the CA certificate are to:

- Change the key used by the CA (in case of actual or suspected compromise)
- Add certificate policies to the CA (qualified subordination)
- Change the CDP or Authority Information Access (AIA) paths
- Partition the Certificate Revocation List (CRL)

Typically, you should *always* change the CA key at each renewal. If you want to renew with the same key, see the procedure "Renewing the Root CA Certificate with the Same Key."

Summary Information

- **Security Requirements**: Local Administrators on CA
- **Frequency**: Every 8 years
- **Technology Requirements**:
  - Certutil.exe
  - MSS scripts
  - Certification Authority MMC snap-in
  - Text editor

Caution: Renewing a Root CA certificate is a very significant event. Be sure to inform any affected application owners of the new root certificate in case they need to configure this new root into their application.

Task Details

▶ **To renew the root CA certificate**

1. Log on to the Root CA as a member of the local Administrators group.
2. If you need to change the key size, you will need to edit the CAPolicy.inf file stored in the %systemroot% directory. Change the value of RenewalKeyLength to the desired bit size. The key size must be supported by the Crypto Service Provider (CSP) used by the CA. In the following example, this value is 2048.

   ```
   [Certsrv_Server]
   RenewalKeyLength=2048
   ```

   Note: If you require a change in validity period or certificate policies of the CA certificate, you must also specify this in the CAPolicy.inf (in %systemroot%) prior to beginning this procedure.

   ---

3. Open the Certification Authority MMC snap-in. From the **Tasks** menu of the CA object, click **Renew CA Certificate**. A Certificate Services warning will display advising you that it will need to stop the CA to renew the certificate.
4. Select the **New Key** option. Certificate Services will restart.

5. View the certificate from the CA properties and verify that the latest CA certificate's **Valid From** date is the current date.
6. Issue a CRL and copy the CRL and new CA certificate to disk with the following commands:

   ```
   Cscript //job:getcacerts c:\MSSScripts\ca_operations.wsf
   Cscript //job:getcrls c:\MSSScripts\ca_operations.wsf
   ```
7. Take the disk to the issuing CA. (You can use any domain member that has certutil.exe and the scripts supplied with this solution installed–it does not need to be the issuing CA.)
8. Log on as a member of the Enterprise PKI Admins group, and then run the following scripts:

   ```
   Cscript //job: PublishCertstoAD c:\MSSScripts\ca_operations.wsf
   Cscript //job: PublishCRLstoAD c:\MSSScripts\ca_operations.wsf
   Cscript //job: PublishRootCertstoIIS c:\MSSScripts\ca_operations.wsf
   Cscript //job: PublishRootCRLstoIIS c:\MSSScripts\ca_operations.wsf
   ```

   Note: It is a good idea to renew all of the subordinate CAs at the same time. However, you are not required to do so. (See "Renewing the Issuing CA Certificate.")
9. Back up the Root CA's certificate and key. (See "Backing Up the CA Keys and Certificates.")
10. Back up the Root CA's certificate database and system state. (See "Backing Up the Root CA Database.")

Renewing the Issuing CA Certificate

You must renew the CA certificate regularly to allow end entities (and subordinate CAs, if there are any) to continue to enroll certificates with this CA. Certificates issued by this CA cannot have an expiration date later than the expiration date of this CA certificate. Other reasons to renew the CA certificate are to:

- Change the key that the CA uses (in case of actual or suspected compromise)
- Add certificate policies to the CA (qualified subordination)
- Change the CDP or AIA paths
- Partition the CRL

Typically, you should *always* change the CA key at each renewal. If you want to renew with the same key, see the procedure "Renewing the Issuing CA Certificate with the Same Key."

Summary Information

- **Security Requirements**:
  - Local Administrators on issuing CA
  - Certificate Managers on Root CA
  - Enterprise PKI Admins
- **Frequency**: Every 4 years
- **Technology Requirements**:
  - Certutil.exe
  - MSS scripts
  - Certification Authority MMC snap-in
  - Text editor

Important: To successfully renew the CA certificate and publish it to the Active Directory NTAuth store (which identifies the CA as an Enterprise CA), you need to perform the CA certificate installation using an account that is *both* a member of Enterprise PKI Admins and Local Administrators groups. 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.

Task Details

▶ **To renew the issuing CA certificate**

1. Log on to the issuing CA as a member of the Local Administrators group.
2. If you need to change the key size, you will need to edit the CAPolicy.inf file stored in the %systemroot% directory. Change the value of RenewalKeyLength to the desired bit size (the key size must be supported by the CSP used by the CA).

```
[Certsrv_Server]
RenewalKeyLength=2048
```

Important: If you require a change in validity period or certificate policies of the CA certificate, you must also specify this in the CAPolicy.inf (in %systemroot%) prior to beginning this procedure.

---

3. Open the Certification Authority MMC snap-in, and from the **Tasks** menu of the CA object, click **Renew CA Certificate**.
4. Select the **New Key** option.
5. When prompted for a CA to which to send the renewal, click **Cancel** to save the request file to disk. Certificate Services will then restart.
6. Copy the certificate request file to disk. The certificate request will be generated and stored in the Shared Folder path (C:\CAConfig). Copy this file *HQ-CA-02.woodgrovebank.com_Woodgrove Bank Issuing CA 1*.req to disk. (replace the Italicized text with your CA details).
7. Take the disk to the Root CA and log on as a member of the local Certificate Managers group.

8. In the Certification Authority MMC snap-in, from the CA **Tasks** menu, click **Submit new request** and then submit the request transferred from the Issuing CA (on the Sub CA Request disk).
9. The Root CA requires that all requests be manually approved. Locate the request in the **Pending Requests** container, verify that the **Common Name** field contains the name of the issuing CA, and then approve (issue) the request.
10. Locate the newly issued certificate in the **Issued Certificates** container and open it.
11. Verify that the certificate details are correct, and then click **Copy to File** to export the certificate to a file. Save it as a PKCS#7 file onto the disk (for transfer back to the Issuing CA).
12. Log back on to the Issuing CA with an account that is a member of *both* Enterprise PKI Admins *and* the local Administrators group. Then insert the disk.
13. In the Certification Authority MMC snap-in, on the CA **Tasks** menu, click **Install Certificate**. Install the issuing CA certificate from the disk. The CA will restart.
14. View the certificate from the CA properties and verify that the latest CA certificate's **Valid From** date is the current date.
15. Publish the new CA certificate to the CDP Web publishing location. (See the procedure "Publishing the Issuing CA Certificate to the Web Server.")
16. Back up the issuing CA's certificate and key. (See the procedure "Backing up the CA Keys and Certificates.")
17. Back up the Root CA's certificate database and system state. (See the procedure "Backing up the Root CA Database.")
18. Back up the issuing CA's certificate database and system state. (See the procedure, "Configuring the Issuing CA Database Backup.") This backup should happen anyway during the normal daily backup.

Renewing the Root CA Certificate with the Same Key

Typically, you should *always* change the key of the Root CA at every scheduled CA certificate renewal (refer to the "Renewing the Root CA Certificate" procedure). You may need to renew the CA certificate without renewing the CA key if you need to change the CA policies or extend the certificate lifetime while keeping the same key pair.

Summary Information

- **Security Requirements**: Local Administrators on CA
- **Frequency**: As required
- **Technology Requirements**:
  - Certutil.exe
  - MSS scripts
  - Text editor

Task Details

▶ **To renew the Root CA certificate without changing the CA key**

- Follow the "Renewing the Root CA Certificate" procedure, except when prompted to renew with a new key click **No**. Changes to the value of RenewalKeyLength in the CAPolicy.inf file will have no effect.

Except for clicking **No** at the prompt to generate a new key, the procedure is identical to "Renewing the Root CA Certificate."

Caution: Renewing a Root CA certificate is a very significant event. Be sure to inform any affected application owners of the new root certificate in case they need to configure this new root into their applications.

Renewing the Issuing CA Certificate with the Same Key

Typically, you should *always* change the key of a CA at every scheduled CA certificate renewal. (See "Renewing the Issuing CA Certificate.") You may need to renew the CA certificate without renewing the CA key if you need to change the CA policies or extend the certificate lifetime while keeping the same key pair.

Summary Information

- **Security Requirements**: Local Administrators on CA
- **Frequency**: As required
- **Technology Requirements**:
  - Certutil.exe
  - MSS scripts
  - Certification Authority MMC snap-in
  - Text editor

Task Details

▶ **To renew the Issuing CA certificate without changing the CA key**

- Follow the procedure for Root CA certificate renewal, except when prompted to renew with a new key click **No**. Changes to the value of RenewalKeyLength in the CAPolicy.inf file will have no effect.

Except for clicking **No** at the prompt to generate a new key, the procedure is identical to the "Renewing the Issuing CA Certificate" procedure.

Publishing an Offline CRL and CA Certificate

You must publish the Certificate Revocation List (CRL) of an offline CA to an online location so that certificate users can check the revocation status of the entire CA chain.

Summary Information

- **Security Requirements**:
  - Local Administrators on CA
  - Enterprise PKI Publishers
- **Frequency**: Every 6 months, or as required
- **Technology Requirements**:
  - Certutil.exe
  - MSS scripts

Task Details

▶ **To publish the offline Root CRL to Active Directory and the Web URL**

1. Log on to the Root CA as a member of the CA Admins group.
2. Issue a CRL and copy the CRL and new CA certificate to disk with the following commands:

   ```
   Cscript //job:getcacerts c:\MSSScripts\ca_operations.wsf
   Cscript //job:getcrls c:\MSSScripts\ca_operations.wsf
   ```
3. Take the disk to the issuing CA. (The server does not need to be the issuing CA–it can be any domain member with certutil.exe and the MSS Scripts installed.)
4. Log on as a member of Enterprise PKI Publishers and run the following scripts:

   ```
   Cscript //job: PublishCertstoAD c:\MSSScripts\ca_operations.wsf
   Cscript //job: PublishCRLstoAD c:\MSSScripts\ca_operations.wsf
   Cscript //job: PublishRootCertstoIIS c:\MSSScripts\ca_operations.wsf
   Cscript //job: PublishRootCRLstoIIS c:\MSSScripts\ca_operations.wsf
   ```

Forcing the Issue of an Online CRL

The CRLs of an online enterprise CA are issued and published automatically; forcing the issue of an online CRL is not usually required. However, forcing the issue of an online CRL may be necessary when a critical revocation has taken place (such as all of the certificates issued by the CA) and a new CRL needs to be published rapidly as possible.

Note: It is not possible to "push" a CRL to clients–they will retain their existing cached copies until the copies expire. However, propagation delays aside, from the moment the new CRL is published, any client requesting a CRL will receive the new one.

Summary Information

- **Security Requirements**: Local Administrators on CA
- **Frequency**: As required
- **Technology Requirements**: Certification Authority MMC snap-in

Task Details

▶ **To issue and publish the offline CA CRL to Active Directory**

1. Log on to the CA as a member of CA Admins and load the Certification Authority MMC snap-in.
2. Click **Publish** to issue a new CRL from the **Tasks** menu of the Revoked Certificates folder.
3. Select **New CRL** to issue a base CRL, or **Delta CRL only** for a new Delta CRL.

Publishing the Issuing CA Certificate to the Web Server

The issuing CA certificate(s) must be published to the HTTP (Hypertext Transfer Protocol) AIA location.

Summary Information

- **Security Requirements**: Enterprise PKI Publishers
- **Frequency**: As required
- **Technology Requirements**:
  - MSS scripts
  - Certutil.exe

Task Details

It is technically possible to configure the CA to publish directly to the Web server folder. However, this method is not always practical for reasons of security and network connectivity. The following method uses a simple file copy technique but can be extended to suit most configurations.

Note: This method may not be suitable for directly publishing to an Internet-connected Web server because it requires direct network connectivity and use server message block (SMB) file sharing, which is usually blocked at firewalls. To publish to an Internet server, use the following method 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 added latency of this method.

The CA certificate is rarely updated, 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 Universal Naming Convention (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 (the default setting 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
   ```

Publishing the Issuing CA CRLs to the Web Server

You must publish the Issuing CA CRL(s) to the HTTP CRL Distribution Point (CDP) location.

Summary Information

- **Security Requirements**: Local Administrators on CA
- **Frequency**: Setup task
- **Technology Requirements**:
  - MSS scripts
  - Certutil.exe
  - Windows Task Scheduler Service
  - SchTasks.exe

Task Details

It is technically possible to configure the CA to publish directly to the Web server folder. However, this method is not always practical for reasons of security and network connectivity. The following method uses a simple file copy technique but can be extended to suit most configurations.

Note: This method may not be suitable for directly publishing to an Internet-connected Web server because it uses server message block (SMB) file sharing and requires direct network connectivity that is usually blocked at firewalls. To publish to an Internet server, use the following method 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 added latency of this method and the effect it might have on the freshness of your CRLs.

The issuing CA frequently (daily or hourly in the case of Delta CRLs) issues CRLs. Therefore, 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 computer account write access to the file system folder (**Modify** access) and to the share (**Change** access) corresponding to the published Web server folder. If the Web server is a member of the forest, you can use the Cert Publishers group to grant access to ensure that any Enterprise CA has the required permissions to publish certificates and CRLs to this folder. You do not need to change the Web server permissions. (See the "Configuring IIS for AIA and CDP Publishing" section of Chapter 6.)
4. Create a scheduled job that uses the following command to copy the CRLs:

   ```
   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 interval is sufficient to cope with a daily or even half-daily Delta CRL publication schedule. If your CRL schedule is more frequent, make the copy job run more frequently. A good guideline is that the copy job schedule should be approximately five to ten percent of the Delta CRL schedule.

Storage Management

Storage management pertains to on-site and off-site data storage for the purposes of data restoration and historical archiving. The storage management team must ensure the physical security of backups and archives. The goal of storage management is to define, track, and maintain data and data resources in the production IT environment.

Configuring the Issuing CA Database Backup

The purpose of this task is to back up a copy of the CA private keys and certificates, the Certificate database, and Certificate Services configuration information. Certificate Services configuration information includes any operating system configuration and other state information on which the CA depends.

Summary Information

- **Security Requirements**: Local Administrators on CA
- **Frequency**: Setup task
- **Technology Requirements**:
  - Windows Backup
  - Organizational backup system
  - Windows Task Scheduler Service
  - SchTasks.exe

Task Details

This task configures a scheduled job to perform a nightly system state backup of the CA server. The procedure assumes that your organization has a server backup system currently in place. This backup process will output to a backup file that your organization's backup system can then back up. The organizational backup may be a networked backup or a local device backup. The solution also assumes that your organization's server backup system runs nightly to back up the disks of the CA server.

Note: If you are using a Hardware Security Module (HSM), this procedure may back up the encrypted key material (depending on how the HSM works), but this backup will typically be unusable on a restored computer without an identical HSM and HSM access keys. Follow the HSM vendor's instructions for backing up and otherwise safeguarding the key material and access keys.

▶ **To configure a CA backup**

1. Make a directory in which to store the temporary backup files (such as C:\CABackup) and secure the directory by running the following command:

   ```
   cacls c:\CABackup /G system:F administrators:F "Backup Operators":C
         "CA Backup Operators":C
   ```

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

2. If you choose a different folder to store the backup you must update the related setting in pkiparams.vbs. Change the path on the following line as required.

```
CONST SYSSTATE_BACKUP_PATH = "C:\CABackup"   'path used by NTBackup
```

Note: Because the same script function is used to back up offline and online CAs, you must make separate copies of the scripts if you are going to use different paths for different CAs.

3. Schedule the backup job to run nightly with the following command. This command sets the job to run at 2:00am each night.

   SCHTASKS /Create /RU system /SC Daily /TN "CA Backup" /TR
   "cscript.exe //job:BackupCADatabase
   \"C:\MSSScripts\ca_operations.wsf\"" /ST 02:00

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

Note: The backslash followed by a quotation mark (\") shown on either side of the script name "C:\MSSScripts\ca_operations.wsf" is only required if there are embedded spaces in the file or path name of this script. The backslash is used to "escape" the quotation marks around the script name so that the script name and path are stored as a single parameter of the schtasks job command line instead of being split into several parts. These characters can be omitted if there are no spaces in the path name.

4. Configure your organization's server backup system to back up the contents of the temporary backup folder (C:\CABackup) each night to removable media. If possible, set a precondition script to check for the lock file (BackupRunning.lck, stored in the temporary backup folder) which is created by the backup script file while it is running. If this file exists it means that the previous backup failed or is still running. Alternatively, have your organization's backup system run the CA backup script as a pre-execution job.

Note: Each time the backup script BackupCADatabase is run, it checks for the lock file. If the file exists, the script writes the following error event to the application log:

Source: CA Operations

Event ID: 30

Event Type: Error

The CA backup could not start because the lockfile C:\CABackup\BackupRunning.lck from a previous job is still present. This could mean that the previous backup is still running.

If your organization's server backup system does not have the capability to perform pre-condition checks or execute scripts, schedule the server backup to begin at a suitable time after the System State backup has started. To estimate the amount of time to allow, run a system state backup (with **verify** on) on the server with Certificate Services service shut down. (Shutting the CA down will prevent the CA logs from being truncated for this test backup.) This backup will back up approximately 500 megabytes (MB) of system state data. Time this process, and

then use the following equation to calculate the approximate time for a CA database plus system state backup:

Ttotal = TSysState x (500 + (Nusers x NCerts x 20KB x 2)) ÷ 500

This equation assumes five certificates per user and per computer, per year, stored for five years in the database before archiving. If you allow 20 kilobytes (KB) per certificate, the result of the calculation is 1 MB of storage per user. If the time to back up System State alone was 10 minutes, allow 70 minutes for a CA with 3,000 users. This calculation is only approximate; to calculate it another way, allow 1 gigabyte (GB) for each 50,000 certificates.

Note: If you are using key archival, the certificate storage requirements will be larger for certificates with archived keys. For these certificates, allow an additional 10 KB per certificate (although additional storage may be required if you have many key recovery agents configured on the CA).

5. Store the backup media appropriately.

Caution: This backup data is highly sensitive because it contains the private key material for the CA. You must transport and store the data with the same attention and security that you provide for the CA. Store the backup data at a different physical site than the CA so that you can recover the CA if all computer equipment at the site is destroyed or becomes inaccessible.

Configuring the Root CA Database Backup

The purpose of this task is to prepare the CA private keys and certificates, the Certificate database, and the Certificate Services configuration information for backup. Certificate Services configuration information includes any operating system configuration and other state information on which the CA depends.

Summary Information

- **Security Requirements**: Local Administrators on CA
- **Frequency**: Setup task
- **Technology Requirements**:
  - Windows Backup
  - Removable media (such as CD-RW or tape)

Task Details

The Root CA will typically only ever issue a handful of certificates, so the data size will never be large. The data will change infrequently–possibly as rarely as once every few years. The procedure would also be the same for any other offline CA, such as an offline intermediate if you have chosen to use intermediate CAs.

The Root CA is offline, so it will require some kind of local backup device (such as a tape drive or writable CA) on which to store the backup file.

Caution: If you are using an HSM, this procedure may back up the encrypted key material (depending on how the HSM works), but the backed up keys will be unusable on a restored computer without an identical HSM and HSM access keys. Follow the HSM vendor's instructions for backing up and otherwise safeguarding the key material and access keys.

▶ **To configure a CA backup**

1. Make a directory in which to store the backup files (such as C:\CABackup) and secure the directory by running the following command:

   ```
   cacls c:\CABackup /G system:F administrators:F "Backup Operators":C
         "CA Backup Operators":C
   ```

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

2. If you choose a different folder to store the backup, you must update the related setting in pkiparams.vbs. Change the path on the following line as required.

   ```
   CONST SYSSTATE_BACKUP_PATH = "C:\CABackup"   'path used by NTBackup
   ```

Backing Up the Root CA Database

The purpose of this task is to create backup copies of the CA private keys and certificates, the Certificate database, and the Certificate Services configuration information. Certificate Services configuration information includes any operating system configuration and other state information on which the CA depends.

Summary Information

- **Security Requirements**: CA Backup Operators
- **Frequency**: Every time a new certificate is issued or revoked
- **Technology Requirements**:
  - Windows Backup
  - Removable media (such as CD-RW or tape)

Task Details

The Root CA will typically only ever issue a handful of certificates, so the data size will never be large. The data will change infrequently–possibly as rarely as once every few years. The procedure would also be the same for any other offline CA, such as an offline intermediate if you have chosen to use intermediate CAs.

The Root CA is offline, so it requires some kind of local backup device (such as a tape drive or writable CA).

Caution: If you are using an HSM, this procedure may back up the encrypted key material (depending on how the HSM works), but the backed up keys will be unusable on a restored computer without an identical HSM and HSM access keys. Follow the HSM vendor's instructions for backing up and otherwise safeguarding the key material and access keys.

▶ **To back up the Root CA**

1. Run the following command to back up the CA data to a temporary file:

   ```
   cscript //job:BackupCADatabase C:\MSSScripts\ca_operations.wsf
   ```

2. This command produces a backup file CABackup.bkf in the path chosen previously (the default path is C:\CABackup). Copy this file to removable media and store the removable media appropriately.

Caution: This backup data is highly sensitive because it contains the private key material for the CA. You must transport and store the data with the same attention and security that you provide for the CA. Store the backup data at a different physical site than the CA itself so that you can recover the CA if all computer equipment at the site is destroyed or becomes inaccessible.

Backing Up the CA Keys and Certificates

The CA certificates and keys should be backed up independently of the Certificate database. The CA private keys and certificates may be required to sign a CRL or certificate in the event that the CA server has failed and cannot be recovered in sufficient time.

Summary Information

- **Security Requirements**: CA Backup Operators
- **Frequency**: Yearly, or every time CA certificate is renewed–whichever is sooner
- **Technology Requirements**:
  - Certutil.exe
  - MSS scripts

Task Details

The CA keys and certificates consume only a few kilobytes of storage, and can therefore be saved to a disk. This task applies to the Root CA and any intermediate and issuing CAs in the organization. If you are backing up the keys to long-term storage such as CD or DVD, you do not need to back up yearly. If you are using magnetic media such as floppy disks or tape, you should back up the keys and certificates yearly as well as after a CA certificate renewal. The recorded signal on magnetic media deteriorates over time, especially if exposed to electrical fields. Although magnetic media may take many years to deteriorate and become unreadable, it is better to err on the side of caution.

Caution: If you are using an HSM, this procedure will not work as indicated. Follow the HSM vendor's instructions for backing up and otherwise safeguarding the key material and access keys.

▶ **To export the certificates and keys to disk**

1. Run the following command:

   cscript //job:BackupCAKeys c:\MMSScripts\ca_operations.wsf

   Make at least two separate backups onto different disks (disks are not always 100 percent reliable). Clearly label and date the disks as appropriate, considering the amount of time that might pass before they are required again.

   This script uses certutil.exe to export the CA keys and certificates to a PKCS#12 (P12) file in the following location:

   A:\CAKeyBackup*CAComputerName**yymmdd_hhmm*\CA Common Name.p12

   CAComputerName is the host name of the CA and *yymmdd_hhmm* is the backup date and time.

2. Enter a password when prompted.

   Important: Record and store this password in a different, but equally secure, location from the key backups themselves. The password record should clearly indicate to which backup (disk label, date, and CA name) it relates. It may be many months or years before these keys are required, and it is unlikely that anyone will remember which password was used at the time. Be sure to destroy all other records of this password. Do not use a password known by the administration staff.

3. Store the disk appropriately. As with CA database backups, these key backups should be highly secured. Store at least two backups of the certificates and keys in two separate secure locations (such as safes).

Testing CA Database Backups

Check the CA backups to ensure that the backup process and technology are performing correctly.

Summary Information

- **Security Requirements**: Local Administrators or Backup Operators on test computer
- **Frequency**:
  - Before the CA becomes operational
  - Monthly
  - Retest when any change is made to backup technology or process
- **Technology Requirements**:
  - Windows Backup
  - Organizational backup system
  - Certutil.exe
  - Cipher.exe

Task Details

You must restore the system state backup to a system with an identical disk layout. For example, Windows must be installed in the same directory path as the backed up system and the drive layout for storing Windows files (such as paging files) and CA database and logs must be the same as the original CA from which the backup was taken.

Important: The restored test server should be kept offline from the point that the system state backup file has been recovered from the backup media and certainly before system state restore is started. This separation from the network will prevent the restored CA keys from being unnecessarily exposed, and will also prevent duplicate name and IP address clashes between the test and original servers.

Warning: If you are using an (HSM), this procedure will not be sufficient to restore the CA completely. Depending on how the HSM works, the restored computer will be unusable without an identical HSM and HSM access keys. This situation may be sufficient for normal testing, but you should regularly perform a full restore with HSM recovery to ensure that your procedures and backup technology are working properly. Follow the HSM vendor's instructions for backing up, restoring and otherwise safeguarding the key material and access keys.

▶ **To restore the CA**

1. Restore the system state backup file from backup media to the C:\CABackup folder.
2. Run the Windows Backup utility and select the restored backup file in C:\CABackup. You will need to be a member of group that has Backup and Restore rights on the machine (such as CA Backup Operators, Backup Operators, or Administrators).
3. Click **Restore**.
4. Restart the system.
5. Verify that everything performed as expected.
6. Securely delete the disk contents of the test server (or at least delete the keys) at the end of the test.

If you decide to only delete the keys, you must first delete the CA key container(s) and then securely erase unallocated parts of the disk. You will need to be a member of the local Administrators group to perform this operation.

▶ **To securely delete the restored CA keys**

1. List the key containers on the test server with the following command:

   ```
   Certutil –key
   ```

2. Make a note of all containers that match the CA name (including those with an index suffix). For example, "Woodgrove Bank Issuing CA 1(1)".
3. Delete each of these key containers from the test server with the following command, replacing KeyContainerName with the values obtained in the previous step:

   ```
   Certutil –delkey KeyContainerName
   ```

4. Securely erase the unallocated space on the drive to ensure that the key data is completely removed from the disk. In the following command, the path %allusersprofile% makes the cipher command operate on the drive holding the key material.

   ```
   Cipher /W:%AllUsersProfile%
   ```

Testing CA Keys Backups

Check the CA key backups regularly to ensure that they are valid in case they are ever required.

Summary Information

- **Security Requirements**: Local Administrators on test computer
- **Frequency**:
  - Setup task (before CA becomes operational)
  - Every 6 months

- **Technology Requirements**:
  - Certutil.exe
  - Cipher.exe

Task Details

You can install the CA keys and certificates on any system. However, because of the highly sensitive nature of these keys, this system should be a trusted and offline system, especially for offline Root CA keys. To ensure that all traces of the key material are removed from the computer, create a separate, temporary local user account on the computer that is dedicated to this purpose (you can use any name for this account).

Caution: If you are using an HSM, this procedure will not work as indicated. Follow the HSM vendor's instructions for backing up, restoring, and otherwise safeguarding the key material and access keys.

▶ **To restore the CA keys**

1. Ensure that the computer is disconnected from the network. Log on as a member of local Administrators and create the TestCAKeys local user account.
2. Log on using the TestCAKeys account.
3. Insert the disk containing the backup of CA keys to be tested.
4. Use Windows Explorer to navigate to the P12 key file and double-click the file. The Certificate Import Wizard will start.
5. Enter the password when prompted. Do not select the check boxes to give high protection to the keys or to make them exportable.
6. Click **Place all certificates in the following store**, then **Browse** and select **Personal store** as the location to which to restore the CA keys.
7. Open the Certificates MMC snap-in and browse to the personal store. Locate the CA Certificate for the restored CA, and then open the certificate to verify that you have a corresponding private key. (You should see this indicated at the bottom of the **General** tab.)

▶ **To test the restored keys**

1. Obtain a CRL or certificate issued by the CA being tested.
2. Depending on whether you chose a CRL or certificate in the previous step, run the relevant one of the following commands, substituting the name of the file obtained in step 1 for *CRLFileName* or *CertFileName*:

   Certutil -sign *CRLFileName.crl NewCRL.crl*

   Certutil -sign *CertFileName.cer NewCertFile.cer*

3. When prompted, select the CA certificate (imported in the previous procedure) as the signing certificate.
4. Run the following certutil command to verify that the signing operation was successful. The output from the command should be similar to the following:

```
C:\CAConfig>certutil -sign "Woodgrove Bank Issuing CA 1.crl"
"Woodgrove Bank Issuing CA 1xxs.crl"
ThisUpdate: 2/10/2003 10:52 PM
NextUpdate: 2/25/2003 3:11 PM
CRL Entries: 0

Signing certificate Subject:
   CN=Woodgrove Bank Issuing CA 1
   DC=woodgrovebank,DC=com
Output Length = 970
CertUtil: -sign command completed successfully.
```

You must now clean the keys from the test system.

▶ **To clean the keys from the system**

1. Log on as a member of local Administrators and delete the user profile of the TestCAKeys account (use **Advanced Properties** in My Computer).
2. Delete the TestCAKeys account.
3. Securely erase unallocated areas of the disk to permanently remove traces of the keys by running the following command:

```
Cipher /W:%AllUsersProfile%
```

Note: Specifying %allusersprofile% as the path ensures that Cipher.exe operates on the drive holding the user profiles. It clears the entire drive, not just the path indicated.

Archiving Security Audit Data from a CA

Archive and store audit logs to comply with legal or regulatory requirements or to comply with internal security policy.

Summary Information

- **Security Requirements**:
  - CA Auditors
  - Local Administrators on CA
- **Frequency**:
  - Monthly (issuing CA)
  - Every 6 months (Root CA)
- **Technology Requirements**:
  - Event Viewer
  - Removable media (such as CD-RW or tape)

Task Details

▶ **To archive the security event log**

1. Log on to the server as a member of CA Auditors and local Administrators (create an account that is a member of both groups).
2. Open Event Viewer (click **Start**, **All Programs**, and then **Administrative Tools**).
3. Click the Security log folder to select it.
4. Right-click the folder, and from the drop-down menu click **Save log as**.
5. Save the log to a temporary file.
6. Copy to removable media (CD-RW) and then delete the temporary file.

Exporting a Certificate Template from Active Directory

You can save certificate template definitions from the directory to allow them to be restored in the future without having to perform a full directory restore.

Summary Information

- **Security Requirements**: Domain users
- **Frequency**: As required
- **Technology Requirements**:
  - ldifde.exe
  - Certificate Templates MMC snap-in

Task Details

This procedure describes a simple way to export a certificate template Active Directory object to file. This object can then be re-imported into the directory if needed. This method only saves the LDAP information of the template object. Other information, notably the security information (such as ownership and permissions information) is not preserved with this process.

Note: The only fully supported way of backing up and restoring Active Directory objects is with a dedicated directory backup method such as Windows System State backup. However, to restore an older version of a changed object requires an Active Directory authoritative restore, which is a complex procedure. This procedure describes a simple way to backup and restore a snapshot of a certificate template object.

▶ **To export a certificate template object**

1. Determine the template name that you want to back up. This name is not necessarily the same as the template display name. Look at the template properties on the **General** tab of the template (using the Certificate Templates MMC snap-in) to see the **Template name** and **Template display name**.
2. Log on to a domain member server or domain controller using a domain user account.
3. Run the following command to save the template details to the file *templatename*.ldif, replacing *templatename* with the name of the certificate template and *DC=woodgrovebank,DC=com* with the DN of your forest:

   ldifde -f *templatename*.ldif -d "cn=*templatename*, cn=Certificate Templates,cn=Public Key Services,cn=Services,cn=Configuration,*DC=woodgrovebank,DC=com*"

   (This command is displayed on more than one line; enter it as a single line.)
4. The *templatename*.ldif file will be saved to the current directory. Store the file *templatename*.ldif file safely.

Importing a Certificate Template to Active Directory

In instances where you want to restore a template from backup–for example, to reverse an unwanted modification to a template–you can re-import a previously saved certificate template definition to Active Directory.

Summary Information

- **Security Requirements**: Enterprise PKI Admins
- **Frequency**: As required
- **Technology Requirements**: ldifde.exe

Task Details

This procedure describes how to restore a certificate template definition from file. The file must have been previously created using the "Exporting a Certificate Template from the Active Directory." This method only restores the LDAP information of the template object. Other information, notably the security information (ownership, permissions, and so on) is not preserved using this process.

Note: The only fully supported way of backing up and restoring Active Directory objects is with a dedicated directory backup method such as Windows System State backup. However, to restore an older version of a changed object requires an Active Directory authoritative restore, which is a complex procedure. This procedure describes a simple way to backup and restore a snapshot of a certificate template object.

This procedure is not a replacement for Active Directory backup and restore, and should only be used in the narrow circumstances described.

▶ **To import a certificate template object**

1. Retrieve the exported template definition file created in the "Exporting a Certificate Template from the Active Directory" procedure.
2. Log on to a domain member server or domain controller as a member of Enterprise PKI Admins.
3. If you are replacing an existing template, make a backup of the unwanted template (using the earlier procedure), make a note of the template permissions, and then delete this template.
4. Open the file in Notepad (or similar text editor) and search for "objectGUID:" at the beginning of a line. The line will look similar to the following, although the characters following the colon will be different:

   ```
   objectGUID:: b/pVt//+I0i9hp8aJ7IWRg==
   ```

5. Delete the line—be careful to make no other changes to the file—and save the file.
6. Run the following command to import the template to the Active Directory from the file *templatename*.ldif, replacing *templatename* with the name of the certificate template:

   ```
   ldifde -f templatename.ldif -i
   ```

7. Verify the procedure has worked by opening the Certificate Templates MMC and viewing the restored template.
8. Apply the permissions to the restored template that you recorded in step 3 or that are appropriate to this template.

Service Monitoring and Control

Service monitoring allows the operations staff to observe the health of an IT service in real time.

Where MOM is referenced in this section, it is assumed that you have a MOM deployment that follows the guidelines in the MOM Operations Guide. MOM is not required, it is simply being used for illustration purposes. See the "More Information" section at the end of this chapter for more information on the MOM Operations Guide.

Categorizing Monitoring Alerts

Your monitoring system should raise only the most significant alerts to operations staff. If all minor errors are escalated to produce incident alerts, operations staff will quickly become confused about what is urgent and what is not.

Summary Information

- **Security Requirements**: None
- **Frequency**: Setup task
- **Technology Requirements**: Operational alert console (such as MOM)

Task Details

The following alert categories are used in this chapter. Of these, only the top three—Service Unavailable, Security Breach, and Critical Error—should produce alerts on the operator console for immediate attention. Errors and warnings are not considered urgent, and should be referred to the PKI operational support staff for resolution. These event categories are the defaults used by MOM, and subsequent task descriptions in this section will refer to them.

Table 11.9: Alert Categories

Alert category	Description
Service Unavailable	When the application or component is 100 percent unavailable.
Security Breach	When the application is being hacked or has been compromised.
Critical Error	When the application has experienced a critical error that requires administrative action soon (but not necessarily immediately). The application or component is operating at a sub-par level of performance but is still able to perform most critical operations.
Error	When the application experiences a transient problem that does not need any immediate or possibly any administrative action or resolution. The application or component is operating at an acceptable level of performance and is still able to perform all critical operations.
Warning	When the application generates a Warning message that does not need immediate or possibly any administrative action or resolution. The application or component is operating at an acceptable level of performance but is still able to perform all critical operations. This situation may, however, go to Error, Critical Error, or Service Unavailable if the problem persists.
Information	When the application generates an Informational Event. The application or component is operating at an acceptable level of performance and is performing all critical and non-critical operations.
Success	When the application generates a Success Event. The application or component is operating at an acceptable level of performance and is performing all critical and non-critical operations.

Monitoring Certificate Services Capacity Constraints

Detecting potential capacity constraints is essential to maintaining service at an optimal level. As subsystems approach the limits of their operating capacities, performance degrades sharply (usually in a non-linear way). Accordingly, it is important to monitor capacity trends and to identify and deal with trends toward future constraints as soon as possible.

Summary Information

- **Security Requirements**: Permission required is dictated by monitoring solution
- **Frequency**: Setup task
- **Technology Requirements**:
  - Performance monitor
  - Performance counter consolidator (such as MOM)
  - Operational alerts console (such as MOM)
  - Capacity planning tools

Task Details

The following performance counters are the most useful for identifying capacity constraints in Certificate Services. Processor and Physical Disk are the two most heavily used resources by Certificate Services and will likely indicate constraints at an earlier stage than Network Interface or Memory.

Table 11.10: Key Capacity Monitoring Counters for Certificate Services

Performance object	Performance counter	Instance
Processor	% Processor Time	_Total
Physical Disk	% Disk Time	_Total
Physical Disk	Avg. Disk Read Queue Length	_Total
Physical Disk	Avg. Disk Write Queue Length	D: (CA–DB) C: (CA–Log)
Network Interface	Bytes Total/sec	NW adapter
Memory	% Committed Bytes in use	——

For more general information about capacity constraints and related performance counters, see the reference in the "More Information" section at the end of this chapter.

It is also essential to monitor capacity indicators on any supporting infrastructure. The key items are:

- **Certificate Services communications to Active Directory**. Enterprise CAs use Active Directory for authentication and authorization services, read and store CA and PKI configuration information, and, depending on certificate type, publish issued certificates to the directory.
- **Client certificate-related communications to Active Directory**. Clients read CA and PKI information from Active Directory. This activity includes downloading CRLs that can be several megabytes in size, per client, per week.)
- **Client certificate-related communications to Web servers**. Clients may retrieve CRLs and CA certificates from the Web server, although this activity is unlikely to produce enough load to cause capacity constraints unless the server is already heavily loaded.

Monitoring Certificate Services Health and Availability

Certification authorities do not typically provide online or real-time services (compared with services such as Active Directory or Microsoft SQL Server™, for example, which have to be online continuously in order to provide a useful service). However, several aspects of a CA operation are critical and require online response from the service:

- **Availability of revocation information**. A current CRL must be available for any certificate user wanting to check the revocation status of a certificate.
- **Validity of CA Certificate**. A CA must have a certificate that is currently valid. An invalid CA certificate prevents validation of any certificate issued by that CA or its children. It also prevents new certificates from being issued.
- **Availability of certificate enrollment service**. No one can enroll or renew a certificate if the CA service is unavailable.

Lack of the availability of either of the first two aspects typically has a much greater impact than the last.

Summary Information

- **Security Requirements**: MOM (or monitoring system) administrator
- **Frequency**: Setup task
- **Technology Requirements**:
  - MSS scripts
  - Operational alerts console (such as MOM or e-mail infrastructure)
  - MOM agents or Windows Task Scheduler Service for execution

Task Details

The events in the following table are the most significant ones for Certificate Services. The table describes the significance of each type of event and what alert criticality (for your operational console) you should assign to that event. The second table lists methods of detecting these incidents–most are detected with the operational scripts supplied with this solution.

The Criticality column relates to the Alert Categories defined earlier in the "Categorizing Monitoring Alerts" procedure.

Table 11.11: Criticality of Main Certificate Services Events

Certificate Services status	Significance	Criticality
CRL expired	A valid CRL is not accessible–this situation is currently causing a loss of service.	Service Not Available
CRL overdue	The CRL is still valid but a new one is overdue and should have been published.	Critical
CRL not available Subevents: CRL cannot be retrieved from Active Directory CRL cannot be retrieved from Web Server	A CRL is not available at a published CRL distribution point. This situation may be causing loss of service.	Critical
CA Server failed	The server is not visible on the network.	Service Not Available
CA operating system health in critical state	Underlying major problem with server hardware or Windows.	Critical
CA operating system health in error/warning state	Underlying problems with server hardware or Windows that are not critical.	Error or Warning (as defined by MOM rules)
Certificate Services not online Subevents: Client Interface offline Admin Interface offline	Certificate Services remote procedure call (RPC) interface is offline–certificates cannot be issued.	Critical
CA Certificate expired Subevents: This CA cert has expired Parent CA cert has expired	The certificate of the CA has expired. This situation is currently causing loss of service.	Service Not Available
CA Certificate has under 1 month validity remaining	The CA certificate will soon expire, leading to loss of service if not corrected. Only very short lifetime certificates are currently being issued.	Error
CA Certificate validity less than half lifetime	A CA certificate should be renewed when it has reached half of its validity period. This may mean that certificates of shorter than expected lifetime are being issued.	Warning
CA Backup failed	System State Backup of CA failed–possible information loss.	Critical or Error

You can use the supplied script (ca_monitor.wsf in the following table) to check for these events. The script includes logic to write event items into the Windows Application log when any detected error occurs. These events can then be noted by MOM agents or another monitoring solution. You will need to set up filtering rules to check for the event source and event IDs produced by the scripts listed in the following table.

The scripts can also send e-mail in response to alert conditions. Where MOM (or another agent-based monitoring system) is used, the scripts should be executed by the MOM client agent. If there is no management agent that can execute the script, use the Windows task scheduler to run these checks at least hourly. Alerts can be e-mailed, or you can use an event log monitoring tool.

The scripts are designed to be run on the online issuing CA, although they also check the status of published certificates and CRLs from offline parent CAs up to the Root CA. Where relevant, the event IDs generated by the monitoring script are shown in the following table. The script syntax is shown after the table.

Table 11.12: Certificate Services Monitoring Scripts

Event	Script or detection method	Source and Event ID
CRL expired	Script: Ca_monitor.wsf Job: CheckCRLs	CA Operations 20
CRL overdue	Script: Ca_monitor.wsf Job: CheckCRLs	CA Operations 21
CRL not available Subevents: CRL cannot be retrieved from Active Directory CRL cannot be retrieved from Web Server	Script: Ca_monitor.wsf Job: CheckCRLs	CA Operations 22 23
CA Server failed	Native MOM server failure detection	
CA operating system health in critical state	Native MOM server health monitoring	
CA operating system health in error/warning state	Native MOM server health monitoring	
Certificate Services service alive Subevents: Client Interface offline Admin Interface offline	Script: Ca_monitor.wsf Job: IsCAAlives	CA Operations 1 2
CA Certificate expired Subevents: This CA cert has expired Parent CA cert has expired	Script: Ca_monitor.wsf Job: CheckCACerts	CA Operations 10
CA Certificate has under 1 month validity remaining	Script: Ca_monitor.wsf Job: CheckCACerts	CA Operations 11
CA Certificate validity less than half lifetime	Script: Ca_monitor.wsf Job: CheckCACerts	CA Operations 12
CA Backup locked (the backup script was unable to run because a lockfile from the previous backup was still there)	Script: Ca_operations.wsf Job: BackupCADatabase	CA Operations 30
CA Backup failed	The failure code for NTBackup.exe is given here, although you should rely on MOM or other monitoring system capabilities to warn about backup problems. (Note that you will need to check for both system state backup and organizational backup)	Ntbackup 8019
Other event	Ca_monitor.wsf execution failure	CA Operations 100

Before deploying the scripts, update the constants.vbs file with the correct alert parameters. The relevant sections from the file are shown here, with items that you may want to change shown in Italics:

```
'Alerting parameters
CONST ALERT_EMAIL_ENABLED     = FALSE 'set to true/false to enable/disable email
CONST ALERT_EVTLOG_ENABLED    = TRUE  'set to true/false to enable/disable event
                                      'log entries
' set to comma-separated list of recipients to get email alerts
CONST ALERT_EMAIL_RECIPIENTS  = "Admin@woodgrovebank.com,Ops@woodgrovebank.com"
'SMTP host to use
CONST ALERT_EMAIL_SMTP        = "mail.woodgrovebank.com"

'String used as the Source in event log events
CONST EVENT_SOURCE            = "MSS Tools"
CONST CA_EVENT_SOURCE         = "CA Operations"

'CA Event IDs
CONST CA_EVENT_CS_RPC_OFFLINE               =       1
CONST CA_EVENT_CS_RPC_ADMIN_OFFLINE         =       2
CONST CA_EVENT_CA_CERT_EXPIRED              =       10
CONST CA_EVENT_CA_CERT_NEARLY_EXPIRED       =       11
CONST CA_EVENT_CA_CERT_RENEWAL_DUE          =       12
CONST CA_EVENT_CRL_EXPIRED                  =       20
CONST CA_EVENT_CRL_OVERDUE                  =       21
CONST CA_EVENT_CRL_NOT_AVAILABLE_LDAP       =       22
CONST CA_EVENT_CRL_NOT_AVAILABLE_HTTP       =       23
CONST CA_EVENT_BACKUP_LOCKED                =       30
CONST CA_EVENT_CA_OTHER                     =       100
```

You need to specify whether you want errors to produce e-mail, event log entries, or both. The default setting is event log entries only. If you specify e-mail alerts, you *must* provide a valid e-mail recipients list (comma-separated) and the SMTP server hostname or IP address. Both of these strings must be in quotes.

If you specify event log alerting, you might want to change the parameters CA_EVENT_SOURCE (used for all CA-related events) or EVENT_SOURCE (used for any non-CA related events).

The syntax and use of the monitoring scripts is described in the following section.

▶ **To check on CA certificate expiry**

Run the following command to check the certificate of the issuing CA (where the script is run) and published certificates of any parent CAs up the hierarchy to the Root CA.

```
Cscript //job:CheckCACerts C:\MSSScripts\ca_monitor.wsf
```

This command gives alerts for the following conditions:

- CA Certificate has expired (Event ID 12)
- CA Certificate with has less than one month before expiry (Event ID 11)
- CA Certificate has passed the mid–point of its validity period (Event ID 12)

▶ **To check on CRL expiry**

Run the following command to check on the issuing CA CRL and published CRLs for all parent CAs up to and including the root CA.

```
Cscript //job:CheckCRLs C:\MSSScripts\ca_monitor.wsf
```

This command gives alerts for the following conditions:

- CRL has expired (Event ID 20)
- CRL has passed its "Next published CRL" date and is due to expire (Event ID 21)
- CRL cannot be retrieved from LDAP CDP (Event ID 22)
- CRL cannot be retrieved from HTTP CDP (Event ID 23)

(Currently, FTP and FILE CDPs are not checked in this script.)

▶ **To check whether the CA service is running**

Run the following command to check the CA on which the script is running.

```
Cscript //job:IsCAAlive C:\MSSScripts\ca_monitor.wsf
```

This command gives alerts for the following conditions:

- The CA RPC Client Interface is not responding (Event ID 1)
- The CA RPC Administration Interface is not responding (Event ID 2)

Certification Authority Security Monitoring

Certificate Services produces a variety of audit log entries in response to different security events. Most of these entries will be the result of day-to-day operational tasks. However, some events indicate major configuration changes, and you may need to investigate them further.

Summary Information

- **Security Requirements**:
  - CA Auditors (to review security log)
  - Designated security monitoring account for monitoring through MOM (or similar system)
- **Frequency**: Setup task
- **Technology Requirements**:
  - Operational alerts console (such as MOM)
  - Event Viewer
  - Eventquery.vbs (Windows command line tool)

Task Details

The following table lists the audit events that Certificate Services produces, together with a recommended alert categorization. Configure your monitoring system to look for these events and raise the appropriate alert level. Alternatively, if you have no centralized event monitoring system, review the CA server security logs regularly (on a daily basis, if possible) to check for these items.

The default alert category for Success events is **Information**. Any Success event that results from possible changes to the security configuration of the CA is treated as a **Warning**. All **Warning** level events indicate significant events that would not normally be expected to occur in day-to-day operations. All **Warning** events should correlate to an approved change request. If there is no such correlation, treat the event as a possible security breach and investigate it immediately.

Failure events are not normally expected during day-to-day operations or during standard changes to the CA. Almost all failure events are significant and require investigation (although they may only indicate incorrect permission assignment rather than a malicious attack).

Note: There are a few exceptions, such as Event 792, **Certificate Services denied a certificate request**. This condition produces both success and failure events for a request that was legitimately denied by a Certificate Manager, but only a failure event when a request denial is attempted by someone without sufficient permission.

Additional exceptions to the list in the following table are due to the different ways in which you can make configuration changes to the CA. Events 789 (change of audit filter), and 795 and 796 (change of CA configuration or property) will only be logged if changes are made using the Certification Authority MMC snap-in. They will not be logged if someone tries to edit the CA registry directly (or uses the certutil -setreg command) to change CA configuration values. Instead, these events will be recorded as simple Event 560 object access audit failures (see the last entry in the following table). Auditing is enabled for the CA registry configuration subkeys and records successful changes and all failed accesses. To track changes to the CA registry keys, use the **Object Name** parameter of the audit event in conjunction with **Event ID** and **Event Type** to create a filter to produce the correct alerts.

As well as auditing Certificate Services events, you must also monitor and generate alerts on standard operating system security events such as logon events, use of privileges, and object accesses. The CA registry and database and log directories are configured to generate alerts for all failed access and any successful change. You should also consider setting auditing on the Public Key Services container (in Configuration\Services) and on the PKI administration groups. These settings have not been made part of this solution because of the difficulty of monitoring audit events distributed across domain controllers. If you have a system (such as MOM) that can consolidate and filter these logs, enable auditing on all Active Directory PKI administration and configuration objects and containers.

Note: Security monitoring of the CA operating system is beyond the scope of this guidance, and may include the handling of security events from specialized intrusion detection agents. If any of these sources indicate a security breach, thoroughly investigate the Certification Authority audit events in conjunction with output from these sources.

The Success and Failure Alert categories in the following table relate to the Alert Categories defined in the "Categorizing Monitoring Alerts" procedure.

Table 11.13: Certificate Services Audit Events

Event ID	Event description	Success Alert category	Failure Alert category
772	The certificate manager denied a pending certificate request	Warning	Error
773	Certificate Services received a resubmitted certificate request	Warning	Error
774	Certificate Services revoked a certificate	Information	Error
775	Certificate Services received a request to publish the certificate revocation list (CRL)	Information	Warning
776	Certificate Services published the certificate revocation list (CRL)	Information	Error
777	A certificate request extension changed	Information	Error
778	One or more certificate request attributes changed	Information	Error
779	Certificate Services received a request to shut down	Warning	Error
780	Certificate Services backup started	Information	–
781	Certificate Services backup completed	Information	–
782	Certificate Services restore started	Warning	–
783	Certificate Services restore completed	Warning	–
784	Certificate Services started	Information	–
785	Certificate Services stopped	Warning	–
786	The security permissions for Certificate Services changed	Warning	Error
787	Certificate Services retrieved an archived key	Information	Error
788	Certificate Services imported a certificate into its database	Information	Warning
789	The audit filter for Certificate Services changed	Warning	Error
790	Certificate Services received a certificate request	Information	Error
791	Certificate Services approved a certificate request and issued a certificate	Information	Error
792	Certificate Services denied a certificate request	Warning	
793	Certificate Services set the status of a certificate request to pending	Information	
794	The certificate manager settings for Certificate Services changed	Warning	
795	A configuration entry changed in Certificate Services	Warning	Error

(continued)

Node: Entry: CRLPeriod or CRLPeriodUnits or CRLDeltaPeriod or CRLDeltaPeriodUnits Describe change in CRL publication schedule. Value of 0 for CRLDeltaPeriodUnits means Delta CRL publishing disabled
Node: PolicyModules\CertificateAuthority_Microsoft Default.Policy Entry: RequestDisposition Value: 1 Set CA to issue incoming requests unless specified otherwise.
Node: PolicyModules\CertificateAuthority_Microsoft Default.Policy Entry: RequestDisposition Value: 257 Set CA to keep incoming requests pending.
Node: ExitModules\CertificateAuthority_Microsoft Default.Exit Entry: PublishCertFlags Value: 1 Allow certificates to be published to the file system.
Node: ExitModules\CertificateAuthority_Microsoft Default.Exit Entry: PublishCertFlags Value: 0 Disallow certificates to be published to the file system.
Node: ExitModules Entry: Active Change in active Exit module. Value specifies name of new module. Blank means none.
Node: PolicyModules Entry: Active Change in active Policy module. Value specifies name of new module.
Node: Entry: CRLPublicationURLs Change in CDPs or AIAs. Value specifies resultant set of CDPs

(continued)

	Node: Entry: CACertPublicationURLs Change in AIAs or CDPs. Value specifies resultant set of AIAs.		
796	A property of Certificate Services changed (see subtypes below).	Warning	Error
	Type: 4 Adding/removing template to/from CA. Value is list of resulting templates by name and OID.		
	Type: 3 Adding KRA cert to CA. Value is Base64 representation of the certificate.		
	Type: 1 Removing KRA certificate from CA. Value is the total KRA certificate count.		
	Type: 1 Adding/removing number of KRA certificates to use for key archival. Value is resulting number of certificates to use.		
797	Certificate Services archived a key.	Information	–
798	Certificate Services imported and archived a key.	Information	–
799	Certificate Services published the CA certificate to Active Directory.	Information	
800	One or more rows have been deleted from the certificate database.	Warning	Error
801	Role separation enabled.	Warning	Error
560	Object Access Where: Object Type: **Key** Object Name: **\REGISTRY\MACHINE\SYSTEM\ ControlSet001\Services\CertSvc\Configuration**	Information	Error

Setting Up SMTP Alerts for Pending Certificate Requests

If you have some certificate types configured to require Certificate Manager approval, they will remain queued in the Pending Requests folder (of the Certification Authority MMC snap-in) until a the request is approved or denied. You may want to configure e-mail alerts to be sent every time a request is queued. Automatically approved requests will not send e-mail alerts.

E-mail alerts can be configured for other CA events as well. The Certificate Services online help documents provide information about how to configure these.

Summary Information

- **Security Requirements**: CA Admins
- **Frequency**: Setup task
- **Technology Requirements**:
  - Text editor
  - SMTP server and recipient mailbox

Task Details

The values for the SMTP server and the SMTP recipients list configured in the file constants.vbs and used by this procedure are also used by the SMTP alerting that is described in the "Monitoring Certificate Services Health and Availability" procedure. If you need to use different settings for the SMTP server and recipients for these two procedures, you can change the values in constants.vbs temporarily and then run this current procedure. The script in this procedure saves these settings to the CA registry. Once run, constants.vbs can be changed back to the previous values to be used by the monitoring script in the "Monitoring Certificate Services Health and Availability" procedure. (The setting to enable or disable e-mail alerts in that procedure–ALERT_EMAIL_ENABLED–has no effect on the alerts in this procedure.)

▶ **To enable e-mail alerts for pending requests**

1. Configure the correct values for e-mail recipients and SMTP server in the script file C:\MSSScripts\constants.vbs:

```
'Alerting parameters
' set to comma-separated list of recipients to get email alerts
CONST ALERT_EMAIL_RECIPIENTS      = "Admin@woodgrovebank.com,
       PKIOps@woodgrovebank.com"
CONST ALERT_EMAIL_SMTP            = "mail.woodgrovebank.com" 'SMTP host to use
```

Note: The indented line in this file excerpt is a continuation of the previous line, which has wrapped to the following line for display–it should be on a single line in the file.

2. Run the following command to enable e-mail alerts for queued pending requests:
   cscript //job:SetupSMTPAlerts C:\MSSScripts\ca_monitor.wsf

Job Scheduling

Job scheduling involves the continuous organization of jobs and processes into the most efficient sequence, maximizing system throughput and utilization to meet service level agreement (SLA) requirements. Job scheduling is closely tied to Service Monitoring and Control and also to Capacity Management.

Scheduling Jobs on the Issuing CA

A number of repetitive tasks need to be run on the CAs in order to maintain the smooth running of the Certificate Services infrastructure. These tasks are automated to reduce operational overhead.

Summary Information

- **Security Requirements**: Local Administrators on CA
- **Frequency**: Setup task
- **Technology Requirements**:
  - Windows Task Scheduler
  - MOM (if appropriate)

Task Details

The following table lists the automated jobs that run on the issuing CA. These jobs are defined in tasks elsewhere in this chapter (shown in the **Referenced task** column); the table below is simply for reference.

Only the issuing CA has automated jobs running. The root CA may be powered down for long periods, so it is impossible to maintain reliable scheduling on this computer.

Table 11.14: List of Scheduled Jobs on Issuing CA

Job description	Schedule	Executed by	Referenced task
System State backup of CA to file	Daily	Windows Task Scheduler	Configuring and Executing an Issuing CA Database Backup Configuring and Executing a Root CA Database Backup
File backup of CA to backup storage	Daily (following System State backup)	Organizational backup scheduler	None (defined by your organization)
Publishing of CRLs to IIS	Hourly	Windows Task Scheduler	Publishing the Issuing CA and Certificate to IIS
Monitoring of online CA health	Hourly	MOM or Windows Task Scheduler	Monitoring Certificate Services Health and Availability
Monitoring CRL issuing and publish state	Hourly	MOM or Windows Task Scheduler	Monitoring Certificate Services Health and Availability
Monitoring CA certificate validity	Daily	MOM or Windows Task Scheduler	Monitoring Certificate Services Health and Availability

Additional Operational Tasks

Numerous other operational tasks are involved with the maintenance of a PKI. Many of these tasks are typically not necessary on regular basis, but may be required occasionally or as part of dealing with a support incident.

The Windows Server 2003 Certificate Services product documentation describes a number of these tasks and provides background information on administration. Many of these tasks are not discussed either in this chapter or the accompanying Build Guide chapter ("Implementing the Public Key Infrastructure"). Even when the task is covered by this solution guide, the product documentation provides useful supplementary information.

See the "More Information" section at the end of this chapter for a link to the document where you can find instructions on how to perform the following administrative tasks:

- Start or stop the certification authority service.
- Set security permissions and delegate control of a certification authority.
- View the certification authority certificate.
- Set security for access to certification authority Web pages.
- Configure certificate manager restrictions.
- Publish certificates in a foreign Active Directory forest.
- Send e-mail when a certification event occurs.
- Use the Certification Authority snap-in.
- Manage certificate revocation.
- Manage certificate requests on a stand-alone certification authority.
- Manage certificate templates for an enterprise certification authority.
- Manage key archival and recovery.
- Change policy settings for a certification authority.
- Change the policy or exit modules of a certification authority.
- Manage role-based administration.

Supporting Quadrant Tasks

The SMFs in the Supporting Quadrant include both reactive and proactive tasks to maintain required service levels. The reactive functions depend on an organization's ability to react and resolve incidents and problems quickly. The more desirable proactive functions try to avoid service disruptions. Through good monitoring of the solution services against predefined thresholds, these functions identify issues before service levels are affected. This provides the operations staff with sufficient time to react and resolve potential problems.

The Supporting Quadrant is closely related to the Service Control and Monitoring SMF described in the Operating Quadrant. Service Control and Monitoring provides the essential information through which operating and support staff can detect problems. The procedures described in this section are intended to address the most common incidents that you will encounter, and enable you to recover from them.

This section contains information that is relevant to the following Service Management Function:

- Incident management

There are no tasks that belong to the remaining SMFs:

- Problem Management (problem diagnosis is covered in the "Troubleshooting" section later in chapter)
- Service Desk

Note: Each task description includes the following summary information: security requirements, frequency, and technology requirements.

Incident Management

Incident management is the process of managing and controlling faults and disruptions in the use or implementation of IT services as reported by customers or IT partners. The primary goal of incident management is to restore normal service operation as quickly as possible, minimize the adverse impact on business operations, and ensure the maintenance of the best possible quality and availability of levels of service. "Normal service operation" is defined here as service operation within the limits of the SLA.

This section is closely related to the "Troubleshooting section." However, the "Troubleshooting" section involves the identification and diagnosis of problems, while this section contains the most common tasks that are used to solve these problems.

The incidents dealt with in the "Troubleshooting" section are:

- Server Not Responsive
- CRL Publishing Failed
- CRL Not Issued
- Client Cannot Enroll
- Security Update Requiring Restart Installed
- Permanent Server Failure
- Orphaned Certificate Needs to be Revoked
- Server Cannot be Restored in Time for CRL or Certificate Issue
- End Entity Certificate is Compromised

- Issuing CA Certificate is Compromised
- Root CA Certificate is Compromised

Most of these incidents relate directly to one or more of the procedures detailed in the following sections. In other cases, for example client enrollment failure, the incident response process required is more complex and discussed in the "Troubleshooting" section.

Restarting the Certificate Services Service

You must restart Certificate Services for a number of operational reasons. (For example, after reconfiguring many CA properties, you will need to restart Certificate Services for the changes to take effect.) In some cases, you may need to restart Certificate Services if the service has stopped responding or is behaving in an unexpected way.

Summary Information

- **Security Requirements**: Local Administrators on CA
- **Frequency**: As required
- **Technology Requirements**:
  - Certification Authority MMC snap-in
  - Net.exe

Task Details

There are numerous methods for restarting a service, any of which are acceptable for this task.

▶ **To restart the CA service**

1. Determine that no one is currently engaged in a transaction with the CA. If time permits, issue a notice to users who may be affected.
2. In the Certification Authority MMC, select the CA object.
3. From the **Tasks** menu, click **Stop service**, or at a command prompt type:
   `net stop "Certificate Services"`
4. From the **Tasks** menu, click **Start service**, or at a command prompt type:
   `net start "Certificate Services"`

Note: When auditing is enabled, Certificate Services may take a long time to shut down and start again–it can take more than 10 minutes for a very large database. The use of the auditing feature will extend the whole server shutdown and startup process, because Certificate Services must calculate a hash of the entire database to create startup and shutdown audit entries. This delay does not occur if startup and shutdown are not audited.

Restarting the CA Server

You may need to restart the CA server for a number of operational reasons, including when an operating system update is applied. You may also need to restart the server if the service has stopped responding or is behaving in an unexpected way and will not restart cleanly using the Service restart procedure.

Summary Information

- **Security Requirements**: Local Administrators on CA
- **Frequency**: As required
- **Technology Requirements**: Net.exe

Task Details

▶ **To restart the CA service**

1. Determine that no one is currently engaged in a transaction with the CA. If time permits, issue a notice to users who may be affected.
2. If possible, run the following command to stop the Certificate Services service to prevent users from connecting to the CA during shutdown:

   ```
   net stop "Certificate Services"
   ```
3. Follow normal operating system procedures to restart the computer. Unless it is clear that the Certificate Services process has stopped responding, do not try to cancel the Certificate Services process or power off the server. Terminating the Certificate Services process may damage the Certificate Services database and require a restore from backup.

Note: As stated in the previous task, auditing the startup and shutdown processes can cause Certificate Services to take a long time to shut down and start again. The delay does not occur if startup and shutdown are not audited.

Restoring the CA from a Backup

If you cannot start a CA due to severe software or hardware damage, you will need to restore the server and key material from backup.

Summary Information

- **Security Requirements**:
  - Local Administrators on CA
  - CA Backup Operators (to perform restore only)
- **Frequency**: As required
- **Technology Requirements**:
  - Windows Backup
  - Organizational backup system

Task Details

Perform the following steps to restore a CA from backup.

Caution: If you are using an HSM, this procedure will not work as indicated. Follow the HSM vendor's instructions for backing up, restoring, and otherwise safeguarding the key material and access keys.

▶ To restore a CA from backup

1. The operating system needs to be recovered to the point where it is viable to run Certificate Services again, which may require the reinstallation of Windows. If so, follow the instructions in the Build Guide to install the basic operating system and system components. There is no need to apply any security or other configuration measures.

   Warning: If you need to re-install Windows on the issuing CA, do not repartition and reformat the second drive. This drive contains the CA database, which may be intact.

2. If possible, preserve CA Database (in %systemroot%\System32\CertLog on the Root CA, or D:\CertLog on the Issuing CA) and CA logs (in %systemroot%\System32\CertLog). Make a file backup of these folders before restoring the CA. The database and the logs may have been unaffected by the system failure. The logs contain information necessary to rerun all transactions on the CA that occurred between the last backup and the server failure. However, restoring a system state backup may overwrite the logs and the existing database, so you should preserve them before beginning a system restore.
3. Insert the backup media with the most recent backup of the CA and restore the system state backup file to a suitable disk area (a second drive is recommended, if available).
4. Start the Windows Backup program. From the **Restore** tab, right-click the **File** object in the left pane and then click **Catalogue File**.
5. Ensure that **Original Location** is selected as the destination to which to restore files, and then click **Start Restore** to restore the system state. After completion, restart the server and stop Certificate Services once the system has restarted.
6. If the CA logs were preserved in step 2, copy them back to the Certificate Services logs folder (%systemroot%\System32\CertLog). The logs are now ready to be rerun against the restored database to insert any transactions that occurred after the last backup.

   Note: If you were able to save the intact CA database and logs in step 2 you can restore these to the server instead of following the procedure in this step (step 6). The Certificate Services service must be stopped before you can copy the CA database and logs back to the server.

7. Start Certificate Services.

Restoring the CA Certificate and Key Pair to a Temporary Computer

If a failed CA cannot be restored in time for the CA to issue a new CRL (or renew a critical certificate), you will need to install the CA certificate and keys on a temporary computer so that you can use them to re-sign and extend the validity period of an existing CRL or certificate.

Summary Information

- **Security Requirements**: Local Administrators on temporary computer
- **Frequency**: As required
- **Technology Requirements**:
  - Certutil.exe
  - Cipher.exe

Task Details

This task describes how to restore the CA certificate and private key to a temporary computer. If the CA has been renewed you will have backups of more than one certificate and key pair. You should restore the most recent key and certificate file for this procedure.

Important: Although this computer has the CA key installed, you should still take the same security precautions with it as you would the CA. If you are restoring the key of an offline CA, ensure that the computer is offline. Consider reformatting the disks of the computer after you have finished with the key.

Caution: If you are using an HSM, this procedure will not work as indicated. Follow the HSM vendor's instructions for backing up, restoring, and otherwise safeguarding the key material and access keys.

▶ **To restore the CA key(s) and certificate(s) to a temporary computer**

1. Ensure that the computer has been disconnected from the network. Log on as a member of local Administrators, then create CAKeySigner as a local user account.
2. Log on using this new account.
3. Insert a disk containing the backup of the CA keys to be tested.
4. Use Windows Explorer to navigate to the P12 key files, select the most recent file and double-click it to begin the Certificate Import Wizard.
5. Enter the password when prompted. Do not select the check boxes to give high protection to the keys or to make them exportable.
6. Select **Personal store** as the location to which to restore the CA keys.
7. Open the Certificates MMC snap-in and browse to the personal store. Locate the CA Certificate for the restored CA, and then open the certificate to verify that you have a corresponding private key.

You can now perform any re-signing tasks required with the restored CA keys. See the following procedure, "Re-signing a CRL or Certificate to Extend Its Validity Period." When complete, clean the keys from the computer using the following procedure.

▶ **To clean the keys from the system**

1. Log on as a member of local Administrators and delete the user profile of the CAKeySigner account (using **Advanced Properties** in My Computer).
2. Delete the CAKeySigner account.
3. Securely erase unallocated areas of the disk to permanently remove traces of the keys by running the following command:

   Cipher /W:%AllUsersProfile%

Note: Specifying %allusersprofile% as the path ensures that Cipher.exe operates on the drive holding the user profiles. It clears the whole drive, not just the path indicated.

Re-Signing a CRL or Certificate to Extend Its Validity Period

If a CA is not available because of server failure of some kind, you can extend the lifetime of CRLs or certificates by re-signing the CRL or Certificate file. This action may be essential to maintain service.

Summary Information

- **Security Requirements**: Temporary account created during CA key restore
- **Frequency**: As required
- **Technology Requirements**: Certutil.exe

Task Details

Re-signing a certificate or CRL will extend its validity period. By default, the existing validity period is used and restarted from the date of signing. For example, if the original validity period of the CRL was one month, the new validity period will be one month starting from the time of re-signing. If necessary, a different validity period can be specified in the Certutil command line.

▶ **To re-sign a CRL or certificate**

1. Obtain a copy of the CRL or certificate to be re-signed.
2. Log on to a computer where the CA key and certificate that was used to originally sign the CRL or certificate has been restored. (See the previous procedure, 'Restoring the CA Certificate and Key Pair to a Temporary Computer.") Log on using the account created in that procedure.
3. Run the following command, replacing *OldFile.ext* with the name of the CRL or certificate file and *NewFile.ext* with the required output name.

   Certutil -sign *OldFile.ext NewFile.ext*

4. When prompted for the certificate to use, select the CA certificate.
5. If you are re-signing a CRL, you must now publish it to the CDPs as required (see the procedures for publishing CRLs in the "Operating Quadrant Tasks" section).

Revoking an End-Entity Certificate

A certificate may need to be revoked for a number of reasons, including:

- The functionality or privileges associated with the certificate have been revoked from the certificate holder.
- The certificate key has been compromised.
- The CA that issued the certificate has been compromised.

Summary Information

- **Security Requirements**: Certificate Managers
- **Frequency**: As required
- **Technology Requirements**: Certification Authority MMC snap-in

Task Details

This procedure describes the steps for revoking an end-entity certificate (that is, a certificate issued to anything other than a CA). Follow the procedures outlined elsewhere for revoking a CA certificate.

▶ **To revoke a certificate**

1. Log on as a member of Certificate Managers, and locate the certificate(s) to be revoked in the Certification Authority database (in the Certification Authority MMC). Use the **Filter** option (in the **View** menu of the CA **Issued Certificates** folder) to locate the certificate(s).
2. Select the certificate(s), and then from the **Tasks** menu, click **Revoke**.
3. Select an appropriate reason code for the revocation. Unless the reason for revocation falls into one of the predefined reason codes, select **Unspecified**.

Important: Only the **Certificate Hold** reason allows reinstating the certificate at a later time. All other reasons result in the permanent disabling of the certificate. However, do not use **Certificate Hold** just because there is a possibility that the certificate may be reinstated. Only use this code when you genuinely need temporary suspension of the certificate.

Revoking an Orphaned Certificate

When you restore a CA from backup after a server failure of some kind, certificates issued between the last backup and the failure may not be in the Certificate database. These certificates are referred to as "orphaned" certificates. This situation will occur if the CA logs are destroyed and cannot be rerun against the CA database after restoring from backup. If this situation happens, it is impossible to revoke any of these "orphaned" certificates with the standard procedure.

Summary Information

- **Security Requirements**: Certificate Managers
- **Frequency**: As required
- **Technology Requirements**: Certutil.exe

Task Details

To revoke an orphaned certificate, it is necessary to either obtain a copy of the certificate to be revoked or the serial number of that certificate.

▶ **To revoke an orphaned certificate**

1. Log on to the CA that issued the certificate to be revoked as a member of Certificate Managers.
2. If a copy of the certificate is not obtainable, run the following command to create a dummy certificate and save it as CertToRevoke.cer. Replace *SerialNumber* with the serial number of the certificate to be revoked.

   Certutil -sign *SerialNumber* CertToRevoke.cer
3. When prompted, select the current CA certificate to sign the dummy certificate.
4. After creating a dummy certificate (or obtaining a copy of the real certificate to be revoked), you need to import it into the CA database. Run the following command to import the certificate into the certificate database. CertToRevoke is either a copy of the actual certificate to be revoked or the dummy created in the previous steps.

   Certutil -importcert CertToRevoke.cer
5. Follow the standard procedure to revoke a certificate (detailed in the previous procedure, "Revoking an End-Entity Certificate").

Important: There is a problem with Certutil versions prior to SP1 of Windows Server 2003 that makes the dummy certificate creation operation fail on a computer running Windows Server 2003. If you are using a version earlier than this and you cannot locate a copy of the original certificate, an alternative approach is to take an existing certificate and use a binary editor to replace the serial number with the serial number of the certificate to be revoked. This modified certificate can be re-signed with the following command:

Certutil -sign ModifiedCert.cer CertToRevoke.cer

The newly created certificate can then be imported into the database using step 4 in this procedure.

Revoking and Replacing an Issuing CA Certificate

If the private key of a CA is compromised in some way (or is even suspected of being compromised), revoke the CA certificate and issue a new CA certificate using a new key pair.

Summary Information

- **Security Requirements**: Certificate Managers
- **Frequency**: As required
- **Technology Requirements**: Certification Authority MMC snap-in

Task Details

Because the Root CA has a very long CRL publishing period, simply revoking the CA certificate and publishing a new CRL will result in a very long delay between the revocation and certificate users receiving notification of that revocation. To ensure that all certificates previously issued by the compromised CA are rejected as soon as possible, all certificates that this CA has issued are also individually revoked.

Important: All certificate users will have to re-enroll for new certificates.

▶ **To revoke an issuing CA certificate**

1. Log on to the issuing CA as member of Certificate Managers and open the Certification Authority MMC snap-in.

2. Select all certificates in the Issued Certificates folder, and then from the **All Tasks** menu click **Revoke Certificate**. Select **CA Compromise** for the reason code.
3. Increase the CRL Publication Interval to match the remaining lifetime of the CA certificate. Increasing this interval will ensure that it is definitely longer than the remaining lifetime of all certificates that the CA has issued.
4. Clear the **Publish Delta CRLs** check box if it is selected.
5. From the **All Tasks** menu of the Revoked Certificates folder, click **Publish** and then click **New CRL**.
6. Log on to the Root CA as member of Certificate Managers and open the Certification Authority MMC.
7. Find the CA certificate to be revoked in the Issued Certificates folder, and from the **All Tasks** menu click **Revoke Certificate**. Select **Key Compromise** for the reason code.
8. Follow the procedure "Publishing an Offline CRL and CA Certificate" in the "Operating Quadrant Tasks" section (you can ignore the CA certificate publishing parts of the procedure).
9. Return to the issuing CA and follow the procedure "Renewing the Issuing CA Certificate" in the "Operating Quadrant Tasks" section.

Certificate users can now re-enroll with the new CA. Autoenrolled certificates will be enrolled automatically.

Revoking and Replacing a Root CA Certificate

If the private key of a root CA is compromised in some way (or is even suspected of being compromised), you must remove the CA certificate from its point of trust and revoke all of the certificates that it and any of its subordinate CAs have issued. You must renew the Root CA certificate and the certificates of all of its subordinate CAs with new keys, and then republish them to Active Directory. It is not normally possible to revoke a root CA certificate. Often, the CA certificate does not include a CDP from which to check revocation status. In any case, it is not strictly legal for a CA to attest to its own revocation. (It would need to use the compromised certificate to sign the CRL containing its own revoked certificate!)

Summary Information

- **Security Requirements**:
  - Certificate Managers
  - Local Administrators on CAs (for CA renewal subtasks)
- **Frequency**: As required
- **Technology Requirements**: Certification Authority MMC snap-in

Task Details

Note: All certificate users will have to re-enroll for new certificates after completing this procedure.

▶ **To revoke a Root CA certificate**

1. Log on to the issuing CA as member of Certificate Managers and open the Certification Authority MMC snap-in.
2. Select all certificates in the Issued Certificates folder, and then from the **All Tasks** menu click **Revoke Certificate**. Select **CA Compromise** for the reason code.

3. Increase the CRL Publication Interval to match the remaining lifetime of the CA Certificate. Increasing this interval will ensure that it is definitely longer than the remaining lifetime of all certificates that the CA has issued.
4. Clear the **Publish Delta CRLs** check box, if it is selected.
5. From the **All Tasks** menu of the Revoked Certificates folder, click **Publish** and then **New CRL**. Repeat steps 1 to 5 for all subordinate CAs.
6. Log on to the root CA as member of Certificate Managers, and open the Certification Authority MMC snap-in.
7. Select all certificates in the Issued Certificates folder, and then from the **All Tasks** menu click **Revoke Certificate**. Select **CA Compromise** for the reason code.
8. Increase the CRL Publication Interval to match the remaining lifetime of the CA Certificate. Increasing this interval will ensure that it is definitely longer than the remaining lifetime of all certificates that the CA has issued.
9. Clear the **Publish Delta CRLs** check box if it is selected.
10. Follow the "Renewing the Root CA Certificate" operations procedure.
11. Return to the issuing CA and follow the "Renewing the Issuing CA Certificate" operations procedure.

Certificate Users can now re-enroll with the new CA. Autoenrolled certificates will be enrolled automatically.

Important: Renewing a Root CA certificate is a very significant event, especially when it involves the revocation of child CAs and issued certificates. Be sure to inform any affected application owners of the new root certificate in case they need to configure this new root into their application.

Optimizing Quadrant Tasks

The optimizing quadrant includes the SMFs to manage costs while maintaining or improving service levels. Tasks include review of outages/incidents, examination of cost structures, staff assessments, availability, and performance analysis, as well as capacity forecasting.

This section contains information relevant to the following SMFs:

- Capacity management

There are no tasks that belong to the remaining SMFs:

- Service level management
- Financial management
- Availability management
- IT service continuity management
- Workforce management

Note: Each task description includes the following summary information: security requirements, frequency, and technology requirements.

Capacity Management

Capacity management is the process of planning, sizing, and controlling service solution capacity so that it satisfies user demand within the performance levels set forth in the SLA. Satisfying this demand requires information about usage scenarios, patterns, and peak load characteristics of the service solution, as well as stated performance requirements.

Determining Maximum Load on the Issuing CA

This section provides some information on the likely maximum load on the issuing CA.

Although CAs do not normally experience a very significant load, there are times when loads can peak sharply. The greatest load on a CA is typically during peak logon or startup time during the rollout of a new certificate type. Similarly, although more rarely, a mass certificate revocation or CA certificate revocation will cause an abnormal peak of activity as users and computers re-enroll.

Summary Information

- **Security Requirements**: None
- **Frequency**: Setup task
- **Technology Requirements**: None

Task Details

Microsoft's internal testing has shown that, for a typical enterprise CA, the performance bottleneck under high load is caused by the interaction with Active Directory. The task of signing and issuing certificates is relatively light compared to the overhead of performing directory lookup to retrieve certificate subject information and then publishing the certificate back to Active Directory.

Consider, for example, the numbers generated in a peak load scenario where a new certificate type has been enabled and all users and computers are required to enroll certificates of this type:

- Number of users: 3000
- Number of computers: 3000
- Approximate maximum issuing speed of an enterprise CA is 30 certificates per second (or 1800 certificates per minute).

These numbers indicate a minimum total enrollment time of 3.3 minutes. For 15,000 users and the same number of computers enrolling simultaneously, the enrollment time would extend to 16.6 minutes.

You must determine what the maximum peak enrollment load is likely to be for your organization and calculate the total enrollment duration. If the time is unacceptably long and you can not stagger the enrollment in any way, you must consider deploying multiple issuing CAs. These issuing CAs should be deployed to separate Active Directory sites so that they use separate domain controllers.

Determining Storage and Backup Requirements for an Issuing CA

This section provides capacity details for CA storage parameters. These details will help capacity planners calculate future storage requirements for online disk and offline backup storage.

Summary Information

- **Security Requirements**: None
- **Frequency**: As required
- **Technology Requirements**: None

Task Details

The following sections list the assumptions and results of the sizing calculations for CA database size, CA database log size, CRL size, and backup window (time to back up the CA database).

The following calculations are based on these assumptions:

- A population of 3000 users, 3000 computers, and 100-300 servers.
- Each end entity is issued with five certificates per year, each with a validity period of one year.
- The certificates are maintained in the database for five years.
- The database is backed up daily (truncating the database logs).

Certificate Database Size

Each certificate entry takes approximately 20 KB in the database (for certificate types that archive the private key with the certificate, you should allow an additional 10 KB of storage per certificate). A quick calculation indicates the following:

- There are 150,000 certificates stored in the database at any one time.
- The total certificate database size is 3 GB.

For an organization of 15,000 users the certificate database size is 15 GB.

Average Certificate Database Log Size

- There are 750 certificates per day.
- The average log size is 5 MB.

For an organization of 15,000 users, 3750 certificates are issued each day, creating a maximum log size of 25 MB.

CRL Size

A CRL entry is approximately 30 bytes. Typically, approximately ten percent of issued certificates will be revoked. Revoked certificates outside their validity period are not included in the CRL.

- 30,000 certificates are within the validity period at any one time.
- 3000 certificates will be in the CRL.
- The CRL size is 90 KB.

For an organization of 15,000 users, 15,000 certificates will be in the CRL, creating a CRL size of 440 KB.

Backup Window for Certificate Database

If you assume a network backup operating in ideal conditions on a dedicated 100 Mbps (megabits per second) switch to the backup server, then a 3 GB database with an additional 500 MB of system state can be backed up in approximately 15-20 minutes. A 15,000-user organization with a certificate database of 15 GB can be backed up in less than two hours.

Changing Quadrant Tasks

The changing quadrant includes the processes and procedures that are required to identify, review, approve, and incorporate change into a managed IT environment. Change includes hard and soft assets, as well as specific process and procedural changes.

The objective of the change process is to introduce new technologies, systems, applications, hardware, tools, processes, and changes in roles and responsibilities into the IT environment quickly and with minimal disruption to service.

This section contains information relevant to the following SMFs:

- Change management
- Configuration management
- Release management

Note: Each task description includes the following summary information: security requirements, frequency, and technology requirements.

Change Management

The change management SMF is responsible for managing change in an IT environment. A key goal of the change management process is to ensure that all parties affected by a given change are aware of and understand the impact of the impending change. Because most systems are closely interrelated, any changes made in one part of a system may have profound impacts on another. In order to mitigate or eliminate any adverse effects, change management attempts to identify all affected systems and processes before the change is deployed. Typically, the “target” or managed environment is the production environment, but it should also include key integration, testing, and staging environments.

All changes to the PKI should follow the following standard MOF change management process:

1. **Change request**. The formal initiation of a change through the submission of a request for change (RFC).
2. **Change classification**. The act of assigning a priority and a category to the change, using its urgency and its impact on the infrastructure or users as criteria. This assignment affects the implementation speed and route.
3. **Change authorization**. The consideration and approval or disapproval of the change by the change manager and the change approvals board (CAB), a board containing IT and business representatives.
4. **Change development**. The planning and development of the change, a process that can vary immensely in scope and includes reviews at key interim milestones.
5. **Change release**. The release and deployment of the change into the production environment.
6. **Change review**. A post-implementation process that reviews whether the change has achieved the goals that were established for it and determines whether to keep the change in effect or back it out.

This section describes the change development procedures for some of the key changes that you are likely to require on a regular basis in your environment. Each change

development procedure will have a companion change release procedure that describes how the change is to be deployed into production.

Managing Operating System Updates

The management of security updates to Certificate Services is part of general Windows patch management. This is covered in two solution guides from Microsoft, which cover delivery of Windows operating system updates using either Microsoft Systems Management Server (SMS) or Microsoft Software Update Services (SUS). See the "More Information" section at the end of this chapter for details on how to obtain it.

Patch management includes release management and configuration management components as well as a change management component. However, all three SMFs are covered by the documents referenced in the preceding paragraph.

Summary Information

- **Security Requirements**: Local Administrators on CA
- **Frequency**: Setup task
- **Technology Requirements**: Security update distribution infrastructure (such as SMS or SUS)

Adding a Certificate Template

You add a new certificate template to allow the issue of a new certificate type, which could be needed because a new application is being deployed or an existing application requires new functionality. This task can also form part of a process to update an existing certificate type.

Summary Information

- **Security Requirements**: Enterprise PKI Admins
- **Frequency**: As required
- **Technology Requirements**: Certification Templates MMC snap-in

Before submitting a request for a new certificate type, test it in a test environment that is representative of the production environment.

Document the request for a new certificate type and include:

- The reasons for the new template
- An assessment of the impact on users and the infrastructure
- An assessment of any impact of not performing the change
- Results of testing the change

The documentation should include the relevant updates to the certificate policies and certificate practices statement (CPS). It then needs to be assessed in terms of its priority and impact. After the change has been approved, it can be implemented (although not yet released).

Task Details

The following procedure should be carried out in a test environment only. The process for performing this change in the production environment is documented in the "Releasing a New Certificate Template" procedure.

▶ **To implement a new certificate template**

1. Log on as a member of Enterprise PKI Admins and open the Certificate Templates MMC snap-in.

2. New templates are created by duplicating an existing template. Select an appropriate template on which to base the new template–one that is as similar as possible to the template that you want to create.

   Important: Be sure to match the basic template type–user or computer–of the source template to the subject type of the new template; the type cannot by changed in the template editor.

3. Edit the template details as required. For detailed information on this step, see the product documentation in the local help system or online at the reference in the "More Information" section.
4. If this template is to replace an existing template, you need to add the replaced templates to the list of **Superseded Templates** in the new template properties. You need to be extremely careful that the replacement template provides the same functionality as, or a superset of the functionality of, the superseded template. Never reduce the functionality unless you are certain that no applications make use of the functionality being removed.
5. Test the changes to ensure that they work as expected and do not negatively impact existing applications.
6. Create the appropriate changes to your certificate policy document and CPS.
7. Follow the steps in the "Releasing a New Certificate Template" and "Releasing a New CPS" procedures (if you publish your CPS).

Updating a Certificate Template

This task describes how to make minor changes to certificate templates. Major changes should be performed through template duplication and forcing the new template to supersede the existing template (as described in the previous task, "Adding a Certificate Template").

Summary Information

- **Security Requirements**: Enterprise PKI Admins
- **Frequency**: As required
- **Technology Requirements**: Certificate Templates MMC snap-in

Task Details

You should only make minor changes–ones that will not have a significant impact on certificate users–to a certificate template. It is much more difficult to control the impact of template modifications and considerably more complex to roll back changes to templates.

Examples of minor changes include:

- Changing the validity period or renewal period
- Adding (but not removing) an allowed CSP type

Implement any changes that affect the functionality of the certificates (such as changing the certificate polices, removing CSP types, and changing the issuance criteria) by creating a new template type and superceding the old template.

Assess and approve the change request as described in the "Adding a Certificate Template" procedure.

You can then implement and test the proposed template change passing the change for release into production. See the "Releasing a Template Update" procedure.

▶ **To update a certificate template**

1. Log on as a member of Enterprise PKI Admins and load the Certificate Templates snap–in into an MMC.
2. Open the template to be modified and make the changes required. For detailed information on this see the product documentation in the local help system or online at the reference in the "More Information" section.
3. Test the update to ensure that it produces the required functionality.
4. Follow the steps in the "Releasing a New Certificate Template" and "Releasing a New CPS" procedures (if appropriate).

Removing a Certificate Template

When a certificate template is no longer required, it can be removed from active status or it can be removed from the directory altogether.

Summary Information

- **Security Requirements**: CA Admins
- **Frequency**: As required
- **Technology Requirements**:
  - Certificate Templates MMC snap-in
  - Certification Authority MMC snap-in

Task Details

Only remove a template when you are sure that no applications depend upon certificates of that type being available. Assess and approve the request to remove the template in the same way as described in the "Adding a Certificate Template" procedure. Always follow the first procedure to remove a template from active use and test the effects of this before deleting a template from the directory completely.

You can then implement and test removing the template change before you release the change into production. See the "Releasing a Template Removal" procedure.

▶ **To remove a certificate template from active use**

1. Log on as a member of CA Admins and load the Certification Authority snap–in into an MMC.
2. From the Certificate Templates folder, right-click the template to be removed and select **Delete**.
3. Repeat steps 1 and 2 for all issuing CAs that currently issue this certificate type.
4. Test any applications that previously used this template to ensure that they are no longer dependent on this certificate type.
5. Follow the steps in the "Releasing a Template Removal" and "Releasing a New CPS" procedures (if appropriate).

▶ **To remove a certificate template from the directory completely**

1. Log on as a member of Enterprise PKI Admins and load the Certificate Templates snap-in into an MMC.
2. Right-click the template to be removed and select **Delete**.

Configuration Management

The configuration management SMF is responsible for the identification, recording, tracking, and reporting of key IT components or assets called configuration items (CIs). The information captured and tracked will depend upon the specific CI, but will often include a description of the CI, the version, its constituent components, its relationships to other CIs, location/assignment, and current status.

Configuration management of a PKI can be grouped into several major areas:

- **Enterprise PKI Configuration**. Common information stored in Active Directory.
- **Certificate Template Configuration**. Configuration details of all active templates.
- **CA Configuration**. CA-specific configuration details.
- **CA and PKI management groups**. Details of PKI management groups and users and what permissions they have.
- **Client configuration**. Configuration of user and computer settings through Group Policy (or other method).

Each of the following sections describes these items in more detail and includes methods for automating the collection of this information if possible.

For additional references on Configuration Management, see the "More Information" section at the end of this chapter.

Collecting Enterprise PKI Configuration Information

Enterprise-wide configuration information is stored in Active Directory, including trusted root CA publication, enterprise CA configuration and advertising information. It also includes certificate templates, although these are discussed separately in a later procedure.

Summary Information

- **Security Requirements**: Domain users
- **Frequency**: As required
- **Technology Requirements**:
  - Certutil.exe
  - DSQuery.exe

Task Details

Maintain records of the following information stored in Active Directory:

- Trusted Root Certification Authorities
- NTAuth store
- Enrollment Services (enterprise CAs)
- Cross certificates
- Published CRLs

Commands to collect this information are provided in the following procedures.

Important: In the following commands you must replace the example root domain Distinguished Name (DN)–*DC=woodgrovebank,DC=com*–with the DN of *your* forest root.

Note: Some of the following commands display on multiple lines, but they should be entered on a single line.

- **To display trusted Root certification authorities**

  certutil -store -enterprise Root

- **To display NT Auth stores**

  certutil -store -enterprise NTAuth

- **To display the certificates of current enterprise CAs**

  certutil -store -enterprise "ldap:///cn=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration, *DC=woodgrovebank,DC=com*?cACertificate?one? objectClass=pkiEnrollmentService"

- **To display intermediate and cross certificates**

  certutil -store -enterprise CA

- **To display the intermediate CA certificates on their own**

  certutil -store -enterprise "ldap:///cn=AIA,CN=Public Key Services,CN=Services,CN=Configuration, *DC=woodgrovebank,DC=com*?cACertificate?one? objectClass=certificationAuthority"

- **To display the cross certificates on their own**

  certutil -store -enterprise "ldap:///cn=AIA,CN=Public Key Services,CN=Services,CN=Configuration, *DC=woodgrovebank,DC=com*?cRossCertificatePair?one? objectClass=certificationAuthority"

- **To display currently published CRLs**

  1. This command will display the **server names** of all CAs that have published CDPs in the Active Directory CDP container:

     dsquery * "cn=CDP,cn=Public Key Services,cn=Services, cn=Configuration,*DC=woodgrovebank,DC=com*" -attr cn -scope onelevel

  2. This command will display the CDPs of each CA that has published CRLs in the Active Directory CDP container. The CDPs are child objects of the server objects displayed in the previous list. The CA uses its common name to name each CDP object. Note that a CA will create a new CDP object for each CA version (incremented each time the CA is renewed); these names are stored as "CACommonName(X)" where X is the CA version number:

     dsquery * "cn=CDP,cn=Public Key Services,cn=Services, cn=Configuration, *DC=woodgrovebank,DC=com*" -attr cn -filter (objectclass=crlDistributionPoint)

3. You can use the information in the previous steps to display the CRL for a given CDP (using the CA common name(s) from step 2 and the CA server name(s) obtained in step 1):

   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=cRlDistributionPoint"

Important: Replace "Woodgrove Bank Root CA" with the common name of the CA, "HQ-CA-01" with the host name of the CA, and "DC=woodgrovebank,DC=com" with the DN of your forest root domain.

Note: You may want to write a simple command file (batch) script to automate this command if you need to run it regularly.

Collecting Certificate Template Configuration Information

Certificate templates are stored in Active Directory. Keep a record of the configuration for each template and keep a record of the certificate enrollment permissions used for each template.

Summary Information

- **Security Requirements**: Domain users
- **Frequency**: As required
- **Technology Requirements**: Certutil.exe

Task Details

Use the following commands to collect this configuration information:

▶ **To produce a list of templates configured in Active Directory**

```
Certutil -template
```

▶ **To dump the configuration of these templates**

```
Certutil -dsTemplate
```

▶ **To dump the permissions of a template**

```
Dsacls "cn=TemplateName,cn=Certificate Templates,cn=Public Key Services,cn=Services,cn=Configuration,DC=woodgrovebank,DC=com"
```

No tool exists that will export the full template permissions in an easily readable form. Dsacls.exe will display the permissions on a template. However, the current version does not display the extended rights "Autoenroll" permission (although it does display "Enroll" and the other extended rights permissions). This means you must keep a record of "Autoenroll" permissions manually. Alternatively, you can write a script or tool using the Active Directory Services Interface (ADSI) to read and display all of the permissions correctly.

Collecting CA Configuration Information

This section describes how to retrieve configuration information stored locally on each CA and, in the case of enterprise CAs, some information stored in Active Directory.

Summary Information

- **Security Requirements**: Local Administrators of CA
- **Frequency**: As required
- **Technology Requirements**: Certutil.exe

Task Details

Maintain records of the following information:

- CA registry information
- CA certificate information
- CA permissions
- CA assigned templates
- CA CPS

Use the following commands to collect this configuration information:

▶ **To display the CA registry configuration**

```
Certutil -getreg
Certutil -getreg CA
```

▶ **To display the current CA certificate**

```
certutil -f -ca.cert %temp%\CAcert.cer > nul && certutil -dump
    %temp%\CACert.cer
```

Note: Some of these commands display on multiple lines, but they should be entered on a single line.

No tool exists to export the complete CA permissions information in a useable form. However, you can write an ADSI script to read and display all of the permissions correctly. Alternatively, keep a manual record of this information.

▶ **To display the templates currently assigned to this CA**

```
Certutil -CATemplates
```

The CA CPS file should be maintained with adequate version control so that it is easy to identify and retrieve the CPS that was in effect at any given point in time.

Collecting CA and PKI Management Groups Information

The membership of the PKI management groups is a very important piece of configuration information because these groups have control over all aspects of the CAs and enterprise PKI information.

Summary Information

- **Security Requirements**: Domain user
- **Frequency**: As required
- **Technology Requirements**: Net.exe

Task Details

For each of the PKI and CA administration groups, list and record the current membership. If any of the members are groups themselves (indicated by an asterisk before the name), list the membership of those groups until you have a complete listing of all users who are members of the PKI groups.

The default groups are:

- Enterprise PKI Admins
- Enterprise PKI Publishers
- CA Admins
- Certificate Managers
- CA Auditors
- CA Backup Operators

You should also include any additional management groups you may have created.

▶ **To list the membership of each group**

```
Net groups groupname /domain
```

Collecting Certificate Client Configuration Information

This task refers to the client configuration information deployed using Group Policy. If you use any other mechanisms–for example, SMS or logon scripts–to deploy PKI-related client settings, you should document those here as well.

Summary Information

- **Security Requirements**: Administrator with permissions to manage Group Policy objects
- **Frequency**: As required
- **Technology Requirements**: Group Policy Management Console

Task Details

Use the Group Policy Management Console (GPMC) to collect and list PKI client configuration information. See the reference in the "More Information" section for how to obtain and use the GPMC.

Release Management

The focus of release management is to facilitate the introduction of software and hardware releases into managed IT environments. Typically, this includes the production environment and the managed pre-production environments. Release management is the coordination point between the release development/project team and the operations groups responsible for deploying the release in production.

In this section we will be dealing with the most common changes–adding, changing, and removing certificate types (using certificate templates). There are other types of change that you also need to release in the same systematic way, including:

- **Changes to PKI configuration**. Examples include templates and OIDs.
- **Changes to CA configuration**. Local registry plus Active Directory settings in enrollment objects.
- **Changes to client configuration**. GPO changes

All of the release procedures use the following general process:

1. Prepare for change release–back up the existing configuration.
2. Test the change in a controlled way.
3. Roll out the change in a controlled way to limited numbers of users or computers.
4. Roll back the change if something goes wrong–Active Directory and CA configuration.

Releasing a New Certificate Template

Introducing a new certificate type represents a significant change to the IT environment, so the release must be handled in a controlled and reversible fashion.

Summary Information

- **Security Requirements**:
  - Enterprise PKI Admins
  - CA Admins
- **Frequency**: As required
- **Technology Requirements**:
  - Certification Authority MMC snap-in
  - Certificate Templates MMC snap-in
  - Other tools as required by dependent tasks

Task Details

The procedure to release a new certificate template into the production environment is as follows:

▶ **To release a new certificate template**

1. Back up the existing certificate template configuration. This backup may be done as part of the regular Active Directory backup or with the technique described in the "Exporting a Certificate Template from the Active Directory" procedure.
2. Create the new template as described in the "Adding a Certificate Template" procedure.
3. Remove all default enroll and autoenroll for groups (look for such objects as Authenticated Users and Domain Users). Create the certificate enrollment group (and/or autoenrollment group) for the template as described in the "Creating Certificate Template Enrollment Groups" procedure.
4. Add the new certificate template to the issuing CA. If you are not also a member of CA Admins you will need to log on (or use the runas command) as a member of this group and run the Certification Authority MMC. Right-click the Certificate Templates folder and select **New**, **Certificate Template to Issue**. Add the template from the list.
5. Add test or pilot users or computers to the certificate enrollment group as described in the "Enabling Enrollment (or Autoenrollment) of a Certificate Type for a User or Computer" procedure.
6. Test the enrollment of the new certificate type to ensure it occurs as expected.
7. Test the certificate functionality to ensure it is as expected.
8. After successful testing, add the final production users, computers, or security groups to the certificate enrollment group(s) as described in the "Enabling Enrollment (or Autoenrollment) of a Certificate Type for a User or Computer" procedure.
9. If this template supersedes one or more existing templates, you can remove the superseded templates from the issuing CA with the Certification Authority MMC snap-in to avoid anyone enrolling these superseded certificate types. Do not delete this template from the directory until you are certain that everyone has transitioned to the new template type.
10. If appropriate, update your CPS to reflect the new certificate functionality.

Rolling back a new template type is relatively straightforward if any superseded templates have not been deleted. If the superseded template has been deleted, you will need to restore a copy from backup with either an Active Directory authoritative restore or the Template export and import procedures described in the earlier "Storage Management" section ("Exporting a Certificate Template from Active Directory" and "Importing a Certificate Template to Active Directory").

▶ **To roll back the addition of a new template**

1. If you have not superseded other templates with this template, you can simply delete it.
2. If you have removed any templates superseded by this template, restore those first. Follow the steps in the "Importing a Certificate Template to Active Directory" procedure. You will need to restore the template permissions as described in that procedure.

Releasing a New CPS

If you publish your CPS, you need to update it to reflect changing certificate policies and practices in your organization.

Summary Information

- **Security Requirements**: Administrator with permissions to modify CPS file on the Web server
- **Frequency**: As required
- **Technology Requirements**: Text or HTML editor as appropriate to the format of the CPS

Task Details

The CPS is typically stored as a simple HTML or text file on a Web or file server. If multiple CAs use the same CPS, the standard is to have all CAs reference the same file.

▶ **To release a new CPS**

1. Back up the existing CPS.
2. Make the required changes to an offline copy.
3. Replace the CPS.
4. Test to ensure that the new CPS file is readable from clients emulating the platform types and locations that you normally service.

Releasing a Template Update

This task describes how to make release changes to existing certificate templates in a controlled and reversible way.

Summary Information

- **Security Requirements**: Enterprise PKI Admins
- **Frequency**: As required
- **Technology Requirements**:
  - Certificate Templates MMC snap-in
  - Other technology as required by referenced procedures

Task Details

You should only make changes to certificate templates that are relatively minor and will not have a significant impact on certificate users. It is much more difficult to control the impact of template modifications and considerably more complex to roll back changes to templates.

▶ **To release a certificate template update**

1. Export the current template to file using the "Exporting a Certificate Template from Active Directory" procedure.
2. Log on as a member of Enterprise PKI Admins and load the Certificate Templates snap-in into an MMC. Perform the changes to the template as described in "Updating a Certificate Template."
3. Update your CPS and follow the steps in the "Releasing a New CPS" procedure (if appropriate)

▶ **To roll back a certificate template update**

- Follow the steps in the "Importing a Certificate Template to Active Directory" procedure (in the "Storage Management" section).

Releasing a Template Removal

When a certificate template is no longer required, you can remove it from active use or remove it from the directory.

Summary Information

- **Security Requirements**: Enterprise PKI Admins
- **Frequency**: As required
- **Technology Requirements**:
  - Certification Authority MMC snap-in
  - Other technology as required by referenced tasks

Task Details

The release procedure for removing a template from active use is relatively straightforward because it is easy to reverse. Removing the template from the directory is more problematic because it requires the template to be re-imported to reverse the change.

▶ **To remove a certificate template from active use**

1. Remove the template from current issuing CAs as described in the "Removing a Certificate Template" procedure.
2. Update your CPS and follow the steps in the "Releasing a New CPS" procedure (if appropriate).

▶ **To roll back removing a template from active use**

1. Log on as a member of CA Admins and use the Certification Authority MMC snap-in to add the templates back to the issuing CAs.
2. Update your CPS and follow the steps in the "Releasing a New CPS" procedure (if appropriate).

▶ **To remove a certificate template from the directory completely**

1. You should only perform this procedure after the certificate template has been successfully removed from active use and any dependent applications have been tested to ensure that they are not negatively impacted.
2. Export the current template to a file with the "Exporting a Certificate Template from Active Directory" procedure.
3. Follow the procedure outlined in "Removing a Certificate Template" for removing a certificate template from the directory completely.

▶ **To roll back removing a template from the directory**

- Follow the procedure for re-importing the deleted template in "Importing a Certificate Template to Active Directory."

Troubleshooting

Troubleshooting refers to both the Incident Management and the Problem Management SMFs. Incident Management is concerned with restoring the service as quickly as possible. Problem Management is more concerned with identifying root causes for incidents and trying to prevent then from recurring.

This section is closely related to the "Supporting Quadrant Tasks" section. Many of the troubleshooting procedures listed here reference tasks defined in that section.

The most common support incidents that you may face are identified in this section, along with strategies and procedures for dealing with them. The emphasis is on restoring service as soon as possible. In some cases, the troubleshooting procedure is a simple reference to a support procedure. However, in other cases there is a more complex diagnostic procedure involved.

The following table lists some major support incidents and how to deal with them. The **Support Process** column lists the procedures to follow. These procedures are described in detail in the "Supporting Quadrant Tasks" section. If no process is listed, refer to the diagnostic procedure appropriate to the problem that follows in the next section.

Table 11.15: Major Support Incidents

Incident	Description	Support process
Server Not Responsive	Software process not responsive to client requests or administrative tools.	Restarting Certificate Services Service or Restarting the CA Server
CRL Publishing Failed	CRL is issued by CA, but latest CRL has not been published to Active Directory and/or Web.	See the following troubleshooting procedure.
CRL Not Issued	Updated CRL has not been issued by CA.	See the following extended troubleshooting procedure.
Client Cannot Enroll Certificate	Client enrollment request fails.	See the following extended troubleshooting procedure.
Client Cannot autoenroll Certificate	Client autoenrollment request fails.	See the following extended troubleshooting procedure.
Security Update Requiring Restart Installed	Security update is installed that requires Windows to be restarted.	Restarting the CA Server
Permanent Server Failure	Corruption or hardware failure requiring restore.	Restoring CA from Backup
Orphaned Certificate Needs to Be Revoked	Following restore of CA, any certificates issued after last backup will not be in database. These cannot be revoked in the normal way.	Revoking an Orphaned Certificate
Server Cannot Be Restored in time for CRL or Certificate Issue	The CRL or certificate needs to be re-signed using the CA's key in order to extend its validity period.	Sequence of tasks: 1. Restoring the CA Certificate to Temporary Computer 2. Resigning a CRL or Certificate to Extend Its Validity
End Entity Certificate Is Compromised	Certificate private key is lost, disclosed, or otherwise compromised.	Revoking an End-Entity Certificate
Issuing CA Certificate Is Compromised	CA certificate private key is lost, disclosed, or otherwise compromised.	Revoking and Replacing an Issuing CA
Root CA Certificate Is Compromised	CA certificate private key is lost, disclosed, or otherwise compromised.	Revoking and Replacing a Root CA

Extended Troubleshooting Procedures

This section describes some troubleshooting procedures that you may find useful for diagnosing and resolving some of the problems listed in the previous table. The procedures cover troubleshooting for the following common problems:

- CRL publishing problems
- CRL not issued
- Client cannot enroll
- Client cannot autoenroll a certificate

CRL Publishing Problems

CRL publishing problems will be indicated by an alert produced by the CheckCRLs script described in the "Service Monitoring and Control" section. This alert will be triggered when a CRL fails to be published to Active Directory and/or Web server in a timely manner. Applications that require revocation checks will begin to fail if the error is not corrected.

Examine the Application event log entry produced by CheckCRLs. This entry should indicate more precisely what the problem is, and will also indicate to which CA the problem CDP or CRL belongs. The problem will be one of the following:

- An up-to-date CRL has not been issued by the CA. This error indicates some problem with the CA.
- The CRL has been issued but has not been published correctly to one or more of the CDPs. This error may indicate a problem with the CA, with communications between the CA and CDP, or with the CDP service (Active Directory or IIS).
- The CRL has been produced and published but is not retrievable from one or more CDP locations. This error indicates a problem with CDP service.

▶ **To troubleshoot CRL publishing problems**

1. Log on to the CA where problems are indicated and check that the CRL at the issuing CA is up to date. Type the following commands to view the CA's CRL (you need to a member of CA Admins to execute the first of these commands).

   Certutil -getCRL %temp%\CA.crl

   Certutil -dump %temp%\CA.crl

2. If the CRL is out of date, see the later procedure "CRL Not Issued."
3. Open the PKI Health tool and look at the CDP entries for the suspect CA. The tool will indicate any inaccessible CDPs and expired CRLs. (However, the tool will not warn about CRLs that have not yet expired but are overdue for renewal—that is, when the **Next CRL Publish** date has passed.)

   Note: You can obtain the PKI Health tool from the Windows Server 2003 Resource Kit, which is referenced at the end of this chapter.

4. If any CDPs are shown as inaccessible, investigate the publishing service for that CDP.
5. If an error (from the event log) is shown with LDAP CDP, check the link to the Active Directory domain controller from the CA using the DCDiag tool from Windows 2003 Support tools. This tool will indicate if there are problems with the domain controller or with CA connectivity to the domain controller. Investigate any errors.
6. Check permissions on the CDP container for the CA with the Active Directory Sites and Services MMC snap-in. (In "cn=CDP,cn=Public Key Services,cn=Services, cn=Configuration,*DC=woodgrovebank,DC=com"* Replace the items in Italics with the DN for your own forest root.)
7. Create a temporary account and add it to the Cert Publishers group. Log on with that account and try to manually publish the CRL that was retrieved in step 1 to the directory. Use the following command:

   certutil -dspublish CA.crl *CAHostname CASubjectName*.

   This command will indicate whether the CAs have sufficient permissions to publish to Active Directory.
8. If an error is shown (in the event log entry) with the HTTP CDP, check the IIS server that is involved. Check connectivity and permissions. Manually run the script to publish CRLs to the IIS server (see "Publishing the Issuing CA CRLs to the Web Server" in the "Operating Quadrant Tasks" section) and check for errors. Try to use the same account/group membership as the CA itself when performing this task.
9. If the CRLs are being published to the CDP services successfully but PKI Health shows an error, a problem with the CDP service (Active Directory or IIS itself) is indicated. Troubleshooting these services is beyond the scope of this document.

CRL Not Issued

This situation is an unlikely occurrence in normal operation. A CA can usually always publish a CRL locally unless you have reconfigured the CA to stop it publishing CRLs to its local system folder (%windir%\system32\certsrv\certenroll). If you have not reconfigured the local publishing path, there may be a serious problem with your CA. Perform the following troubleshooting procedure to determine the cause of the problem. Although this procedure is targeted at CRL problems, most of the steps are generic and can be used with any low level Certificate Services problem.

▶ **To troubleshoot CRL issuing**

1. Examine the event log for any errors logged by Certificate Services.
2. Try to manually force a CRL issue (log on as a member of CA Admins) with the following command:

   ```
   Certutil -CRL
   ```
3. If this step fails, examine the event log again for any new errors.
4. Examine the CA certificate and all of the certificates in the chain to the root CA to see if there are any problems with the certificates such as certificates being expired or revoked.
5. Check that you can re-sign a certificate or CRL with the CA key (see the "Re-signing a Certificate or CRL to Extend its Validity Period" procedure in the "Supporting Quadrant Tasks" section).
6. Restart the CA and rerun these checks.
7. If the CRL still is not being issued, enable debug logging (see "Certificate Services Logging" later in this chapter). Then try to issue the CRL and examine the log for errors.

Client Cannot Enroll a Certificate

Follow this procedure to diagnose problems with certificate enrollment.

▶ **To diagnose a certificate enrollment problem**

1. Verify that the certificate template has been assigned to a CA.
2. Verify that the user or computer has permissions to enroll on the CA where the template has been assigned.
3. Verify that the template corresponds to the subject type. User templates can only be enrolled by users and computer templates can only be enrolled by computers.
4. Verify that the CA has access to its own published CRLs and those of its parent CAs. The CA always performs a revocation check prior to issuing a certificate.
5. Verify that the certificate template does not enforce the use of CSPs that are not available to the enrolling subject. For example, smart card CSPs for a computer or (when the user does not have a smart card) RSA SChannel CSP for users.
6. Verify that the certificate template does not require information to be put into the **Subject** or **Alternate Subject** fields that does not exist in Active Directory. One common problem is specifying that the e-mail address be included in the subject name but not having the e-mail field completely filled out in the user's Active Directory object.

Client Cannot Autoenroll a Certificate

The definitive guide for understanding and troubleshooting autoenrollment can be found in the article "Certificate Autoenrollment in Windows XP" (see the reference at the end of this chapter).

Check that a client can manually enroll the certificate that you are trying to autœnroll. Load the Certificates MMC snap-in and request a new certificate. If the certificate type does not appear, or if it appears but produces an error when trying to enroll, follow the procedure in the preceding section, "Client Cannot Enroll a Certificate."

If manual enrollment is possible, continue with the following steps.

1. Verify that the correct platform is being used. Only Windows 2000 and later support computer certificate autoenrollment. Only Windows XP and Windows Server 2003 support user certificate autoenrollment.
2. Verify that the user or computer has Autoenroll permissions on the certificate template for the required certificate type.
3. Verify that the autoenrollment Group Policy setting has been properly specified. For autoenrollment to function correctly, the GPO in which autoenrollment is configured needs to have a higher precedence than all other GPOs. For example, if the Autoenrollment GPO is created at the domain level, it needs to have a higher priority than the default domain policy. You can check this precedence of GPOs with the Resultant Set of Policy MMC snap-in.
4. Verify that the certificate template does not require manual approval or Registration Authority (RA) signatures. Certificate requests that require certificate manager approval will be submitted for approval but the certificate will not be issued to the user until manually approved. Requests that require RA signatures will be rejected because there is no mechanism to add additional signatures to an autoenrollment request.
5. Verify that the certificate template is not set to expect that the subject information be supplied in the request. Autoenrolled certificates must have their subject (and alternate subject) set by the CA.

Troubleshooting Tools and Techniques

This section discusses some tools that are useful in diagnosing and solving problems with the PKI. It also describes Certificate Services logging and how to enable more detailed logging for Certificate Services and client autoenrollment.

PKI Health

PKI Health is primarily a CDP and AIA diagnostic tool that attempts to build a view of all CAs across the enterprise. It is very useful for diagnosing connectivity and CDP and AIA publishing problems, and it allows you to download and view the CRLs or certificates referenced by the CDP or AIA. It is available as part of the Windows Server 2003 Resource Kit.

Certutil

Certutil is the single most important tool for managing and troubleshooting Windows CAs. For discussion of some of the key uses of the tool, see the white paper "Using Certutil.exe to Manage and Troubleshoot Certificate Services," which is referenced at the end of this chapter.

However, there are also a number of other options (not discussed in the white paper) available for a wide variety of management and diagnostic purposes. You can display the full list of available Certutil actions (or verbs) by typing the command with a parameter of "-?" Inserting the verb on which you need more help will display detailed syntax for that action. For example:

```
Certutil -dsPublish -?
```

Other diagnostic tools

Some other useful diagnostic and management tools are:

- **Certreq.exe**. Allows you to create, submit and retrieve certificate requests from the command line.
- **DCDiag.exe**. Helpful for diagnosing Active Directory problems that may be affecting the CAs.

Certificate Services Logging

Certificate Services and its associated tools produce several types of logs that can be invaluable in troubleshooting.

- Certificate Services (the CA process itself) logs to %systemroot%\certsrv.log (when debug logging is enabled)
- Certutil.exe logs to %systemroot%\certutil.log
- The Certification Authority MMC logs to %windir%\certmmc.log

▶ **To enable debug logging on Certificate Services**

- Run the following command:

```
certutil -setreg CA\Debug 0xffffffe3
```

The log entries will be saved to %windir%\certsrv.log

▶ **To disable debug logging**

- Run the following command:

```
certutil -delreg CA\Debug
```

Autoenrollment Logging

You need to add a registry value to enable additional logging of autoenrollment events. Enhanced logging is enabled separately for user and computer certificate autoenrollment.

▶ **To enable user autoenrollment logging**

1. Create a new registry DWORD value named **AEEventLogLevel** in the key HKEY_CURRENT_USER\Software\Microsoft\Cryptography\Autoenrollment.
2. Set the value to **0**.

▶ **To enable computer autoenrollment logging**

1. Create a new registry DWORD value named **AEEventLogLevel** in the key HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Autoenrollment.
2. Set the value to **0**.

Note: All failures and errors are automatically logged. It is not necessary to enable the registry key to turn on failure logging.

Configuration Tables

The following tables contain the site-specific and solution-specific configuration values that are used by the procedures in this chapter. These tables are a subset of the planning configuration tables in Chapter 7, "Implementing the Public Key Infrastructure," and are shown here only for reference.

Table 11.16: User-Defined Configuration Items

Configuration item	Setting
DNS name of Active Directory forest root domain	woodgrovebank.com
DN of forest root	DC=woodgrovebank,DC=com
Server name of Root CA	HQ-CA-01
Server name of Issuing CA	HQ-CA-02
X.500 CN of Root CA	Woodgrove Bank Root CA
X.500 CN of Issuing CA	Woodgrove Bank Issuing CA 1
Full qualified host name of Web server used to publish CA certificate and revocation information	www.woodgrovebank.com

Table 11.17: Solution-Defined Configuration Items

Configuration item	Setting
Administrators of Public Key Services configuration container	Enterprise PKI Admins
Allowed to publish CRLs and CA certificates to Enterprise configuration container	Enterprise PKI Publishers
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
Administrative group that approves certificate enrollment and revocation requests; a CA Officer role	Certificate Managers
Administrative group that manages CA audit and security logs	CA Auditors
Administrative group that manages CA backups	CA Backup Operators
Name of IIS virtual directory used to publish CA certificate and CRL information	pki
Physical path on Issuing CA that maps to IIS virtual directory	C:\CAWWWPub
Drive and path to store Certificate Services request files	C:\CAConfig
Drive and path to store Certificate Services database	%systemroot%\System32\CertLog
Drive and path to store Certificate Services database logs	D:\CertLog
Path for installation scripts	C:\MSSScripts

More Information

- An updated paper, "Managing a Windows Server 2003 PKI," based on this chapter is also available at www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/mngpki.mspx.
- For more information about the MOF process model and team model, see the Microsoft Operations Framework page at www.microsoft.com/technet/itsolutions/techguide/mof/default.mspx.
- For more information about capacity constraints and related performance counters, see Microsoft Knowledge Base Q146005, "Optimizing Windows NT for Performance" at http://support.microsoft.com/default.aspx?kbid=146005.
- For information on MOM deployment, download the *Microsoft Operations Manager 2000 (MOM) Service Pack 1 (SP1) Operations Guide* at www.microsoft.com/downloads/details.aspx?FamilyID=556A7746-75DF-4ACD-8CDE-26CB12148161&displaylang=en.
- For more information about additional operational tasks, see the Administer a certification authority page at www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_CS_procs_admin.asp.
- For more information about security patch management on the Microsoft platform, see "Improve Platform Manageability – Best Practice: Security Patch Management" at http://go.microsoft.com/fwlink/?LinkId=16284.
- For information about patch management with Microsoft SMS 2003, see "Patch Management Using Microsoft Systems Management Server 2003" at www.microsoft.com/technet/itsolutions/techguide/msm/swdist/pmsms/2003/pmsms031.mspx.
- For information about patch management using Microsoft SMS 2.0, see "Patch Management Using Microsoft Systems Management Server 2.0" at www.microsoft.com/technet/itsolutions/techguide/msm/swdist/pmsms/20/pmsmsin.mspx.
- For information about patch management using Microsoft Software Update services, see "Patch Management Using Microsoft Software Update" at www.microsoft.com/technet/itsolutions/techguide/msm/swdist/pmsus/pmsus251.mspx.
- For detailed information about Certificate Template properties, see "Understanding Certificate Templates" in the online product Help at www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/ctcon_concepts_under.asp.
- For more information about obtaining and using the Group Policy Management Console, see "Enterprise Management with the Group Policy Management Console" at www.microsoft.com/windowsserver2003/gpmc/default.mspx.
- For more information on CRL publishing problems, see Troubleshooting Certificate Status and Revocation at www.microsoft.com/technet/prodtechnol/WinXPPro/support/tshtcrl.asp.
- To obtain the PKI Heath tool (PKIView.msc), download the Windows Server 2003 Resource Kit Tools at www.microsoft.com/downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd&DisplayLang=en.

- For Certutil troubleshooting instructions, see the white paper "Using Certutil.exe to Manage and Troubleshoot Certificate Services" at www.microsoft.com/windows2000/techinfo/administration/security/certutil.asp.
- For the definitive guide for understanding and troubleshooting autoenrollment, see the article "Certificate Autoenrollment in Windows XP" at www.microsoft.com/technet/prodtechnol/winxppro/maintain/certenrl.mspx.

12

Managing the RADIUS and Wireless LAN Security Infrastructure

Introduction

This chapter describes the operational procedures required to manage the Remote Authentication Dial-in User Service (RADIUS) infrastructure and wireless LAN (WLAN) security implemented as part of this *Securing Wireless LANs* guidance. The structure is based on the Microsoft Operations Framework (MOF) categories and concepts discussed in Chapter 10, "Introduction to the Operations Guide."

This chapter will help you implement a full management system for your RADIUS infrastructure and WLAN security, including all of the setup tasks to begin monitoring and maintaining the system. This chapter also includes regular operational tasks to keep the infrastructure working properly and procedures to help you manage support incidents, manage changes to the environment, and optimize the performance of the system.

There are two main parts to the chapter. The first part consists of two sections, "Essential Maintenance Tasks" and "RADIUS and WLAN Security Administrative Roles." These sections are brief and meant to be read in their entirety; they provide essential information about setting up a properly managed environment for the system. The remainder of the chapter is intended to be used primarily as a reference. You will need to implement some tasks from the reference sections when the system is deployed, but they are clearly indicated in the "Essential Maintenance Tasks" section.

Although you do not need to absorb all the details of the reference sections, you should look through them to familiarize yourself with the contents so that you can quickly locate items that you need in the future.

Chapter Prerequisites

You should be familiar with the MOF concepts described in Chapter 10, "Introduction to the Operations Guide." Detailed knowledge of MOF is not required.

You should be familiar with concepts of RADIUS and the Microsoft® Internet Authentication Service (IAS) in particular, as well as 802.11, 802.1X and EAP-TLS concepts. For more information on these technical topics, see the references in the Planning Guide chapters.

Familiarity with Microsoft Windows® 2000 Server (or later) is also required in the following areas:

- Basic operations and maintenance of Microsoft Windows Server™ 2003 (including the use of tools such as Event Viewer, Computer Management and NTBackup).
- Active Directory® directory service concepts and tasks. This includes Active Directory structure, tools, manipulating users, groups, other Active Directory objects, and the use of Group Policy.
- Windows system security concepts such as users, groups, auditing, access control lists; the use of security templates; and the application of security templates using Group Policy or command line tools.
- Internet Authentication Service administration.
- Windows Scripting Host (WSH) and Microsoft Visual Basic® Scripting Edition (VBScript) language. Knowledge of batch programming syntax will help you get the most out of the supplied scripts, but is not essential.

In addition, before reading this chapter you should read the Planning Guide and Build Guide chapters and have a thorough understanding of the architecture and design of the solution.

Chapter Overview

The following list describes each of the major sections of this chapter.

- **Essential Maintenance Tasks**. Contains two tables listing the tasks you need to perform to set up the management system and the regular list of tasks that need to be performed to maintain the system.
- **Administrative Roles**. Describes the administrative roles used in the solution, what the capabilities of each role are, and how these map to the MOF role clusters and the administrative security groups defined for the solution.
- **Operating Quadrant Tasks**. Includes all of the tasks related to the normal maintenance of the RADIUS infrastructure and WLAN security. This section includes monitoring, backups, and directory and security operations.
- **Supporting Quadrant Tasks**. Includes all of the procedures related to recovering from system problems. This section includes restoring from backup and operations to deal with a failed IAS server.
- **Optimizing Quadrant Tasks**. Includes some capacity management planning procedures.
- **Changing Quadrant Tasks**. Includes common tasks that relate to making changes to the IAS server configuration and releasing them into production in a controlled manner. Procedures to help you gather and maintain essential configuration information about the IAS server are also included.

- **Troubleshooting**. Contains procedures to help you troubleshoot common problems that you may encounter with your RADIUS infrastructure and WLAN security. It also includes descriptions of useful troubleshooting tools and procedures to enable logging of different components.
- **Configuration Tables**. Contains a subset of the configuration parameters used in the Build Guide chapters. These values are used as examples in the body of the procedures.
- **More Information**. Lists extra information sources referred to in the text.

Essential Maintenance Tasks

This section lists the key tasks that you must perform to successfully operate the RADIUS infrastructure and WLAN security. The tasks are listed in two tables: initial setup tasks and ongoing operational tasks. The task names listed in the tables are described in detail in later in the document. The tasks are grouped by MOF quadrant, and the MOF service management function (SMF) that the task belongs to is listed next to the task to help you find the required task easily.

This section also includes a list of tools and technologies used in the procedures in this chapter.

Initial Setup Tasks

The following table shows the tasks that must be performed to put the operation of the RADIUS infrastructure and WLAN security into production. Depending on your operational standards and practices, you may not need to perform all of these tasks. However, you should review each task detail and decide if you need to do it. Some of these tasks may also need to be performed again at some point. For example, if a new IAS server is installed you will need to configure its backup and monitoring jobs.

Table 12.1: Initial Setup Tasks

Task name	Service Management Function
Operating Quadrant	
Adding RADIUS clients to IAS Servers	Network Administration
Enabling Wireless Settings on Computers	Directory Services Administration
Adding Computers and Users to Remote Access Policy Groups	Directory Services Administration
Categorizing Monitoring Alerts	Service Monitoring and Control
Monitoring IAS Capacity Constraints	Service Monitoring and Control
Configuring the IAS configuration export	Storage Management
Exporting RADIUS client configuration	Storage Management
Configuring Backup of IAS Data Directories	Storage Management
Testing the IAS Backup	Storage Management
Optimizing Quadrant	
Determining Maximum Load on the IAS Server	Capacity Management
Determining Storage and Backup Requirements for an IAS Server	Capacity Management
Changing Quadrant	
Managing Operating System Updates	Change Management Release Management

Maintenance Tasks

The following table shows the tasks that must be performed on a regular basis to keep your RADIUS infrastructure and WLAN security operating correctly. You can use this table to help plan the resources needed and to plan the operational schedule for administering the system.

There may be some tasks that you do not need to perform, but you should review each task detail and decide if you need to do it. Also, some of these tasks might be performed on an as-needed basis and some according to a schedule. For example, if a RADIUS client is added to an IAS server, you will need to perform an export/backup of the server configuration even if it is not scheduled. Such tasks are noted in the Frequency column. Dependencies such as these are also noted in the task details themselves.

Table 12.2: Ongoing Maintenance Tasks

Task name	Frequency
Adding RADIUS Clients to IAS Servers	As wireless APs are added to the network
Removing RADIUS Clients from IAS Servers	As wireless APs are removed from the network
Enabling Wireless Settings on Computers	As computers are added to the network
Adding Computers and Users to Remote Access Policy Groups	As employees are granted WLAN access
Exporting RADIUS Client Configuration	As wireless APs are added to the network
Testing the IAS Backup	Monthly
Accessing the IAS RADIUS Request Logs	Daily or weekly (dependent upon security requirements)
Reviewing IAS RADIUS Authentication Event Log Entries	Daily or weekly (dependent upon security requirements)
Archiving and Deleting IAS RADIUS Log Entries	Monthly
Managing Operating System Updates	Daily

Technology Required in Operations Guide

The following tables list the tools or technologies used in the procedures described in this chapter.

Table 12.3: Required Technology

Item name	Source
Active Directory Users and Computers MMC snap-in	Windows Server 2003
MSS scripts	This solution
Text editor	Notepad–Windows Server 2003
Windows Task Scheduler Service	Windows Server 2003
SchTasks.exe	Windows Server 2003
Windows Backup	Windows Server 2003
Event Viewer	Windows Server 2003
Performance Monitor	Windows Server 2003
Net.exe	Windows Server 2003
Operational Alert Console	Microsoft Operations Manager (MOM)
Removable media for off machine storage	Floppy disk, CD-RW or tape
IAS server backup	Network backup service or Local backup device
Group Policy Management Console	Web download from Microsoft.com
IASParse	Windows Server 2003 Support Tools
Microsoft Access 2002	Microsoft Office XP

Table 12.4: Recommended Technology

Item name	Source
Operational alert console	Microsoft Operations Manager or other service monitoring system
E-mail infrastructure–for operational alerts (alternative to MOM)	SMTP/POP3/IMAP server and client, such as Microsoft Exchange Server and Microsoft Outlook®
Eventquery.vbs	Windows Server 2003
Capacity planning tools	Microsoft Operations Manager or other capacity planning tools
Security update distribution system	Microsoft Systems Management Server or Microsoft Software Update Services

RADIUS and WLAN Security Administrative Roles

Many different roles are involved in the management of a RADIUS infrastructure and WLAN security. The following two sections divide them into core roles and supporting roles.

Core RADIUS and WLAN Roles

The roles in the following table are central to the management of a RADIUS infrastructure and WLAN security.

Table 12.5: Core RADIUS and WLAN Security Roles

Role name	Scope	Description
Internet Authentication Service Administrator	Enterprise	Responsible for overall administration and configuration of IAS for the enterprise
Internet Authentication Service Auditor	Enterprise	Responsible for reviewing, archiving, and deleting RADIUS logs located on IAS server computers
Internet Authentication Service Backup Operators	Enterprise	Responsible for backup and restoration of IAS configuration state and historical data
WLAN Helpdesk Staff	Enterprise	Senior Helpdesk staff responsible for troubleshooting WLAN issues

Supporting RADIUS and WLAN Security Roles

The operational roles in the following table are not central to the management of the RADIUS infrastructure and WLAN security but provide supporting functions to the core roles.

Table 12.6: Supporting RADIUS and WLAN Security Roles

Role name	Scope	Description
Monitor Operator	Enterprise	Responsible for monitoring events
Capacity Planner	Enterprise	Responsible for analyzing performance and loading to predict future capacity requirements
Active Directory Administrator	Enterprise	Responsible for configuration and support of Active Directory infrastructure
Active Directory Operations	Enterprise	Responsible for day-to-day maintenance of directory, such as security group maintenance, account creation, and so on
Desktop Administrator	Enterprise	Responsible for configuration and support of desktop computers
Change Approvals Board	Enterprise	Business and technical reps required to approve changes to infrastructure

Mapping of Roles to Security Groups

The following table lists the security groups that are defined for this solution and briefly describes the capabilities or permissions of each group.

For IAS servers, the domain and local security groups are used to apply permissions that are applicable to each role. Domain accounts are used to populate the role groups. It is acceptable for single accounts to be members of multiple role groups if this supports your organization's security and IT policies.

Table 12.7: Mapping of RADIUS and WLAN Security Roles to Security Groups

Role name	Domain security group	Local security group	Capabilities
Internet Authentication Service Administrator	IAS Admins	Administrators	Full administration capabilities on the IAS server, including starting/stopping the IAS service and changing its configuration
Internet Authentication Service Auditors	IAS Security Auditors	N/A	The ability to read and delete RADIUS request log files on the logging volume
IAS Backup Operators	N/A	Backup Operators	Full backup and restoration of operating system state and IAS configuration data
WLAN Helpdesk Staff	N/A	N/A	Works with IAS Administrators to resolve IAS authentication issues. (May be granted read permissions on the same resources as IAS Security auditors in some cases.)

Operating Quadrant Tasks

The Operating Quadrant includes the IT operating standards, processes, and procedures that are applied regularly to service solutions to achieve and maintain service levels within predetermined parameters. The goal of the operating quadrant is a highly predictable execution of both manual and automated day-to-day tasks.

This section contains information that is relevant to the following SMFs:

- Network Administration
- Directory Services Administration
- Security Administration
- Storage Management
- Service Monitoring and Control
- Job Schedule

There are no tasks that belong to the remaining SMFs:

- Systems Management
- Network Management
- Print and Output Management

Note: Each task description includes the following summary information: security requirements, frequency, and technology requirements.

Network Administration

The Network Administration role is responsible for the design and maintenance of the physical components that make up the organization's network, such as servers, routers, switches, and firewalls. For wireless networks, these components include wireless access points (APs) and the RADIUS servers to support them.

Adding RADIUS Clients to IAS Servers

Wireless APs need to be authorized to perform authentication and accounting with IAS servers. Enabling new wireless APs as RADIUS clients is one of the few incremental changes that need to occur on a deployed production IAS server. This task authorizes the wireless APs to participate in RADIUS authentication and accounting with the IAS server. Perform this task each time new wireless APs are deployed and configured to participate in network authentication.

Summary Information

- **Security Requirements**: Membership in the IAS Admins security group
- **Frequency**: As new wireless APs are added to the network
- **Technology Requirements**:
  - Internet Authentication Server MMC snap-in
  - MSS scripts (for the GenPwd script command)
  - Floppy disk drive or other removable writable media drive
  - Floppy disk or other removable writable media

Task Details

Use a random password (secret) that is unique to each wireless AP when adding the AP to each IAS server. Using the same RADIUS secrets for multiple wireless APs increases the risk that the shared secret will not remain secret for very long.

Windows Server 2003 Enterprise Edition allows administrators to add wireless APs in bulk to IAS by adding a dedicated RADIUS client subnet and using a shared secret for all the APs on that subnet. However, although it simplifies management of these secrets, it results in a weaker security solution than using unique secrets.

This solution implements cryptographically random secrets that are generated by the GenPwd script included with these guides.

▶ **To add RADIUS clients individually to IAS**

1. From the Internet Authentication Service MMC snap–in, right-click the **RADIUS Clients** folder and then click **New RADIUS Client**.
2. Enter the **Friendly name** and the **Client address (IP or DNS)** of the wireless AP. You should use IP address rather than DNS name because IAS will attempt to resolve each RADIUS client upon server startup. In large environments with many wireless APs, resolving clients through their DNS names can degrade startup time. Click **Next**.
3. Select **RADIUS Standard** as the client-vendor attribute and enter the shared secret for this particular wireless AP.

   Note: The following steps include the use of a floppy disk or other removable writable media. Locate a formatted media disk and label it "RADIUS Clients for <*Server Name*>."

   ---

4. You can use the GenPwd script included with these guides to generate a random strong secret for individual use by each AP that is configured as a RADIUS client. GenPwd will generate a 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. However, if you have a method for generating strong RADIUS secrets, you may use it instead of GenPwd in the next few steps.

   Note: GenPwd uses a CryptoAPI function to generate a base64 encoded, cryptographically random string. It does not use the VBScript random number function.

   ---

5. Open a command prompt and make the A:\ directory your current directory. Your file system directory location is important because the Clients.txt file in the current directory will automatically be appended with the new information. If no Clients.txt file exists, one will be created.

6. Execute the following command. Be sure to substitute <*client_name*> for the friendly name of the wireless access point. This can be a DNS name, IP address, or other string:

   cscript //job:GenPwd C:\MSSScripts\wl_tools.wsf /client:*client_name*

   After it is created, the comma-separated file can easily be imported into a spreadsheet or database application for reference and editing.

   Important: RADIUS secrets should be changed for each IAS server and wireless AP regularly. Ensure that you use the GenPwd or some other utility to generate strong secrets and store the new secret and wireless AP name in the Clients.txt file. The data in the clients.txt file is extremely sensitive. Do not copy this file to the server; store it in a secure place, such as a safe.

7. Within the Internet Authentication Service MMC snap-in, enter the RADIUS shared secret in the **Shared secret** and **Confirm shared secret** fields. Select the **Request must contain the Message Authenticator attribute** and click **Finish**.

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

Removing RADIUS Clients from IAS Servers

Removing unwanted wireless APs as RADIUS clients is one of the few incremental changes that you must make on a deployed production IAS server. This task prevents the wireless AP from participating in RADIUS authentication and accounting with the IAS server. Perform this task each time wireless APs are retired to prevent them from using RADIUS authentication and accounting services.

Summary Information

- **Security Requirements**: Member of the IAS Administrators group
- **Frequency**: As wireless APs are removed from the network
- **Technology Requirements**:
  - Internet Authentication Server MMC snap-in
  - Notepad.exe or other text file editor

Task Detail

Remove each wireless access point from IAS independently. You should also delete the corresponding entry in the Clients.txt file found on the RADIUS clients floppy disk stored in secure storage. The Clients.txt file is created by following the procedure in the "Adding RADIUS Clients to IAS Servers" task.

▶ **To remove RADIUS clients from the IAS Server**

1. From within the Internet Authentication Server MMC snap-in, select the RADIUS Clients folder.
2. From the right pane, select the entry that represents the RADIUS client to be removed and then press **Delete**.

3. When prompted for confirmation, click **Yes**.

Note: The following steps include the use of a floppy disk or other removable writable media labeled "RADIUS Clients for <*Server Name*>," which was created in a previous section. Be sure to use the correct disk with the appropriate server to avoid loss of data.

4. Locate the RADIUS client floppy disk for this server and open the A:\Clients.txt file with Notepad.
5. Find and delete the entry for the RADIUS client to be retired.

Directory Services Administration

Directory services allow users and applications to find network resources such as users, servers, applications, tools, services and other information over the network. Directory services administration involves the day-to-day operations, maintenance, and support of the enterprise directory. Directory services administration ensures that information is accessible through the network by any authorized requester through a simple and organized process.

Enabling WLAN Access for Users and Computers

Three separate tasks must be performed to enable access to the WLAN. These tasks are all controlled by security group membership, and so can be easily automated using a VBScript, Jscript, or command (batch) file script. These tasks are documented separately because many organizations will perform them in different phases of their WLAN rollout.

Important: This solution uses custom security groups to control which users and computers receive WLAN certificates and policy settings as well as to control which users and computers are allowed access to the WLAN by IAS. Separate groups are used for these three items to allow a phased deployment of certificates, policy settings, and WLAN access. If you do not want such precise control, you can enable all users and computers for any or all of these items. The easiest way to enable all users and computers is by adding Domain Users or Domain Computers to the relevant certificate enrollment group, WLAN Group Policy group (computers only), and WLAN Access group.

▶ **To enable WLAN access for a computer**

1. Follow the "Enabling Enrollment (or Autoenrollment) of a Certificate Type for a User or Computer" procedure in Chapter 11, adding the computer account to the certificate enrolment group **AutoEnroll Client Authentication–Computer Certificate**.
2. Follow the procedure (later in this section), "Enabling Wireless Settings on Computers," to deploy the correct network settings to the computer. Add the computer account to the policy group **Wireless Network Policy–Computer**.
3. Follow the procedure (later in this section) "Adding Computers and Users to Remote Access Policy Groups" to authorize the computer to connect to the WLAN. Add the computer account to the Remote Access security group **Remote Access Policy–Wireless Computers**.

Important: These steps can be carried out in any order. During a large deployment, all of these steps can be carried out well in advance of enabling the WLAN hardware. The computer *must* be rebooted at least once for it to receive the group memberships assigned in each of these procedures. The computer logon token will time out after a while and cause the group memberships to be refreshed, but this process can take up to a week.

The computer *must* be connected to a wired network to receive the initial certificate and initial wireless settings. Certificate renewals and future changes to wireless settings will be received over the WLAN.

▶ **To enable WLAN access for a user**

1. Follow the procedure in Chapter 11, "Enabling Enrollment (or Autoenrollment) of a Certificate Type for a User or Computer," adding the user account to the certificate enrollment group **AutoEnroll Client Authentication–User Certificate**.
2. Ensure that the user is logging on using an authorized and configured WLAN computer (as described in the previous procedure). In particular, the computer must have been configured with the correct WLAN policy settings.
3. Follow the procedure (later in this section) "Adding Computers and Users to Remote Access Policy Groups" to authorize the computer to connect to the WLAN. Add the computer account to the Remote Access security group **Remote Access Policy–Wireless Users**.

Important: These steps can be carried out in any order; they can also be carried out any time in advance of actually deploying and enabling the WLAN hardware. The users *must* log off and then log back on again at least once to receive the group memberships assigned in each of these procedures. The user logon token will time out after a while and cause the group memberships to be refreshed, but this process can take up to a week.

The computer *must* be connected to a wired network in order for users to receive the initial certificates. Certificate renewals will be received over the WLAN.

Enabling Wireless Settings on Computers

The configuration of wireless networking settings (such as 802.11 and 802.1X settings) on client computers is automated with Active Directory Group Policy. You control which computers receive these wireless network settings by adding them to security groups. The security groups are used to filter the Group Policy Object (GPO) so that only members of the group receive the policy settings. Perform this task each time a new computer is introduced to the environment that needs to use the wireless network.

Summary Information

- **Security Requirements**: Membership in Domain Admins or permission to add users to the Wireless Network Policy–Computer security group in Active Directory
- **Frequency**: As mobile computers are added to the network
- **Technology Requirements**: Active Directory Users and Computers MMC snap-in

Task Details

After Wireless Network Policies are configured and functional, adding computers to the security groups controlling application of the policy is straightforward.

▶ **To add computers to the Wireless Networking Group Policy security group**

1. In the Active Directory Users and Computers MMC snap-in, locate the Wireless Network Policy–Computer security group corresponding to the Wireless Network policy to be applied. You must be logged on as a user that has Modify Membership permissions for the group.
2. Add the computer to the selected security group.

Note: The computer must be restarted to reflect this new group membership and apply the wireless policies. The first time a wireless policy is applied, the computer *must* be connected to a wired network to receive the wireless settings. Subsequent changes can then be applied across a WLAN.

Adding Computers and Users to Remote Access Policy Groups

Adding computers and users to the remote access policy security group authorizes access to the WLAN. IAS uses membership of this group within remote access policy as a condition that must match before access is allowed. You must add computers and users to the remote access policy groups to enable successful authorization to the WLAN.

Summary Information

- **Security Requirements**: Membership in Domain Admins or permission to modify membership of the Remote Access Policy–Wireless Users and the Remote Access Policy–Wireless Computers security groups in Active Directory
- **Frequency**: As users are granted access to the WLAN
- **Technology Requirements**: Active Directory Users and Computers MMC snap-in

Task Details

After the remote access policy security groups are created, adding additional computers and users to the security groups controlling WLAN access is fairly straightforward.

▶ **To add users to the Remote Access Policy security group**

1. Log on to an administration computer as a member of Domain Admins or someone with the permission to modify membership of the Remote Access Policy–Wireless Users security group.
2. In the Active Directory Users and Computers MMC snap-in, locate the Remote Access Policy–Wireless Users security group that corresponds to the remote access policy controlling wireless LAN access.
3. Add the user to the selected security group.

Note: The user must log off and on again to receive the new group membership and access the WLAN.

▶ **To add computers to the Remote Access Policy security group**

1. Log on to an administration computer as a member of Domain Admins or someone with the security permission to modify membership of the Remote Access Policy–Wireless Computers security group.
2. In the Active Directory Users and Computers MMC snap-in, locate the Remote Access Policy–Wireless Computers security group that corresponds to the remote access policy controlling wireless LAN access.

3. Add the computer to the selected security group.

Note: The computer must be restarted for it to receive this new group membership and access the WLAN.

Service Monitoring and Control

Service monitoring allows the operations staff to observe the health of an IT service in real time.

Where Microsoft Operations Manager (MOM) is referenced in this section, it is assumed that you have a MOM deployment that follows the guidelines in the MOM Operations Guide. However, MOM is not required; it is simply being used as an example. See the "More Information" section at the end of this chapter for information on the MOM Operations Guide.

Categorizing Monitoring Alerts

Your monitoring system should raise only the most significant alerts to operations staff. If all minor errors are escalated to produce incident alerts, operations staff will quickly become confused about what is urgent and what is not urgent but requires longer term investigation.

Summary Information

- **Security Requirements**: None
- **Frequency**: Setup task
- **Technology Requirements**: Operational alert console (such as MOM)

Task Details

The following alert categories are used in this document. Of these, only the top three–Service Unavailable, Security Breach, and Critical Error–should produce alerts on the operator console for immediate attention. Errors and warnings are not considered urgent and should be referred to the RADIUS and WLAN operational support staff for resolution. These event categories are the defaults used by MOM, and subsequent task descriptions in this section will refer to them.

Table 12.8: Alert Categories

Alert category	Description
Service Unavailable	When the application or component is 100 percent unavailable.
Security Breach	When the application is being hacked or has been compromised.
Critical Error	When the application has experienced a critical error that requires administrative action soon (but not necessarily immediately). The application or component is operating at a sub-par level of performance but is still able to perform most critical operations.
Error	When the application experiences a transient problem that does not need any immediate or possibly any administrative action or resolution. The application or component is operating at an acceptable level of performance and is still able to perform all critical operations.

(continued)

Warning	When the application generates a Warning message that does not need immediate or possibly any administrative action or resolution. The application or component is operating at an acceptable level of performance but is still able to perform all critical operations. This situation may, however, change to Error, Critical Error, or Service Unavailable if the problem persists.
Information	When the application generates an Informational Event. The application or component is operating at an acceptable level of performance and is performing all critical and non-critical operations.
Success	When the application generates a Success Event. The application or component is operating at an acceptable level of performance and is performing all critical and non-critical operations.

Monitoring IAS Capacity Constraints

Detecting potential capacity constraints is essential to maintaining service at an optimal level. As subsystems approach the limits of their operating capacities, performance degrades sharply (usually in a non–linear manner). Accordingly, it is important to monitor capacity trends and to identify and deal with trends toward future constraints early.

Summary Information

- **Security Requirements**: Permissions required are dictated by monitoring solution
- **Frequency**: Setup task
- **Technology Requirements**:
  - Performance monitor
  - Performance counter consolidator (such as MOM)
  - Operational alert console (such as MOM)
  - Capacity planning tools

Task Details

The following performance counters are the most useful for identifying capacity constraints in IAS. Processor and Disk are the two resources that IAS uses most heavily, and will likely indicate constraints at an earlier stage than network or memory.

Table 12.9: Items to Monitor for IAS Capacity Constraint

Performance object	Performance counter	Instance
Processor	% Processor Time	_Total
Physical Disk	% Disk Time	_Total
Physical Disk	Avg. Disk Read Queue Length	_Total
Physical Disk	Avg. Disk Write Queue Length	D: (IAS–DATA)
Network Interface	Bytes Total/sec	NW adapter
Memory	% Committed Bytes in use	---

For more general information about capacity constraints and related performance counters, see the reference in the "More Information" section at the end of this chapter.

It is also essential to monitor capacity indicators on supporting infrastructures. The key items are:

- **IAS communications to Active Directory**. IAS uses Active Directory extensively for authentication and some authorization services.
- **RADIUS clients such as wireless APs**. These clients communicate to both clients and IAS using Extensible Authentication Protocol (EAP) and RADIUS protocols.
- **Client-related communications to Active Directory**. Wireless LAN clients use Active Directory domain controllers for Group Policy and native domain authentication.

Storage Management

Storage management deals with on-site and off-site data storage for the purposes of data restoration and historical archiving. The storage management team must ensure the physical security of backups and archives. Storage management defines, tracks, and maintains data and data resources in the production IT environment.

Configuring the IAS Configuration Export

This task schedules a nightly task that exports partial IAS configuration state to facilitate a system restoration after a catastrophic event. Full IAS configuration state includes RADIUS client configuration, which is security-sensitive information. Therefore, instruction for exporting the RADIUS client portion of the configuration state is detailed separately. You will require both types of backups to perform a full restoration of each IAS server to full production service.

A complete backup of the IAS server includes any operating system configuration and other state information on which the IAS server depends. This task has been developed so that a server may be reinstalled, the optional IAS component reinstalled, and configuration state restored. This configuration facilitates restoration of service for a server that is no longer in a known configuration state (unreliable) or had its security compromised.

Summary Information

- **Security Requirements**: Member of the local Administrators security group
- **Frequency**: Setup task
- **Technology Requirements**:
  - MSS scripts
  - Windows Task Scheduler Service
  - SchTasks.exe

Task Details

This task configures a scheduled task to perform a nightly configuration state backup of the IAS server. The IAS backup assumes that your organization has an enterprise server backup system currently in place; the backup in this procedure will output to a file that, in turn, the backup system can back up. Your main backup system may be a network backup, a storage area network (SAN) backup or a local device backup. The solution also assumes that the server backup system runs nightly to back up the disks of the IAS server.

▶ **To configure an IAS configuration backup**

1. Schedule the backup job to run nightly by running the following command. This command sets the job to run at 2:00am each night.

   ```
   SCHTASKS /Create /RU system /SC Daily /TN "IAS Backup" /TR
   \"C:\MSSScripts\IASExport.bat\" /ST 02:00
   ```

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

   Note: The slash mark and quotation mark shown on either side of the script name C:\MSSScripts\IASExport.bat are only required if there are spaces in the path name or file name. The backslash character is used to "escape" the quotation marks around the script name so that they are stored as part of the schtasks job command line. These characters can be omitted if there are no spaces in the path name.

2. Configure your server backup system to back up the contents of the D:\IASConfig directory each night to removable media. If possible, set a precondition script to check that the date and time of the IAS configuration text files created from the IASExport.bat file are less than 24 hours old. If the files have a date and time stamp more than 24 hours old, it means that the previous backup failed or is still running.

Note: The IASExport.bat script can be used as a starting point for this task. You can modify the logic of the IASExport.bat script so that error conditions from the **netsh** tool used within the script generate events or notifications that can be detected by operations staff.

You should consider enabling Windows file auditing on the D:\IASConfig directory and instructing server security auditors to review auditing data periodically for unusual activity (failed access, for example). Information in the D:\IASConfig directory could help an attacker understand how to compromise network access control.

Exporting RADIUS Client Configuration

You must export RADIUS client configuration from the IAS server to ensure that it is possible to recover this information in the event of a catastrophic server failure. RADIUS client information is security-sensitive because it contains RADIUS secrets used between each server and wireless AP. Therefore, exported RADIUS client data is exported to removable media that you should store in a secure location. The exported RADIUS client configuration data is (usually) unique to each IAS server.

To achieve a full restoration of an IAS server configuration, you need restore the RADIUS client configuration data, which is created in this task, and the IAS system configuration data, which was created with the IASExport.bat script in the previous procedure.

Summary Information

- **Security Requirements**: Member of the IAS Admins security group
- **Frequency**: Setup task
- **Technology Requirements**:
  - MSS scripts
  - Floppy disk or other removable writable media

Task Details

RADIUS client information is exported using the **netsh** command. This guide includes a batch file that will export the RADIUS client information to a floppy disk or other removable media.

▶ **To Export RADIUS Client Configuration**

1. Log on to the IAS server from which you want to save the RADIUS client data and execute the following command from a command prompt:

   C:\MSSScripts\IASClientExport.bat

2. Investigate any errors or warnings that display and rectify them. After the situation is rectified, execute the script again.
3. Store the backup media appropriately. This backup data is very sensitive because it contains secrets that could be used to gain access to your corporate WLAN. You must treat this data with the same level of security as you treat the IAS server itself. You should store the backup data at a different physical site than the IAS server itself, which will allow you to recover the IAS server if all computer equipment at the site is destroyed or becomes inaccessible.

Configuring Backup of IAS Data Directories

The purpose of this task is to provide guidance on which directories on your IAS server require backup to allow a full system recovery of IAS configuration state and RADIUS log data after a catastrophic server event. A complete backup of the IAS server includes any operating system configuration and other system state information on which the IAS server depends.

Summary Information

- **Security Requirements**: Member of the local Backup Operators security group
- **Frequency**: Setup task
- **Technology Requirements**:
  - Windows Backup or enterprise backup system
  - Windows Task Scheduler Service
  - SchTasks.exe

Task Details

This task lists the directories that must be backed up to ensure that a full restoration of IAS configuration state and log file data is possible. This task assumes you have an enterprise server backup system currently in place. This system may be a network backup, SAN backup or a local device backup. The solution also assumes that the enterprise server backup system runs nightly after the IAS configuration state backup (02:00) to back up the disks of the IAS server.

▶ **To configure an IAS data directory backup**

1. Verify the IAS configuration state backup is properly scheduled and running successfully. The IAS configuration state scheduled task outputs the IAS configuration state to files on the hard disk.

2. Use Notepad to create a file called backuptest.txt in the D:\IASLogs directory. Within the file, type **Used for backup and restoration verification purposes**. Save the file and close Notepad. This file will be used in restoration verification procedures later.

   Configure your enterprise server backup system to perform a full, incremental or differential backup the following directories:

   - D:\IASConfig
   - D:\IASLogs

3. View the log files of your server backup system to ensure that no errors or warnings have occurred. Should you find errors or warnings, consider running the IAS configuration export scripts manually and performing another full backup of both directories.
4. Store the backup media appropriately. This backup data is sensitive because it contains the configuration of server software that allows access to your organization's WLAN. You must treat it with the same level of security that you provide to the IAS server. You should store the backup data at a different physical site than the IAS server itself, which will allow you to recover the IAS server if all computer equipment at the site is destroyed or becomes inaccessible.

Testing the IAS Backup

The purpose of this task is to ensure that the backup process and technology are performing correctly by performing a test restoration. Full restoration of backups on spare server hardware ensures the highest level of confidence that backup procedures are working correctly. However, this procedure has been created so that customers who do not have access to spare server hardware may test their restoration procedures on production hardware with some degree of risk. Testing restoration procedures on production servers carries the risk that partial restoration may leave a server in an unusable state.

Testing backups ensures that should a catastrophic event occur, restoration steps are well known and free from procedural or technical error that may inhibit completion.

IAS server restoration data is comprised of the following:

- **IAS Configuration state export data**. Located in the D:\IASConfig directory. When restored from tape, this information is used to import configuration back to the IAS server and is created by following the steps in the "Configuring the IAS Configuration Export" task in this chapter.
- **RADIUS client export data**. Located on the floppy disk or other removable writable media labeled "RADIUS Clients for <*Server Name*>." This information is used to restore RADIUS client configuration to the IAS server and is created by following the steps in the "Exporting RADIUS Client Configuration" task in this chapter.
- **RADIUS request log data**. Located in the D:\IASLogs directory. When restored from tape, this information contains historical data used by IAS security auditors. This data is created over time as the IAS service logs RADIUS information to disk.

Before performing a test restoration, you should manually perform an export of IAS configuration export data and RADIUS client export data. Follow this with an unscheduled backup of server data to special tapes, and place these aside for use only in the case of a problem during the test restore. This approach mitigates some risk that bad tapes and errors that may pass unnoticed during normal backups do not result in a partial restoration of a production server.

Summary Information

- **Security Requirements**: Local Administrators or Backup Operators on test computer
- **Frequency**:
  - Before the IAS server becomes operational
  - Monthly
  - Retest when any change is made to backup technology or process
- **Technology Requirements**:
  - Windows Backup or enterprise backup system
  - MSS scripts

Task Details

This task details the restoration and verification of IAS data. All three types of data will be restored and special procedures will be used to validate restoration. Be sure that you use a recent (previous night's) full backup that has completed successfully. Also, be sure before starting the test that no administration work (for example, a configuration change of some kind) has been performed on the target server since the last backup.

If you are attempting to restore to a newly installed copy of Windows Server 2003 you must complete the prerequisite server build steps from Chapter 8, "Implementing the RADIUS Infrastructure for Wireless LAN Security," to ensure the server hardware and software is properly configured for IAS.

Note: You may need to re-select the newly installed RAS and IAS Server Authentication certificate within the restored WLAN remote access policy.

▶ **To test the IAS backup**

Note: The first step in this procedure is optional and is used in a test lab environment on non-production server hardware. It is helpful to ensure that a server can be recovered from an unstable or security-compromised state.

---

1. To restore a server that has suffered an unrecoverable hardware or software failure or a security compromise (such as a virus infection), reinstall Windows Server 2003 as directed in Chapter 8, "Implementing the RADIUS Infrastructure." Be sure to copy the MSS scripts from the distribution media to the C:\MSSScripts directory your server.
2. Navigate to the D:\IASLogs directory and look for the file backuptest.txt. If it does not exist, continue to the next step. If you find a backuptest.txt file, delete it. The backuptest.txt file was created during the "Configuring Backup of IAS Data Directories" procedure. It is backed up along with the IAS RADIUS request logs and allows you to check that you can restore data from the backup without having to restore the RADIUS logs. If you prefer, you can restore the actual RADIUS request log data from D:\IASLogs instead. However, overwriting log file data may result in data loss if the restore fails.

3. Open the Internet Authentication Service MMC snap-in, select the properties of the **Internet Authentication Service (local)** object and inspect the **General** tab. Append the text **"(Restore Test)"** to the **Server description** field. Click **OK** to close the IAS properties dialog. Changing the server description string allows you to see if the IAS configuration settings that were previously backed up have been restorated. After restoring the previous IAS configuration settings, the **Server description** string will have been overwritten by the old value and the **"(Restore Test)"** text will have disappeared.
4 Using the **Internet Authentication Service** MMC snap-in, right-click the **RADIUS Clients** folder and select **New RADIUS Client**. Enter **Restore Test** for the **Friendly name** and type **127.0.0.1** for the **Client address (IP or DNS)**. Enter a password in the **Shared secret** and **Confirm shared secret** field for this RADIUS client and click **Finish**. A successful restoration will overwrite the RADIUS client information and this new RADIUS will have disappeared.
5. Locate the backup media that you want to test (such as last night's scheduled backup) and use it to restore the following data to the server hard disk:
   - D:\IASConfig*.*
   - D:\IASLogs\BACKUPTEST.TXT
6. Execute the following at a command prompt to restore the IAS configuration saved previously as text files to the IAS database. Be sure to investigate any errors or warnings that appear during script execution:

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

Note: The following steps include the use of a floppy disk or other removable writable media labeled "RADIUS Clients for <*Server Name*>." Be sure to use the correct disk with the appropriate server to avoid loss of data.

---

7. Locate the RADIUS Client configuration floppy disk (or other removable, writable media) for this server, and insert it into the drive on the server. Execute the following at a command prompt. Be sure to investigate any errors or warnings that appear during script execution:

   ```
   C:\MSSScripts\IASClientImport.bat
   ```
8. Close and re-open the **Internet Authentication Service** MMC snap-in, select the properties of the **Internet Authentication Service (local)** object and inspect the **General** tab to ensure the **(Restore Test)** text no longer appears in the **Server description** field. Click **OK** to close the **IAS properties** dialog.
9. Select the RADIUS Clients folder and ensure that the **Restore Test** RADIUS client no longer appears in the list of clients in the right pane.
10. All other configuration within the **Internet Authentication Service** MMC snap-in should show the settings prior to restoration testing.
11. Navigate to the D:\IASLogs directory and ensure the backuptest.txt file is present. If the restoration steps in this procedure have been performed on a production server, have an IAS Security Auditor inspect the log files to ensure they are intact and recent, at least up to the time of backup.
12. You should return the backup media and the floppy disk to secure storage.

Security Administration

Security administration is responsible for maintaining a safe computing environment. Security is an important part of any enterprise IT infrastructure. Most information systems with a weak security foundation will eventually experience a security breach.

Accessing IAS RADIUS Request Logs

IAS can optionally record various events that arise from wireless AP RADIUS requests to RADIUS request logs located on the server hard disk. RADIUS logs are useful for a number of reasons, including to identify potential attacks on the system and unauthorized access to the organization's network. This task describes methods to inspect RADIUS request logs, although detailed discussion of RADIUS request log analysis is outside the scope of this guide.

A number of methods can be used to analyze RADIUS request logs, because they are stored as text in either IAS format or database-import format. This solution chose database-import format for the log files because of the relative ease of importing them into applications that accept comma-delimited text files. Methods for reviewing IAS RADIUS request logs include:

- **Browsing the log files directly with the IASPARSE utility**. This tool is available from the Windows Server 2003 Support Tools and, for performance reasons, is typically installed and run on the IAS server itself. Therefore, a Remote Desktop connection (or other means of remote execution) session is required. By default, this solution is not configured to support this method of log file viewing.
- **Importing log files into Microsoft Access 2002 from a remote administration computer**. This method allows an administrator to import the logs into a Microsoft Access table for impromptu queries or as part of a structured reporting and archival scheme. This method of log file viewing is the option used by this solution because it strikes a good balance between simplicity and flexibility. Enterprise customers may also want to consider the following option using Microsoft SQL Server™ 2000-based logging.
- **Accessing the log information through a central SQL Server 2000 cluster** to which data has been replicated from MSDE-2000 on each IAS server. Each IAS server logs to its local instance of MSDE. Setting up this arrangement is rather complex; however, Microsoft has produced a whitepaper and code to assist you with the process. For assistance with setting up SQL logging in this manner, please see your Microsoft partner or contact your Microsoft account executive, who can connect you with the appropriate partner or Microsoft Consulting Services professionals.

Summary Information

- **Security Requirements**: Member of the IAS Security Auditors security group
- **Frequency**: Daily or weekly–dependent upon security requirements
- **Technology Requirements**:
  - IASPARSE
  - Microsoft Access
  - Microsoft Excel

Task Details

RADIUS request logs are generated on each server in this solution and stored on a dedicated disk volume. Steps to access these log files include making a network connection to each IAS server, reviewing the log files, and then deleting them when they

are no longer needed. The IAS servers in this solution are configured to create a new RADIUS request log file each month but you can change this interval to suit your particular needs.

The table that you create with Access is formatted according to the type of data that is contained in each field. Although this example shows you how to create a new table, you can also import a log into an existing table.

▶ **To import RADIUS request log files into Microsoft Access**

1. Log on to an administration workstation as a member of the Active Directory IAS Security Auditors security group and map a drive connection to the IAS server whose logs are to be reviewed. Enter the following command at a command prompt, replacing HQ-IAS-01 with the name of your IAS server:

   NET USE X: \\HQ-IAS-01\IASLogs
2. Locate the log file that represents the month you wish to view. The log file name uses a format, that shows the date the file was created. Make a copy of the log file and rename the copy with a **.**txt file name extension.
3. Add the two complete lines in the text file C:\MSSScripts\IASAccessPrep.txt to the beginning of the copied log file. The first line contains the attribute names of each field in the log, and Access uses them to create the field names in its table. Using attribute names in the table makes it easier to interpret the log entries. Access uses the second line to set up the appropriate data type for each column in its table. After you import the log file, you should delete these entries from the Access table.
4. In Access 2002, click **Blank Database**. In **File New Database**, specify a file name, and then click **Create table by entering Data**. Click **File**, click **Get External Data**, and then click **Impor**t.
5. Click **Import**, click **Files of type**, click **Text Files**, locate the IAS log file, select it, and then click **Import**. In the **Import Text Wizard**, click **Advanced**.
6. Click **Import Specification**:
7. From **File Format**, click **Delimited**.
8. From **Field Delimiter**, select **,** (comma).
9. From **Text Qualifier**, select " (quotation mark).
10. From **Dates, Times, and Numbers**, select **Four Digit Years** and **Leading Zeros in Dates**, and then type the appropriate **Date Order** (such as MDY), **Date Delimiter** (such as **/** or **forward slash**), **Time Delimiter** such as **:** (colon), and **Decimal Symbol** such as **.** (period).
11. In the **Import Text Wizard** dialog box, click **Next**, select **First Row Contains Field Names**, and then click **Next**. Select **In a New Table** and then click **Next**.
12. Leave the defaults in **Field Options**, and then click **Next**. Click **Let Access add primary key**, and then click **Next**. In **Import to Table**, type the name of the new table. Click **Finish**.
13. In the **FileName:Database** dialog box, enter the name of your database, and then click **Open** to view your table.

Reviewing IAS RADIUS Authentication Event Log Entries

Security auditors may use this task periodically to check for unauthorized access attempts to the wireless network. Your internal security policy may dictate the need to review RADIUS authentication events in the Event Log periodically to detect authentication attempts or the use of stolen certificate credentials. You can also use a management tool such as MOM to raise alerts when suspicious events are logged.

This task is optional and can be viewed as an alternative to the IAS RADIUS logging described earlier. This task requires membership of either the IAS Admins group or server local Administrators group.

Summary Information

- **Security Requirements**: Membership in the IAS Admins group or the local built-in Administrators group
- **Frequency**: Daily or weekly–dependent upon security requirements
- **Technology Requirements**:
  - Event Viewer
  - Optionally, EventCombMT or EventFilter from the Windows Server 2003 Resource Kit

Task Details

This task is suitable for IT environments in which IAS security auditors and IAS system administrators are the same people. In contrast, RADIUS logs can be viewed by operators who are not local administrators of the server. This solution does not provide local Administrator privilege to security auditors. Before you can perform this task, you must add the auditor into the IAS Admins security group in Active Directory.

▶ **To check the Event Log for failed authentication attempts using Event Viewer**

1. Log on to one of the IAS servers as a member of the IAS Admins security group.
2. Open Event Viewer (by clicking **Start**, clicking **All Programs**, and then clicking **Administrative Tools**).
3. Click the **System Event Log**.
4. From the **View** menu, click **Filter.**
5. Select an **Event Source** of **IAS** and an **Event ID** of **2**.
6. Investigate any frequent authentication failures or other suspicious entries.

Note: You may also use the Eventquery tool (in Windows XP and Windows Server 2003) and the EventFilter or EventCombMT tools from the Windows Server 2003 Resource Kit to view IAS events.

Archiving and Deleting IAS RADIUS Log Files

IAS includes a feature to delete the oldest IAS RADIUS log file when the logging disk becomes full. If you do not use this automated facility you will need to manually archive and delete IAS RADIUS request log files to ensure IAS does not run out of disk space. Running out of space will cause IAS to stop servicing authentication and accounting requests from wireless APs. You can also automate log archival using a script or an automated SQL Server 2000 replication strategy (as described in the "Accessing IAS RADIUS Request Logs" task earlier in this chapter).

Note: This solution uses the IAS feature to automatically delete the oldest log file upon a disk full event.

Summary Information

- **Security Requirements**: Membership in the IAS Security Auditors Active Directory security group
- **Frequency**: Monthly
- **Technology Requirements**: Native Windows commands

Task Details

Numerous archival and deletion methods exist for RADIUS authentication and accounting request logs. For example, a server-based backup script can notify IAS security auditors by e-mail that log file backup completes successfully. Security auditors can then connect to the IAS server and delete the oldest log files. Or IAS security auditors can back up the RADIUS log files to a tape or CD–RW device connected to their administration computer, and then connect to the IAS server and delete the oldest log files that are no longer required.

In this solution, IAS is configured to create a new log file each month.

You should devise a strategy that keeps enough data online to reconstruct network access information for various scenarios. For example, if you have three months worth of data online in three separate log files, you may require only the latest two log files to reconstruct network access information to track security events . You can therefore archive and delete the oldest of the three log files and leave the latest two.

Information on backing up RADIUS request logs as well as other IAS data can be found in the "Configuring Backup of IAS Data Directories" task detailed in this chapter. This task provides guidance for archiving and deleting RADIUS logs from an administration station.

▶ **To archive and delete RADIUS request log files**

1. Log on to an administration workstation as a member of the IAS Security Auditors security group.
2. Map a drive to the IAS server that will have log files archived using the following command, replacing HQ-IAS-01 with the name of your IAS server:

   ```
   NET USE X: \\HQ-IAS-01\IASLogs
   ```

3. Identify the oldest log files on the IAS server that are to be archived and deleted from the server. Use NTBACKUP, the **copy** command, or other utility to archive the selected log files from the online share to secondary media.
4. Delete the unwanted log files from the online share.

Supporting Quadrant Tasks

The SMFs within the Supporting Quadrant provide both reactive and proactive tasks to maintain required service levels. The reactive functions depend on an organization's ability to react and resolve incidents and problems quickly. The more desirable, proactive functions try to avoid any disruption in service by identifying and resolving problems before any service levels are affected. These functions use good monitoring of the service solution against predefined thresholds, and provide the operations staff with sufficient time to react to potential problems before they become service disruptions. The Supporting Quadrant is closely related to the Service Control and Monitoring SMF that is described in the Operating Quadrant. Service Control and Monitoring provides the essential information by which operating and support staff can detect problems. The procedures described in this section are intended to address the most common incidents that you will encounter and enable you to recover from them.

This section contains information relevant to the following SMFs:

- Incident Management

There are no tasks that belong to the remaining SMFs:

- Problem Management
- Service Desk

Note: Each task description includes the following summary information: security requirements, frequency, and technology requirements.

Incident Management

Incident management is the process of managing and controlling faults and disruptions in the use or implementation of IT services as reported by customers or IT partners. Incident management tries to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring the maintenance of the best possible quality and availability of levels of service. Normal service operation is defined here as service operation within the limits of the service level agreement (SLA).

Note: For general troubleshooting of Windows XP wireless client issues, see the references in the "More Information" section at the end of this chapter.

Checking Client Network Connections Folder Status

The Network Connections folder and the Windows XP notification icons provide information about the state of WLAN authentication. This task enables an end user or Helpdesk staff member to check the status of the wireless connection on the client computer. If an authentication requires additional information from the user, such as the selection of one of multiple user certificates, a text balloon displays that instructs the user. This task is used during troubleshooting.

Summary Information

- **Security Requirements**: Membership in the local Administrators security group to make modifications to WLAN settings
- **Frequency**: When troubleshooting a user issue
- **Technology Requirements**: Windows XP Professional

Task Detail

Within the Network Connections folder, the text that displays under the name of the connection corresponding to the wireless network adapter describes the state of the authentication.

When you view status of the connection, you can see the signal strength on the **General** tab and the IP address configuration on the **Support** tab. If the wireless adapter has an Automatic Private IP Addressing (APIPA) address (169.254.0.0/16) or if it was configured with the alternate IP address set in the Transmission Control Protocol/Internet Protocol (TCP/IP) properties of the adapter, authentication has failed but the Windows XP wireless client is still associated with the wireless access point. If the authentication fails and the association is still in place, Windows enables the wireless adapter and TCP/IP performs its normal configuration process. In this example, because the client was not successfully authenticated to the WLAN, a Dynamic Host Configuration Protocol (DHCP) server cannot be found–so TCP/IP automatically configures an APIPA or alternate address. In such cases, it is recommended that you review the reason for WLAN authentication failure on the IAS server or enable and review tracing on the client computer.

▶ **To check the status of the Network Connections folder**

- Click **Start**, **Run**, type **ncpa.cpl** and then click **OK**.

Enabling and Disabling Tracing on Client Computers

Windows supports detailed tracing information to assist Helpdesk staff and developers resolve issues with software components. Tracing provides a level of detail beyond that found in Event Logs and stores this information in text log files.

To obtain detailed information about the EAP authentication process, you must enable tracing for the EAP over LAN (EAPOL) and Remote Access Service–Transport Layer Security (RASTLS) components.

Summary Information

- **Security Requirements**: Membership in the local Administrators security group
- **Frequency**: As required when troubleshooting a client WLAN issue
- **Technology Requirements**:
  - Windows XP Professional
  - Notepad.exe

Task Detail

After the following commands are issued, try the authentication process again and view the Eapol.log and Rastls.log files in the %systemroot%\Tracing folder.

▶ **To enable tracing on client computers**

- Run the following commands:
  - **netsh ras set tracing eapol enabled**
  - **netsh ras set tracing rastls enabled**

▶ **To disable tracing on client computers**

- Run the following commands:
  - **netsh ras set tracing eapol disabled**
  - **netsh ras set tracing rastls disabled**

Note: Tracing consumes system resources and creates log files that grow rapidly. Be sure to disable tracing again when troubleshooting is complete.

Verifying Domain Name String on Client Computers

The following task is useful if you have opted to enable the certificate domain name checking on client computers. This setting is not enabled in this solution because it may generate potentially confusing WLAN dialog boxes for users. Windows XP Professional SP1 also has this option disabled by default.

Client computers cannot perform certificate revocation checking during EAP-TLS mutual authentication, because certificate revocation list (CRL) locations are typically not available before access is granted to the WLAN. Windows clients can, however, validate all or part of the server name in the certificate presented by the IAS server. This capability is configured in the Wireless Network Policies settings in the wireless clients GPO. (The settings here have a similar user interface to the Wireless Networks properties on the client computer's wireless network adapter properties.)

If the wireless client tries to validate the server certificate and you have entered an incorrect value for the IAS server domain in the **Connect if the server name ends with** field, authentication will fail. You may need to perform this task when troubleshooting client authentication problems if you have opted to enable the **Connect to these servers option**.

Summary Information

- **Security Requirements**: Membership in the local Administrators security group
- **Frequency**: Setup or during troubleshooting of user WLAN issues
- **Technology Requirements**: Windows XP Professional

Task Detail

This task allows you to verify that the domain name string is correct in the **Properties** dialog box of the WLAN network adapter network connection on the client or in the Wireless Network Policies GPO.

▶ **To verify the domain name string on client computers**

1. Click **Start**, **Run**, type **ncpa.cpl** and then click **OK**.
2. View the properties of the wireless network connection.
3. On the **Wireless Networks** tab, select the network Service Set Identifier (SSID) of the target network from preferred networks and view its properties.
4. On the **Authentication** tab, view the properties and ensure that the **Connect if the server name ends with** string equals the domain name for the IAS server(s).

Viewing IAS Authentication Events in the Event Log

Client authentication success and failure events are recorded in the System Event Log on the IAS servers and can be useful for troubleshooting. Event logging is enabled for all types of IAS events (rejected, discarded, and successful authentication events) by default on the **Service** tab for the IAS server properties in the Internet Authentication Service MMC snap-in.

This task allows IAS administrators to assist Helpdesk staff in troubleshooting computer and user authentication issues by viewing authentication events in the IAS Server Event Logs.

If IT Helpdesk staff require access to wireless client authentication information in the IAS System Event Logs, you have several options:

- Enlist the help of an IAS administrator who is a member of the IAS Admins security group and thus has access to the IAS System Event Log messages. This task uses this option.
- Use an enterprise Event Log management system such as MOM to export logs to a location where Helpdesk staff can access them.
- Grant Helpdesk staff Read permission on both the IASLogs share and the underlying NTFS D:\IASLogs directory. Instruct them how to browse log files using tools such as IASPARSE described in the "Accessing IAS RADIUS Request Logs" task in this chapter. Most customers will want to consider this option because it requires the least infrastructure and does not pose an excessive security risk.

Granting users who are not administrators access to IAS System Event Logs may pose a security risk. This is especially a concern for servers that combine IAS and domain controller server roles.

Summary Information

- **Security Requirements**: Membership in the local IAS Administrators security group or a group with Read/Save access to the System Event Log
- **Frequency**: When troubleshooting client authentication issues
- **Technology Requirements**: Event Viewer MMC snap-in or EventCombMT from the Windows Server 2003 Resource Kit

Task Detail

Viewing the authentication attempts in the System Event Log is useful for troubleshooting authentication attempts being rejected by IAS. When you have multiple remote access policies configured, you can use the log to determine the name of the remote access policy that either accepted or rejected the connection attempt (see Policy-Name in the event description). In addition, the authentication event (Source: IAS, Event ID 1 for accept and 2 for reject) shows reason codes that have corresponding descriptions and are mentioned in Windows Server 2003 Help and Support.

Enabling IAS event logging and reading the text of IAS authentication events in the System Event Log is the most useful tool for troubleshooting failed IAS authentications.

▶ **To view the System Event Log for authentication events**

1. Click **Start**, **Run**, type **Eventvwr** and then click **OK**.
2. Select **System Event Log**.
3. From the **View** menu, select **Filter**, choose **IAS** as the **Event Source**, and then click **OK**.

Enabling and Disabling Tracing on the IAS Server

Windows supports detailed tracing information to assist Helpdesk staff and developers resolve issues with software components. Tracing provides a level of detail beyond that which is found in Event Logs and stores this information in text log files.

Microsoft Windows Server 2003 has an extensive tracing capability that you can use to troubleshoot complex problems for specific components. You can enable the components in Windows 2003 Server to log tracing information to files with the **netsh** command.

Summary Information

- **Security Requirements**: Membership in the local Administrators security group on the IAS server
- **Frequency**: As required when troubleshooting client WLAN connection issues
- **Technology Requirements**:
  - Netsh
  - Notepad
  - Regedit

Task Detail

Use the **netsh** command to enable and disable tracing for specific components or for all components. The most useful components to enable for tracing of EAP-TLS based 802.1X authentication issues are the following:

- **IASSAM** (**the Iassam.log file in the %*systemroot%*\tracing folder)**. This log is the most commonly used trace file for IAS issues because it describes functions such as cracking user names, binding to a DC, verifying credentials. It is the "heart" of the IAS trace files and is usually required to debug any authentication related issues.
- **RASTLS (the Rastls.log file in the %*systemroot%*\tracing folder)**. For all EAP and PEAP related authentications, this log holds most of the vital debugging information. However, this log file is challenging to read. Microsoft is working to produce information that may make this information easier to interpret.

The following tracing information for IAS is typically not required for troubleshooting 802.1X authentication using EAP-TLS but may be useful for troubleshooting other tasks:

- **IASRAD (the Iasrad.log file in the *%systemroot%*\tracing folder)**. This log describes all RADIUS protocol related operations. It will describe the ports the server is listening on etc. This is also rarely used in debugging issues on the IAS server.
- **IASSDO (the Iassdo.log file in the *%systemroot%*\tracing folder)**. The IASSDO log tracks transactions from the UI to the MDB files that store the server's configuration and dictionary. This is the log used to debug any service or UI-related issues.

▶ **To enable tracing on the IAS server**

- Run the **netsh** command(s) that correspond to the tracing information you require. When troubleshooting EAP-TLS with 802.1X authentication issues, the IASSAM and RASTLS logs are recommended.

  The corresponding **netsh** commands are:
  - **netsh ras set tracing iassam enabled**
  - **netsh ras set tracing rastls enabled**
  - **netsh ras set tracing iasrad enabled**
  - **netsh ras set tracing iassdo enabled**

▶ **To disable tracing on the IAS server**

- Run the **netsh** command(s) that correspond to the tracing information you wish to disable.

  The corresponding **netsh** commands are:
  - **netsh ras set tracing iassam disabled**
  - **netsh ras set tracing rastls disabled**
  - **netsh ras set tracing iasrad disabled**
  - **netsh ras set tracing iassdo disabled**

Note: Because tracing consumes system resources, you should use it sparingly to help identify network problems. After the trace is captured or the problem is identified, you should immediately disable tracing.

Because IASSAM tracing logs default to only one megabyte (MB), valuable information may be overwritten in log files during heavy loads. Perform the following steps to set the IASSAM tracing log to 15 MB. When the log's size reaches 15 MB, the file is renamed to IASSAM.old and a new IASSAM.log is created. This procedure allows you to keep 30 MB of data on the server.

▶ **To set the IASSAM tracing log file to 15 MB**

1. Start Regedit.exe.
2. Go to the following registry key: **\HKLM\Software\Microsoft\Tracing**.
3. Update the **IASSAM** key with a value of **MaxFileSize**, a type of **REG_DWORD** and a data value of **0xF00000**.

Enabling SChannel Logging on the IAS Server

Secure channel (SChannel) is a security support provider (SSP) that supports a set of Internet security protocols, such as Secure Sockets Layer (SSL) and Transport Level Security (TLS).

Summary Information

- **Security Requirements**: Membership in the local Administrators security group
- **Frequency**: As required when troubleshooting client connection issues on the IAS server
- **Technology Requirements**:
  - Regedit
  - Notepad

Task Detail

Logging of client certificate validation failures is a secure channel event, and is not enabled on the IAS server by default.

▶ **To enable SChannel logging on the IAS server**

You can enable additional secure channel events by changing the following registry key value from **1** (**REG_DWORD** type, data **0x00000001**) to **3** (**REG_DWORD** type, data **0x00000003**):

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\EventLogging

---

Warning: Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

Be sure to disable SChannel logging when you are through troubleshooting, because it consumes system resources and can flood the Event Log with unwanted entries.

Optimizing Quadrant Tasks

The Optimizing Quadrant includes the SMFs to manage costs while maintaining or improving service levels. This quadrant includes review of outages/incidents, examination of cost structures, staff assessments, availability, performance analysis, and capacity forecasting.

This section contains information relevant to the following SMFs:

- Capacity Management

There are no tasks that belong to the remaining SMFs:

- Service Level management
- Financial Management
- Availability Management
- IT Service Continuity Management
- Workforce Management

Note: Each task description includes the following summary information: security requirements, frequency, and technology requirements.

Capacity Management

Capacity management is the process of planning, sizing, and controlling service solution capacity so that it satisfies user demand within the performance levels set forth in the SLA. This process requires information about usage scenarios, patterns, and peak load characteristics of the service solution, as well as stated performance requirements.

Determining Maximum Load on the IAS Server

This section provides some information on the likely maximum load on the IAS server.

Performance is rarely an issue for IAS RADIUS servers that are properly sized and configured. IAS RADIUS servers are most stressed during times of peak load, such as morning hours when many users simultaneously log on, shortly after a major network outage, or during a RADIUS server failure when wireless APs failover to a backup server.

Summary Information

- **Security Requirements**: None
- **Frequency**: Setup task
- **Technology Requirements**: None

Task Details

Microsoft's internal testing has shown that IAS can achieve a peak load on modest hardware, which will service most customers' needs. Estimations for the number of authentications IAS can service are best represented as authentications per second. IAS has achieved the following performance figures on an Intel Pentium 4 2GHz server running Windows Server 2003 with Active Directory on a separate Intel Pentium 4 2GHz server.

Table 12.10: Determining Load on the IAS Server

Authentication type	Authentications per second
New EAP-TLS authentications	36
New EAP-TLS authentications with offload card support	50
Authentications with fast reconnect	166

Note: This information is provided without warranty of accuracy and should only be used as a guideline for capacity planning purposes and not for performance comparisons

IAS can be configured to generate disk based text logs containing varying amounts of RADIUS request information. You should plan for a high performance disk for storing RADIUS logs because of the overhead that RADIUS logging has on the RADIUS Servers. Slow disk subsystems can delay IAS RADIUS responses to wireless APs, leading to protocol timeouts and unnecessary failover of wireless APs to secondary RADIUS Servers. For more information about RADIUS logging options, see Chapter 5, "Designing the RADIUS Infrastructure for Wireless LAN Security."

Also, enabling Windows 2003 Server software tracing features (as described in the earlier section "Enabling and Disabling Tracing on the IAS Server") will apply additional load on IAS servers. However, it may be required occasionally to troubleshoot network access issues. IAS servers should have the capacity to run with tracing enabled for limited periods of time while continuing to service the production load.

Determining Storage and Backup Requirements for an IAS Server

This section provides capacity details for IAS storage parameters. These details will help capacity planners calculate future storage requirements for online disk and offline backup storage.

Summary Information

- **Security Requirements**: None
- **Frequency**: As required
- **Technology Requirements**: None

Task Details

IAS RADIUS log files are the single component on IAS servers that require storage planning. RADIUS request logs for this solution are configured to create a new log each month, and hardware tested during development of this solution included a dedicated 18 GB disk volume for log files.

You must estimate the load on the IAS servers in your environment, then select logging options and perform testing in a lab environment to simulate production wireless clients authenticating to IAS and generating log data. Estimations can use logic similar to the following:

The average number of users per wireless AP is 25 (users or computers). Each user or computer performs an initial authentication and re-authenticates every 10-60 minutes (depending on security requirements) . Each authentication generates one kilobyte (KB)of disk log information, with authentication requests logged, auditing requests logged, and interim requests not logged (file size varies with logging options). You should calculate the amount of disk log space generated per wireless AP per hour when

supporting 25 clients. Then estimate the largest number of wireless APs that your primary IAS server will support in times of network stress or server failover.

IAS RADIUS request logs are highly compressible data. Although not recommended for normal use, compression can be enabled on the RADIUS request log file folder if needed. You should be prepared for extra load on an IAS server that needs to compress data.

Backup Window for IAS RADIUS Log Files

If a network backup operating in ideal conditions on a dedicated 100 Mbps (megabits per second) switch to the backup server is assumed, a 3-gigabyte (GB) database plus 500 MB of system state can be backed up in approximately 15-20 minutes.

Changing Quadrant Tasks

The Changing Quadrant includes the processes and procedures required to identify, review, approve, and incorporate change into a managed IT environment. Change includes hard and soft assets, as well as specific process and procedural changes.

The objective of the change process is to introduce new technologies, systems, applications, hardware, tools, and processes as well as changes in roles and responsibilities into the IT environment quickly and with minimal disruption to service.

Change Management

The Change Management SMF is responsible for managing change in an IT environment. A key goal of the change management process is to ensure that all parties affected by a given change are aware of and understand the impact of the impending change. Because most systems are heavily interrelated, any changes made in one part of a system may have profound impacts on another. Change management attempts to identify all affected systems and processes before the change is deployed to mitigate or eliminate any adverse effects. Typically, the “target” or managed environment is the production environment, but it should also include key integration, testing, and staging environments.

All changes to the RADIUS infrastructure and WLAN security should use the following standard MOF change management process:

1. **Change request**. The formal initiation of a change through the submission of a request for change (RFC).
2. **Change classification**. The assignment of a priority and a category to the change, using its urgency and its impact on the infrastructure or users as criteria. This assignment affects the implementation speed and route.
3. **Change authorization**. The consideration and approval or disapproval of the change by the change manager and the change review board (CAB), a board that contains IT and business representatives.
4. **Change development**. The planning and development of the change, a process that can vary immensely in scope and includes reviews at key interim milestones.
5. **Change release**. The release and deployment of the change into the production environment.
6. **Change review**. Post-implementation process that reviews whether the change has achieved the goals that were established for it and determines whether to keep the change in effect or remove it.

The procedures in this section outline the change development procedures for some of the key changes that you are likely to require on a regular basis in your environment. Each change development procedure will have a companion change release procedure that describes how the change is to be deployed into production.

Managing Operating System Updates

The management of security updates to RADIUS and WLAN software components is part of general Windows patch management. This topic is discussed in two solution guides from Microsoft that describe Windows operating system updates using either Microsoft Systems Management Server (SMS) or Microsoft Software Update Services (SUS). See the "More Information" section at the end of this chapter for details on how to obtain them.

Patch management includes release management and configuration management components as well as a change management component. However, all three SMFs are covered by the documents referenced in the preceding paragraphs.

Configuration Tables

The following tables contain the site-specific and solution-specific configuration information values that are used by the procedures in this chapter. These tables are a subset of the planning configuration tables in Chapter 8, "Implementing the RADIUS Infrastructure," and Chapter 9, "Implementing the Wireless LAN Security Infrastructure," and are shown here only for reference.

Per–Site Configuration Parameters

Table 12.11: User-Defined Configuration Items

Configuration item	Setting
DNS name of Microsoft 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

Solution Configuration Parameters

Table 12.12: 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
[Accounts] Active Directory global group that contains users requiring 802.1x authentication certificates	AutoEnroll Client Authentication–User Certificate
[Accounts] Active Directory global group that contains computers requiring 802.1x authentication certificates	AutoEnroll Client Authentication–Computer Certificate
[Accounts] Microsoft Active Directory global group that contains IAS servers requiring 802.1X authentication certificates	AutoEnroll RAS and IAS Server Authentication Certificate
[Accounts] Pre-Windows 2000 name for the Microsoft Active Directory global group that contains 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] 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 global group that contains computers requiring configuration of wireless network properties through Active Directory Group Policy	Wireless Network Policy–Computers

(continued)

[Certificates] Certificate template used to generate certificates for user client authentication	Client Authentication–User
[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
[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
[Remote Access Policy] Policy name	Allow Wireless Access
[Group Policy] Microsoft Active Directory Group Policy Object name	Wireless Network Policy
[Group Policy] Wireless Network policy within the Group Policy Object	Client Computer Wireless Configuration

More Information

- For more information about the MOF process model and team model, see the Microsoft Operations Framework page at www.microsoft.com/technet/itsolutions/techguide/mof/default.mspx.
- For more information about capacity constraints and related performance counters, see Microsoft Knowledge Base Q146005, "Optimizing Windows NT for Performance" at http://support.microsoft.com/default.aspx?kbid=146005.
- For more information about troubleshooting wireless network problems, see the following:
  - The Microsoft Knowledge Base article Q313242 "How to troubleshoot wireless network connections in Windows XP" at http://support.microsoft.com/?scid=313242.
  - The white paper "Troubleshooting Windows XP IEEE 802.11 Wireless Access" at www.microsoft.com/windowsxp/pro/techinfo/administration/networking/troubleshooting.asp.
- For information about MOM deployment, see the *MOM 2000 SP1 Operations Guide* at www.microsoft.com/resources/documentation/mom/2000sp1/all/opsguide/en-us/1_in781g.mspx.
- For information about patch management with Microsoft SMS 2003, see "Patch Management Using Microsoft Systems Management Server 2003" at www.microsoft.com/technet/itsolutions/techguide/msm/swdist/pmsms/2003/pmsms031.mspx.
- For information about patch management using Microsoft SMS 2.0, see "Patch Management Using Microsoft Systems Management Server 2.0" at www.microsoft.com/technet/itsolutions/techguide/msm/swdist/pmsms/20/pmsmsin.mspx.
- For information about patch management using Microsoft Software Update services, see "Patch Management Using Microsoft Software Update" at www.microsoft.com/technet/itsolutions/techguide/msm/swdist/pmsus/pmsus251.mspx.
- More information about security patch management on the Microsoft platform can be found in "Improve Platform Manageability" at http://go.microsoft.com/fwlink/?LinkId=16284.
- For more information about obtaining and using the Group Policy Management Console (GPMC), see "Enterprise Management with the Group Policy Management Console" at www.microsoft.com/windowsserver2003/gpmc/default.mspx.