



# Windows Server 2003 PKI Operations Guide

Microsoft Corporation

Author: David B. Cross and Ayman AlRashed

### Abstract

How to configure and operate a Windows certificate authority, with operational scenarios, custom configuration information, sample commands, and best practices.



Information in this document, including URL and other Internet Web site references, is subject to change without notice.  Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.  Complying with all applicable copyright laws is the responsibility of the user.  Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document.  Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2005 Microsoft Corporation.  All rights reserved.

Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

# Contents

[Windows Server 2003 PKI Operations Guide 7](#_Toc124739975)

[Basic Administrative Tasks 8](#_Toc124739976)

[Adding Certificate Templates to a CA 8](#_Toc124739977)

[Delegating Administration of Certificate Templates 9](#_Toc124739978)

[Issuing Certificates 10](#_Toc124739979)

[Revoking Certificates 11](#_Toc124739980)

[Migrating from a Stand-alone to an Enterprise CA 12](#_Toc124739981)

[Windows Server 2003 PKI and Role-Based Administration 20](#_Toc124739982)

[Roles and Activities 23](#_Toc124739983)

[Assigning Roles 27](#_Toc124739984)

[Role Separation 28](#_Toc124739985)

[Windows 2000 and Windows Server 2003 Role-Based Administration 29](#_Toc124739986)

[Role Separation Validation 30](#_Toc124739987)

[Certificate Managers 30](#_Toc124739988)

[Backup/Restore and Auditing under Role Separation 30](#_Toc124739989)

[CA Auditing 31](#_Toc124739990)

[CA Audit Groups 31](#_Toc124739991)

[Back Up and Restore the CA Database 32](#_Toc124739992)

[Change CA Configuration 32](#_Toc124739993)

[Change CA Security Settings 32](#_Toc124739994)

[Issue and Manage Certificate Requests 33](#_Toc124739995)

[Revoke Certificates and Publish CRLs 33](#_Toc124739996)

[Store and Retrieve Archived Keys 33](#_Toc124739997)

[Start and Stop Certificate Services 33](#_Toc124739998)

[Setting Up CA Auditing 34](#_Toc124739999)

[Enabling Object Access Auditing 34](#_Toc124740000)

[When the CA Is on a Domain Controller 34](#_Toc124740001)

[When the CA Is on a Member or a Workgroup Server 35](#_Toc124740002)

[Enabling Auditing on the CA 35](#_Toc124740003)

[Auditing and Event Management 35](#_Toc124740004)

[Event IDs Used by Certificate Services 35](#_Toc124740005)

[Breakdown of Shared Event IDs 37](#_Toc124740006)

[CA Audit Specification 39](#_Toc124740007)

[CA Maintenance 44](#_Toc124740008)

[CA Remote Maintenance 44](#_Toc124740009)

[Publish the CRL of an Offline CA 44](#_Toc124740010)

[CRL Re-Sign 46](#_Toc124740011)

[Administrative Process for Offline CRL Publication 47](#_Toc124740012)

[Certification Authority Renewal 47](#_Toc124740013)

[Best Practices for Renewing CAs 47](#_Toc124740014)

[CRL Partitioning 49](#_Toc124740015)

[Automatic RootCA Cross-Certificate Generation 51](#_Toc124740016)

[Key Backup 51](#_Toc124740017)

[Backup/Recovery 52](#_Toc124740018)

[Removing a CA from Active Directory 52](#_Toc124740019)

[Uninstalling an Enterprise Certification Authority 53](#_Toc124740020)

[Active Directory Objects 55](#_Toc124740021)

[CA Database 57](#_Toc124740022)

[Domain Controller Cleanup 57](#_Toc124740023)

[Best Practices for CRLs 58](#_Toc124740024)

[Certificate Revocation List Defaults 58](#_Toc124740025)

[Application Reliability 58](#_Toc124740026)

[Revoking Large Numbers of Certificates 59](#_Toc124740027)

[Controlling CRL Size 60](#_Toc124740028)

[Remove Expired CRLs 61](#_Toc124740029)

[Custom CA Configuration 61](#_Toc124740030)

[Ignore Offline CRL Errors on the CA 61](#_Toc124740031)

[Configure Serial Number Generation 61](#_Toc124740032)

[CA Key Usage 62](#_Toc124740033)

[Disable DN Length Enforcement 63](#_Toc124740034)

[Maintaining the CA Database 63](#_Toc124740035)

[Securing DCOM Interfaces 63](#_Toc124740036)

[Enrollment Processing 64](#_Toc124740037)

[Enabling Referrals Across Forests 64](#_Toc124740038)

[Enabling Netscape Browser Enrollment 64](#_Toc124740039)

[Adding CRL Information in an Authority Revocation List 65](#_Toc124740040)

[Allowing and Blocking Extensions in Certificate Requests 65](#_Toc124740041)

[Adding an E-Mail Address to the SubjectAltName Extension 67](#_Toc124740042)

[How to Change the Validity Period for Certificates Issued from a CA 68](#_Toc124740043)

[Tuning CA Database Performance 68](#_Toc124740044)

[Increasing CA Database Session Limit 68](#_Toc124740045)

[Viewing Extended Information 69](#_Toc124740046)

[Viewing Request Attributes 69](#_Toc124740047)

[Removing CA Information from the Directory 69](#_Toc124740048)

[Managing Subject Relative Distinguished Names in the Certificate Subject 69](#_Toc124740049)

[Enabling the Netscape Revocation Method 71](#_Toc124740050)

[Configuring the SMTP Exit Module 72](#_Toc124740051)

[Sample Configuration Batch File 72](#_Toc124740052)

[Revocation Status 76](#_Toc124740053)

[Using SSL to Communicate with Exchange Server 77](#_Toc124740054)

[Related Links for Windows Server 2003 PKI Operations 78](#_Toc124740055)

[Appendix A for Windows Server 2003 PKI Operations 79](#_Toc124740056)

# Windows Server 2003 PKI Operations Guide

By David B. Cross and Ayman AlRashed

Microsoft Corporation

This document provides a guide for administrators on how to configure and operate a Windows certification authority. Various operational scenarios, custom configuration information, sample commands, and best practices are provided.

Windows Server 2003 provides a flexible and low TCO solution for deploying a public key infrastructure. Due to the complexity of customer environments and various organization requirements, a Windows Server 2003 certification authority (CA) may require configuration changes. This white paper provides operational best practices and configuration walkthroughs for some of the more common scenarios. It is not intended to cover the entire scope of all operational scenarios and configuration parameters possible with the Windows Server 2003 CA.

# Basic Administrative Tasks

For day to day tasks, it is usually preferable to create a standard procedure. A procedure is usually organization-dependent as the processes and people differ from organization to organization. There are usually common practices employed by most organizations when doing the common day to day administrative tasks.

## Adding Certificate Templates to a CA

A certificate template profiles certificates based on their intended use. When requesting a certificate from a Microsoft certification authority (CA), depending on their access rights, the certificate requester will be able to select from a variety of certificate types that are based on certificate templates, such as User and Basic EFS. The certificate template saves users from low-level, technical decisions about the type of certificate that they need. Instead, they can rely on the judgment of their administrators and use the template name that indicates the purpose of the certificate. If none of the preset certificate templates meets your needs, you can create new certificate templates and customize them for a variety of different uses.

Note

In addition to assigning the correct permissions for enrollment on a certificate template in Active Directory; you also need to add the template to the list of certificate templates a CA can issue if you want your users to start enrolling for this template.

Note

Only Windows Server 2003 and Windows 2000 Enterprise CAs can issue certificates based on certificate templates; stand-alone CAs cannot use certificate templates.

Note

You need to be part of the Enterprise Admins or the Domain Admins, or you need to have enough permissions to write to the Certificate Templates container in Active Directory.

To change the permissions on a certificate template for user enrollment

|  |
| --- |
| 1. Right-click the Certificate Templates node in the Certification Authority snap-in and select Manage.2. Double-click a certificate template.3. On the Security tab, check the Allow boxes for the Read and Enroll permissions. |

To add a certificate template to a CA

|  |
| --- |
| 1. Right-click the Certificate Templates node in the Certification Authority snap-in, and on the New submenu, select Certificate Template to Issue.2. Select the appropriate template and click OK. |

Note

You need to be a CA Administrator to add templates to the CA.

## Delegating Administration of Certificate Templates

Although most of the CA-related tasks are achieved through the administration of the CA itself, certain tasks are controlled through Active Directory, such as administration of Certificate Templates.

To delegate the administration of Certificate Templates

|  |
| --- |
| 1. Right-click the Certificate Templates node in the Certification Authority snap-in and select Manage.2. Double-click a certificate template.3. On the Security tab, check the Allow boxes for the Read and Write permissions. |

## Issuing Certificates

There are some questions you need to answer and document before issuing a certain certificate. These questions are more relevant to how the certificate is issued from an operational side rather than a technical side.

1. Does my organization currently employ a Certificate Practice Statement (CPS) for this CA? If it does, did the requester meet all the requirements for enrollment?

2. Are there special requirements that the person issuing the certificate (such as being an Officer) that I must fulfill as an administrator?

3. Are there any documented operational procedures for my organization that I must follow when issuing certificates (such as backup)?

4. Are there any special attributes that must be included in the certificate that are not included in the request (such as Certificate Policy)?

When these questions are answered, and all the requirements are fulfilled, issue the certificate by logging on as a user with Certificate Manager (CA Officer) permissions:

1. Left-click the Pending Requests node in the Certification Authority snap-in.

2. Right-click the request, then select Issue on the All Tasks submenu.

If one of the requirements is not met, you can either ensure that requirements are met (such as making the user supply more authentication information) then issuing the certificate, or you can deny the request.

To deny the request

|  |
| --- |
| 1. Left-click the Pending Requests node in the Certification Authority snap-in.2. Right-click the request, then select Deny on the All Tasks submenu. |

In either case, make sure you document your actions and the answers to all four questions.

Important

The policy module will always re-process requests that are pended and if template, configuration, or user group information has changed after the request was originally submitted, the policy module will re-evaluate the request on the new information only.

Note

To re-submit a failed request and issue the failed request, a user must have both the CA Officer and CA Admin permissions on the CA. Obviously, this capability will not be possible when role separation is enabled on the CA.

## Revoking Certificates

Although certificates are usually used to enhance the trust in an organization, removing the trust from a certain certificate is sometimes required. Before you revoke a certificate, make sure you answer and document the following questions:

1. What is the reason for revoking this certificate?

2. Who requested the revocation of this certificate?

3. Will I ever need this certificate again (such as verification of signatures or decryption of messages)? If yes, what is the need (that is, verification of signatures, decryption of messages, normal usage)?

4. Are there special requirements for the person revoking the certificate (such as being an Officer) that I must fulfill as an administrator?

5. Are there any documented operational procedures for my organization that I must follow when revoking certificates (such as backup)?

When all of these questions are answered, and all the requirements are fulfilled, revoke the certificate.

To revoke the certificate

|  |
| --- |
| 1. Left-click the Issued Certificates node in the Certification Authority snap-in.2. Right-click the certificate and select Revoke Certificate on the All Tasks submenu.3. Choose the correct reason for revocation and click Yes. |

Make sure you document your actions and the answers to all five questions.

Note

If you answered yes to question 3, and the need will be full or normal usage, make sure you choose Certificate Hold as the reason. This is the only reason that could allow a revoked certificate to be unrevoked.

If you revoke a certificate and the reason is Certificate Hold, and you decide later that you want to unrevoke the certificate, you need to answer and document the following questions:

1. Why am I revoking this certificate?

2. Who requested this task?

3. Are there special requirements from the person unrevoking the certificate (such as being an Officer) that I must fulfill as an administrator?

4. Are there any documented operational procedures for my organization that I must follow when revoking certificates (such as backup)?

5. Does my organization currently employ a Certificate Practice Statement (CPS) for this CA, and if it does, did the requester meet all the requirements for unrevoking the certificate?

When all of these questions are answered, and all the requirements are fulfilled, unrevoke the certificate.

To unrevoke the certificate

|  |
| --- |
| 1. Left-click the Revoked Certificates node in the Certification Authority snap-in.2. Right-click the revoked certificate, and select Unrevoke Certificate on the All Tasks submenu. |

Make sure you document your actions and the answers to all four questions.

Note

Unrevoking a certificate is considered dangerous if misused. Ensure proper operations and documentation when you unrevoke a certificate.

# Migrating from a Stand-alone to an Enterprise CA

Despite the best planning intentions, it may be necessary to change the configuration of a Windows-based certification authority from a stand-alone mode to an enterprise mode. It may also be necessary to change the configuration of a CA that was first installed as an NT 4.0 certification authority that was included in the NT 4.0 Option Pack. For example, an NT 4.0 CA may be upgraded in place to a stand-alone CA and later converted to an enterprise CA to work with Exchange 2000. For NT 4.0 upgrade procedures, see the help files in Windows 2000 or Windows Server 2003. This section provides a walkthrough of the steps required to convert a Windows Server 2003 stand-alone CA to an enterprise CA.

Note

It is not possible to convert a root CA to a subordinate CA, or vice versa.

The first step in migrating the CA is backing up the existing key pairs used by the CA and its database. To backup the CA keys and database, right-click the CA node in the MMC and choose Back up CA under All Tasks.



Next, you must back up the certificate database, the CA certificate, and the CA private key. Select Private key and CA certificate and Certificate database and certificate database log, then choose the appropriate path for the backup files.

Note

The backup path should not contain old backup files. Use the command-line tool Certutil.exe if you want to overwrite old backup files.



Enter a strong password. This password is used to protect the CA's private key.

Important

Do not lose this password or you will not be able to restore the keys on the new CA.

Review the summary, and click Finish to complete the backup.



You have now successfully backed up the CA keys and database. Next, you should remove the stand-alone CA from the server by uninstalling it. Uninstall the CA by removing the Certificate Services from the Windows Components.



Join the computer to a domain in the forest if it is not already joined to one.

Best Practice The recommended best practice is to install CAs as a member of the root domain in the forest to provide centralized administration and control of the PKI services. For additional best practices, see the Windows Server 2003 Resource Kit.

Reinstall the CA by adding the Certificate Services to the Windows Components.



Select Enterprise root CA as the CA Type, and select custom settings for the key generation.

Note

You must be an Enterprise Admin to install an Enterprise CA.



Choose the CSP that has access to the old CA keys, and choose the same keys and certificate used with the old CA.

Note

If your CA has multiple keys, choose the original key used by the old CA. This can be determined by the number appended to the key where no number means oldest.



Select Preserve existing certificate database to use the old database. This enables the new Enterprise CA to keep track of any pending requests to the old stand-alone CA, as well as any certificates issued or revoked by it.



When prompted for stopping the IIS service, click Yes to finish the installation of the CA.

# Windows Server 2003 PKI and Role-Based Administration

Windows 2000 Server CA administration is changed significantly with Windows Server 2003 CA role-based administration. Windows 2000 Server administrators can perform any activity on a Windows 2000 Server CA, but once CA roles are assigned on a Windows Server 2003 CA, its administrators are subject to its roles. Administrators who could perform all tasks on a Windows 2000 Server CA will only be able to perform the tasks associated with their role on the Windows Server 2003 CA. After upgrading a Windows 2000 Server CA to a Windows Server 2003 CA, its administrators need to be assigned to the roles defined in the role-based administration for the Windows Server 2003 CA.

Windows Server 2003 was designed with the needs of organizations in mind to provide role-based administration of a public key infrastructure. Windows Server 2003 certification authorities were also designed to meet the role definitions defined in version 1.0 of Certificate Issuing and Management Components Family of Protection Profiles found at <http://csrc.nist.gov/pki/documents/CIMC_PP_20011031.pdf>

Role-based administration can be used to organize CA Administrators into separate, predefined task-based roles, each with its own set of tasks. Roles are assigned using each user's security settings. Roles are assigned to a user by assigning that user the specific security settings that are associated with the role. A user who has one type of permission, such as Manage CA permission, may perform specific CA tasks that a user with another type of permission, such as Issue and Manage Certificates permission, may not perform. Role-based administration is supported by both Windows Server 2003 enterprise and stand-alone certification authorities.

Role-based administration involves CA roles users and groups. To assign a role to a user or group, you must assign the role's corresponding security permissions, group memberships, or user rights to the user or group. These security permissions, group memberships, and user rights are used to distinguish which users have which roles. The following table describes the CA roles of role-based administration and the groups relevant to role-based administration.

|  |  |  |
| --- | --- | --- |
| Roles and Groups  | Security Permission  | Description  |
| CA Administrator | Manage CA permission | Configure and maintain the CA. This is a CA role and includes the ability to assign all other CA roles and renew the CA certificate. This is a separate role from the local Administrator role. |
| Certificate Manager | Issue and Manage Certificates permission | Approve certificate enrollment and revocation requests. This is a CA Officer role. |
| Backup Operator | Back up files and directories and Restore files and directories permissions | Perform system backup and recovery. This is an operating system role. |
| Auditor | Manage auditing and security log permissions | Configure, view, and maintain audit logs. This is an operating system role. |
| Enrollees | Authenticated Users | Enrollees are clients who are authorized to request certificates from the CA. This is not a CA role for the purposes of administration. |
| Read | All (except Enrollees)  | Allows an entity to read records from the database. |

With the default installation, all CA roles are assigned and modified by local Administrators on the machine, Enterprise Admins and Domain Admins (if joined to a domain). Local Administrators, Enterprise Admins and Domain Admins are CA Administrators by default on an Enterprise CA. Only local Administrators are CA Administrators by default on a stand-alone CA. If the stand-alone CA is joined to an Active Directory domain, Domain Admins are also CA Administrators.

The CA Administrator and Certificate Manager roles can be assigned to either Active Directory users or local users in the local Security Accounts Manager (SAM) database. As a best practice, it is recommended to assign roles to group accounts instead of individual user accounts. Only CA Administrator, Certificate Manager (as Officer in the CIMC), Auditor (as Auditor in the CIMC), and Backup Operator (as Operator in the CIMC) are CA roles. The other users described in the following table are relevant to role-based administration and should be understood before assigning CA roles.

Only CA Administrators and Certificate Managers are assigned using the Certification Authority Microsoft Management Console (MMC) snap-in. Other roles, users, and groups are specified in their related consoles. To change the roles of a user, you must change the user's security permissions, group membership, or user rights.

When key archival is configured on an enterprise CA running Windows Server 2003 Enterprise Edition, the subject obtaining a certificate from a CA will provide their private key to the CA. The CA stores that private key in its database until key recovery is desired. Only a Certificate Manager can get the encrypted private key blob out of the CA database, which is then passed on to key recovery agents (KRAs). For more information, see the Key Archival and Management in Windows Server 2003 white paper.

## Roles and Activities

Each CA role has a specific list of CA administration tasks associated with it. The following table lists all the CA administration tasks along with the roles in which they are performed. One of the most important distinctions is the local Administrator versus CA Administrator role. The local Administrator applies to the local operating system privilege which may be required to perform some tasks associated with the operations of the CA. The CA Administrator role applies only to specific tasks within the functionality of the CA. The local Administrator will always have full control of the system including the CA and cannot be blocked from taking control of the CA. Therefore, it is very important to keep this fact in mind when assigning operational and delegated roles to the CA for management purposes.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Activity | CA Administrator | Certificate Manager | Auditor | Backup Operator | Local Administrator | Notes |
| Install CA |   |   |   |   | X  |   |
| Configure policy and exit module | X  |   |   |   |   |   |
| Stop and start the Certificate Services service | X  |   |   | X (only stop) |   |   |
| Configure extensions | X  |   |   |   |   |   |
| Configure roles | X  |   |   |   |   |   |
| Renew CA keys and certificates |   |   |   |   | X  |   |
| Define key recovery agents | X  |   |   |   |   |   |
| Configure Certificate Managers restrictions | X  |   |   |   |   |   |
| Delete single row in database | X  |   |   |   |   |   |
| Delete multiple rows in database (bulk deletion) |   |   |   |   | X  |   |
| Enable role separation |   |   |   |   | X  |   |
| Issue and approve certificates |   | X  |   |   |   |   |
| Deny certificates |   | X  |   |   |   |   |
| Revoke certificates |   | X  |   |   |   |   |
| Reactivate certificates placed on hold |   | X  |   |   |   |   |
| Enable, publish, or configure CRL schedule | X  |   |   |   |   |   |
| Recover archived key |   | X  |   |   |   | Only a Certificate Manager can retrieve the encrypted key data structure from the database. The private key of a valid Key Recovery Agent is required to decrypt the key data structure and generate a PKCS#12 file. |
| Configure audit parameters |   |   | X  |   |   | By default, the local Administrator holds the system audit privilege. |
| Audit logs |   |   | X  |   |   | By default, the local Administrator holds the system audit privilege. |
| Back up system |   |   |   | X  |   | By default, the local Administrator holds the system backup privilege. |
| Restore system |   |   |   | X  |   | By default, the local Administrator holds the system restore (backup) privilege. |
| Read CA database | X  | X  | X  | X  | X  | By default, the local Administrator holds the system audit and backup privileges. |
| Read CA configuration information | X  | X  | X  | X  | X  | By default, the local Administrator holds the system audit and backup privileges. |

Note

By default, enrollees are allowed to read CA properties and certificate request lists (CRLs), and can request certificates. On an Enterprise CA, a user must also have Read and Enroll permissions on the certificate template to request a certificate. CA Administrators, Certificate Managers, the Auditor, and Backup Operators have implicit Read privileges on the CA. An Auditor is based on a user that holds the system audit privilege. The local Administrator by default on each machine always holds the system audit privilege. If role separation is enabled, a separate user must be configured to hold the system audit privilege.> A Backup Operator is based on a user that holds the system backup privilege. In addition, the Backup Operator has the ability to stop the Certificate Services service (but not start it). As many or as few roles may be configured and used. It is not necessary to define all roles if only one specific role is assigned to a security group. It is required to have both CA Administrator and CA Manager roles to do bulk deletion, so any person who has both the roles will be able to perform bulk deletion. If role separation is enabled, this feature is not available. For issuing failed requests, it is required to have both CA Administrator and CA Manager permissions. If role separation is enabled, this feature is not available.

## Assigning Roles

The CA Administrator for a CA assigns users to the separate roles of role-based administration by giving each user the security settings required by a role. The CA Administrator can assign a user to more than one role, but the CA is more secure when each user belongs to one role only. When each CA role belongs to one user only, fewer CA tasks can be compromised if a user's account becomes compromised.

The default installation setting for a stand-alone CA is to have members of the local Administrators security group as CA Administrators. The default installation setting for an Enterprise CA is to have local Administrators, Enterprise Administrators, and Domain Administrators as CA Administrators. To limit the power of any of these accounts, they should be removed from the CA Administrator and Certificate Manager roles once all CA roles are assigned; and they should also be removed from the Administrators group on the CA machine if it is not a Domain Controller. To list the roles a current user holds with a given CA, see the sample script in Appendix A.

Best Practice As a best practice, group accounts that have been assigned CA Administrator or Certificate Manager roles should not be members of the local Admin security group. Also, CA roles should only be assigned to group accounts and not individual user accounts.

Note

Membership in the local Administrators group on the CA is required to renew the CA certificate. Members of this group are considered to be all powerful on the CA with administrative authority over all other CA roles.

# Role Separation

The separation of CA roles can be enforced using role separation. Once enforced, role separation only allows a user to be assigned a single role. If a user is assigned to more than one role and attempts to perform an operation on the CA, the operation is denied. For this reason, before role separation is enabled, a user should be assigned only one CA role. This feature is valuable for large enterprises where the separation of roles ensures that the compromise of a user's account does not compromise the entire CA administered by the user.

Important

Before role separation is enabled, each user assigned a CA role on the CA must only be assigned a single CA role on that CA. If a user is assigned more than one CA role, when role separation is enabled, the Certificate Services service will detect that a user has more than one role and deny the user's attempts to operate the CA.

Only members of the local Administrators security group on a CA can enable and disable role separation. Enabling role separation requires editing the registry of the Windows Server 2003 Enterprise Edition running the Certificate Services service. Once this registry setting is edited to enable role separation, any assigned roles are in effect until the local Administrator of the server disables role separation through the registry. CA roles can be assigned and changed by the CA Administrator while role separation is enabled or disabled. While role separation is enabled, the CA Administrator cannot assign a user to more than one CA role. If the CA Administrator attempts to assign a user to a second CA role, the operation is refused.

Important

It is possible for a user assigned a role to become locked out of administering a CA when role separation is enabled if the user is also assigned to a second CA role. If the CA Administrator is assigned to a second role, or assigns another role holder to a second role, the CA Administrator violates the rules of role separation by allowing a user to have two roles. Once the user is assigned to two roles, role separation will not allow that user to perform any activity on the CA, including, in the case of the CA Administrator, the activity of removing himself from one of the roles.

To correct this configuration, the local Administrator of the server must disable role separation, remove the CA Administrator from the second role, and then restart the Certificate Services service. Following these steps, role separation can be enabled again.

## Windows 2000 and Windows Server 2003 Role-Based Administration

During the upgrade from a Windows 2000 CA to a Windows Server 2003 CA, Windows 2000 CA permissions are upgraded to Windows Server 2003 CA roles according to the rules in the following table.

|  |  |
| --- | --- |
| Windows 2000 Permission | Windows Server 2003 Role or Permission |
| Manage CA permission | CA Administrator and Certificate Manager |
| Revoke Certificate permission | Certificate Manager |
| Approve/Issue Certificate permission | Certificate Manager |
| Enroll permission | Enroll permission |
| Read permission | Read permission |
| All other permissions listed in the Windows 2000 CA advanced security settings | Read permission |

Note

You can assign certification authority roles for role-based administration on servers running any version of the Windows Server 2003 family, but you can only enable role separation on servers running Windows Server 2003 Enterprise Edition and Windows Server 2003 Datacenter, including the 64-bit version of Windows Server 2003 Enterprise Edition and 64-bit version of Windows Server 2003 Datacenter.

To enable role separation, open a command prompt window and type

|  |
| --- |
| certutil -setreg ca\RoleSeparationEnabled 1  |

The Certificate Services service must now be stopped and started.

To stop and start the Certificate Services service, at the command prompt, type

net stop certsvc

net start certsvc

To disable role separation, open a command prompt and type

certutil -delreg ca\RoleSeparationEnabled

Again, the Certificate Services service must be stopped and started.

To display the role separation setting, at the command prompt, type

certutil -getreg ca\RoleSeparationEnabled

The following command will display all CA information including CA role separation status:

Certutil.exe –cainfo

## Role Separation Validation

All role operations are performed through the ICertAdminD DCOM interface once the CA is configured into role separation mode. Role separation may not be enabled nor enforced when role assignments are made. Role separation validation is only enforced when a person (administrator, operator, and so on) performs an action. Role separation enforcement rules are stored and read by the CA in the registry as binary blobs. Each role is defined as a bit (allow/deny). For more information about this interface, see the Platform SDK in MSDN.

## Certificate Managers

The capability of Certificate Managers is supported to prevent a CA Officer from issuing certificates to everyone. This is implemented through an authorization callback and is stored in a virtual Security Descriptor in the registry of the CA. A second access check is performed on the Officer role to validate what user(s) and group(s) they manage (approve and revoke certificates). The GUI for each Certificate Manager has a list of users and groups that the Officer can approve, revoke, and so on.

If an Officer attempts to approve a request for a user to which the Officer is not authorized to manage, an access denied error will occur. This does not reject the request or remove it from the pending approval queue. In addition, a new user or group may be added to the Certificate Managers authorized list AFTER the certificate request has been made.

## Backup/Restore and Auditing under Role Separation

When you enable Role Separation, members of the local Administrators group, including the local Administrator account, will not be able to back up or restore the CA, nor will they be able to enable auditing on the CA. Because Administrators have the permission to back up and restore the CA as well as enable auditing on the CA, the CA will not allow them to do any tasks because they are assigned multiple roles.

To assign the backup permission to another user, either add the user to the local Backup Operators group, or assign the user the Backup files and directories privilege in the Local Security Policy snap-in under User Rights Assignment. To assign the restore permission to another user, either add the user to the local Backup Operators group, or assign the user the Restore files and directories privilege in the Local Security Policy snap-in under User Rights Assignment. To give the permission needed to enable auditing, assign the user the Manage auditing and security log in the Local Security Policy snap-in under User Rights Assignment.

Note

You may need to refresh the local security policy by typing gpupdate.exe at the command prompt. To open the Local Security Policy, type secpol.msc at the command prompt.

# CA Auditing

Auditing certification authority (CA) operations is supported for Windows Server 2003 Enterprise Edition. The audit events will be logged in the Security log and can be viewed using the Event Viewer utility. CA auditing is dependent on system object access auditing, and therefore, it is necessary for the system administrator to first enable object access auditing on the target system.

CA auditing is enabled by selecting which group of CA operations to audit in the MMC snap-in. The following sections describe each group of CA operations that can be audited.

## CA Audit Groups

The following group of events can be configured to be audited:

 Back Up and Restore the CA Database

 Change CA Configuration

 Change CA Security Settings

 Issue and Manage Certificate Requests

 Revoke Certificates and Publish CRLs

 Store and Retrieve Archived Keys

 Start and Stop Certificate Services

## Back Up and Restore the CA Database

By enabling auditing on this group, successful or failed attempts to back up the CA database will be logged to the system Security log. In addition, the CA service will detect on restart that the CA database has been restored. The restore events are logged to the system Security log.

## Change CA Configuration

By enabling auditing on this group, successful or failed attempts to change CA configuration will be logged to the system Security log. This includes the following operations:

 Add/Remove Templates to the CA

 Configure the CRL Publication Schedule

 Modify Request Disposition for the Policy Module

 Modify Publish Cert Flags for the Exit Module

 Configure CRL Distribution Points (CDP)

 Configure Authority Information Access (AIA)

 Change the Policy Module

 Change the Exit Module

 Configure Key Archival and Recovery (KAR)

## Change CA Security Settings

By enabling auditing for this group, successful or failed attempts to change CA security settings will be logged to the system Security log. This includes the following operations:

 Configure CA Roles for Role-Based Administration of the CA

 Configure Restrictions on Certificate Managers

 Configure CA Auditing

## Issue and Manage Certificate Requests

By enabling auditing for this group, successful or failed attempts to issue and manage certificate requests will be logged to the system Security log. This includes the following operations:

 Incoming Certificate Requests

 Certificate Issuance

 Certificate Import

 Deletion of Rows in the CA Database

## Revoke Certificates and Publish CRLs

By enabling auditing for this group, successful or failed attempts to revoke certificates and publish CRLs will be logged to the system Security log. This includes the following operations:

 Certificate Revocation

 CRL Publication

## Store and Retrieve Archived Keys

By enabling auditing for this group, successful or failed attempts to store and retrieve archived keys will be logged to the system Security log. This includes the following operations:

 Archival of Subject Keys

 Retrieval of Subject Keys

## Start and Stop Certificate Services

By enabling auditing for this group, successful or failed attempts to start and stop Certificate Services will be logged to the system Security log. This includes the following operations:

 Starting Certificate Services

 Stopping Certificate Services

# Setting Up CA Auditing

CA auditing depends on system object access auditing to be enabled. Therefore, to set up CA auditing for a system, a system administrator will have to

1. Enable Object Access Auditing on the system.

2. Enable auditing for the CA by selecting which group of events to audit in the MMC snap-in.

The following sections describe these steps in detail.

## Enabling Object Access Auditing

### When the CA Is on a Domain Controller

To enable object access auditing when the CA is on a Domain Controller (DC)

|  |
| --- |
| 1. Select Start > Programs > Administrative Tools > Domain Controller Security Policy.2. Expand Default Domain Controllers Security.3. Expand Computer Configuration.4. Expand Windows Settings.5. Expand Security Settings.6. Expand Local Policies.7. Select Audit Policy.8. Right-click Audit object access and select Properties.9. Check Define these policy settings.10. Check Success and Failure under Audit these attempts.11. Click OK. |

### When the CA Is on a Member or a Workgroup Server

To enable object access auditing when the CA is on a member or a workgroup server

|  |
| --- |
| 1. Select Start > Programs > Administrative Tools > Local Security Policy.2. Expand Local Policies.3. Select Audit Policy.4. Right-click Audit object access and select Properties.5. Check Success and Failure under Audit these attempts.6. Click OK. |

### Enabling Auditing on the CA

To enable auditing of the CA

|  |
| --- |
| 1. Open the MMC snap-in.2. Right-click the CA and select Properties.3. Click the Audit tab.4. Check which groups of CA operations to audit.5. Click OK. |

# Auditing and Event Management

## Event IDs Used by Certificate Services

The following event IDs are currently used by Certificate Services:

772. The Certificate Manager denied a pending certificate request.

773. Certificate Services received a resubmitted certificate request.

774. Certificate Services revoked a certificate.

775. Certificate Services received a request to publish the certificate revocation list (CRL).

776. Certificate Services published the certificate revocation list (CRL).

777. A certificate request extension changed.

778. One or more certificate request attributes changed.

779. Certificate Services received a request to shut down.

780. Certificate Services backup started.

781. Certificate Services backup completed.

782. Certificate Services restore started.

783. Certificate Services restore completed.

784. Certificate Services started.

785. Certificate Services stopped.

786. The security permissions for Certificate Services changed.

787. Certificate Services retrieved an archived key.

788. Certificate Services imported a certificate into its database.

789. The audit filter for Certificate Services changed.

790. Certificate Services received a certificate request.

791. Certificate Services approved a certificate request and issued a certificate.

792. Certificate Services denied a certificate request.

793. Certificate Services set the status of a certificate request to pending.

794. The Certificate Manager settings for Certificate Services changed.

795. A configuration entry changed in Certificate Services.

796. A property of Certificate Services changed.

797. Certificate Services archived a key.

798. Certificate Services imported and archived a key.

799. Certificate Services published the CA certificate to Active Directory.

800. One or more rows has been deleted from the certificate database.

801. Role separation enabled.

### Breakdown of Shared Event IDs

##### 796:

Property: 29

Index: 0

Type: 4

Adding/removing template to/from CA. Value is list of resulting

templates by name and object identifier.

Property: 26

Index: <KRA cert index>

Type: 3

Adding KRA cert to CA. Value is Base64 representation of the

certificate.

Property: 25

Index: 0

Type: 1

Removing KRA certificate from CA. Value is the total KRA certificate count. For example, you can add 7 KRA cert to CA but configure it to use 3 only. In this case, the property 25 (CR\_PROP\_KRACERTCOUNT) will be 7 and the property 24 (CR\_PROP\_KRACERTUSEDCOUNT) will be 3.

Property: 24

Index: 0

Type: 1

Adding/removing number of KRA certificates to use for key archival. Value is resulting number of certificates to use. A value of 0 indicates that KAR is disabled. For example, you can add 7 KRA cert to CA but configure it to use 3 only. In this case, the property 25 (CR\_PROP\_KRACERTCOUNT) will be 7 and the property 24 (CR\_PROP\_KRACERTUSEDCOUNT) will be 3.

##### 795:

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\_MicrosoftDefault.Policy

Entry: RequestDisposition

Value: 1

Set CA to issue incoming requests unless specified otherwise.

Node: PolicyModules\CertificateAuthority\_MicrosoftDefault.Policy

Entry: RequestDisposition

Value: 257

Set CA to keep incoming requests pending.

Node: ExitModules\CertificateAuthority\_MicrosoftDefault.Exit

Entry: PublishCertFlags

Value: 1

Allow certificates to be published to the file system.

Node: ExitModules\CertificateAuthority\_MicrosoftDefault.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.

Node:

Entry: CACertPublicationURLs

Change in AIAs or CDPs. Value specifies resultant set of AIAs.

## CA Audit Specification

The following tables provide more information about the data contained in the CA audit events.

Certificate Request Events

|  |  |
| --- | --- |
| Audit Event | Audit Data |
| Certificate Request Submission | Request IDUPN of Requestor |
| Certificate Request Processing | Request IDDistinguished Name of SubjectResult of Processing (Issue, Pend, or Deny) |
| Certificate Issuance | Request IDCertificate Serial NoHash of CertificateCertificate Template and VersionSequence Number from CSP |
| Certificate Publication | Request IDDistinguished Name of Object UpdatedDC NameCertificate Serial No |
| Certificate Revocation | Certificate Serial NoTime for RevocationReason for Revocation |
| Key Archived | Request IDUPN of RequestorList of Hashes of Recovery Agents Certificate(s) |

Certificate Management Audit Events

|  |  |
| --- | --- |
| Audit Event | Audit Data |
| Certificate Revocation Request | Issuer Name and Serial No of Signing Certificate (if signed)Revocation ReasonUPN of Certificate Manager |
| Request Resubmission | Request IDUPN of Certificate Manager |
| Denied Request | Request IDUPN of Certificate Manager |
| Certificate Import | Request IDUPN of Certificate Manager |
| Archived Key Retrieval | Request IDCertificate Serial NumberHash of Encrypted BlobUPN of Certificate Manager |

CA Administration Audit Events

|  |  |
| --- | --- |
| Audit Event | Audit Data |
| Service Start or Stop | Hash of the Certificate Services Database DirectoriesHash of the Database Log DirectoriesList of All Hashes of the Certificate Services CertificatesSequence Number from CSP |
| CA Certificate Renewal Request | URN of RequestorSKI |
| CA Certificate Installation | UPN of InstallerHash of CertificateIssuer NameAKISKI |
| CRL Creation and Publication | CRL TypeAKIHash of CRLBase and/or Delta CRLCRL This UpdateCRL Next updateURL Used to PublishSKI (Identifier of CA)UPN of Service Manager |
| Configure CRL Publication Policy | List of All CRL Policies EntriesUPN of Service Manager |
| Selecting Policy Module | Name of Active Policy Module (relative registry path)UPN of Service Manager |
| Selecting Exit Module | Name of Active Exit Module (relative registry path)UPN of Service Manager |
| Configure Policy Module | Name of Policy ModuleConfiguration Entry NameNew Configuration Entry ValueUPN of Service Manager |
| Configure Exit Module | Name of Exit ModuleConfiguration Entry NameNew Configuration Entry ValueUPN of Service Manager |
| Certificate Template Update | Template NameTemplate Major and Minor Version NosList of Template AttributesUPN of Service Manager |
| Key Archive Policy Change | Subject Name of Key Recovery Agent CertificateHash of Key Recovery Agent CertificateNumber of Key Recovery Agent Certificates UsedUPN of Service Manager |
| Data Base Row Deletion | TableRowUPN of Service Manager |
| Configure Certificate Managers Restrictions | Enable/Disable RestrictionsUPN of Each Certificate Manager, List of Users to Manage, Type of ACE(Allow/Deny)UPN of Service Manager |
| Configure CA Security | UPN of Each User, Control Access Type, Type of ACE(Allow/Deny)UPN of Service Manager |
| Configure CDP | List of All CDPsUPN of Service Manager |
| Configure AIA | List of All AIAsUPN of Service Manager |

Backup/Restore Events

|  |  |
| --- | --- |
| Start Service Backup | UPN of OperatorBackup TypeBackup Set IDData Integrity Check On\Off |
| Finish Service Backup |   |
| Cancel Service Backup |   |
| Start Service Restore | UPN of OperatorRestore TypeBackup Set IDData Integrity Check On\Off |
| Finish Service Restore | Integrity Check OK (if integrity checking on) |
| Cancel Service Restore | UPN of Operator |

Audit Events

|  |  |
| --- | --- |
| Audit Filter Change | Value of New Audit FilterUPN of Auditor |

# CA Maintenance

Setting up the PKI is a small step compared to the management and operational tasks that are associated with the public key infrastructure.

## CA Remote Maintenance

A CA that is connected to the network can be maintained locally or through a remote connection; however, the CA maintenance and administration tools are best designed for local operation. This is because the CA administration is a sensitive operation and should be kept as secure as possible.

If the Certificate Services MMC Snap-In should be used for remote administration, see Users Allowed to Manage the CA Cannot Access It Remotely [271470] to take the appropriate steps to make the CA remotely accessible.

Even if it is technically possible, a CA should not be maintained through a Terminal Server session because it increases the attack spectrum, and because some administration tools—like certutil.exe—do not work properly if used in a Terminal Server session.

Note

A Windows 2000 CA may not be managed using the Windows Server 2003 version of the Certification Authority MMC snap-in, or vice-versa.

### Publish the CRL of an Offline CA

The actual offline CRL publication should be performed at a minimum of several days before the actual expiration of the previously issued CRL. This should be performed to provide a safety factor in case the offline root CA has a hardware or publication failure. Adequate time should be allotted to ensure that any errors or failures can be corrected and to enable actual publication and replication of the CRL to all CDP locations.

Once the CDP extensions have been updated on the CA, new CRL(s) should be published so that all clients who download the CRL have the latest download information (for example, Delta CRL URL).

To manually publish a CRL on an offline CA

|  |
| --- |
| 1. Select the Revoked Certificates node of the certification authority MMC snap-in.2. Right-click, select All Tasks, and then click Publish.A new base and delta (if configured) CRL will be published.ws03pkog09A prompt will be displayed asking to confirm which type(s) of CRL(s) should be published with this request. Since only base CRLs are being published from the offline root CA, only the New CRL option will be available.3. Click OK.ws03pkog104. Root CA certificates may be published manually to Active Directory using the Windows Server 2003 version of the certutil.exe –dspublish command from the command line if logged in as an account that is a member of the Enterprise Admin Group or a domain admin from the root (first) domain in the forest.The equivalent command in Windows 2000 is called dsstore.exe. For more information about pushing CA certificates manually into Active Directory, see the following Knowledge Base article: HOW TO: Use the Directory Services Store Tool to Add a Non-Windows 2000 Certification Authority (CA) to the PKI in Windows 2000 [[313197](http://support.microsoft.com/default.aspx?scid=kb;en-us;313197&sd=tech)] |

### CRL Re-Sign

In some scenarios, it may not be possible to publish a CRL from an offline CA. In this case, with Windows Server 2003, the old CRL may be re-signed without using the certification authority. This process assumes the availability of the CA private key(s) outside of the CA to actually sign the CRL. To update an expiring CRL, the old CRL file will need to be retrieved first. It will be available in Active Directory if the CA is an Enterprise CA or if Active Directory was accessible when the CA was installed, or in the %windir%\System32\CertSrv\CertEnroll directory on the CA machine itself.

The simple syntax for re-signing a CRL is

certutil -sign <existing CRL file name> <resigned CRL file name>

You can also add or remove serial numbers, or remove extensions, or change the length of time the CRL will be valid through the certutil.exe –sign command.

The default is to re-sign the CRL to be valid starting 10 minutes prior to the signature (to allow for clock skew), and a lifetime (NextUpdate) equal to the old CRL. Use the following command to publish the CRL to Active Directory. Certutil will state whether the object in Active Directory was updated or if it was already up-to-date.

certutil -dspublish <resigned CRL file name>

Publishing to a file://, ftp:// or an http:// location can be done by copying the CRL file manually to that location. The following command executed on the CA machine should display the next time the CA expects to wake up and publish the next CRL:

certutil -getreg ca\CRLNextPublish

Dumping the CRL with the certutil command will display the 1.3.6.1.4.1.311.21.4 (Next CRL Publish) extension, which should be equivalent to the CRLNextPublish registry value (but the syntax of the two displays is different). Certutil -sign strips this extension out of re-signed CRLs, because the next issue date is misleading at best after re-signing. Dumping a certificate issued by the CA with the certutil command will display the ldap:///, http://, and file:// URLs where the CRL is stored.

### Administrative Process for Offline CRL Publication

The following is a sample process outline that may be followed for publishing an offline CA's CRL:

Several days before the current CRL is due to expire, the offline Root CA system is removed from its protected location (usually in secured storage such as double-locked closet, combination safe, or other physically well-protected locations); normally two or more staff are present (for example, one IT administrator as well as a supervisory manager).

The root CA machine is powered up and logged on with an account with appropriate permissions.

The MMC is started and the CA's CRL is published to the local drive.

The CRL is copied to a disk or other removable media.

The offline Root CA server is logged out and shut down, and placed into a secured storage.

The removable media is taken to the publishing or staging servers, and the CRL is copied to the appropriate location(s), according to the current CDP locations published in non-expired certificates from the CA.

Important

It is extremely important for administrators to perform regular (test) restores of their offline CAs to see if the procedure for backup/restore performs as expected. Disaster recovery procedures and testing are paramount in operating a public key infrastructure.

## Certification Authority Renewal

### Best Practices for Renewing CAs

Certification authorities are renewed or replaced for a multitude of reasons. The following are the most common reasons for CA renewal:

 Increase the lifetime of the CA

 Change the key used by the CA

 Increase the key size of the CA

 Add certificate policies to the CA (qualified subordination)

 CRL partitioning

The first three reasons may be performed by using a capolicy.inf file when renewing the CA. If renewing a root CA, it is important to understand that the root CA certificate will need to be re-distributed to all clients that will trust the root CA. Otherwise, existing clients will only be aware of the exiting root CA certificate and will have no mechanism for discovery of the renewal event.

When a CA is renewed, various objects and attributes will be updated or changed. If the CA is an Enterprise root or subordinate CA, the following objects in Active Directory will be updated:

The updated CA certificate (cACertificate) and cross-certificate (CrossCertificatePair if renewal with a new key pair is performed) will be published to the AIA container.

A new CRL will be published for every key pair the CA has used.

The new certificate will be published to the NTAUTH object.

The new certificate will replace the existing certificate in the enrollment services container.

Note

If the enrollment services container had been previously deleted, it will be replaced on renewal and the default templates will be re-installed as well, if they have been deleted.



### CRL Partitioning

CRL partitioning is another main reason why administrators often renew an issuing CA. When a CA is renewed with a new key, a new key and certificate are generated for that CA. When a new key and certificate are generated, the CA will use the new key as well as any unexpired previous keys corresponding to previous certificates when generating revocation information. Therefore, a CA may be using multiple keys at the same time and will publish multiple CRLs corresponding to those keys. This may be seen in the Certification Authority MMC snap-in by selecting the CA properties.



The renewal status of the CA may also be determined by examining the CA certificate itself. The CA version extension will identify how many times a CA has been renewed and how many times with a new key. In this case, the CA has been renewed three times and with each instance, a new key, hence the 3.3 version number as displayed in the following screen.



Once a CA has been renewed with a new key, only the new key will be used in signing new certificates. The unexpired previous key(s) will continue to be used to sign CRLs for certificates that were signed using the previous keys. Therefore, a CA may publish multiple CRLs at the same time, each using a different key. This method of CA renewal may be an ideal method for CRL size control and effective CRL partitioning using the Microsoft CA.

### Automatic RootCA Cross-Certificate Generation

Windows Server 2003 has introduced the capability for Microsoft root certification authorities with access to Active Directory to automatically issue and publish a cross-certificate for a root CA that has been renewed. For example, when a Windows Server 2003 root CA is renewed with a new key, the root will cross-certify the renewed root CA certificate as being a qualified subordinate to the old root CA certificate. For more information about qualified subordination, see the Planning and Implementing Qualified Subordination for Using Windows Server 2003 Enterprise Server white paper.

This functionality is especially important to customers who have had an existing root CA trusted by other organizations, bridge CAs, or cross-certified by other organizations. To configure or disable this functionality, the following commands may be performed on the root CA.

 To force the root CA to use the CrossCA certificate template, the following command should be run. Otherwise, without this flag, the CA will never use the CrossCA certificate template (even if it is available), and will fall back to generating a certificate without the template, using predefined extensions:

|  |
| --- |
| certutil -setreg ca\CRLFlags +CRLF\_USE\_CROSS\_CERT\_TEMPLATE  |

 To disable automatic CrossCA certificate generation, run the following command:

|  |
| --- |
| certutil -setreg ca\CRLFlags +CRLF\_DISABLE\_ROOT\_CROSS\_CERTS  |

 To enable automatic CrossCA certificate generation again, run the following command:

|  |
| --- |
| certutil -setreg ca\CRLFlags -CRLF\_DISABLE\_ROOT\_CROSS\_CERTS  |

 To force the root CA to use the CAExchange certificate template when generating CA encryption certificates on demand, run the following command. Without this flag, the CA will use the CAExchange cert template when available, and fall back to generating a certificate without the template, using predefined extensions.

|  |
| --- |
| certutil -setreg ca\CRLFlags +CRLF\_USE\_XCHG\_CERT\_TEMPLATE  |

### Key Backup

If you are using a smartcard or other hardware key and the machine fails, you will need to move the smartcard or key device to another machine, install the CA certificate, and possibly add the KeyProvInfo property to the CA certificate, so the private key's CSP and container name, and so on, will be available. This may be accomplished using the certutil.exe –repairstore command (see below). This is usually done automatically when a smart card is inserted into a reader.

If you are using a software-based CSP and the machine fails, it is necessary to use the certutil -backupkey command prior to the hardware failure to save the CA's keys and certificates in a PFX file (PKCS #12) encrypted with a password, and use certutil -restorekey on the second machine.

To add the KeyProvInfo property, use the following command. Include the -user option if the certificate may have been imported into the HKEY\_CURRENT\_USER personal store.

|  |
| --- |
| certutil -repairstore my CACertSHA-1Hash  |

or

|  |
| --- |
| certutil -repairstore -user my CACertSHA-1Hash  |

If necessary, dump the certificate with certutil.exe –dump <file name> to display the SHA-1 certificate hash.

## Backup/Recovery

Best practice Backing up the certification authority database, the CA certificate, and the CA keys is essential to protect against the loss of critical data. The CA should be backed up on a regular basis (daily, weekly, monthly) based on the number of certificates issued over the same interval. The more certificates issued, the more frequently the CA should be backed up.

For additional information, see the Microsoft Knowledge Base:

Certificate Server Does Not Create Backups of Installed Keys [[216922](http://support.microsoft.com/default.aspx?scid=kb;en-us;216922&sd=tech)] (This article applies to Windows 2000 only.)

## Removing a CA from Active Directory

Removing a CA from any public key infrastructure or Active Directory environment may have a significant impact on applications and services. Therefore, careful planning is always recommended before removing a CA. Always perform a complete backup and maintain that backup for a period of time should a restore be required at a later date.

### Uninstalling an Enterprise Certification Authority

To decommission a root certification authority, all outstanding certificates issued by that CA should be revoked. After revocation, the Certificate Revocation List (CRL) should be published.

1. Revoke all issued certificates.

 Start the Certification Authority MMC snap-in.

 Click the Issued Certificates folder.

 Highlight one of the issued certificates, and then press CTRL+A to select all issued certificates.

 Right-click the highlighted certificates, select All Tasks, and then click Revoke Certificate.

 In the Certificate Revocation dialog box, select Cease of Operation as the reason for revocation.

 Click OK.

2. Increase the CRL publication interval.

 In the Certification Authority MMC snap-in, right-click the Revoked Certificates folder.

 Select Properties.

 Increase the Publication Interval to a suitably long value (5 years).

 The lifetime of the CRL should be longer than the remaining lifetime of the certificates that have been revoked.

 Clear the Publish Delta CRLs check box if it is selected.

 Click OK.

3. Publish the new CRL.

 In the Certification Authority MMC snap-in, right-click the Revoked Certificates folder.

 Select All Tasks, and then select Publish.

 Choose New CRL as the type of CRL to publish.

 Click OK.

4. Stop Certificate Services.

 At the command prompt, type

|  |
| --- |
| certutil –shutdown |

5. List all the key stores for the local computer.

 At the command prompt, type

|  |
| --- |
| certutil –key |

This will display the names of all the installed Cryptographic Service Providers (CSP) and the key stores associated with each provider. Among the listed key stores, you will see the name of your CA listed several times. The following is the sample output.

|  |
| --- |
| Microsoft Strong Cryptographic Provider:  Enterprise Root CA  AT\_SIGNATURE  Enterprise Root CA(11)  AT\_SIGNATURE  Enterprise Root CA(13)  AT\_SIGNATURE  Enterprise Root CA(4)  AT\_SIGNATURE  Enterprise Root CA(14)  AT\_SIGNATURE  Enterprise Root CA(9)  AT\_SIGNATURE  Enterprise Root CA(7)  AT\_SIGNATURE  Enterprise Root CA(6)  AT\_SIGNATURE  MS IIS DCOM Server  AT\_SIGNATURE, AT\_KEYEXCHANGE  Enterprise Root CA(2)  AT\_SIGNATURE  Enterprise Root CA(12)  AT\_SIGNATURE  Enterprise Root CA(16)  AT\_SIGNATURE  Enterprise Root CA(1)  AT\_SIGNATURE  Microsoft Internet Information Server  AT\_SIGNATURE, AT\_KEYEXCHANGE  Enterprise Root CA-Xchg(7)  AT\_KEYEXCHANGE  Enterprise Root CA(5)  AT\_SIGNATURE  Enterprise Root CA(8)  AT\_SIGNATURE  Enterprise Root CA(15)  AT\_SIGNATURE  Enterprise Root CA(3)  AT\_SIGNATURE  |

6. Delete the private keys associated with the CA.

 At the command prompt, type

|  |
| --- |
| certutil –delkey <CA Name>  |

If your CA name contains spaces, enclose it in quotation marks.

Note

Repeat this step for all the key containers of your CA. You will need to do this if your CA has multiple certificates.

7. List the key stores again to verify that the private key for your CA has been deleted.

8. Use Add or Remove Programs to uninstall Certificate Services.

### Active Directory Objects

When Microsoft Certificate Services is installed on a server that is a member of a domain, several objects are created in the Configuration container in Active Directory. These objects are

 certificateAuthority object

 Located in CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=

 Contains the CA certificate for the Certification Authority

 Published Authority Information Access location

 crlDistributionPoint object

 Located in CN=<servername>,CN=CDP,CN=Public Key Service,CN=Services,CN=Configuration,DC=

 Contains the CRL periodically published by the certification authority

 Published CRL Distribution Point location

 certificationAuthority object

 Located in CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=

 Contains the CA certificate for the certification authority

 pKIEnrollmentService object

 Located in CN=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration,DC=

 Created by Enterprise CAs. Contains information about the types of certificates the CA has been configured to issue. Permissions on this object can control which users are allowed to enroll against this CA.

 msPKI-PrivateKeyRecoveryAgent object

 Located in CN=KRA,CN=Public Key Services,CN=Services,CN=Configuration,DC=

 Contains the Key Recovery Agent certificate(s)

When the CA is uninstalled, only the pKIEnrollmentService object is removed. The other objects are left in place because there are likely still outstanding certificates issued by the CA. In order for clients to successfully process these outstanding certificates, they need to locate the AIA and CDP paths in Active Directory. Good practice is to revoke all outstanding certificates (Reason: Cease of Operation), extend the lifetime of the CRL, and publish it in Active Directory. When those outstanding certificates are processed by the various clients, validation should fail and those certificates will not be used.

If maintaining the CDP and AIA in Active Directory is not a priority, these objects can be safely removed.

To remove all Certification Services objects from Active Directory

|  |
| --- |
| 1. Start Active Directory Sites and Services.2. Click the View menu option, and select Show Services Node.3. Expand the Services, and then expand Public Key Services.4. Select the AIA node.5. In the right-hand pane, locate the certificateAuthority object for your Certification Authority. Delete the object.6. Select the CDP node.7. In the right-hand pane, locate the Container object for the server where Certification Services is installed. Delete the container and the objects it contains.8. Select the Certification Authorities node.9. In the right-hand pane, locate the certificateAuthority object for your Certification Authority. Delete the object.10. Select the Enrollment Services node.11. In the right-hand pane, verify that the pKIEnrollmentService object for your Certification Authority was removed when Certificate Services was uninstalled. If not, delete it.12. Select the Certificate Templates node.13. In the right-hand pane, delete all the Certificate Templates.caution_ddCaution Delete all the Certificate Templates only if no other Enterprise CAs are installed in the forest. If the templates are inadvertently deleted, restore the templates from backup.14. Click the Public key Services node and locate the NTAuthCertificates object.15. If there are no other Enterprise or Stand-alone CAs installed in the forest, delete the object, otherwise leave it alone. |

### CA Database

When Certification Services is uninstalled, the CA database is left intact in case the CA is to be recreated on another server.

To remove the CA database

|  |
| --- |
|  Delete the %systemroot%\system32\certlog folder. |

### Domain Controller Cleanup

Once the CA has been taken down, the certificates that have been issued to all the domain controllers need to be removed. This can be done quite easily using DSSTORE.EXE from the Resource Kit.

To remove old domain controller certificates

1. At the command prompt on a domain controller, type

|  |
| --- |
| certutil -dcinfo deleteBad  |

2. Certutil.exe will attempt to validate all the DC certificates issued to the domain controllers. Certificates that fail to validate will be removed.

At this point, you can reinstall Certificate Services. After the installation is finished, the new root certificate will be published to Active Directory. When the domain clients refresh their security policy, they will automatically download the new root certificate into their trusted root stores.

To force application of the security policy

 At the command prompt, type

|  |
| --- |
| gpupdate /target:computer  |

## Best Practices for CRLs

### Certificate Revocation List Defaults

Certificates that are revoked prior to expiration will remain in a published base CRL for one full base CRL period (defined by CA) after they expire. Certificates that expire will no longer be included in published CRLs after one additional base CRL is expired.

Note

The CRL table for the CA can be exported and converted to a tab-separated file for Microsoft Excel or other programs using the following commands:

certutil –view <name of CRL file> > crl.txt

The following registry setting may be enabled on a CA to ensure that revoked certificates that have now expired are not removed from the CRL. Although most applications do not check CRLs for certificates that have expired, it is sometimes desirable in specific scenarios to maintain a public list of signing certificates that have been revoked.

To enable this option on the CA, use the following command:

certutil –setreg ca\CRLFlags +CRLF\_PUBLISH\_EXPIRED\_CERT\_CRLS

### Application Reliability

Many applications rely on the availability of the certificate revocation list (CRL) and will fail completely should the CRL be inaccessible or out of date. One such example is the smartcard logon process. During smartcard logon, the client validates the domain controller certificate and the domain controller validates the user (client) certificate. If either validation fails, the smartcard logon process will fail. Therefore, it is highly desirable to keep the following best practices in mind when publishing CRLs:

1. The CRL should be valid for a reasonable period of time that would allow recovery of the CA should hardware or software failures occur. For example, a one-hour CRL publication period is most likely not adequate time to perform a hardware or software restoration in case of failure.

2. Set a reasonable CRL overlap period to dampen and overcome CRL publication or replication issues. For CRL overlap settings, see the next section. The CRL schedule for frequently publishing issuing CAs must be able to survive network and server downtime as well as take the replication latency of Active Directory into consideration. The CRL publication schedule must be longer than the maximum replication latency. In addition, the validity of a certificate must allow enough time to repair a broken network connection or to restore a down system. To enable this, the publication schedule must be shorter than the validity period of the CRL.

3. The private key of the CA and a copy of the CRL may be kept securely offline to manually sign and publish a valid CRL through certutil.exe when a catastrophic failure occurs.

4. For immediate denial of logon certificates, the account in Active Directory should be disabled. It is more efficient to delete or disable user accounts when a certificate should be revoked when a user should be denied access immediately.

5. CRLs should be published using Active Directory methods whenever possible for highest availability and best network performance. Always consider the expected propagation delay with a minimum replication time of 10 minutes.

6. CRLs should not be published to Active Directory when the CRL publication period is shorter than the replication convergence time for the Active Directory forest.

### Revoking Large Numbers of Certificates

When a large number of certificates are revoked, such as during an employee layoff, the Delta CRL size may increase significantly due to the large number of entries, and almost all clients will refer to the older Base CRL. This situation will happen even if a new base CRL is published right after the revocation of the certificate until the new base is fully propagated.

To overcome this particular scenario where the Delta CRL is very large, perform the following steps on the CA:

1. Modify the registry values under the following registry key:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<Name of CA>

- Set the CRLOverLapPeriod to minutes. The default is hours.

- Set the ClockSkewMinutes to 1minute. The default is 10.

2. Restart the CA.

3. Publish a new Base CRL. The Base CRL will have a CRLPropagationComplete time that will be just two minutes and any subsequent Delta CRLs will refer to this base CRL.

Once this has been completed, you can then restore the CRLOverLapPeriod and ClockSkew to the default values.

### Controlling CRL Size

Often, it may be necessary to perform CRL partitioning to control the size of a Base CRL that is published from the CA. This is especially important for controlling both the data size that is replicated to Active Directory as well as the size of the data object downloaded by clients when performing revocation checks on certificates. CRL partitioning may be performed through CA key renewal which effectively creates a partitioned CRL for all subsequently issued certificates. For more information about this process, see the section on CA renewal.

Depending on the revocation reason chosen, the CRL will grow linearly in size by 29 bytes for every certificate that is revoked and added to the CRL. Accordingly, revoked certificates will be removed from the CRL when the certificate reaches its original expiration date. CAs may consider renewing the CA with a new key every 100-125K certificates to maintain a reasonable CRL size. This issuance number is based on the assumption that approximately 10 percent of the issued certificates will be revoked prior to their natural expiration date. If the actual or planned revocation rate is higher or lower for your organization, adjust the key renewal strategy accordingly.

Important

The more keys and certificates used by a CA will affect its performance in service restarts as each certificate and key must be validated before the CA will be operational.

Note

Windows 2000 and Windows Server 2003 do not support the issuance of the IDP extension for partitioned CRLs; however, Windows XP and Windows Server 2003 clients may use a partitioned CRL (using IDP extension). This is technically different from the method identified previously.

### Remove Expired CRLs

By default, a CA will maintain an expired CRL in the database and will keep this CRL also in the directory at the last known CDP publication point for historical purposes. Once the key of a CA expires, the CRL is published one final time and no additional changes are made to that CRL. A best practice is to maintain this CRL in the CA database for long-term validation and audit purposes. However, it may be removed by using the following command:

certutil –setreg ca\CRLFlags + CRLF\_DELETE\_EXPIRED\_CRLS

For more information about how CRL checking and revocation status work in the Windows platform, see the paper at <http://www.microsoft.com/technet/prodtechnol/winxppro/support/tshtcrl.mspx>

# Custom CA Configuration

This section highlights various custom configuration scenarios that may be employed with a Windows Server 2003 certification authority to achieve various operational environment requirements. Various scenarios may apply differently to stand-alone or enterprise CAs.

## Ignore Offline CRL Errors on the CA

Normally, a Windows Server 2003 CA will always check revocation on all certificates in the PKI hierarchy (except the root CA certificate) before issuing an end-entity certificate. To disable this feature, use the following command on the CA, and then restart the CA service:

|  |
| --- |
| certutil –setreg ca\CRLFlags +CRLF\_REVCHECK\_IGNORE\_OFFLINE  |

## Configure Serial Number Generation

In a Windows 2000 CA, two types of fixed-length serial numbers are generated. The registry can be modified to generate one or the other type. The default serial number is (from high to low): a DWORD from GetTickCount() + a USHORT CA cert index (0 to start) + a DWORD RequestId (10 bytes/20 hexadecimal digits). The alternate form is: one byte derived from the registry + a DWORD RequestId + 8 bytes of CryptGenRandom output + a USHORT CA cert index + a DWORD RequestId (19 bytes/38 hexadecimal digits).

To enable the alternate form and set the byte derived from the registry, use the following command:

certutil –setreg ca\HighSerial 0x33

The byte value specified will be modified to clear the sign bit and to set a bit in the high nibble to work around serial number encoding ambiguity bugs in certain non-Microsoft PKI applications.

In a Windows Server 2003 CA, three types of fixed-length serial numbers are generated. The default and alternate forms are the same as in Windows 2000. The Windows 2000 alternate form uses a new random 8 bytes generated by CryptGenRandom for each serial number. The new alternate form for Windows Server 2003 uses a fixed random 8 bytes from CryptGenRandom, generated during the first attempt to issue a certificate, and saved in the registry as 8 bytes of fixed CryptGenRandom output + a USHORT CA cert index + a DWORD RequestId (14 bytes/28 hexadecimal digits).

To enable the new alternate form in the registry, use the following command:

certutil –setreg ca\HighSerial 0xffffffff

Since the fixed random 8 bytes from CryptGenRandom are encoded as a string and saved in the registry, you could set them directly and cause them to be used for new serial numbers. In fact, any length hexadecimal string could be set in the registry (but there must be an even number of digits). The number of bytes used from the registry will be reduced if it would overflow a total of 19 bytes for the serial number. The high byte is manipulated as described previously to avoid problems with certain non-Microsoft applications. The IETF standards specify a maximum of 20 byte serial numbers.

## CA Key Usage

Normally, a stand-alone CA certificate will contain digital signature, Certificate Signing, and CRL Signing as key usage values. For a stand-alone CA to issue a subordinate CA certificate without the digital signature key usage value, the following command must be performed on the stand-alone CA and the CA service restarted before the subordinate CA request is issued:

certutil -setreg policy\EditFlags -EDITF\_ADDOLDKEYUSAGE

Note

Enterprise CAs enforce the key usage based on the subordinate CA template settings.

## Disable DN Length Enforcement

The original CCITT spec for the OU field says it should be limited to 64 characters. Normally, the CA enforces x.500 name length standards on the subject extension of certificates for all requests. It is possible that deep OU paths may exceed normal length restrictions.

To disable name length enforcement, run the following command on the CA, and then restart the CA service:

certutil -setreg ca\EnforceX500NameLengths 0

To restore the default setting, run the following command on the CA, and then restart the CA service:

certutil -setreg ca\EnforceX500NameLengths 1

## Maintaining the CA Database

Windows Server 2003 allows certificate records to be purged manually through certutil.exe should the need arise to remove expired certificate records. The certutil.exe –deleterow command may be used for this task. Only a local administrator may delete multiple rows from a CA database. Standard JET database tools such as ESEUTIL.EXE may also be used with the certificate server database to perform defragmentation maintenance, and so on. For additional information, see the Windows Server 2003 help files.

## Securing DCOM Interfaces

The Windows Server 2003 CA does not enforce encryption on the ICertRequest or ICertAdmin DCOM interfaces by default. Normally, this setting is not required except in special operational scenarios and should not be enabled. Only Windows Server 2003 machines by default support DCOM encryption on these interfaces. For example, Windows XP clients will not by default enforce encryption on certificate request to a Windows Server 2003 CA.

To enable encryption to be forced, perform the following procedures from the command line:

certutil -setreg ca\InterfaceFlags [+|-]IF\_ENFORCEENCRYPTICERTREQUEST

certutil -setreg ca\InterfaceFlags [+|-]IF\_ENFORCEENCRYPTICERTADMIN

# Enrollment Processing

## Enabling Referrals Across Forests

Windows Server 2003 native Active Directory domains now support Kerberos trust and referrals across forests. By default, a Windows Server 2003 CA will not chase a referral for user or machine information in a trusted forest. When referrals are not chased and the user information is not available, the request will be denied if the user is enrolling from another forest. Referral chasing is not enabled by default as unintended template enumeration and enrollment may occur in some scenarios.

To enable referral chasing, use the following command on the certification authority and stop and start the service:

certutil -setreg policy\EditFlags +EDITF\_ENABLELDAPREFERRALS

Note

For this to work, you need to use Kerberos Forest Trust as opposed to normal External Domain Trust. For more information, see the Windows Server 2003 help files.

## Enabling Netscape Browser Enrollment

The following configuration change must be made to a Windows Server 2003 CA to permit Netscape 6.2.2 and later browsers to perform enrollment through the Web enrollment pages.

To enable the parsing of request attributes for subject information, which is required for Netscape browser enrollment, use the following command:

certutil -setreg ca\CRLFlags +CRLF\_ALLOW\_REQUEST\_ATTRIBUTE\_SUBJECT

The certification authority must be stopped and re-started for this change to take effect. If this is not enabled, Netscape clients will receive the following error in the event log when the enrollment fails: The request subject name is invalid or too long.

## Adding CRL Information in an Authority Revocation List

Neither Windows clients nor Windows certification authorities use or process authority revocation lists. However, some manual steps may be followed to artificially create an ARL.

To place a CRL in the ARL attribute in the directory, use the following command where the CAName, MachineName, Domain information, and name of the CRL are specific to the PKI environment and must be specified by the administrator:

certutil -addstore "ldap:///CN=CAName(KeyIndex),CN=MachineName,CN=CDP,CN=Public Key

Services,CN=Services,CN=Configuration,DC=Domain2,DC=Domain1,DC=com?auth

orityRevocationList" <name of CRL file.crl>

To delete an old CRL from the same attribute, use the same command, but use the –delstore instead of –addstore flag and specify the hash of the CRL instead of the CRL file as the last parameter. To display all CRLs with that attribute, use the –store flag and no ending parameter.

## Allowing and Blocking Extensions in Certificate Requests

The template extension processing takes place \*before\* the three object identifier lists in the registry are processed.

The following configuration change must be made to a Windows Server 2003 CA to configure the CA to allow custom extensions to be added or blocked in certificates issued by the CA. Due to the fact that custom extensions comprise custom ASN.1 data, the CA is unable to parse and validate the information contained in the extension. If the certificate request contains the custom extension information properly encoded, the CA can be configured to pass the extension into issued certificates without validating the information. The extension must exist in the request as the CA will not generate this information. The request should be evaluated by a Registration Authority process before processing such requests.

To enable custom extension passing by using the object identifier of the custom extension defined by the organization, use the following command:

certutil -setreg policy\EnableRequestExtensionList +< object identifier of extension to be added>

The certification authority must be stopped and re-started for this change to take effect.

Example The Netscape certtype extension is not enabled by default on a Microsoft CA and must be enabled using the previous mechanism.

To accept the Netscape certtype revocation extension to be included in issued certificates, use the following command:

certutil -setreg policy\EnableRequestExtensionList +2.16.840.1.113730.1.1

To add a custom extension during CA installation through a capolicy.inf file or to submit a request using certreq.exe and a policy.inf file, the following information can be added to the extensions section of the \*.inf file as an example. The object identifier of the extension must be specified followed by the Base64 representation of the value to be included in the extension. For example, AwIBBg== is the Base64 representation of the ASN.1 value: 03 02 01 06.

[Extensions]

1.3.6.1.5.5.7.1.3= AwIBBg==

To disable a certificate extension from being added to a certificate that is included by default in certificates issued by an enterprise CA, such as the S/MIME capabilities extension, use the following command, and then re-start the CA:

certutil -setreg policy\DisableExtensionList +<object identifier of extension to be added>

Note

When encountering template extensions with conflicting object identifiers, an Enterprise CA will override the EnableRequestExtensionList and EnableEnrolleeRequestExtensionList registry value behavior. If the certificate request includes extensions whose object identifiers conflict with the template extensions, the template extensions will override the request extensions. The EnableRequestExtensionList and EnableEnrolleeRequestExtensionList registry values merely cause the disabled bit to be cleared for any extensions in the two registry object identifier lists that exist. Extensions supplied by the template will already have the disabled bit clear. The object identifier list in EnableEnrolleeRequestExtensionList is only processed for templates that are configured to allow the request supply subject information. The object identifier list in EnableRequestExtensionList is processed for all templates. The object identifier list in DisableExtensionList causes the disabled bit to be \*set\* for any extensions in the list that exist—without regard to the origin of the extension (request or template). This prevents the listed extensions from appearing in issued certificates. This object identifier list is also processed for all templates.

## Adding an E-Mail Address to the SubjectAltName Extension

The following configuration option applies to stand-alone CAs only. Enterprise CAs may add e-mail address information to certificates automatically (if specified in the template) based on the user account information in Active Directory. One of the few configuration options that may be set for subject naming on a stand-alone CA is the ability for the CA to place the e-mail address of the requestor (authenticated user making the request) in the SubjAltName extension of an issued certificate.

To set the policy module to allow this option, perform the following steps using regedit.exe on the stand-alone CA:

Set the following REG\_SZ value to Email in the registry, and then restart the CA:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<CAName>\PolicyModules\CertificateAuthority\_MicrosoftDefault.Policy\SubjectAltName2

The <CAName> is the name of the local CA.

Set the e-mail request attribute to the users e-mail name by specifying the following request attribute string in the Web enrollment pages: email:joe@northwindtraders.com. As an alternative, set the e-mail name as part of the subject name E= email:joe@northwindtraders.com as part of the full subject distinguished name, or just joe@northwindtraders.com if there is a separate e-mail text box on the Web page.

The following is the syntax for specifying a Subject Alt Name 2 extension as a request attribute; it will only work on a Windows Server 2003 CA server and requires enabling the flag to process this attribute in the registry:

SAN:1.2.3.4={asn}Base64String&email=sample@bar.com&dns=sample.bar.com&dn="CN=xxx,OU=xxx,DC=xxx"&url="http://sample.com/default.htlm"&ipaddress=172.134.10.134&oid=1.2.3.4&upn=sample@bar.com&guid=f7c3ac41-b8ce-4fb4-aa58-3d1dc0e36b39

To set the Subject Alt Name 2 extension to a specific UPN value:

SAN:upn=sample@bar.com

To set it to a specific DNS name:

SAN:dns=sample.bar.com

To set both:

SAN:upn=sample@bar.com&dns=sample.bar.com

To enable the registry flag for a CA:

certutil –setreg policy\EditFlags +EDITF\_ATTRIBUTESUBJECTALTNAME2

or certutil –setreg policy\EditFlags +0x40000

And restart the CA.

## How to Change the Validity Period for Certificates Issued from a CA

Enterprise CAs set the validity of issued certificates through the settings on Active Directory-based templates. Stand-alone CAs enforce the validity period of issued certificates based on registry values. To change the default validity period intervals for all certificates that are issued by a stand-alone CA, set the following registry values:

HKLM\system\currentcontrolset\services\certsvc\configuration\<ca name>\validityperiod (=days/months/years)

HKLM\system\currentcontrolset\services\certsvc\configuration\<ca name>\validityperiodunits (=number of above)

# Tuning CA Database Performance

## Increasing CA Database Session Limit

By default, the Windows Server 2003 certification authority allows only 20 concurrent sessions to the JET BLUE database, which is used for storing certificate information, and so on. The CA itself can use several connections as well as client enrollment requests or management tools that view the database. In general, the 20 concurrent session limit should be sufficient for most operations. To increase the max session limit, use the following command to increase the maximum number of sessions to 30, which is the highest limit tested with the Windows Server 2003 certification authority:

certutil -setreg DBSessionCount 30

The certification authority must be stopped and re-started for this change to take place.

# Viewing Extended Information

## Viewing Request Attributes

Request Attributes are name-value string pairs that are passed to the certificate server and stored in the database for possible use by the policy module or exit module. They are intended to be used for customer-specific purposes to control the behavior of a custom policy or exit module. They do not directly affect the certificate content. They may be used by the policy module to affect certificate content, but that is determined by the custom policy module, not the default policy module. To review a Request Attribute for a specific request, use the following command, replacing nnnn with the Request ID of the request being examined:

certutil –view –restrict requested=nnnn –out attrib:all

## Removing CA Information from the Directory

Enterprise CA information is stored in the configuration container of Active Directory, most specifically in the Enrollment Services container of the Public Key Services node. Various pieces of information stored in the Public Key Services node of the configuration partition in Active Directory can be viewed or removed with the PKI Health Tool.

# Managing Subject Relative Distinguished Names in the Certificate Subject

For the subject relative distinguished names in certificates issued by a Windows Server 2003 certification authority, the following list contains the object identifiers that are supported in the platform:

COUNTRY\_NAME "2.5.4.6"

ORGANIZATION\_NAME "2.5.4.10"

ORGANIZATIONAL\_UNIT\_NAME "2.5.4.11"

COMMON\_NAME "2.5.4.3"

LOCALITY\_NAME "2.5.4.7"

STATE\_OR\_PROVINCE\_NAME "2.5.4.8"

TITLE "2.5.4.12"

GIVEN\_NAME "2.5.4.42"

INITIALS "2.5.4.43"

SUR\_NAME "2.5.4.4"

DOMAIN\_COMPONENT "0.9.2342.19200300.100.1.25"

RSA\_emailAddr "1.2.840.113549.1.9.1"

STREET\_ADDRESS "2.5.4.9"

RSA\_unstructName "1.2.840.113549.1.9.2"

RSA\_unstructAddr "1.2.840.113549.1.9.8"

DEVICE\_SERIAL\_NUMBER "2.5.4.5"

By default, the following relative distinguished names elements are allowed in the subject of certificates and in the following order when also specified in a version 2 template:

 0: CommonName

 1: OrganizationalUnit

 2: Organization

 3: Locality

 4: State

 5: Country

 6: EMail

The default list can be displayed on a CA by running the following command:

certutil -getreg ca\SubjectTemplate

A relative distinguished names component can be added to the allowable list by running the following command. In this example, the title is added to the end of the list in the registry of the CA.

certutil -setreg ca\SubjectTemplate +title

To add DC= to the subject of a certificate issued by a subordinate stand-alone CA, run the following command:

certutil -setreg ca\SubjectTemplate +DomainComponent

# Enabling the Netscape Revocation Method

To enable a legacy Netscape (iPlanet) application certificate revocation service with a Windows Server 2003 CA, runs the following command on the CA:

certutil -SetReg Policy\RevocationType +AspEnable

If the IIS (ASP) pages are to be hosted on a separate machine or if the default URL to be used by the Netscape application server is different from the default, it may be reviewed by using the following command-line example:

certutil -getreg Policy\RevocationURL

Where the value is stored in the following registry key:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\ <CAName> \PolicyModules\CertificateAuthority\_MicrosoftDefault.Policy\RevocationURL:

RevocationURL REG\_SZ = https://%1/CertEnroll/nsrev\_%3.asp

The URL may be changed in the registry. Restart the CA after making a change. The following replacement variables may be used in the revocation URL:

SERVERDNSNAME "%1"

SERVERSHORTNAME %2"

SANITIZEDCANAME "%3"

CERTFILENAMESUFFIX "%4"

DOMAINDN "%5"

CONFIGDN "%6"

SANITIZEDCANAMEHASH "%7"

CRLFILENAMESUFFIX "%8"

CRLDELTAFILENAMESUFFIX "%9"

DSCRLATTRIBUTE "%10"

DSCACERTATTRIBUTE "%11"

DSUSERCERTATTRIBUTE "%12"

DSKRACERTATTRIBUTE "%13"

DSCROSSCERTPAIRATTRIBUTE "%14"

Note that for this revocation service to work, the application, service, or account connecting to this URL must have READ permissions in the certification authority MMC snap-in. If IIS is using a local account, follow the steps for enabling anonymous access in IIS and allowing Anonymous READ access to the CA.

Important

Allowing anonymous access to the CA may expose privacy or security concerns.

# Configuring the SMTP Exit Module

The Windows Server 2003 certification authority has the capability to send SMTP (e-mail) messages to users, administrators, and Certificate Managers regarding various operations on the certification authority. This function is enabled through the default exit module of the CA and is configured in the registry. By default, no messages are enabled for the CA.

## Sample Configuration Batch File

The following batch file may be used as a sample to configure the SMTP exit module capabilities of the CA without editing the registry directly. The SMTP exit module may use various values stored in the CA database. BodyArg is a list of database columns to be defined and later called by variable names such as %%1, %%2, and so on. Variables must be called in sequential order as they are defined. The following text may be used in a batch file to configure the SMTP exit module options on a CA:

@echo off

cd\

%systemdrive%

:Setup\_SMTP\_Server // Section for setting the name of the exchange

server to be used and type of authentication to be used. 1 means to use

NTLM, 2 means to user Kerberos, 0 is for Basic authentication

certutil -setreg exit\smtp\SMTPServer "exchange1.nwtraders.com"

certutil -setreg exit\smtp\SMTPAuthenticate 1

:Setup\_CA\_For\_Exit\_Module // Section for turning events on or off. In

this case, on.

certutil -setsmtpinfo -p "administrator" Administrator

certutil -setreg exit\smtp\eventfilter +EXITEVENT\_CRLISSUED

certutil -setreg exit\smtp\eventfilter +EXITEVENT\_CERTDENIED

certutil -setreg exit\smtp\eventfilter +EXITEVENT\_CERTISSUED

certutil -setreg exit\smtp\eventfilter +EXITEVENT\_CERTPENDING

certutil -setreg exit\smtp\eventfilter +EXITEVENT\_CERTREVOKED

certutil -setreg exit\smtp\eventfilter +EXITEVENT\_SHUTDOWN

certutil -setreg exit\smtp\eventfilter +EXITEVENT\_STARTUP

:CrlIssued // Section for setting CRLIssued parameters.

certutil -setreg exit\smtp\CRLissued\To "Administrator@nwtraders.com"

certutil -setreg exit\smtp\CRLissued\From "administrator@Nwtraders.com"

certutil -setreg exit\smtp\CRLissued\CC "administrator@Nwtraders.com"

certutil -setreg exit\smtp\CRLissued\bodyformat "A new CRL has been

issued"

certutil -setreg exit\smtp\CRLissued\titleformat "A new CRL was issued by %%1"

certutil -setreg exit\smtp\CRLissued\BodyArg ""

certutil -setreg exit\smtp\CRLissued\TitleArg +"SanitizedCAName"

:Denied // Section for setting Denied parameters

certutil -setreg exit\smtp\Denied\From "administrator@Nwtraders.com"

certutil -setreg exit\smtp\Denied\CC "administrator@Nwtraders.com"

certutil -setreg exit\smtp\Denied\titleformat "Your certificate request

was denied by %%1"

certutil -setreg exit\smtp\Denied\BodyArg ""

Certutil -setreg exit\smtp\Denied\BodyFormat ""

call Stop\_Start\_CA

certutil -setreg exit\smtp\Denied\BodyArg +"Request.RequestID"

certutil -setreg exit\smtp\Denied\BodyArg +"Request.RequesterName"

certutil -setreg exit\smtp\Denied\BodyArg +"Request.SubmittedWhen"

certutil -setreg exit\smtp\Denied\BodyArg +"Request.DistinguishedName"

certutil -setreg exit\smtp\Denied\BodyArg +"Request.DispositionMessage"

certutil -setreg exit\smtp\Denied\BodyArg +"Request.StatusCode"

Certutil -setreg exit\smtp\Denied\BodyFormat +"Your Request ID is: %%1"

Certutil -setreg exit\smtp\Denied\BodyFormat +"The Requester Name is: %%2"

Certutil -setreg exit\smtp\Denied\BodyFormat +"The Request Submission Date was: %%3"

Certutil -setreg exit\smtp\Denied\BodyFormat +"Subject Name: %%4"

Certutil -setreg exit\smtp\Denied\BodyFormat +"Request Disposition Message: %%5"

Certutil -setreg exit\smtp\Denied\BodyFormat +"Request StatusCode: %%6"

certutil -setreg exit\smtp\Denied\TitleArg +"SanitizedCAName"

:Certificate\_Issued // Section for setting Issued parameters.

certutil -setreg exit\smtp\Issued\From "administrator@Nwtraders.com"

certutil -setreg exit\smtp\Issued\CC "administrator@Nwtraders.com"

certutil -setreg exit\smtp\Issued\titleformat "Your certificate has been issued by %%1"

certutil -setreg exit\smtp\Issued\BodyArg +"RawCertificate"

Certutil -setreg exit\smtp\Issued\BodyFormat ""

net stop certsvc

call Stop\_Start\_CA

Certutil -setreg exit\smtp\Issued\BodyFormat +"Request ID: %%1"

Certutil -setreg exit\smtp\Issued\BodyFormat +"UPN: %%2"

Certutil -setreg exit\smtp\Issued\BodyFormat +"Requester Name: %%3"

Certutil -setreg exit\smtp\Issued\BodyFormat +"Serial Number: %%4"

Certutil -setreg exit\smtp\Issued\BodyFormat +"Valid not before: %%5"

Certutil -setreg exit\smtp\Issued\BodyFormat +"Valid not after: %%6"

Certutil -setreg exit\smtp\Issued\BodyFormat +"Distinguished Name: %%7"

Certutil -setreg exit\smtp\Issued\BodyFormat +"Certificate Template: %%8"

Certutil -setreg exit\smtp\Issued\BodyFormat +"Certificate Hash: %%9"

Certutil -setreg exit\smtp\Issued\BodyFormat +"Request Disposition Message: %%10"

Certutil -setreg exit\smtp\Issued\BodyFormat +"Copy and paste the

following in Notepad, save and install"

Certutil -setreg exit\smtp\Issued\BodyFormat +"Binary Certificate: %%11"

:Certificate\_Pending // Section for setting Pending parameters.

certutil -setreg exit\smtp\Pending\From "administrator@Nwtraders.com"

certutil -setreg exit\smtp\Pending\CC "administrator@Nwtraders.com"

certutil -setreg exit\smtp\Pending\titleformat "Your certificate is pending on %%1"

Certutil -setreg exit\smtp\Pending\BodyFormat ""

call Stop\_Start\_CA

Certutil -setreg exit\smtp\Pending\BodyFormat +"Request ID: %%1"

Certutil -setreg exit\smtp\Pending\BodyFormat +"UPN: %%2"

Certutil -setreg exit\smtp\Pending\BodyFormat +"Requester Name: %%3"

Certutil -setreg exit\smtp\Pending\BodyFormat +"Time submitted: %%4"

Certutil -setreg exit\smtp\Pending\BodyFormat +"Distinguished Name: %%5"

Certutil -setreg exit\smtp\Pending\BodyFormat +"Certificate Template used: %%6"

Certutil -setreg exit\smtp\Pending\BodyFormat +"Request Disposition Message: %%7"

:Certificate\_Revoked // Section for setting Revoked parameters.

certutil -setreg exit\smtp\Revoked\From "administrator@Nwtraders.com"

certutil -setreg exit\smtp\Revoked\CC "administrator@Nwtraders.com"

certutil -setreg exit\smtp\Revoked\titleformat "Your certificate was revoked by %%1"

Certutil -setreg exit\smtp\Revoked\BodyFormat ""

call Stop\_Start\_CA

Certutil -setreg exit\smtp\Revoked\BodyFormat +"Request ID: %%1"

Certutil -setreg exit\smtp\Revoked\BodyFormat +"Revoked when: %%2"

Certutil -setreg exit\smtp\Revoked\BodyFormat +"Effective: %%3"

Certutil -setreg exit\smtp\Revoked\BodyFormat +"Reason for being revoked: %%4"

Certutil -setreg exit\smtp\Revoked\BodyFormat +"UPN: %%5"

Certutil -setreg exit\smtp\Revoked\BodyFormat +"Requester Name: %%6"

Certutil -setreg exit\smtp\Revoked\BodyFormat +"Serial Number: %%7"

Certutil -setreg exit\smtp\Revoked\BodyFormat +"Was not valid until: %%8"

Certutil -setreg exit\smtp\Revoked\BodyFormat +"Was not valid after: %%9"

Certutil -setreg exit\smtp\Revoked\BodyFormat +"Distinguished Name: %%10"

Certutil -setreg exit\smtp\Revoked\BodyFormat +"Certificate Template: %%11"

Certutil -setreg exit\smtp\Revoked\BodyFormat +"Certificate Hash: %%12"

Certutil -setreg exit\smtp\Revoked\BodyFormat +"Request Status: %%13"

:Certificate\_Authority\_Shutdown // Section for setting Shutdown parameters.

certutil -setreg exit\smtp\Shutdown\To "administrator@Nwtraders.com"

certutil -setreg exit\smtp\Shutdown\From "administrator@Nwtraders.com"

certutil -setreg exit\smtp\Shutdown\CC "administrator@Nwtraders.com"

:Certificate\_Authority\_Startup // Section for setting Startup parameters.

certutil -setreg exit\smtp\Startup\To "administrator@Nwtraders.com"

certutil -setreg exit\smtp\Startup\From "administrator@Nwtraders.com"

certutil -setreg exit\smtp\Startup\CC "administrator@Nwtraders.com"

:Stop\_Start\_CA // This is just a sub-routine for stopping and starting the CA.

net stop certsvc & net start certsvc

:Exit

echo Certificate Services SMTP Exit module has now been configured.

echo .

pause

exit

## Revocation Status

The SMTP exit module allows for e-mail notification when a certificate has been revoked. However, one of the database columns, Request.RevokedReason, can only be used to return a revocation value to the user in the e-mail body, instead of the string. For example, "Key Compromise" would be displayed as a value of 1. The revocation values and their corresponding definitions as defined in RFC 2459 are as follows:

0 = Unspecified

1 = Key Compromise

2 = CA Compromise

3 = Change of Affiliation

4 = Superseded

5 = Cease of Operation

6 = Certificate Hold

It may be necessary to list the values in the body of the e-mail message to easily interpret the revocation reason.

# Using SSL to Communicate with Exchange Server

A best practice in using the SMTP exit module of a certification authority with a Microsoft Exchange 2000 Server is to configure the CA to communicate with the Exchange Server via SSL (SMTP Protocol). The following steps should be implemented to enable this enhanced security configuration once the SMTP exit module is already configured on the CA for operation:

Make sure the Root CA that issued the server certificate for the Exchange Server is trusted by the CA.

Configure the Exchange Server SMTP Protocol to use SSL by enrolling for a Server Certificate using the Wizard in the Exchange System Manager console.

Open the Exchange System Manager on the Exchange machine by selecting Start >

Programs > Microsoft Exchange > System Manager.

In the left-pane view, expand Servers > SERVER\_NAME > Protocols > SMTP > Default SMTP Virtual Server.

Right-click Default SMTP Virtual Server, and then select Properties.

Click the Access tab, and then select the Certificate button under Secure communication.

Follow the directions in the Wizard and when completed, go back to the Default SMTP Virtual Server Properties and select Communication.

Select the Require secure channel checkbox. It is recommended to set Require 128-bit encryption.

At a CMD prompt on the CA, type the following command:

certutil -setreg exit\smtp\http://schemas.microsoft.com/cdo/configuration/smtpusessl 1

Note

This will add a REG\_SZ value: http://schemas.microsoft.com/cdo/configuration/smtpusessl with a value of 1 to the SMTP key in the registry.

# Related Links for Windows Server 2003 PKI Operations

For the latest information about Windows Server 2003, see the Windows Server 2003 Web site at <http://www.microsoft.com/windowsserver2003/default.mspx>

Windows XP Home Page

<http://www.microsoft.com/windowsxp/default.asp>

Whats New in Windows XP and Windows Server 2003 PKI?

<http://www.microsoft.com/technet/prodtechnol/winxppro/plan/default.mspx>

Windows XP Technical Articles

<http://www.microsoft.com/technet/prodtechnol/winxppro/default.mspx>

CMC - Certificate Management Messages over CMS

<http://www.ietf.org/rfc/rfc2797.txt?number=2797>

Troubleshooting Certificate Status and Revocation white paper

<http://www.microsoft.com/technet/prodtechnol/winxppro/support/tshtcrl.mspx>

Certificate Auto-enrollment in Windows XP

<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/default.mspx>

# Appendix A for Windows Server 2003 PKI Operations

The following basic VBScript can be run by an end user or administrator to enumerate all the enterprise CAs in the forest, list the individual CAs, and display the role(s) held by the current user for each of the CA(s) as appropriate:

on error resume next

dim certadm

dim configobj

dim config

dim index

dim roles(9)

roles(0) = "CAADMIN"

roles(1) = "OFFICER"

roles(2) = "AUDITOR"

roles(3) = "OPERATOR"

roles(8) = "READ"

roles(9) = "ENROLL"

set certadm = CreateObject("CertificateAuthority.Admin")

Call ExitOnError("Createobject CertificateAuthority.Admin")

set configobj = CreateObject("CertificateAuthority.Config")

Call ExitOnError("Createobject CertificateAuthority.Config")

index = 0

do while index <> -1

    config = ""

    config = configobj.GetField("config")

    if(config <> "") then

        wscript.echo "CA: ", config

        PrintRoles(config)

    end if

    index = configobj.Next()

    Call ExitOnError("ICertConfig::Next")

loop

sub PrintRoles(config)

    value = certadm.GetMyRoles(config)

    Call ExitOnError("GetMyRoles")

    wscript.echo "Roles: 0x" & hex(value)

    for count=0 to 9

        if((count<4 or count>7) and value mod 2) then

            wscript.echo "      ", roles(count)

        end if

        value = value \ 2

    next

End Sub

Sub ExitOnError(failedCall)

'    if err.number <> 0 then

 '   wscript.echo "Error calling " + failedCall + " : " + err.value

  '  end if

End Sub

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

2003. Microsoft Corporation. All rights reserved. Microsoft, Active Directory, Visual Studio, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.