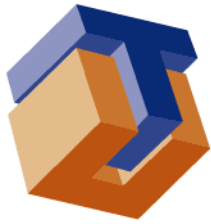


TC TrustCenter GmbH



TRUSTCENTER
a company of **CHOSENSECURITY**

**TC AutoEnrollment Server
Administrator's Guide**

v1.6b

Dieses Dokument ist urheberrechtlich geschützt. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung von TC TrustCenter unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Verbreitungen, Übersetzungen oder die Verwendung in elektronischen Systemen. Ausgenommen hiervon ist das Kopieren und der Ausdruck zum eigenen Gebrauch.

Alle Informationen in diesem Dokument wurden mit größter Sorgfalt erstellt. Weder TC TrustCenter noch der Autor können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Dokumentes stehen.

„TC TrustCenter“, das TC TrustCenter Logo, „Ident Point“, „TC PKI“, „TC Info Line“, „TC fit“, „Trust Alliance“, „TC QUICKSTART“, „PortalKeeper“, „TC Qsign“ und „Entry PKI“ sind eingetragene Marken der TC TrustCenter GmbH.

Alle in diesem Dokument verwendeten, aber hier nicht genannten Marken- oder Produktnamen sind Marken oder Warenzeichen der entsprechenden Inhaber.

Copyright © 2008 TC TrustCenter GmbH, Sonninstrasse 24 - 28, 20097 Hamburg, Germany.
Alle Rechte vorbehalten.

All rights reserved. No information or images, fully or partially, in any form or by any means, may be reproduced, copied, duplicated, published or used in electronic systems or translations without the prior written consent of TC TrustCenter. This represents a crime, excluding printing and duplicating for one's own use.

All information in this document is compiled with great care. Neither TC TrustCenter nor the author is liable for any damages may occur in connection with the use of this document.

“TC TrustCenter”, the TC TrustCenter logo, “Ident Point”, “TC PKI”, “TC Info Line”, “TC fit”, “Trust Alliance”, “TC QUICKSTART”, “PortalKeeper”, “TC QSign” and “Entry PKI” are registered trademarks of the TC TrustCenter GmbH.

All brands, product names and trademarks used in this document, but not listed above, are trademarks or service marks of the respective owners.

Copyright © 2008 TC TrustCenter GmbH, Sonninstrasse 24 – 28, 20097 Hamburg, Germany.

Table of Contents

1. Introduction.....	1
1.1. Intended audience.....	1
1.2. About the TC TrustCenter AutoEnrollment Server.....	1
1.3. The Autoenrollment Process.....	2
1.4. Contents of the CD.....	2
1.5. Interoperating with Active Directory.....	3
1.6. Renewing certificates and private keys for autoenroll clients.....	4
1.7. External References.....	4
2. Preparing your Windows Environment.....	5
2.1. Supported Windows Operating Systems.....	5
2.2. Active Directory.....	6
2.3. Adding a Domain Controller.....	6
2.3.1. Deploying DNS for Active Directory.....	7
2.3.2. Installing Active Directory.....	7
2.4. Configuring the machine's DCOM Access Rights.....	8
2.5. Adapting firewall settings.....	11
2.6. Setting up group policies.....	12
2.7. Preparing a Windows 2008 Server.....	16
3. Installing the TC AutoEnrollment Server Software.....	17
3.1. Installing the software.....	17
3.2. Setting Autoenrollment permissions.....	19
3.3. Setting autoenrollment service properties.....	23
3.4. Allow publishing to Active Directory.....	25
4. Configuring the TC AutoEnrollment Server.....	27
4.1. Using the Configuration tool.....	27
4.2. Downloading the configuration data.....	35
4.3. Saving AEConfig's settings.....	36
4.4. Advanced Configuration.....	37
5. Using the TC AutoEnrollment Server.....	41
5.1. Starting and stopping the server.....	41
5.1.1. Using AEConfig to start or stop the service.....	41
5.1.2. Using the Windows service Manager to start or stop the service.....	43
5.2. Preparing certificate templates.....	44
5.2.1. Certificate template versions.....	45
5.2.2. Certificate templates used by the TC AutoEnrollment Server	45
5.2.3. Browsing and editing template values.....	46
5.2.4. Key archival.....	48
5.2.5. Assigning group/user access to templates.....	49
5.3. Replicating certificate templates and policies.....	51
5.4. Manually requesting a certificate.....	52
5.5. Autoenrolling for a certificate.....	58
5.6. Monitoring enrollment activities.....	59
5.6.1. Checking the number of pending requests.....	59
5.6.2. Analyzing the log file.....	60
5.6.3. Using the Windows Event Viewer.....	61
5.7. Software update of TC AutoEnrollment Server.....	62
6. Frequently Asked Questions.....	64
6.1. Problems related to Publishing to ADS.....	64

6.1.1. Certificates cannot be published (permission denied).....	64
6.1.2. CRLs cannot be published (cannot get object).....	65
6.1.3. CRLs cannot be published (permission denied).....	65
6.2. Problems related to certificate requests.....	66
6.2.1. Template not registered.....	66
6.2.2. Unknown profile.....	66
6.2.3. Certificate Request Wizard cannot be started.....	66
6.2.4. Request hit CA_ERROR.....	67
6.2.5. How to find detailed information about the enrollment process.....	67
6.3. Miscellaneous problems.....	69
6.3.1. Problems with SC Logon and/or domain controller authentication.....	69
7. Known Issues.....	70
8. Troubleshooting.....	71
8.1. Repeating an action with a higher log level.....	71
9. Appendix.....	72
9.1. Understanding the different log levels.....	72
9.1.1. Format of Log file Messages.....	72
9.1.2. Audit messages (Level 0).....	73
9.1.3. Error Messages (Level 0).....	74
9.1.4. Warning Messages (Level 1).....	75
9.1.5. Info Messages (Level 2).....	75
9.1.6. Trace Messages (Level 3).....	76
9.2. List of Figures.....	77
9.3. List of Tables.....	78

1. Introduction

By specifying group policy settings for domains, users and machines certificate templates can be used to automatically enroll users for certificates when logging on to modern Windows operating systems such as Windows XP Professional.

PKIs (Public key infrastructures) can be easily implemented by issuing certificates that – among other applications – can be used for smart card logon, SSL connections, encrypted file system transactions and for exchanging encrypted mail.

The increasing demand for high-level security and highly available PKI services can not be satisfied by a company's IT department alone. To provide your organization with these high-quality security services the TC TrustCenter AutoEnrollment Server connects your network infrastructure with the TC TrustCenter Certification Authority.

1.1. *Intended audience*

This guide assumes you have thorough knowledge about Windows network administration and basic understanding of PKI components, workflows and cryptographic systems in general, but it is not necessary to have an in-depth knowledge about how cryptographic algorithms or other technical details work.

If you are reading the PDF version of this guide you can visit the websites this guide refers to by clicking on them in Adobe Reader. If you are reading the printed version you can find the actual web addresses behind each reference at the end of this document.

1.2. *About the TC TrustCenter AutoEnrollment Server*

The TC TrustCenter AutoEnrollment Server handles the following aspects of the autoenrollment process:

- Requesting certificates
- Pending requests and certificate renewal
- Renewing a certificate
- Key-archival

It enables you to provide your network computers and end users with certificates issued by the TC TrustCenter CA (Certification Authority).

It needs to be installed within a Windows domain including an Active Directory Server providing information on policies, certificate templates and users. The operating system will automatically request certificates for users of the domain when they log onto the network using the Windows XP client. The system will keep track of the certificates' validity and request a renewal as a certificate is about to expire.

1.3. The Autoenrollment Process

The Windows autoenrollment client sends a certificate request to the autoenrollment server. The server verifies the information contained in the request against the user's account details. It can retrieve information from Active Directory to perform further checks or to enforce restrictions regarding the certificate's content. The TC TrustCenter AutoEnrollment Server will then submit the request to TC TrustCenter's CA and will wait for the request to be processed by the CA.

If the CA finishes processing the request and issues the certificate within the configured amount of time the certificate is returned to the autoenrollment server, which returns it to the client immediately. If the CA cannot complete processing the request in time it is marked as pending by the autoenrollment server. The client will contact the CA later to check for the status of the certificate.

1.4. Contents of the CD

The TC TrustCenter AutoEnrollment CD provides you with the following files:

1. A Microsoft Installer Package (*.msi) containing the TC AutoEnrollment server software and the AutoEnrollment configuration tool AEConfig
2. This guide in PDF format

Please refer to Chapter 3 “Installing the TC AutoEnrollment Server Software” on page 18 for step-by-step instructions on how to install the TC AutoEnrollment software.

1.5. Interoperating with Active Directory

Your installation of the TC TrustCenter AutoEnrollment Server software requires you to operate an Active Directory Server within your network domain. It is used as follows:

- The TC TrustCenter AutoEnrollment Server communicates with ADS and provides it with information about TC TrustCenter's certification services and requirements. It also stores the certificate templates in ADS. This data is stored in ADS when configuring the autoenrollment server.
- Upon logon of users to the system the Windows autoenrollment client contacts ADS to see which certificates are required. This accounts for new certificates as well as for certificates that must be renewed. The information contained in the templates identify the CA the client must use to obtain the required certificates.
- The client passes the requests on to the autoenrollment server which validates the information contained within the requests. The server may correct or add data it obtains from ADS.
- Once TC TrustCenter has issued the certificate the autoenrollment server populates the ADS with the newly created certificates and CRLs.

The following illustration shows the data flow involved with the autoenrollment process:

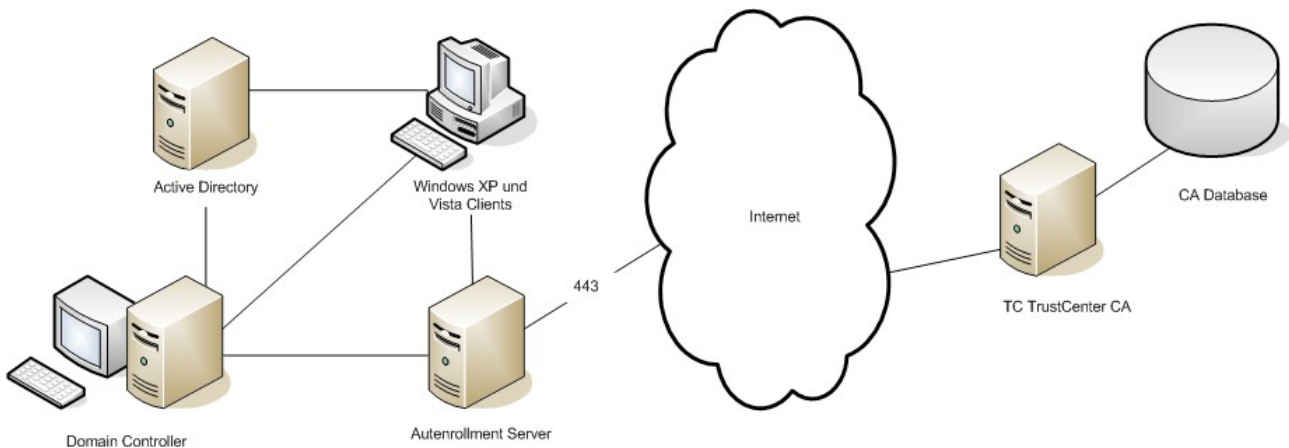


Figure 1: Data Flow of the Autoenrollment Process

1.6. *Renewing certificates and private keys for autoenroll clients*

The process of renewing expiring certificates is nearly identical to the process of requesting a new certificate, except that the autoenrollment client includes a reference to the certificates that have to be renewed. By default, renewal of certificates is carried out six weeks before expiry. Please refrain from editing any certificate templates, except as specifically directed in this manual, because they might get overwritten when downloading an updated set of configuration data.

The Windows XP autoenrollment client automatically requests renewal of certificates when 80% of the certificate's lifetime has expired or when the above-mentioned certificate renewal period has been reached, whichever time frame is smaller.

The autoenroll client normally generates a new key. However, if it detects that the smart card's CSP has only limited storage space, the existing private key is reused for the renewal request.

See sections 5.4 “Manually requesting a certificate” and 5.5 “Autoenrolling for a certificate” for further details on how the actual enrollment process works.

1.7. *Users using different Computers*

When a user uses multiple computers (e.g. shared desktops or notebook and desktop) the certificate and related private key must either be accessible on all computers (using roaming profile) or the user will autoenroll for certificate on every computer separately.

Roaming profiles and roaming credentials will store the private key and certificate in the users profile on the domain controller. The profile will be copied on each computer the user logs in. Roaming profiles and roaming credentials can't be used simultaneously.

For more information on how to setup roaming profiles or credential roaming see

- [Roaming Profile Support](#)
- [Using credential roaming](#)
- [Credential roaming best practices](#)

1.8. External References

- Microsoft, [*Certificate autoenrollment in Windows Server 2003*](#)¹, April 2003.
- Microsoft, [*Implementing and Administering Certificate Templates in Windows Server 2003*](#)², 2003.
- Microsoft, [*Using credential roaming*](#).
- RFC 2247, Kille, S., M. Wahl, A. Grimstad, R. Huber, and S. Sataluri,
- *Using Domains in LDAP/X.500 Distinguished Names*, January 1998.
- RFC 1035/STD 0013, P.V. Mockapetris, *Domain names – implementation and specification*, November 1987.

2. Preparing your Windows Environment

The TC TrustCenter AutoEnrollment Server integrates itself closely into the Windows operating system. It handles certificate requests generated by the Autoenrollment client software, passes them on to TC TrustCenter's CA and stores the issued certificates together with up-to-date revocation information in your domain's Active Directory.

When using the TC TrustCenter AutoEnrollment Server to issue certificates with TC TrustCenter's CA instead of the built-in Microsoft CA, a number of prerequisites must be met before you can successfully use the software.

We advise you to carefully plan the forest structure of your network. 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](#)³.

For enabling autoenrollment with the TC TrustCenter CA the main tasks are:

1. Adding a domain controller to your domain
2. Configuring the machine's DCOM Access Rights
3. Setting group policies

For more information on how to operate and administer your autoenrollment setup and ADS see

- [Certificate autoenrollment in Windows Server 2003](#)⁴
- [Implementing and Administering Certificate Templates in Windows Server 2003](#)⁵

2.1. Supported Windows Operating Systems

The TC TrustCenter AutoEnrollment Server can be used with the following versions of Windows operating systems for client and server installations:

<i>User</i>	<i>Supported Systems</i>
Client	Windows XP Professional Windows 2003 Server Windows Vista Business Windows 2008 Server (x86 and x64) Windows 7 Enterprise (x86 and x64)
Server	Windows 2003 Server Enterprise Edition Windows 2008 Server Enterprise (x86 and x64)

Table 1: Supported Windows operating systems

The TC AutoEnrollment Server can only be installed on “Server” operating systems.

2.2. Active Directory

In order for Active Directory to properly work on the desired machine you need to:

- Ensure that the server's TCP/IP networking settings are correct and that it is deployed in a DNS server on your domain's network.
- Add at least one NTFS file system partition to your ADS server. ADS needs an NTFS partition to store its SYSVOL folder and contents.
- Enable the Windows Firewall
- Install / Enable the Security Configuration Wizard.

See [Active Directory Best Practices](#)⁶ on Microsoft Technet for more information on how to secure your ADS.

2.3. Adding a Domain Controller

You must have a domain controller in your network for autoenrollment to work. In an existing Windows domain, you do not need to set up an additional domain controller. If you do not have a domain yet you need to set up a Windows computer on your network as a domain controller, i.e. promote a Windows server to be the domain controller of your network. When setting up a domain controller you must have a DNS (Domain Name Server) on your network.

2.3.1 Deploying DNS for Active Directory

By promoting a Windows server computer to a domain controller you install Active Directory Services on the machine as well. ADS will check for a DNS server and allow you to install a local DNS server on the same machine if no DNS server could be found during installation. This local DNS server will become the system's preferred DNS.

You should carefully plan your domain's organization, i.e. the topology of the network, before installing any software. There are introductory and in-depth articles on this subject on [Microsoft's Technet website](#)⁷.

If you choose to deploy DNS to support ADS make sure to plan the network's topology as well as the DNS namespace. You can find more details about DNS deployment for ADS in [Deploying Domain Name System \(DNS\)](#)⁸.

2.3.2 Installing Active Directory

When adding domain controller capabilities to a Windows server operating system you actually install Active Directory on that machine. Please follow these steps to install Active Directory:

- Start the Configure Your Server Wizard by double-clicking on **Administrative Tools** in the system's Control Panel.
- On the **Server Role** page, click Domain Controller (Active Directory), and then click **Next**.
- The Active Directory Installation Wizard is started and asks to select one of the following options:
 - Creating an additional domain controller for an existing domain
 - Creating a domain controller for a new forest
 - Creating a domain controller for a new child domain
 - Creating a domain controller for a new domain tree

Consult the MS Technet article at [Configuring a domain controller](#) for details on determining which domain controller role type you need. Complete the remainder of the Installation Wizard.

- After rebooting your server you will be presented with a screen stating that this computer now is a domain controller.
- Be sure to visit Windows Update to download any additional updates that are available.

- In addition, you should also run the Security Configuration Wizard to further secure your domain controller.

2.4. Configuring the machine's DCOM Access Rights

The TC TrustCenter AutoEnrollment Server is invoked via the Distributed Component Object Model (DCOM) which is a communication protocol designed by Microsoft for software components to communicate with each other across several networked computers. In order to use the autoenrollment services you must configure the system to allow global DCOM object access. Otherwise, the autoenrollment server can not be used across the network.

By default, Windows is configured for local DCOM access for system processes and accounts with administrative privileges. However, you must allow remote DCOM access to use the autoenrollment server across multiple machines.

1. Open **Administrative Tools | Component Services**, click on **Component Services**, in the left pane, and expand the tree view on the left to **Computers**.
2. Right-click **My Computer** and select **Properties**.
3. Select the **COM Security** tab.
4. Click **Edit Limits** under the **Access Permissions** group.

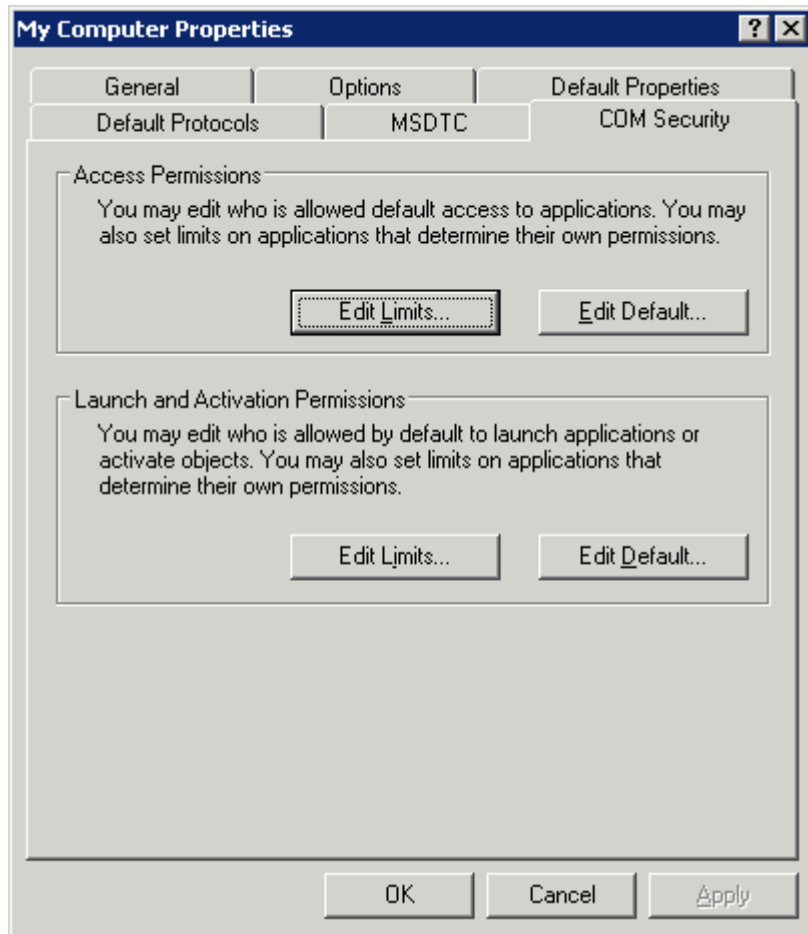


Figure 2: Setting the machine's DCOM Access Permissions

5. Add the Domain Computers group:
 1. Click **Add** and type Domain Computers in the **Enter the object names** field.
 2. Click OK.
 3. In the **Allow** column, select the **Local Access** and **Remote Access** check boxes. Deselect the corresponding entries in the **Deny** column.
6. Click OK.
7. Add and configure both the **Domain Users** and the **Domain Controllers** group as you did with **Domain Computers** in step 5.

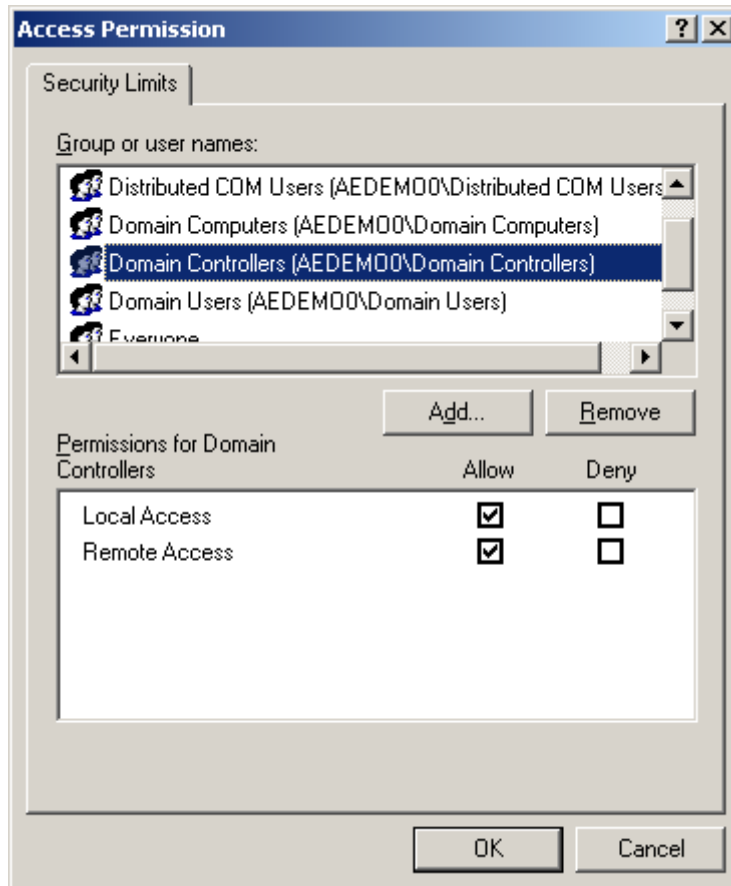


Figure 3: Adding the Domain Computers and Domain Users groups

8. Click **Edit Limits** in the **Launch and Activation Permissions** section, add the **Domain Computers** and **Domain Users** groups and highlight **Domain Computers** in the list.
9. In the **Allow** column, select the **Local Activation** and **Remote Activation** check boxes but deselect the **Local Launch** and **Remote Launch** options. Deselect all entries in the **Deny** column

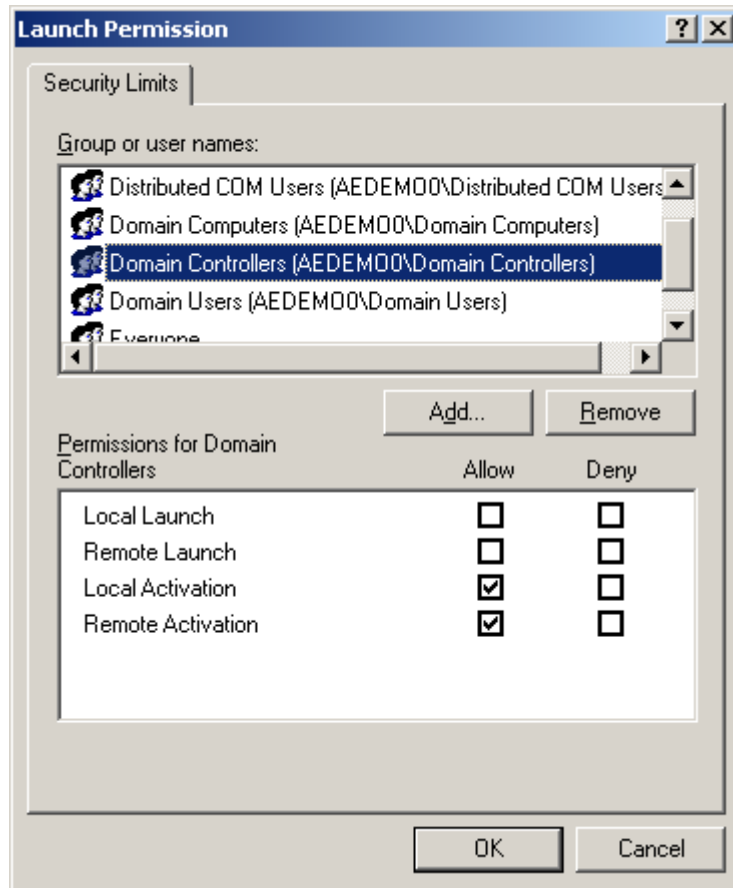


Figure 4: Setting DCOM Launch Permissions

10. Repeat step 9 for both the **Domain Users** and the **Domain Controllers** group.
11. Click OK to apply your changes and exit **Component Services**.

2.5. Adapting firewall settings

Enable an exception on the Firewall of the computer the TC AutoEnrollment Server is running on.

1. **Start | Control Panel | Windows Firewall** go to tab **Exceptions** and mark the **AutoEnrollmentDCOMsrv** option.

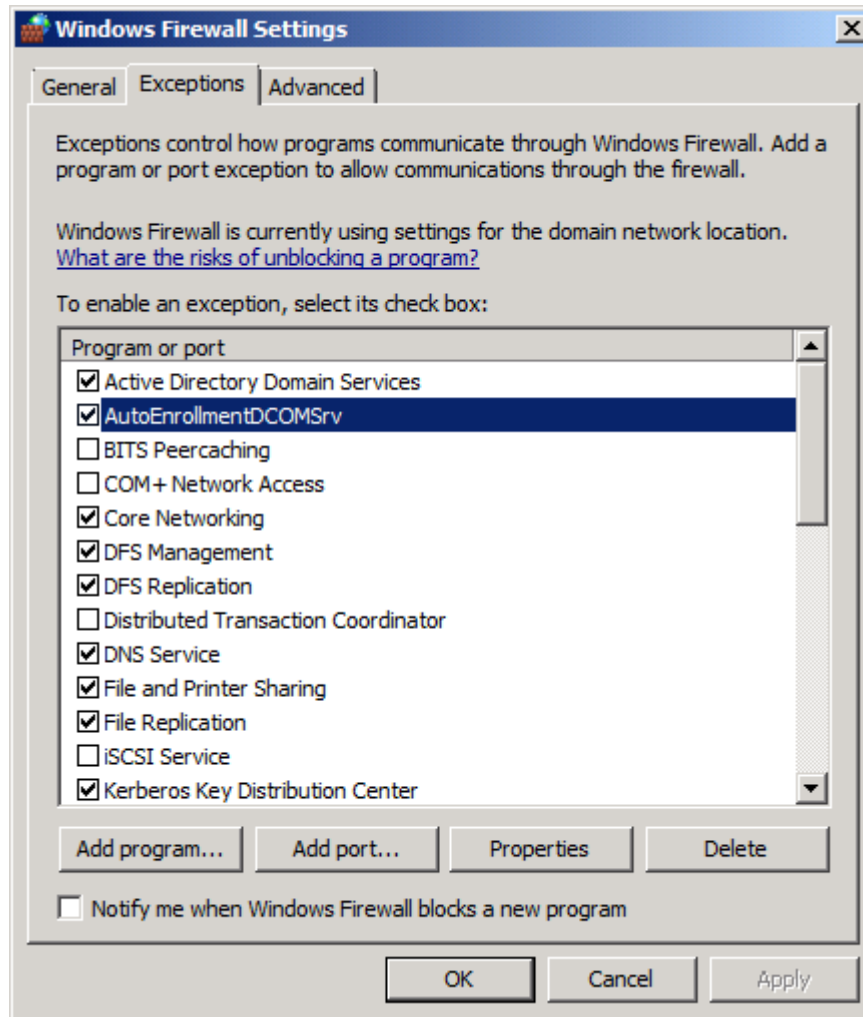


Figure 5: Windows Firewall Settings

2.6. Setting up group policies

In addition to assigning groups access to templates, you have to set autoenrollment permissions for the groups your users and computers belong to. For example you must configure the permission settings for the respective domain or user group to enable the autoenrollment mechanism for its members.

To configure a group policy for users:

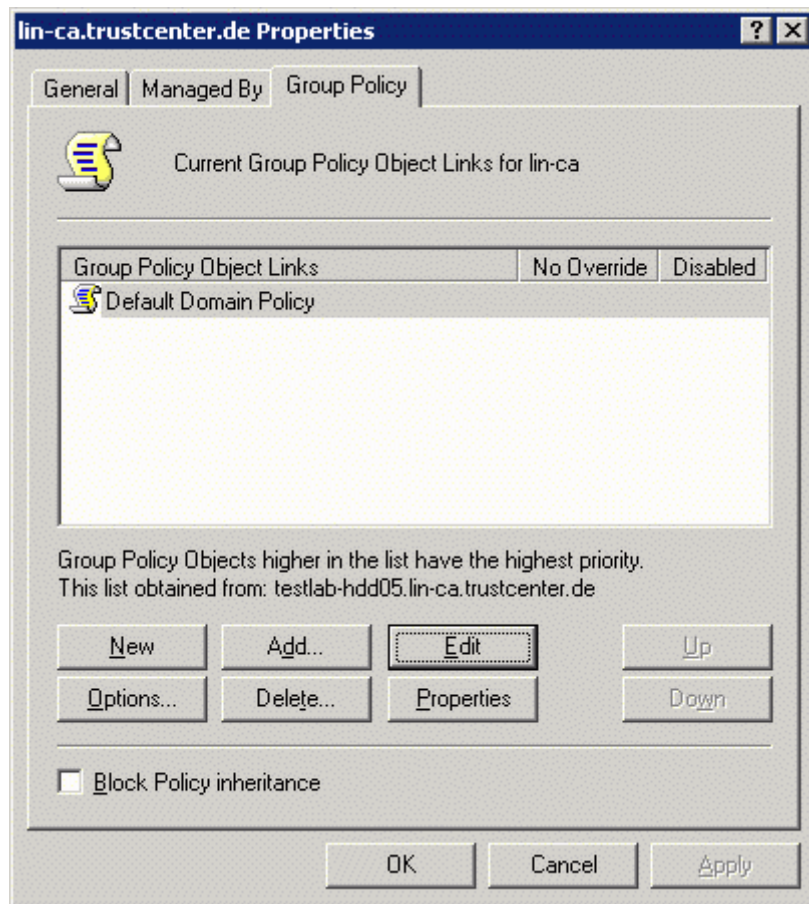


Figure 6: Setting Group Policies

1. Open the Active Directory Users and Computers MMC snap-in by selecting **Start | Administrative Tools | Active Directory Users and Computers**. Right-click the site, domain, or OU object for the users requiring autoenrollment and then click **Properties**.
2. Click the **Group Policy** tab and then click **Edit**.

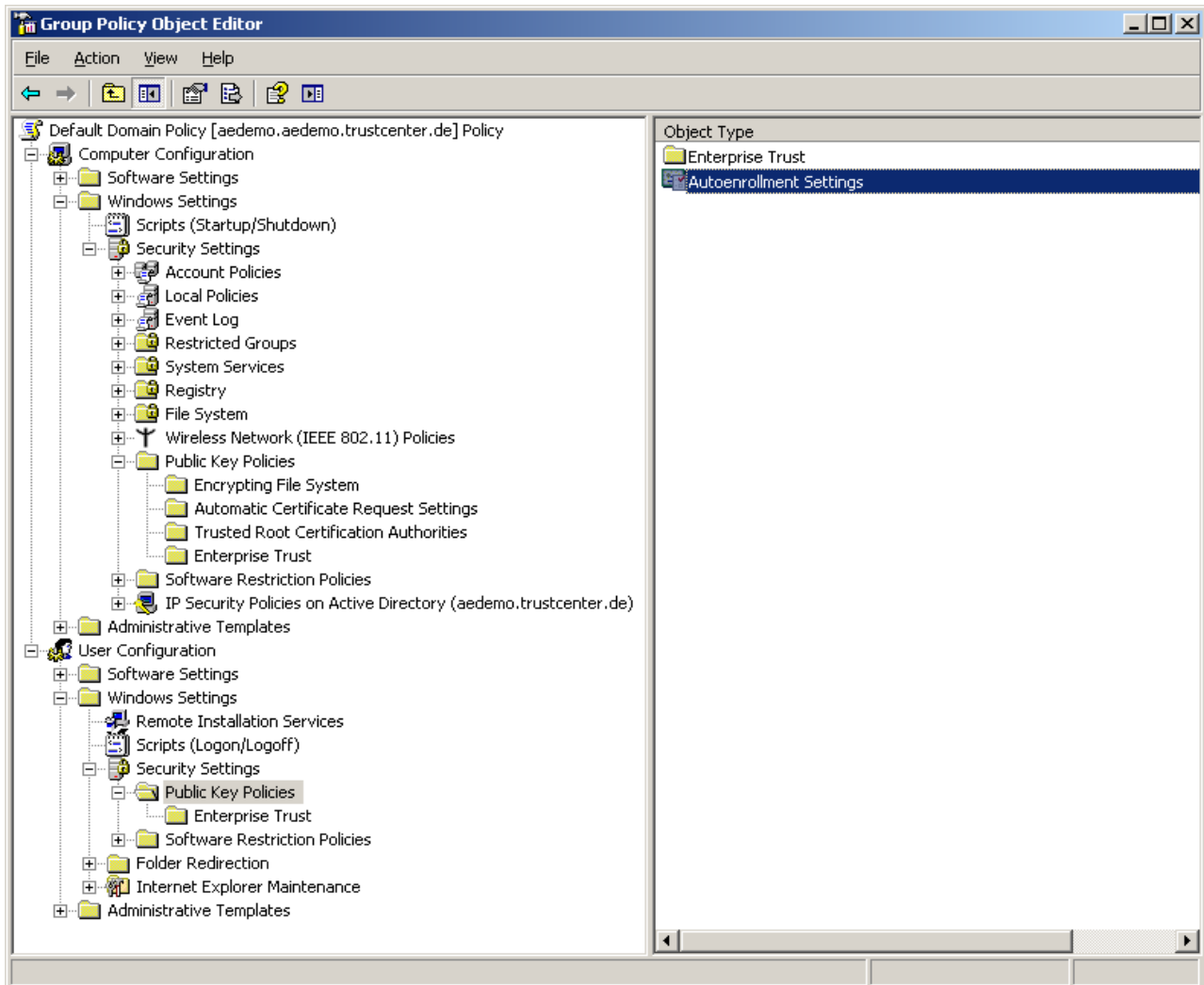


Figure 7: Navigating to the autoenrollment settings

3. In the tree view on the left expand the branch down to **User Configuration | Windows Settings | Security Settings | Public Key Policies**.
4. Right-click on **Autoenrollment Settings** and select **Properties** from the context menu.

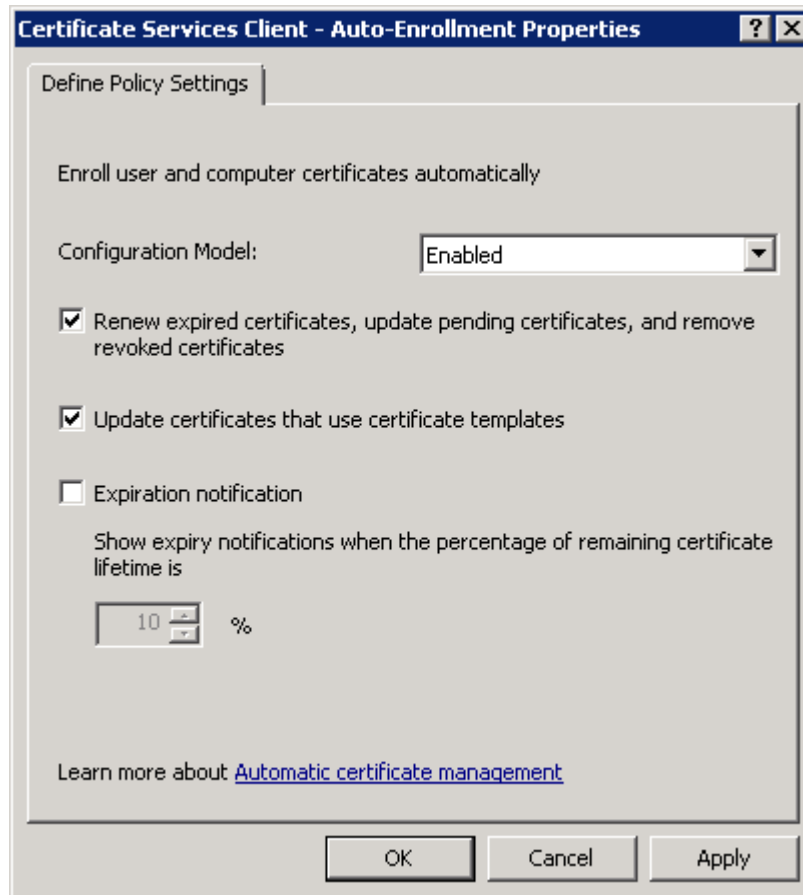


Figure 8: Setting Group Policy Autoenrollment Options

5. Select **Enroll certificates automatically** and both the **Renew** and **Update** options. You must select all three options to enable Certificate management and publishing in Active directory.
6. Click OK to close the dialog. You have now enabled autoenrollment for the selected object.
7. Repeat the above steps for any additional site, domain, or OU object for which you want to enable autoenrollment.
8. You should also repeat the configuration for **Computer Configuration** if you plan to autoenroll computer certificates (e.g., domain controller certificates).



Group Policy Objects (GPOs) are valid in a domain. If you have set up a forest domain structure you need to copy the GPO to every DC the GPO should apply.

2.7. Preparing a Windows 2008 Server

The Certificate Template SnapIn for mmc must be installed separately on the Windows 2008 Server:

1. **Start | All Programs | Server Manager** right click on **Server Manager** and choose **Add Features**.
2. Open **Remote Server Administration Tools | Role Administration Tools | Active Directory Certificate Services Tools** and select **Certification Authority Tools**.

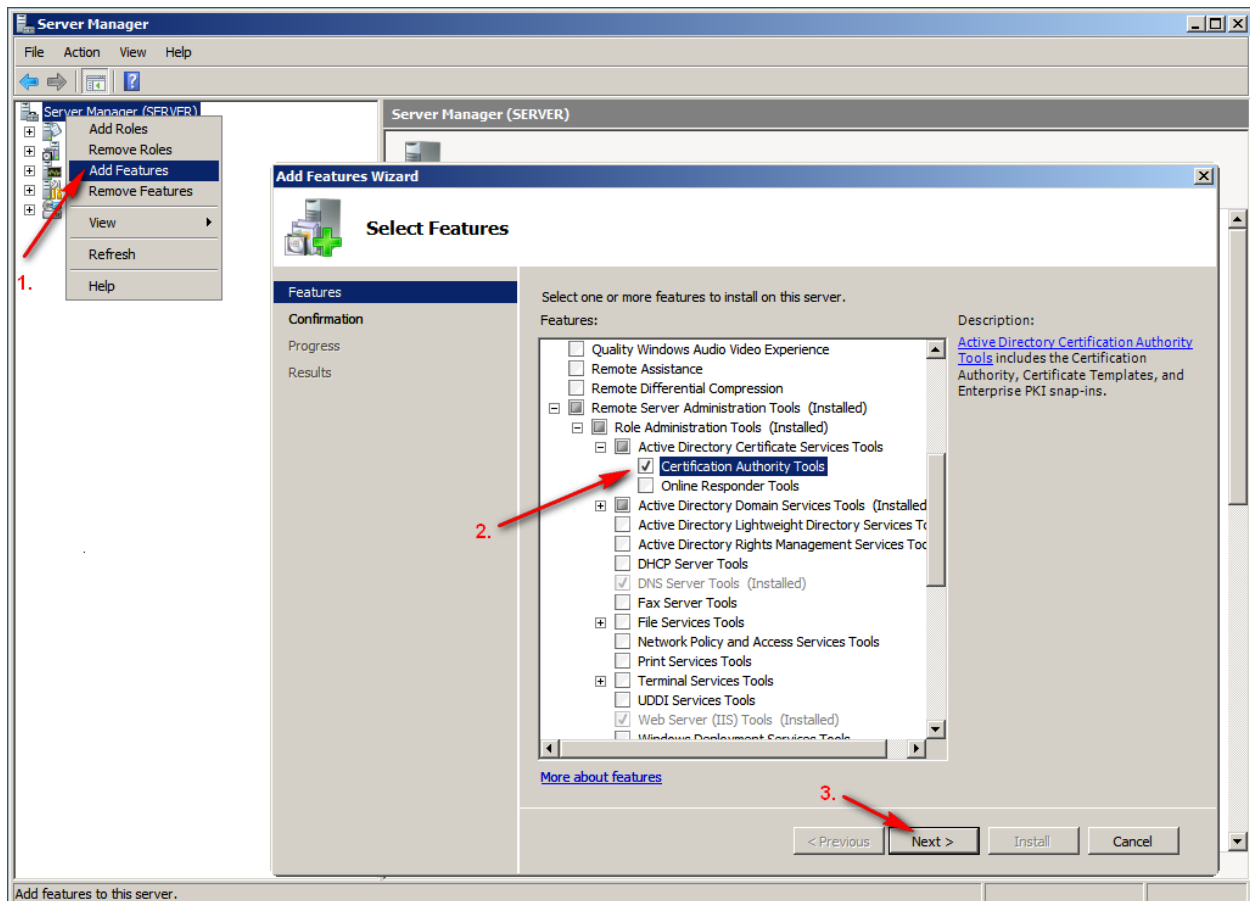


Figure 9: Add Certificate Templates SnapIn on Windows 2008 Server

3. Click **Next** Button. After the installation is completed you can use these templates described in section 5.2.3 „Browsing and editing template values“.



It is not required to install the Microsoft Certificate Server. If you want to install the Microsoft Certificate Server it *must* be installed on a separate machine (not on the same computer as the TC AutoEnrollment Server).

3. Installing the TC AutoEnrollment Server Software

To successfully install the TC AutoEnrollment Server Software make sure both your system and network environment meet the requirements discussed in Chapter 2 “Preparing your Windows Environment”. For example, you need to have a server operating system promoted to a domain controller by installing Active Directory Services on it. See Chapter 2 for further information.



You can not use the TC TrustCenter AutoEnrollment Server unless you have contacted TC TrustCenter and agreed on a set of certificate templates, configuration parameters and encryption keys. After TC TrustCenter has setup your project you will be able to configure and run your autoenrollment server.

The installation procedure includes the following steps:

- Installing the TC AutoEnrollment Server files on your system
- Setting up autoenrollment permissions
- Setting autoenrollment service properties

3.1. *Installing the software*

To install the TC AutoEnrollment Server software:

1. Logon as Administrator to the computer you wish to install the software on.
1. Insert the product's CD-ROM into the computer's CD drive.
2. Locate the file named TC-AutoEnrollmentServer.msi (or TC-AutoEnrollmentServer-x64.msi) and double-click it to start the installation procedure.

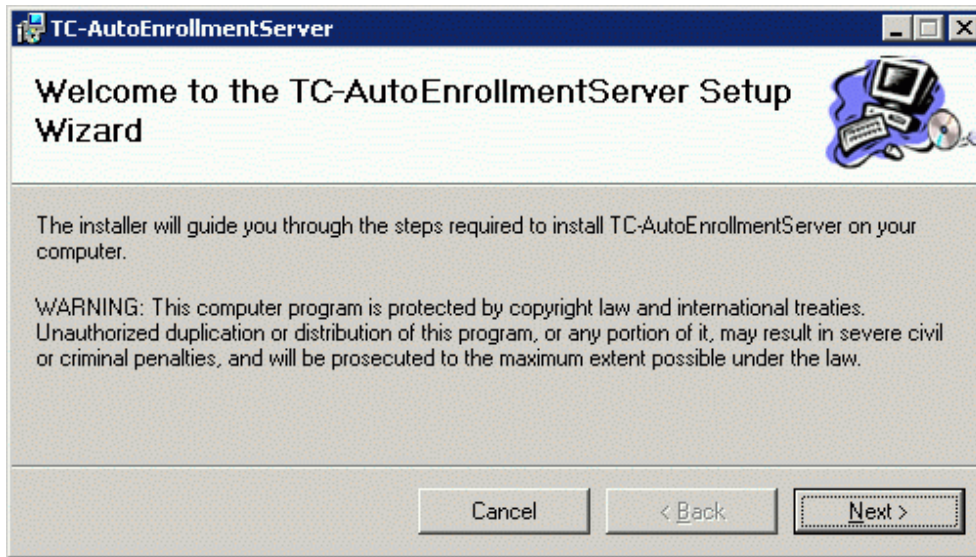


Figure 10: Installing the software - Welcome screen

3. This Microsoft Installer Package (msi) will guide you through the process of installing the software on your system. Click **Next** to continue.

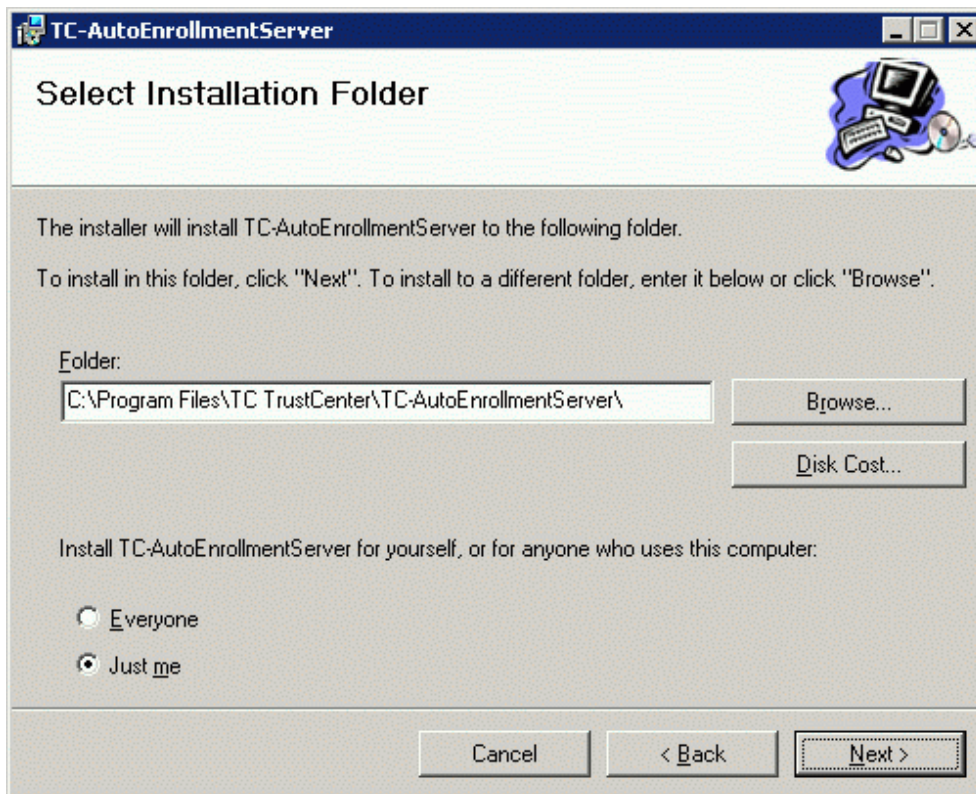


Figure 11: Installing the software - Selecting the installation folder

4. Select the folder in which you want to install the TC AutoEnrollment Server components and specify whether you want the installer to create start menu links for all users or only for the current user. Click **Next** to continue.

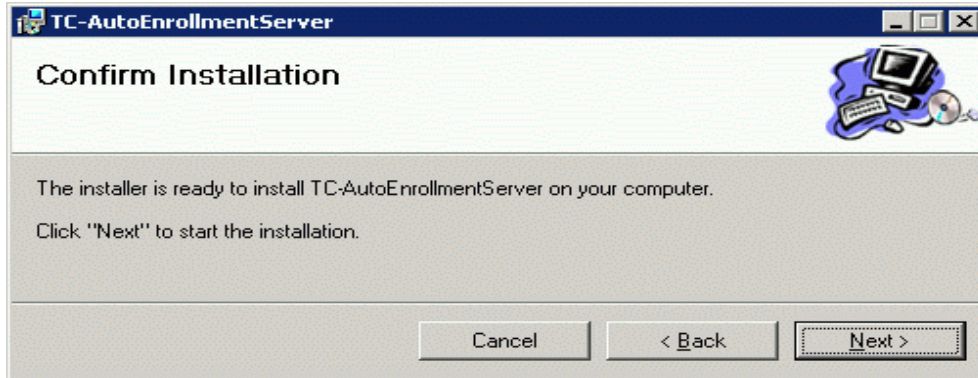


Figure 12: Installing the software - Confirming the installation

5. Click **Next** to start the installation.

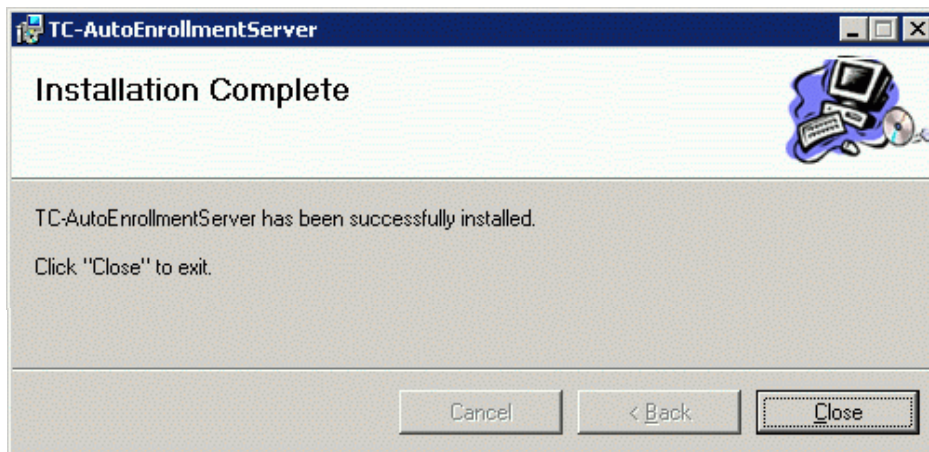


Figure 13: Installing the software - Installation is completed

6. When all the files have been installed on your system, the Microsoft installer presents the above last page of the installation procedure.
7. Continue with the instructions in section 3.2 “Setting Autoenrollment permissions” to complete the installation.

3.2. Setting Autoenrollment permissions

After installing the actual software as described in the previous section you have to check and set a few parameters manually. Complete the following steps:

1. Click on **Start | Administrative Tools | Component services** and navigate to DCOM Config as shown in figure 14.

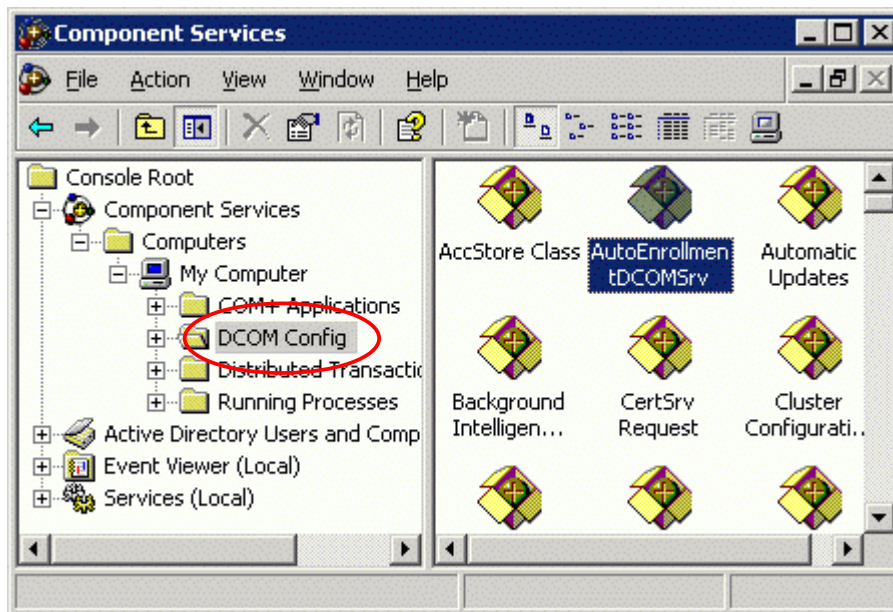


Figure 14: Setting enrollment permission for the new server

2. In the pane on the right locate the entry AutoEnrollmentDCOMsrv and open its context menu by right-clicking on the icon. In the context menu select **Properties**.
3. Select the **Security** tab.

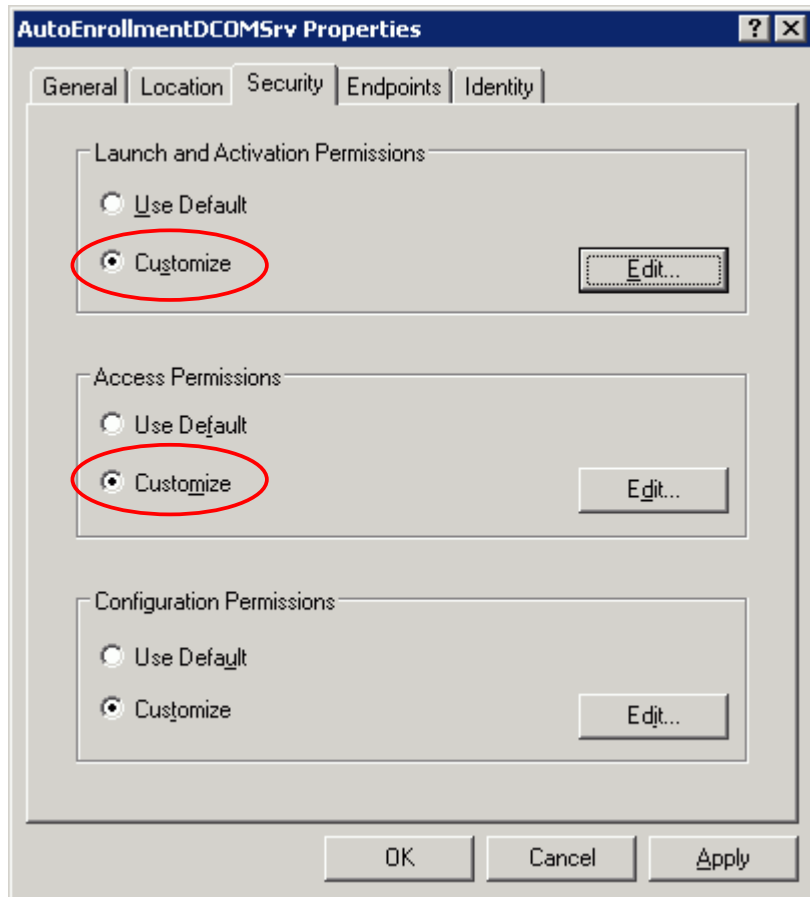


Figure 15: Setting enrollment permissions - the Security tab

4. Under **Launch and Activation Permissions** select the **Customize** option and click on **Edit**.

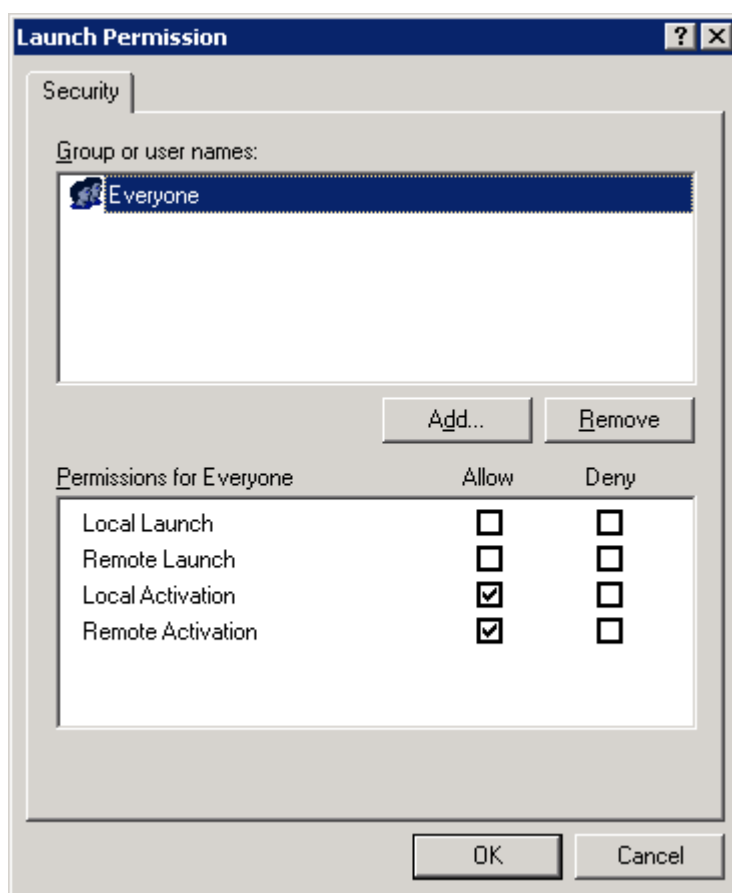


Figure 16: Setting enrollment permissions - Launch and Activation settings

5. Make sure to check both **Local Activation** and **Remote Activation** but to uncheck **Local Launch** and **Remote Launch** for each group of users and/or machines you want to be able to enroll for certificates. In case the desired groups are not listed yet you can add them by clicking **Add** and supplying their names in the dialog box. If you have no special security requirements, you may want to grant local and remote activation to the group **Everyone** and remove the other trustees from the list.
6. Repeat steps 4 and 5 for the **Access permissions**. Again, you must add your domain groups if they are not already listed. Here you have to grant local and remote access to the groups you want to be able to enroll for certificates. If you have no special security requirements, you may want to grant **Local Access** and **Remote Access** to the group **Everyone** (see figure 17) and remove the other trustees from the list:

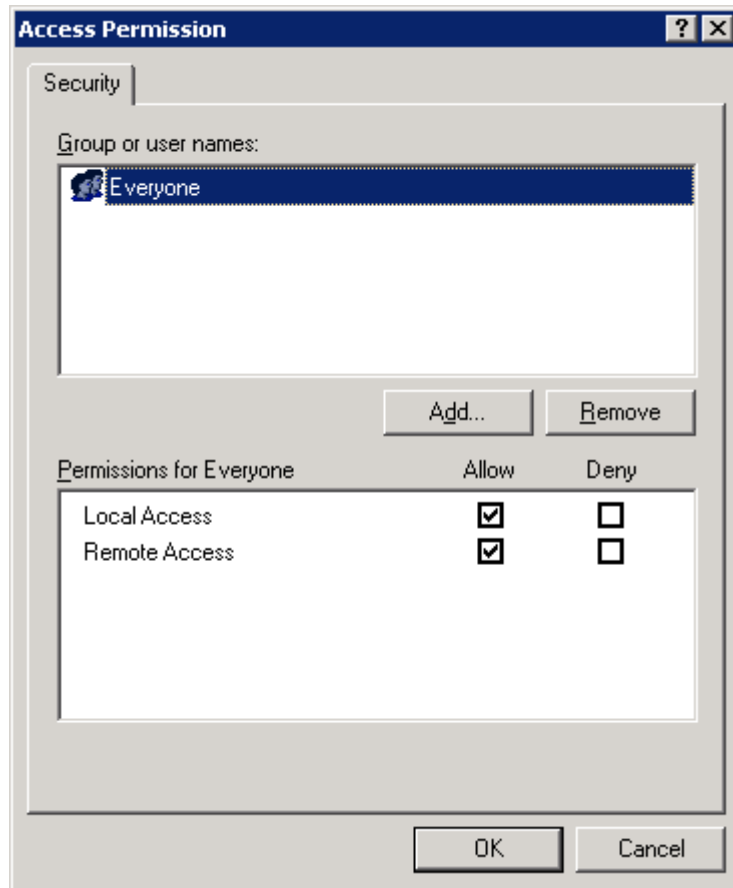


Figure 17: Setting enrollment permissions - Access permissions

7. Click OK to close the dialog and apply the changes.



Anytime the TC TrustCenter AutoEnrollment Server is updated or re-installed, you will need to reconfigure the changes as described in this chapter.

3.3. Setting autoenrollment service properties

This section describes how to check and set autoenrollment service properties. To display or change the settings of the autoenrollment service:

1. Click on **Start | Administrative Tools | Services** to open the Windows Service Manager.

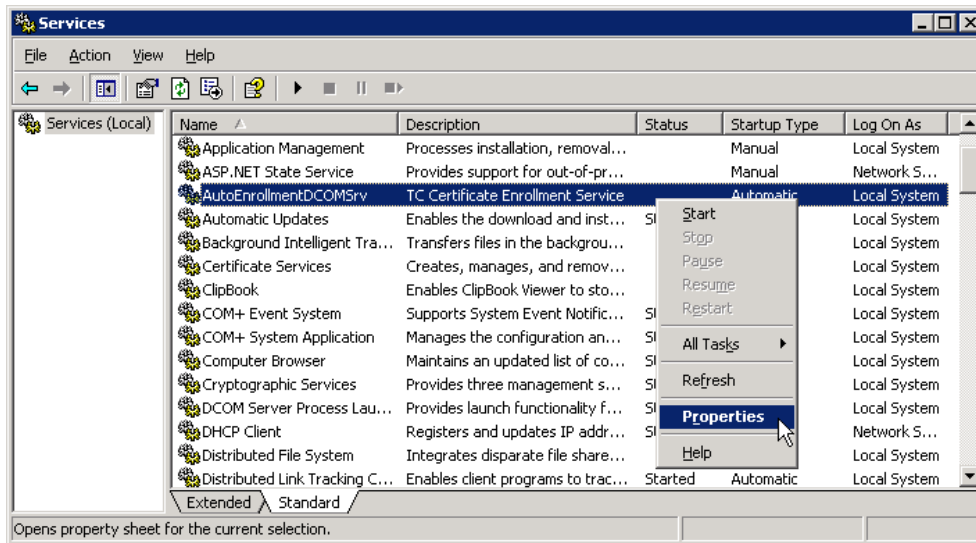


Figure 18: Opening the autoenrollment service's properties

2. Click on **Properties** in the context menu of the AutoEnrollmentDCOMsrv element.

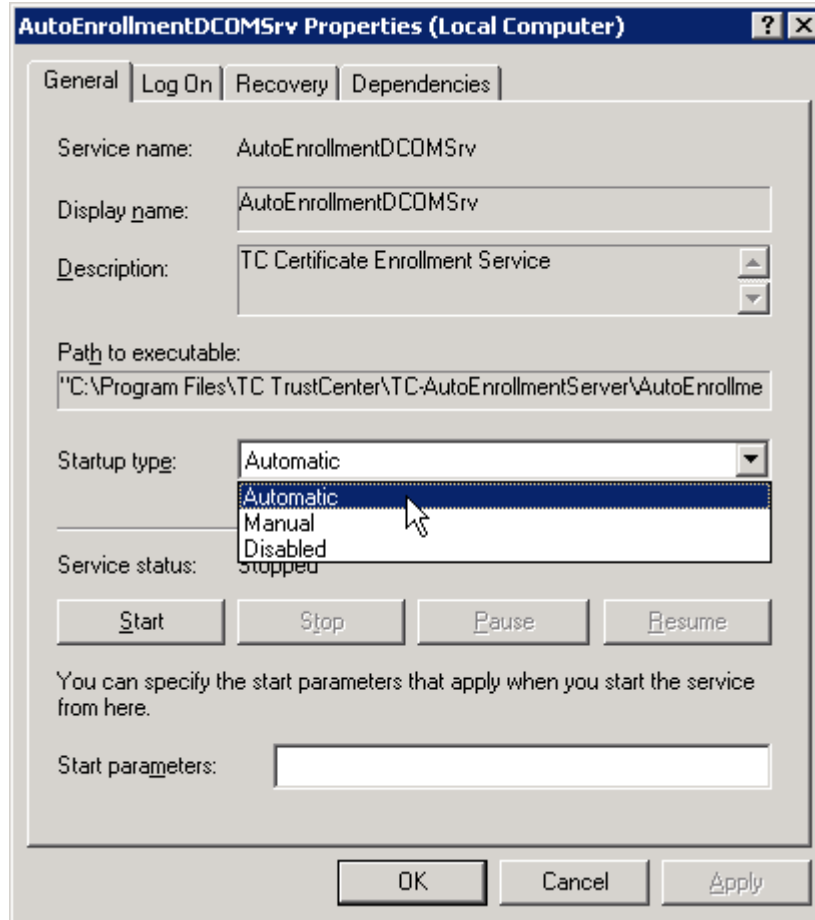


Figure 19: Setting the service's startup type

3. Make sure to select Automatic under **Startup type**. This will ensure that the TC AutoEnrollment Service is started automatically by the operating system whenever the computer is rebooted.



The service properties dialog offers a set of buttons to start, stop, pause and resume the service. Please do not start the service for now, because you first have to configure it. See Chapter 4 “Configuring the TC AutoEnrollment Server” for details.

4. Click OK to apply the settings.

3.4. Allow publishing to Active Directory

The computer running the TC TrustCenter AutoEnrollment Server must be a member of the Active Directory group **Cert Publishers** in order to be

allowed to publish newly issued certificates and certificate revocation lists (CRLs) to the ADS. To make the server's computer a member of the cert publishers group:

1. Log on as an administrator.
2. Select **Administrative Tools | Active Directory Users and Computers**
3. Expand the tree view on the left to display your domain and click on **Users**.
4. Double-click the **Cert Publishers** group in the right panel and select the **Members** tab.
5. Click **Add** and add the computer running the server.

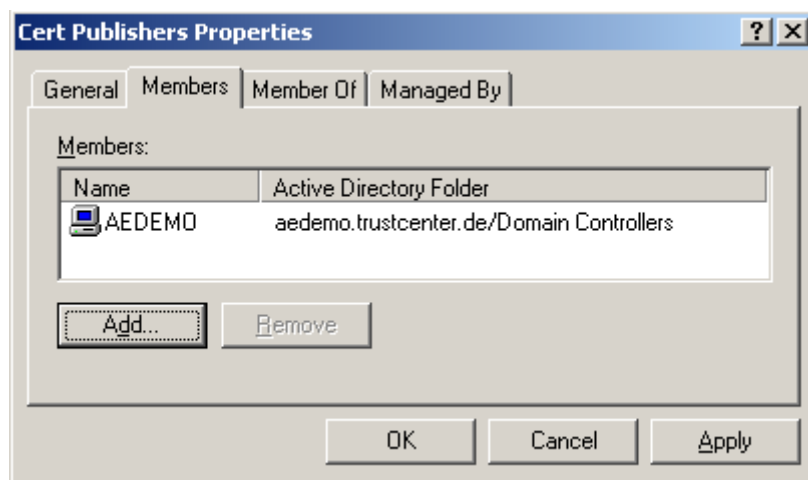


Figure 20: Publishing to Active Directory

In order for the new group membership to take effect you run `grpupdate /force`.

4. Configuring the TC AutoEnrollment Server

After installing the software and setting up autoenrollment permissions you have to configure the TC TrustCenter AutoEnrollment Server for your company. This Chapter will guide you through the steps to configure and run your new autoenrollment server. Topics in this Chapter include:

- starting the AEConfig configuration tool.
- setting up the PSE and logging values
- retrieving configuration data from TC TrustCenter by clicking the **Fetch Config** button.
- saving the setup

4.1. Using the Configuration tool

To use the TC TrustCenter AutoEnrollment Server you must first set a number of configuration values by using the configuration tool. This tool is called AEConfig. The tool requires the user to have administrative privileges in order to write data to ADS.

1. Logon to the computer as Administrator or as another user who is a member of the **Domain Administrators** group. In order to properly retrieve the configuration data, you need to be **enterprise admin**, i.e. have write access to **CN=Public Key Services,CN=Services,CN=Configuration** in the **Configuration** partition of Active Directory.using ADSI Edit.
2. Run AEConfig by clicking on **All Programs | TC TrustCenter | TC AutoEnrollmentServer | Autoenrollment Configuration** in the Start menu.

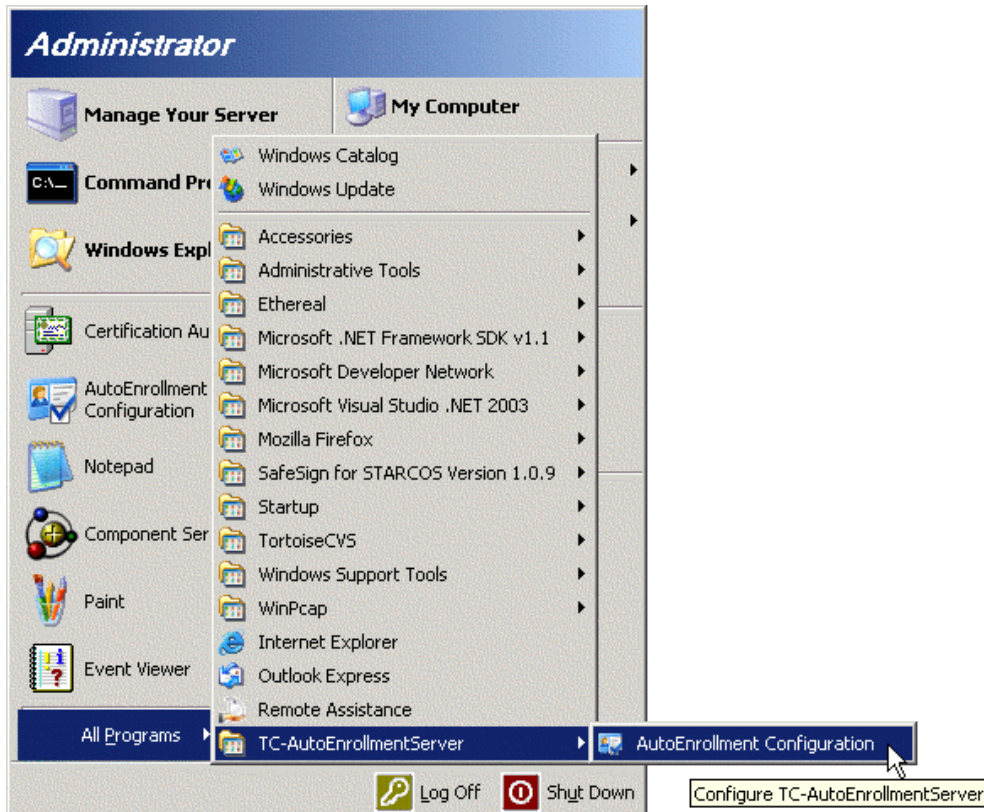


Figure 21: Starting the configuration tool

When you run AEEConfig for the first time, it presents you with the following dialog:

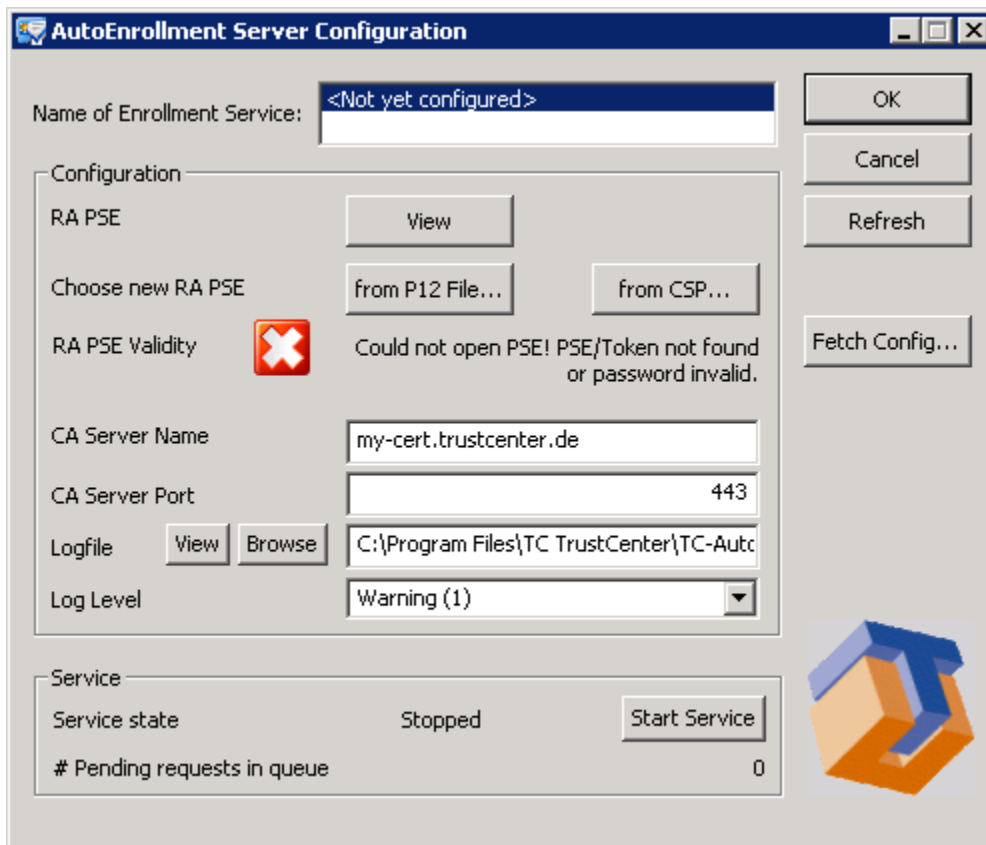


Figure 22: Running AEConfig for the first time

To configure the autoenrollment service AEConfig accepts the following values and settings:

- **RA PSE: View**
Click the **View** button to display information about the selected RA PSE.
- **Choose new RA PSE**
You must select the PSE (Personal Security Environment) that is used to sign and send requests to the TC TrustCenter CA. The PSE is provided by TC TrustCenter either as a file or on a USB security token device. You can select it in either of two ways:
 - a. **... from .P12 file**
Click on this button to open a dialog that lets you pick the .p12 file containing the desired PSE:

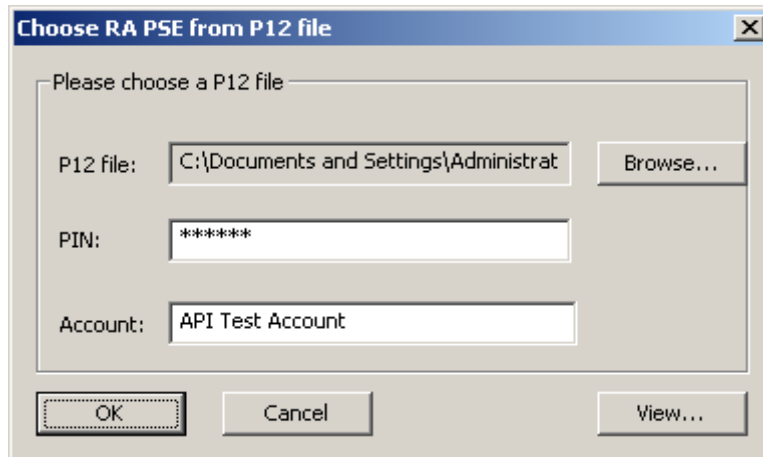


Figure 23: Choosing a PSE from a .p12 file

You must provide the path to a PKCS#12 (.p12) file containing the Personal Security Environment (PSE).

- a. Click on **Browse...** to navigate to the desired file system folder. Highlight the filename and click on **Open** to use the selected file.
 - b. Fill in the PSE's PIN to unlock the PSE.
 - c. Enter the name of your TC Enterprise ID or TC EID QuickStart Account (see **Configuration | Account Settings field | Account Name** in the TC Enterprise ID or TC EID QuickStart web portal). If you are using AutoEnrollment in conjunction with TC Enterprise ID 2008 or prior versions this field must remain empty as there is no account concept.
 - d. Click on **OK** to close the dialog.
2. **... from CSP**
Click on this button to open a dialog that lets you pick the desired certificate:

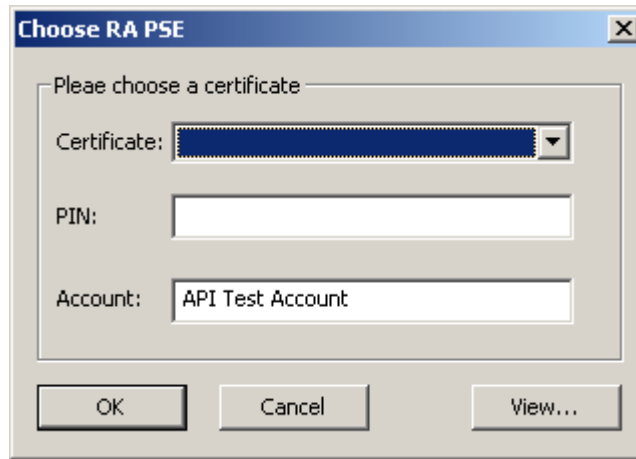


Figure 24: Choosing a PSE from the CSP list

The drop down list contains all hardware-based certificates currently available to the system.

- a. Select the desired certificate from the drop down list.
 - b. Fill in the PIN to unlock the private key of the certificate.
 - c. Enter the name of your TC Enterprise ID or TC EID QuickStart Account (see **Configuration | Account Settings field | Account Name** in the TC Enterprise ID or TC EID QuickStart web portal). If you are using AutoEnrollment in conjunction with TC Enterprise ID 2008 or prior versions this field must remain empty as there is no account concept.
 - d. Click on **OK** to close the dialog
- **RA PSE Validity**
When you have selected a PSE file and supplied the correct PIN, AEConfig will update the message about the token's validity. Here is an example of AEConfig's validity check:

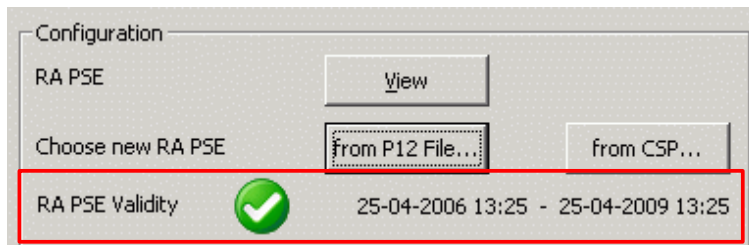


Figure 25: Checking the PSE's validity using AEConfig

- **CA Server Name and CA Server Port**

Fill in the URL and the port number of the web server holding the configuration data provided by TC TrustCenter. AEConfig uses the PSE to authenticate to the web server and to download the configuration for your autoenrollment server installation. In addition to that, the URL and Port values will be used by the autoenrollment service to submit requests to the TC TrustCenter CA.

The values for TC Enterprise ID 2008 with TC AE Server are:

- **CA Server Name** `pki.trustcenter.de`
- **CA Server Port** 443

The values for using TC EID QuickStart or TC Enterprise ID 2009 with TC AE Server are:

- **CA Server Name** `my-cert.trustcenter.de`
- **CA Server Port** 443

- **log file**

The path and filename of the log file. This file will contain information logged by the autoenrollment service as well as by AEConfig.

- **Logfile: View**

Click the **View** button to open the log file in a text editor.

- **Logfile: Browse**

Click the **Browse** button to navigate to the directory where you want the log file to be written. Input or highlight the desired filename and click on **Save** to use the selected file.

- **Log level**

There are four different predefined log levels: **Audit**, **Warning**, **Info** and **Trace**. See section 9.1 “Understanding the different log levels” for details.

- **Service: Service State and Start Service**

Service State indicates whether the autoenrollment service is currently running or not.

Start/Stop Service When you have completely configured the autoenrollment service you can start/stop the service with the button on the right.

- **Pending Requests in Queue**

This indicates the number of pending certificate requests (initial and renewal requests).

- **Fetch Config**

To fetch the configuration, the enterprise admin rights are required,

in particular write access to **CN=Public Key Services,CN=Services,CN=Configuration** in the partition of Active Directory.



AEConfig needs to be able to establish an encrypted SSL connection with TC TrustCenter's servers for downloading your configuration data. For this connection the port number specified under **CA Server Port** will be used. If your organization's network is secured by a firewall to block unwanted incoming connections or to restrict outbound connections originating from inside the network, make sure to configure your firewall to allow outbound connections to TC TrustCenter's download server on port 443 from the machine running AEConfig.

If you want to use a non-standard port number for downloading the configuration data you must setup internal port forwarding on your network to route network traffic from/to port 443 of TC TrustCenter's download server. Please contact your network administrator for assistance.

The certificate used for SSL client authentication must belong to a user with PKI Administrator role.



Since the TC TrustCenter AutoEnrollment Server runs as a service, it doesn't know anything about the proxy settings of Microsoft Internet Explorer run as some Administrator account. To copy the current user's proxy settings to the service account use `proxycfg -u`.

Proxycfg.exe is included with Windows Server 2003 (in path `%WINDIR%\system32`).

On Windows Server 2008 use `netsh.exe` with command `winhttp set proxy`.

AEConfig's display should now look similar to that depicted in figure 26.

When you have configured all the above options use AEConfig's **Fetch Config** button to download your configuration data from TC TrustCenter. See Section 4.2 "Downloading the configuration data" for details.

Note that the name of the enrollment service will be displayed as soon as you downloaded the configuration data from TC TrustCenter.

Before you can use new Affiliates from the TC EID QuickStart Account you need to restart the Auto Enrollment service. For more Information about

the Affiliates and the TC AE Server see the FAQ on our website (www.trustcenter.de/en/infocenter/faq.htm)

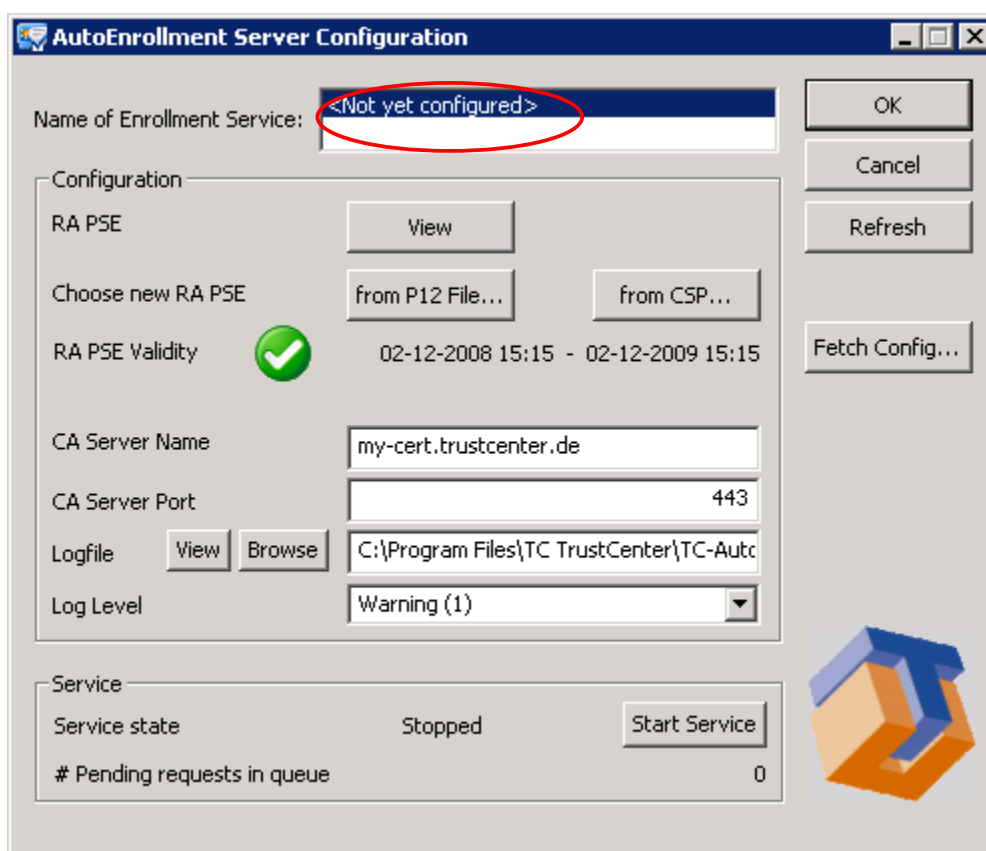


Figure 26: AConfig is now ready to download the configuration data

Do not start the service unless you successfully configured all the above options and downloaded your configuration data from TC TrustCenter's web servers.



After changing one or more configuration settings in AConfig, e.g. the log level, you have to restart the service in order for the changes to take effect.

The autoenrollment service will publish issued certificates and CRLs to Active Directory. AConfig will take care of creating the CDP in ADS for you upon downloading the configuration from TC TrustCenter.

4.2. Downloading the configuration data

In the previous section we described how to setup AEConfig in order to download the configuration data from TC TrustCenter's web servers. You need this data to use your autoenrollment service with TC TrustCenter's CA.

The configuration data is published in the Active Directory and includes:

- details about the enrollment service and the templates it supports.
- the list of certificate templates offered by the CA.
- TC TrustCenter's CA certificate.



To have AEConfig successfully store the configuration data in ADS and the system's registry you need administrative privileges. If you have insufficient privileges to write to these resources, AEConfig will not be able to publish and install the configuration data. Subsequently, your autoenrollment service will not operate properly.

Complete the following steps to download the configuration data from TC TrustCenter:

1. In order to be able to download the configuration data make sure the autoenrollment service is not running. You can stop it by clicking on the **Stop Service** button in AEConfig.
2. Start the download process by clicking on **Fetch Config**.
3. AEConfig displays a warning message telling you that downloading and installing configuration data may overwrite already existent templates, certificates and enrollment service settings. Templates and settings that are not a part of the autoenrollment server will not be changed in any way.

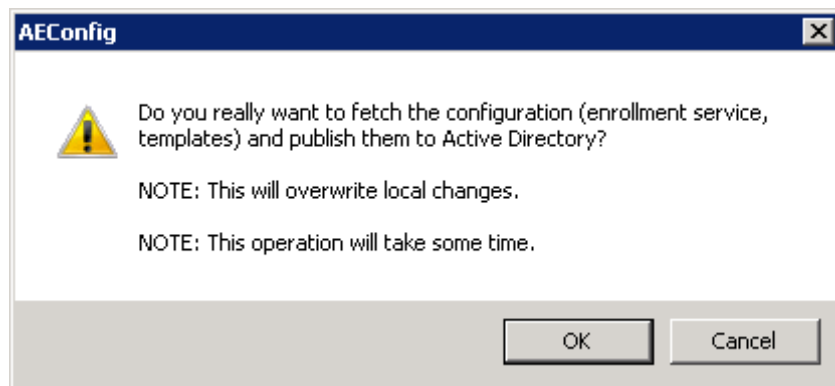


Figure 27: Fetching the configuration data with AEConfig

Click on **OK** to proceed with the download or click on **Cancel** to abort.

4. AEConfig informs you about the status of the download and publishing progress by displaying a series of message boxes.
5. The last message box informs you that the publishing process has finished successfully.



It can take some time for the certificates and enrollment service to be published and visible on every machine on the network. See section 5.3 “Replicating certificate templates and policies” for details on how to force a group policy update for a specific machine.

Figure 28 illustrates a set of freshly installed certificate templates. To check your installed templates:

1. Click **Start | Run**.
2. Type `mmc` in the **Open** field and press Enter.
3. Double-click **Certificate Templates** to expand the list of available templates in the right pane of the console.

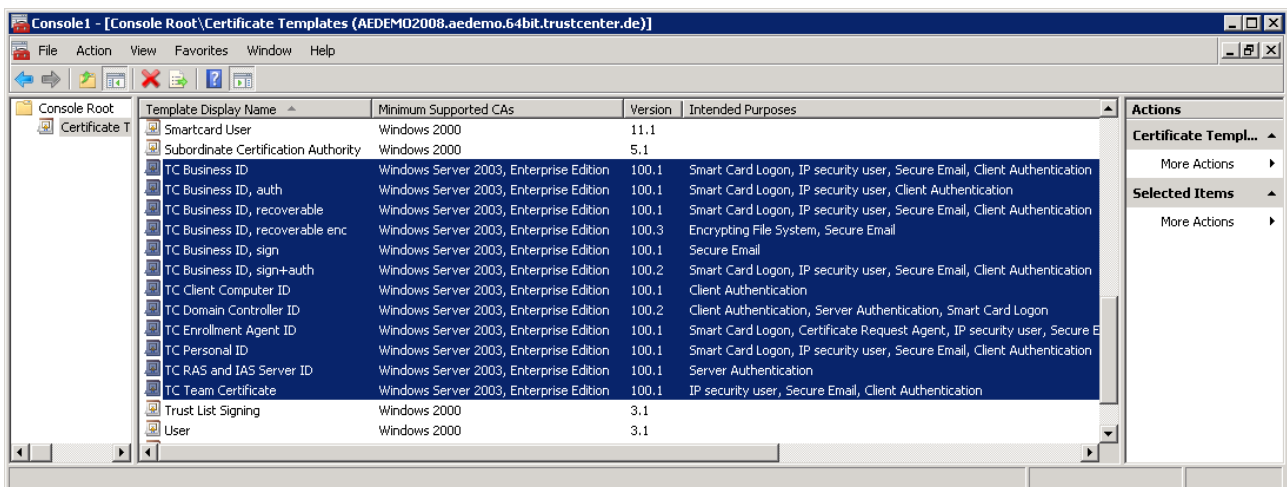


Figure 28: Certificate Templates provided by TC TrustCenter

4.3. Saving AEConfig's settings

AEConfig stores its settings in the operating system's registry.

To save the configured values – such as the server and port number and the name of the log file – click on **OK**.

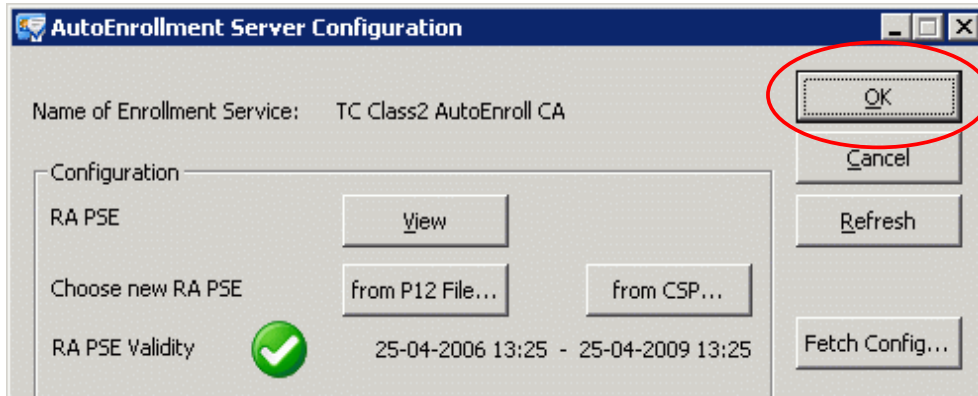


Figure 29: Saving AEConfig's settings

4.4. Advanced Configuration

The TC AutoEnrollment Server retrieves information about the certificate requester from the the Active Directory. The following table shows the mapping of Active Directory LDAP Attributes to user data fields in the back-end system.

<i>LDAP Attribute</i>	<i>User Data Field</i>	<i>Comment</i>
Common-Name (Attribute-Id 2.5.4.3)	(only used for TC Enterprise ID 2008 and prior)	The LDAP Attribute source can be modified using the registry entry GetCommonNameFrom (REG_SZ)
Title (Attribute-Id 2.5.4.12)	Salutation	The LDAP Attribute source can be modified using the registry entry GetTitleFrom (REG_SZ). If the title field is used for a different purpose, set the GetTitleFrom registry entry to an empty string ("").
Employee-Number (Attribute-Id 1.2.840.113556.1.2.610)	External ID	The LDAP Attribute source can be modified using the registry entry GetExternalIDFrom (REG_SZ). If the Employee-Number should not occur in the certificate, set the

<i>LDAP Attribute</i>	<i>User Data Field</i>	<i>Comment</i>
		GetExternalIDFrom registry entry to an empty string (“”).
Surname (Attribute -Id 2.5.4.4)	Last Name	Value must be non-empty for each user.
Given-Name (Attribute-Id 2.5.4.42)	First Name	Value must be non-empty for each user.
Initials (Attribute-Id 2.5.4.43)	Middle Initials	
Department (Attribute-Id 1.2.840.113556.1.2.141)	Department	
Company (Attribute-Id 1.2.840.113556.1.2.146)	Affiliate	A matching affiliate is searched by matching the Company attribute with an Affiliate Displayname .
User-Principal-Name (Attribute-Id 1.2.840.113556.1.4.656)	User Principle Name	This value is required for using certificates for smart card logon.
E-mail Addresses (Attribute-Id 0.9.2342.19200300.100.1.3)	Email and Username	Value must be non-empty for each user.

Table 2: Relevant LDAP Attributes

The TC AutoEnrollment Server supports the following registry settings. These settings are usually maintained using the AEConfig tool.

<i>Name</i>	<i>Default</i>	<i>Comment</i>
GetCommonNameFrom	cn	Name of LDAP attribute to be used as common name in the certificate.
GetExternalIDFrom	employeeNumber	Name of LDAP attribute to be used as External ID (i.e. serialNumber in the certificate's Subject-DN). Set this entry to an empty string if no External ID should be used.
GetTitleFrom	title	Name of LDAP attribute to be

<i>Name</i>	<i>Default</i>	<i>Comment</i>
		used as salutation. Set this entry to an empty string if no salutation should be used. Please note that email templates might rely on it.
ServiceCN-Postfix	(empty string)	The value of this entry will be appended to the Name of the Enrollment Service (Service-CN). If you want to set up multiple enrollment servers servicing the same certificate types (i.e. high availability configuration) you must set a different value for each of the instances. The main instance should have an empty string.
ConfigName	MultiCA	This value is used to identify the configuration in the CA backend. Do not change this entry!
AccountName		The name of your TC Enterprise ID or TC Enterprise ID QuickStart account.
CAHostname	my-cert.trustcenter.de	Servename of the CA backend.
CAPort	443	Port of the CA backend.
CANames		List of supported CAs. Do not change this entry!
DBName		Name of the queue for the requests.
LogFile		Name of the logfile
LogLevel		LogLevel
RA_PSE_Fingerprint		This value identifies the certificate to be used for client authentication to the CA backend. Do not change this entry!
RA_PSE_Password		This is the encrypted password to access the certificate/private key for client authentication to

<i>Name</i>	<i>Default</i>	<i>Comment</i>
		the CA back-end. Do not change this entry!
TARGETDIR		Installation folder. Do not change this entry!
EnrollServiceDisplayName		Displayname of the default enrollment service. Do not change this entry!
EnrollServiceName		Name of the default enrollment service. Do not change this entry!

Table 3: Description of Registry Settings



Do not change any of these values while the TC AutoEnrollment Server or the AConfig tool is running!

*After changing **AccountName**, **CAHostname**, **CAPort**, or **ServiceCN-Postfix** you have to do **Fetch Config** again (see section 4.2 “**Downloading the configuration data**”) to activate the changes.*

5. Using the TC AutoEnrollment Server

After installing and configuring your TC TrustCenter AutoEnrollment Server you can now start to use the service to request certificates from the TC TrustCenter CA. In this Chapter the following topics are discussed:

- Starting and stopping the server
- Preparing certificate templates
- Replicating certificate templates and policies
- Requesting certificates
- Autoenrolling for a certificate
- Monitoring enrollment activities
- Software update of TC AutoEnrollment Server

5.1. Starting and stopping the server

Starting and stopping the autoenrollment server means to start or stop the autoenrollment service. To start or stop the service you can use the built-in Windows service maintenance interface but we recommend to use the AEConfig tool. By default, the autoenrollment service is started automatically upon system startup.

5.1.1 Using AEConfig to start or stop the service

1. Logon to the computer as Administrator.
2. Run AEConfig by clicking on **All Programs | TC TrustCenter | TC AutoEnrollmentServer | AutoEnrollment Configuration** in the Start menu.
3. Depending on the service's current status – either **Running** or **Stopped** –
 - Click on **Start Service** to start the autoenrollment service or
 - Click on **Stop Service** to stop the autoenrollment service.

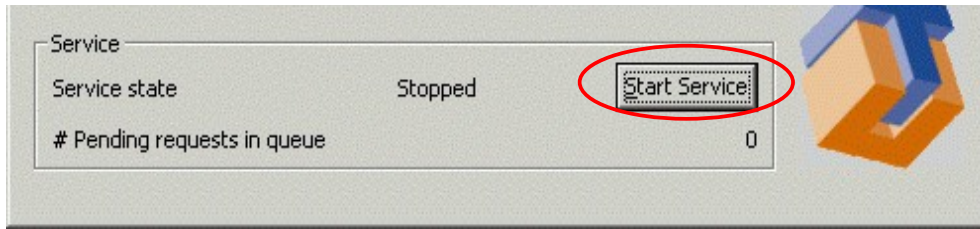


Figure 30: Starting the autoenrollment service

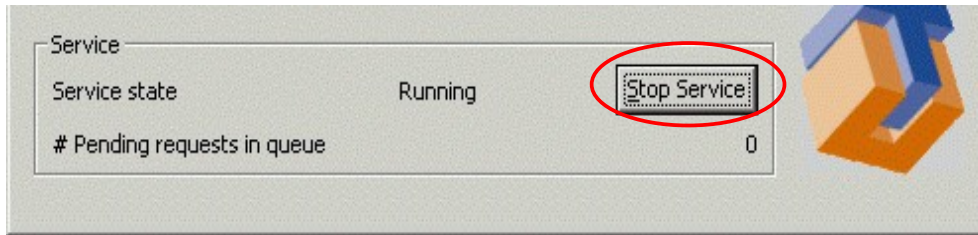


Figure 31: Stopping the autoenrollment service

Please note that the service state may not always be accurately displayed if the service is started and stopped using the Windows Service Manager. In AEConfig, please click on **Refresh** to update the display of the service state.



When the service is running, you can neither configure the desired PSE nor download the configuration data from TC TrustCenter. You have to stop the autoenrollment service first. Figure 32 illustrates the normal appearance of AEConfig while the autoenrollment service is running.

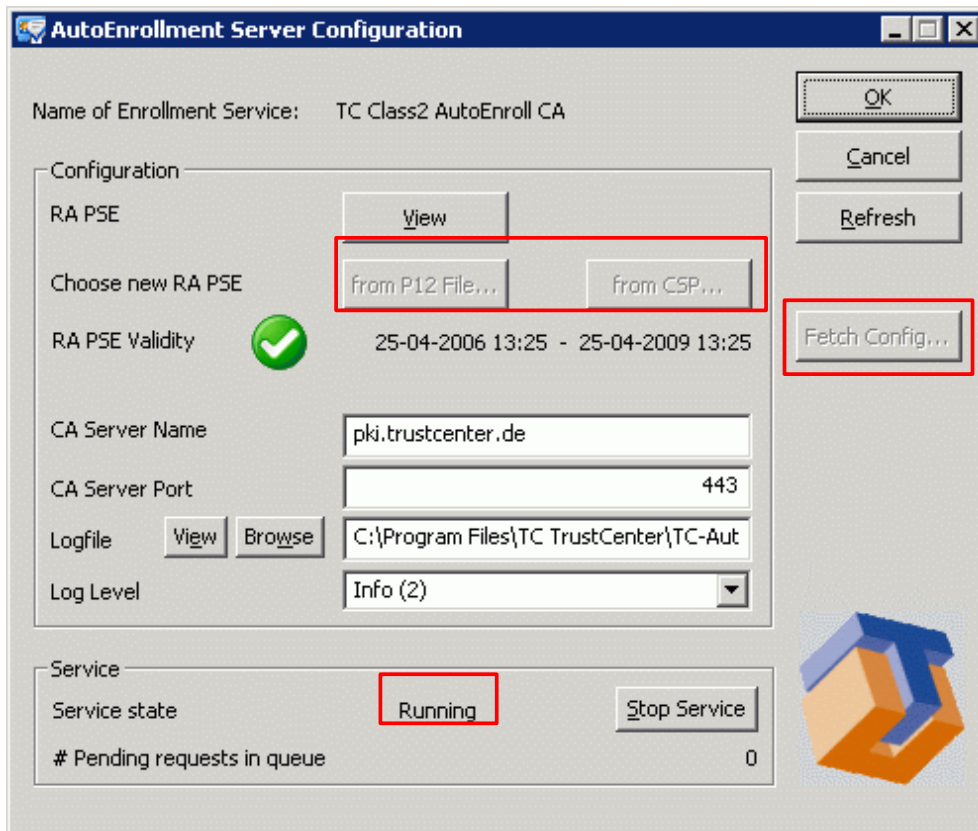


Figure 32: Some controls are disabled while the service is running

5.1.2 Using the Windows service Manager to start or stop the service

1. Logon to the computer as Administrator.
2. Click on **Start | Administrative Tools | Services** to open the Windows Service Manager.
3. Click on **Properties** in the context menu of the AutoEnrollmentDCOMsrv element.

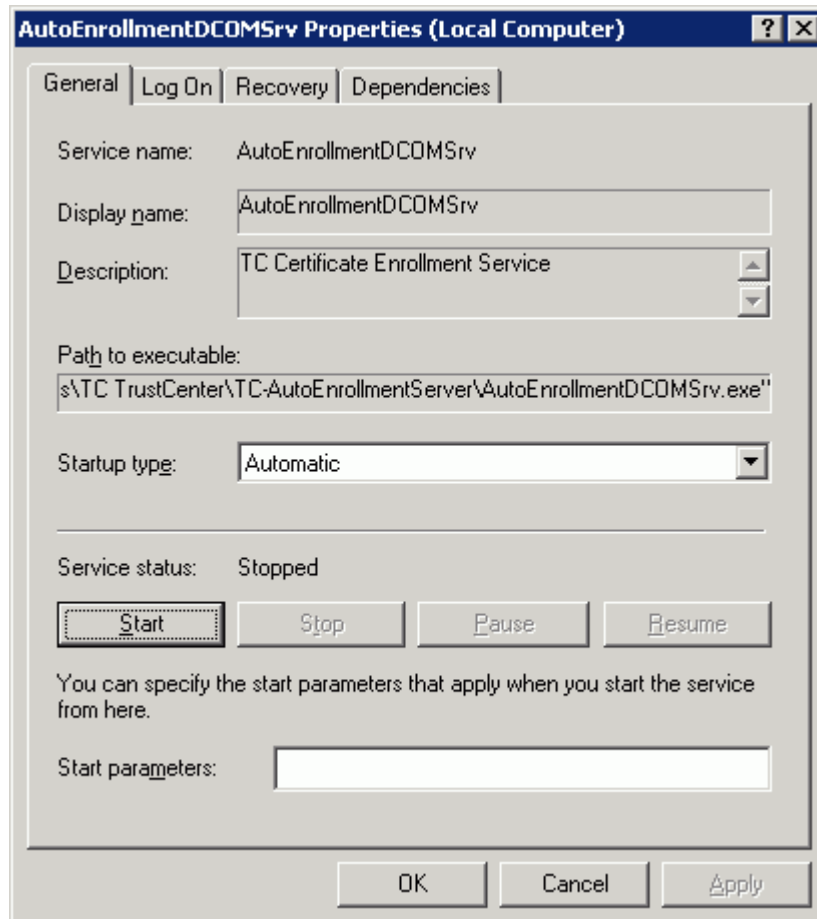


Figure 33: Starting or stopping the autoenrollment service

4. Click on **Start** to start the TC AutoEnrollment Server or click on **Stop** to stop the service.
5. Depending on the service's current status – either **Started** or **Stopped** –the status will change from ...
 - Started → Stopping → Stopped
 - Stopped → Starting → Started
6. Click on OK to close the properties dialog.

5.2. Preparing certificate templates

The default set of certificate templates has been automatically installed when downloading the configuration (see section 4.2). In order to deploy certificates you must assign the enroll and/or autoenroll permissions to the appropriate groups or users for each certificate template separately.

5.2.1 Certificate template versions

TC TrustCenter provides customers with v2 certificate templates.

The older v1 templates may not be used for autoenrollment and are not supported by the TC AutoEnrollment Server. Nevertheless, you can supersede v1 templates by v2 templates.

5.2.2 Certificate templates used by the TC AutoEnrollment Server

TC TrustCenter provides a set of pre-configured templates. These templates are automatically assigned to the autoenrollment service in Active Directory associating TC TrustCenter as the certification authority that handles requests generated by use of these templates.

As each certificate template refers to a specific TC TrustCenter certificate product with a pre-configured set of requirements, restrictions and features, it doesn't make much sense to modify these templates using the corresponding MMC snap-in.

The templates cover a large number of autoenrollment application areas such as:

- Computer certificates for computers in the domain
- Smartcard Logon for users
- IPSec for remote users
- Client certificates for users

5.2.3 Browsing and editing template values

Please refrain from changing any template values. Instead, if you need to adjust any template values contact a TC TrustCenter representative to agree on changes and to have your templates updated automatically.



TC TrustCenter neither supports nor recommends to change any values of the provided templates. Changing these values will cause conflicts resulting in erroneous requests when processed by the TC TrustCenter CA. Furthermore, applied changes may be lost upon certificate template updates initiated by TC TrustCenter.

TC TrustCenter provides you with a set of pre-configured certificate templates which will be installed by the AutoEnrollment Configuration Tool. In case you need additional templates or different template settings you need to contact TC TrustCenter.

You use the Certificate Templates Microsoft Management Console (MMC) to access and create templates. To open Certificate Templates:

1. Log on as an administrator.
2. Click **Start | Run**.
3. Type `mmc` in the **Open** field and press Enter.
4. Select **File | Add | Remove Snap-in** and click **Add**. Windows displays the available snap-ins.

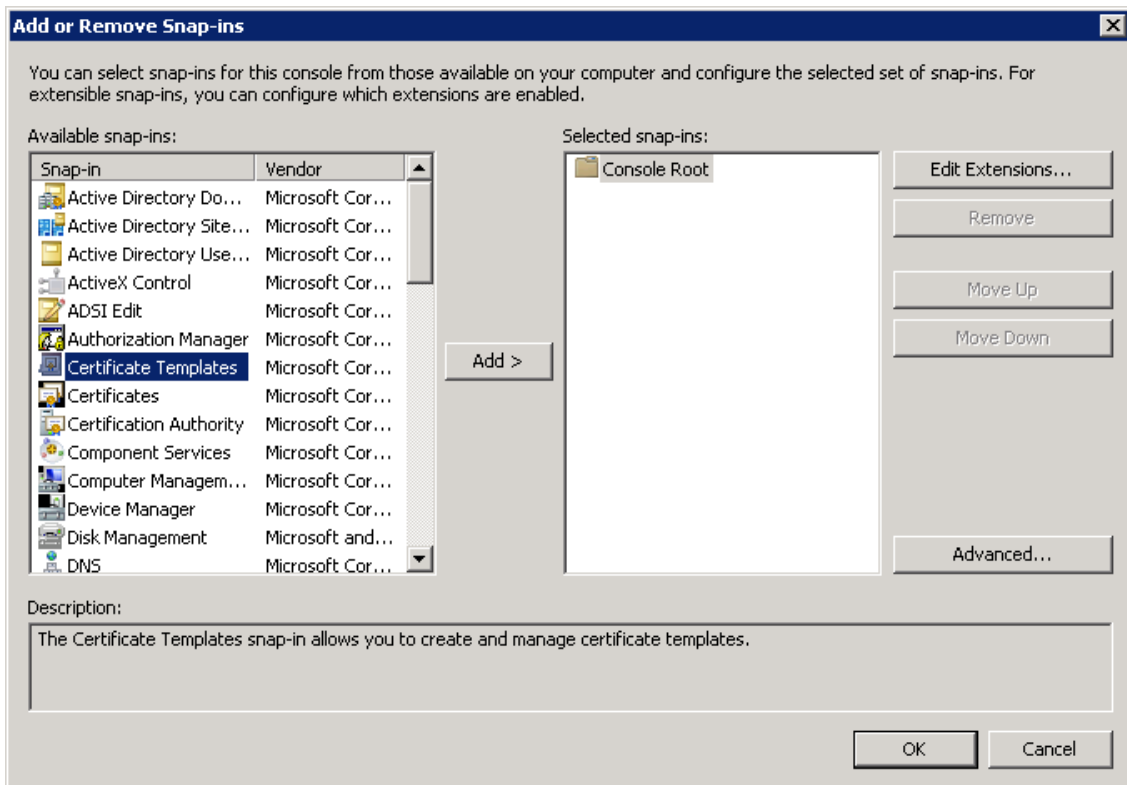


Figure 34: Adding Snap-Ins to the MMC

5. Select **Certificate Templates** and click **Add**.
6. Click **Close** and then **OK**.
7. Double-click **Certificate Templates** to expand the list of available templates in the right pane of the console.

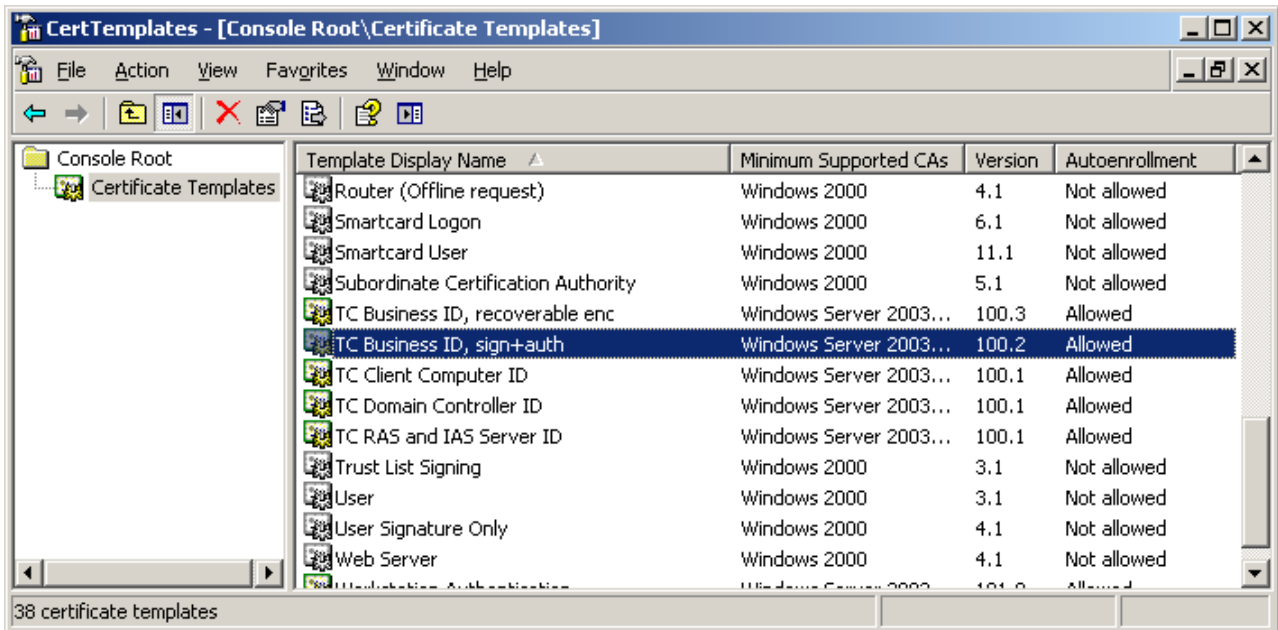


Figure 35: Select Certificate Template for Manual Enrollment

8. v1 and v2 templates can be distinguished by an icon next to the certificate template's name. A gray icon denotes a v1, a colored icon a v2 template. For a full list of Microsoft templates see default templates in [Implementing and Administering Certificate Templates in Windows Server 2003⁹](#).

5.2.4 Key archival

Key archival is a mechanism to backup the private portion of your encryption keys for potential key recovery at a later time.

The TC AutoEnrollment Server supports key archiving.

The process to recover the key (i.e. key recovery) is done using the web interface.

Do not change the default setting for **Archive subject's encryption private key** in the certificate template since it must match the back-end PKI configuration.

5.2.5 Assigning group/user access to templates

The Certificate Template property page contains the **Security Tab**. The **Security tab** allows you to define the DACL (Discretionary Access Control List) for a specific certificate template. The permissions that you assign to the certificate template define which security principals can read, modify, enroll, or auto-enroll for a specific certificate template.

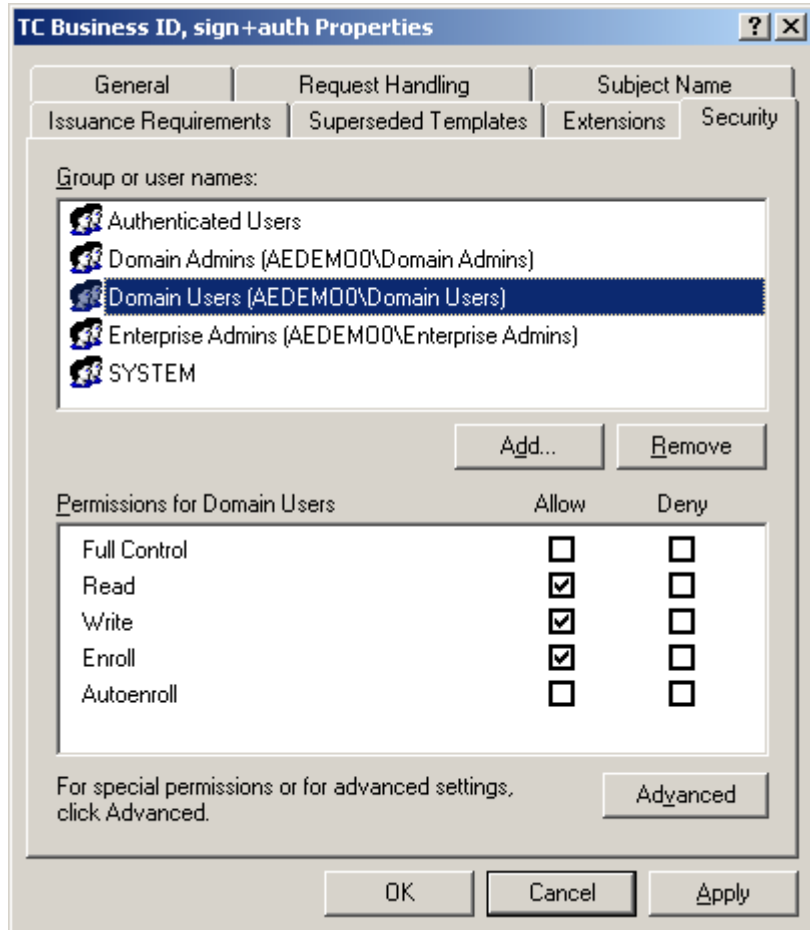


Figure 36: Defining DACL properties for a specific certificate template

Under **Group or user names** the dialog lists all groups and users holding privileges on the currently opened certificate template.

You can add your own network specific group names if you do not use the default group names like **Domain Users** and **Domain Computers**. Once you have added your domain-specific groups assign the appropriate combinations of enroll and auto-enroll permissions to them.

The dialog lists the following permissions: **Full Control**, **Read**, **Write**, **Enroll** and **Autoenroll**.

- **Full Control**
This permission allows a security principal to modify all attributes of

a certificate template, including the permissions for the certificate template.

- **Read**
This permission allows a security principal to see the certificate template when enrolling for certificates. It is required for a security principal to enroll or auto-enroll a certificate; it is required by the certificate server to find the certificate templates in Active Directory.
- **Write**
This permission allows a security principal to modify the attributes of a certificate template, including the permissions assigned to the certificate template.
- **Enroll**
This permission allows a security principal to enroll for a certificate based on the certificate template. To enroll for a certificate, the security principal must also have Read permissions for the certificate template.
- **Autoenroll**
This permission allows a security principal to receive a certificate through the auto-enrollment process. Auto-enrollment permissions require that the user has both Read and Enroll permissions in addition to the Auto-enroll permission.
If **Autoenroll** is enabled every User/Machine that logs on to the domain automatically enrolls for a certificate. To enable autoenrollment you have to
 - Open the Certificate Template you want to autoenroll for (right click on **properties**)
 - Open tab **Issuance Requirements** and make sure nothing is marked.
 - Select the **Security** tab. Be sure that the Users you want to Autoenroll have the permissions for it. Check the two groups **Authenticated Users** and the **Domain Users** and be sure you have marked **Read**, **Enroll**, and **Autoenroll** (see Figure 36 on page 50).

Depending on the specific certificate template you should activate **Read** and **Enroll** and/or optionally **Autoenroll** for the desired group or users.



We highly recommend to use only global or universal groups instead of individual users or computer accounts when assigning template access permissions. Especially in large infrastructures this rule facilitates administration of access rights and it will help you to avoid conflicts and inconsistencies across multiple domain controllers' contexts.

A few more tips and recommendations:

1. Make sure the TC TrustCenter AutoEnrollment Server belongs to a group that also has permission to enroll the template it will use to process requests.
2. It is regarded as a best practice to assign **Read permission to Authenticated group** for all certificate templates. This way all users and computers can read the certificate templates in Active Directory.
3. Restrict **Write** and **Full Control** permissions to **CA managers** to ensure that the templates are not improperly configured.

You can find more details and template access permissions in [Implementing and Administering Certificate Templates in Windows Server 2003](#)¹⁰ at Microsoft Technet.

5.3. Replicating certificate templates and policies

ADS's replication mechanism is used to make certificate templates and policies available to domain controllers existing in your domain. All domain controllers in the forest will receive a copy of any updated configuration container automatically.

Certificates and CRLs are also stored in ADS and they are replicated to each domain controller in the forest. The process of replicating data amongst ADS instances can take up to eight hours. Replication for all computers will occur earlier if the domain controller computer is rebooted. The policy information of a particular machine is refreshed whenever that computer is rebooted.

You can use the **certutil** tool from the Windows 2003 Server Resource Kit to force a client to refresh its policy information:

```
certutil -pulse          (on Windows 2003 and 2008 systems)
```

or

```
dsstore -pulse          (on Windows 2000 systems)
```



You have to repeat this replication step after every modification of certificate templates in order to have the changes be effective immediately. The automatic replication will need more time.

5.4. Manually requesting a certificate

After installing the server and starting the autoenrollment service you should request a few certificates for testing purposes from the TC TrustCenter AutoEnrollment CA. This section will walk you through the process of manually requesting a **TC Business ID** certificate.

1. Log on to the system as Administrator and click **Start | Run**.
2. Type `mmc` in the **Open** field and press Enter.
3. Select **File | Add | Remove Snap-in** and click **Add**. Windows displays the available snap-ins.
4. Select **Certificates** and click **Add**.

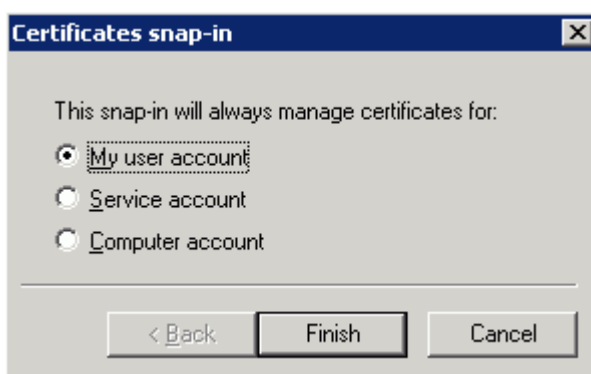


Figure 37: Setting the certificate snap-in to manage the current user's certificates

5. Choose **My user account** from the option group
6. Click on **Finish**, **Close** and then **OK** to return to the MMC console.
7. Expand the tree view on the left to display **Console Root | Certificates – Current User | Personal | Certificates**.
8. Rightclick in the right pane and click on **All Tasks | Request New Certificate...**

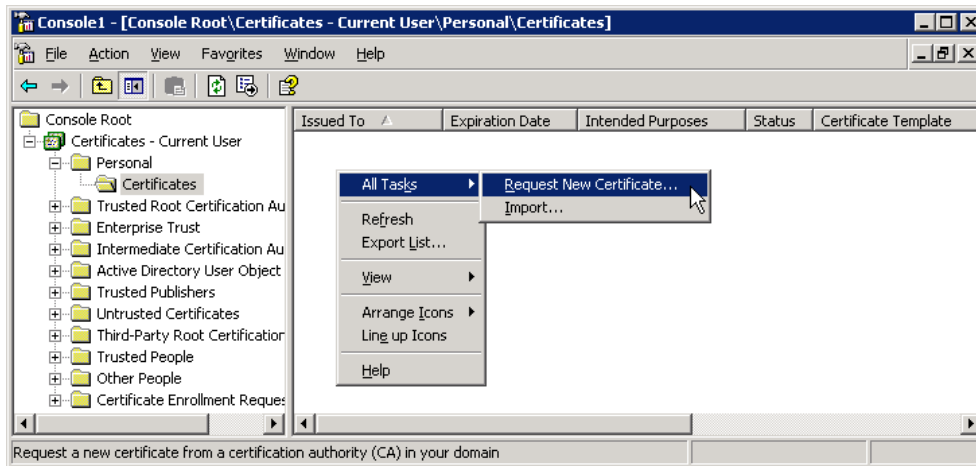


Figure 38: Requesting a test certificate

The MMC snap-in will startup the Certificate Request Wizard as shown in Figure 39:



Figure 39: The Certificate Request Wizard

9. Click on **Next** to proceed to the next wizard page.

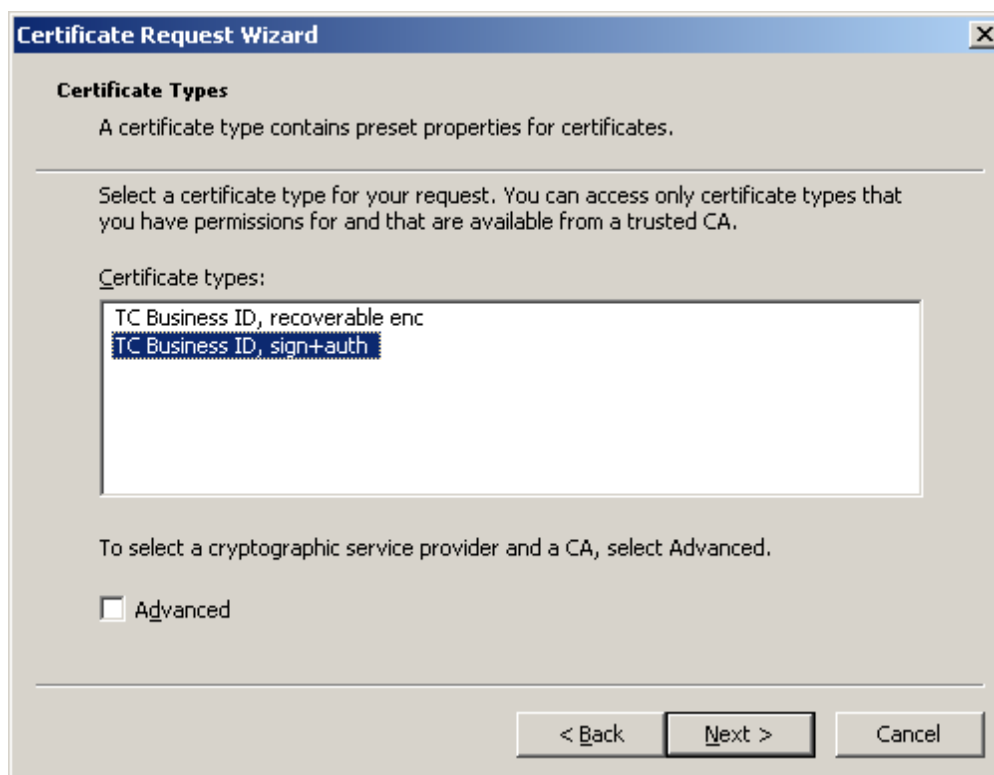


Figure 40: Selecting the certificate type

10. For the purpose of this test select **TC Business ID, sign+auth, 1yr** from the list of certificate types and click **Next**.



Please note that the list only contains certificate templates with the **Enroll** right enabled for the particular user which are intended to be requested by a client as compared to a computer.

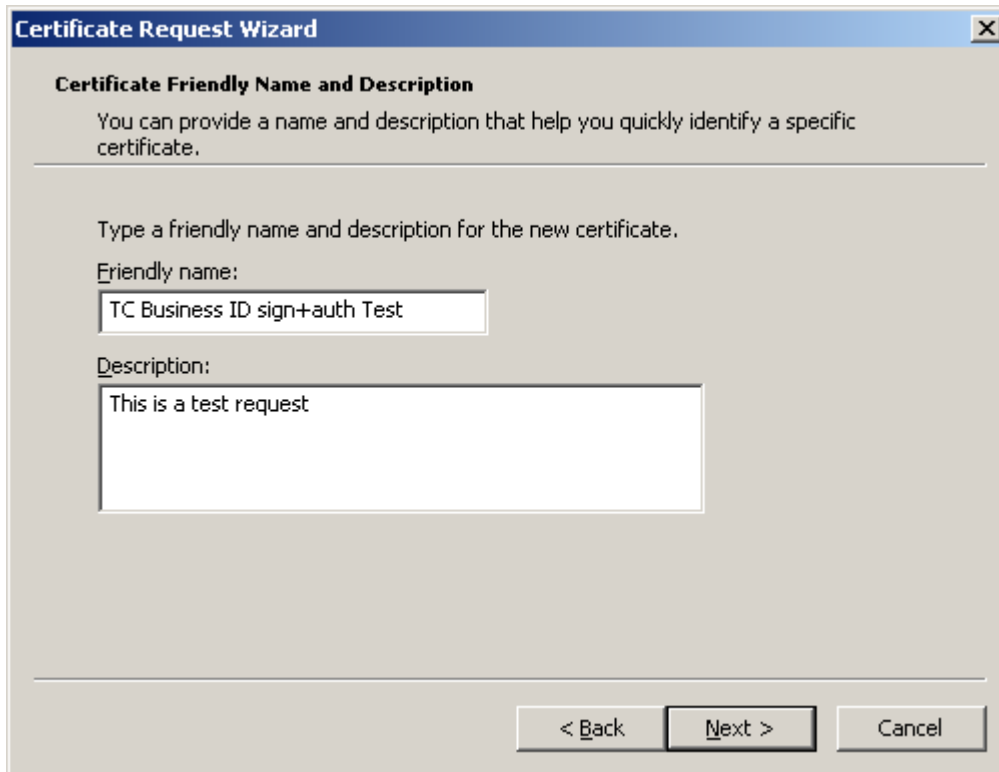


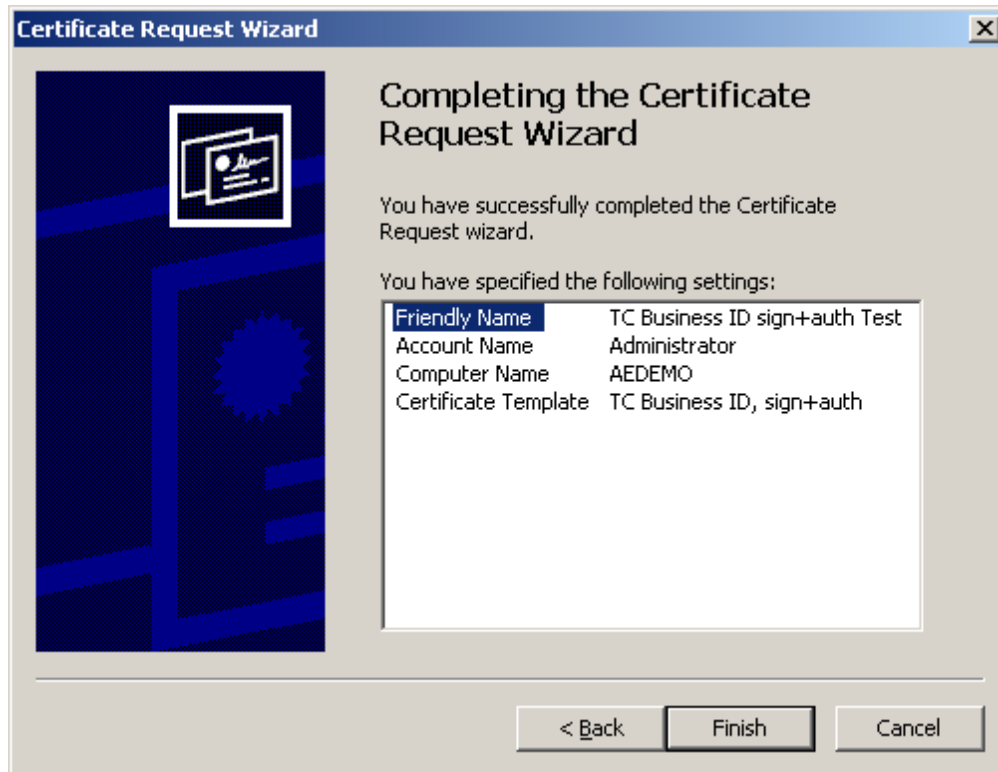
Figure 41: Providing a Friendly Name for the test certificate

11. To make it easier for you to find the issued certificate later input the following data:

Friendly Name: TC Business ID sign+auth Test
Description: This is a test request

and click **Next**.

The wizard will display a summary page similar to that in Figure 42:



- Click **Finish** to have the wizard request the certificate from the TC TrustCenter CA. While waiting for the certificate the mouse pointer is turned into an hourglass to indicate the wizard's ongoing activity.

Upon completion of the request, the wizard will display a short message:



Figure 43: The test certificate has been issued

- Click on the Certificate node in the tree view on the left and press F5 to refresh the display on the right. The test certificate should now be visible in the data pane:

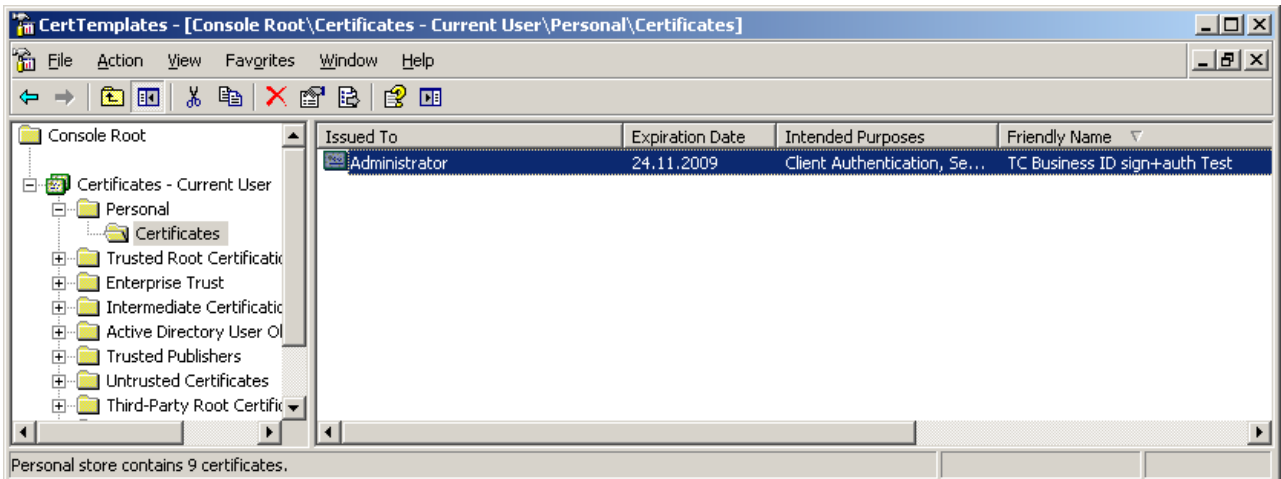


Figure 44: Displaying the test certificate using the certificates snap-in

14. Right-click on the certificate to display its properties:

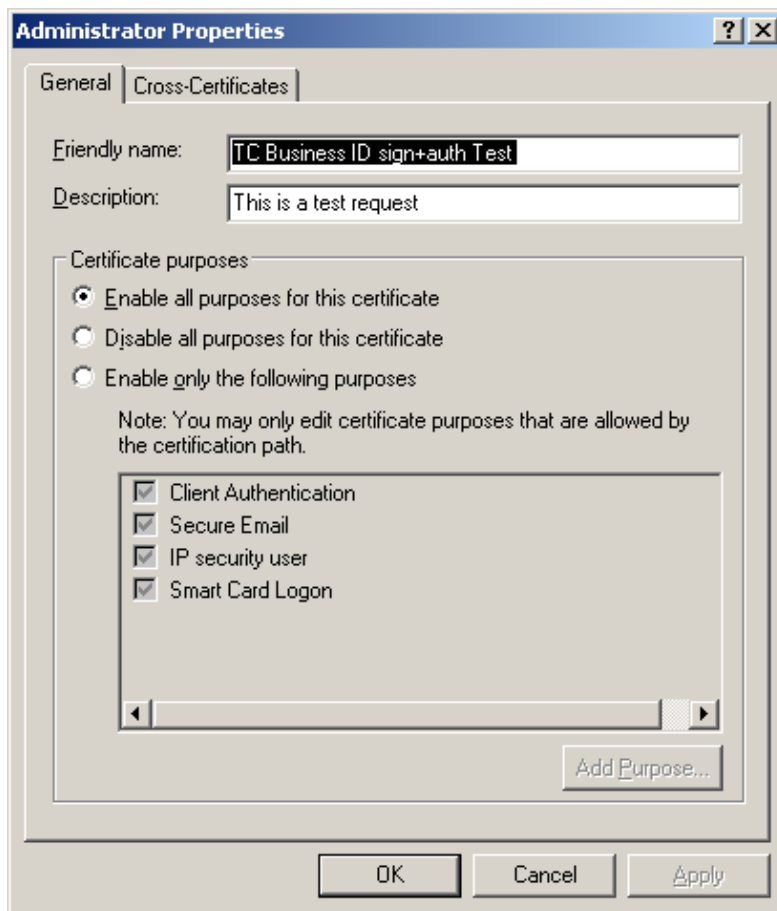


Figure 45: Displaying certificate properties

15. Click **OK** to close the properties page.

Congratulations! You have successfully requested your first certificate from the TC TrustCenter CA!

5.5. Autoenrolling for a certificate

This section describes what an end user will see on the screen when the relevant certificate template is marked for user intervention and when the system detects new certificate templates in ADS which qualify to autoenroll for or when one or more of the user's certificates have expired. The Windows operating system checks your certificates and displays a balloon similar to the following figure:



2. The operating system displays a dialog box as shown in Figure 47. Click **Start** to request the needed certificates or click on **Remind Me Later** to bypass autoenrollment of new certificates.

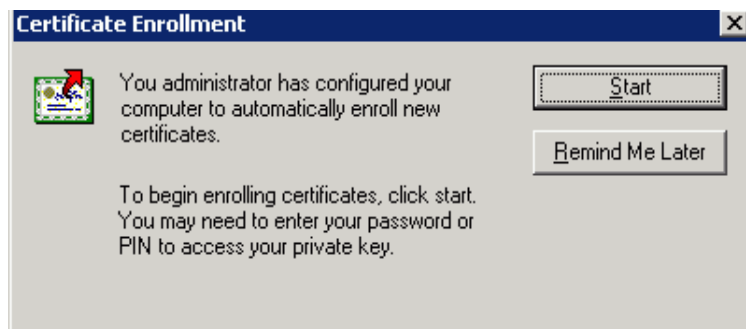


Figure 47: Starting autoenrollment of certificates

If you clicked **Start** the system will begin requesting new certificates as illustrated in the following figure:

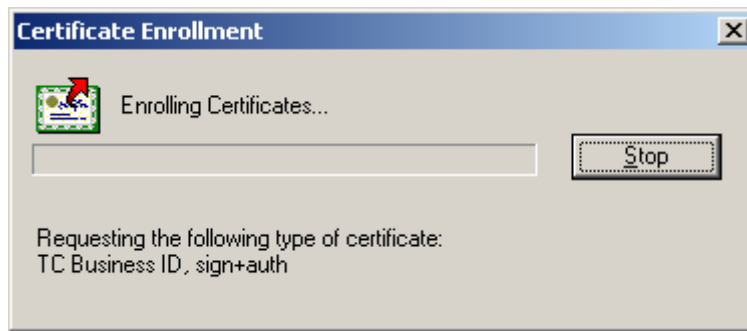


Figure 48: Autoenrolling certificates status

You can abort this process by clicking **Stop** but you should let the process finish its work. When the certificates have been received from TC TrustCenter's servers, the status dialog disappears. You now have received all new and renewed certificates.

5.6. Monitoring enrollment activities

This section describes how to monitor the autoenrollment server's activities. There are three ways to track activities and events of the Autoenrollment process:

- Checking the number of pending requests
- Analyzing the log file
- Using the Windows Event Viewer

5.6.1 Checking the number of pending requests

You can use AEConfig, the Autoenrollment Configuration Tool, to display the number of pending requests, i.e. the number of requests which could not be processed by the TC TrustCenter CA immediately. The autoenrollment client is notified that the request will be processed later.

To check the number of pending requests:

1. Open AEConfig by clicking on **All Programs | TC TrustCenter | TC AutoEnrollmentServer | Autoenrollment Configuration** in the Start menu.

2. AEConfig does not update the number of pending requests automatically. So click on **Refresh** to update the number of pending requests with the current value.



Figure 49: Checking the number of pending requests

5.6.2 Analyzing the log file

Both AEConfig and the autoenrollment service write logging information to the configured log file. In case your are confronted with a problem you should always check the log file for hints on what could have caused the problem. In addition to that you can track autoenrollment activities by analyzing the log file's contents. The following figure shows an example log file excerpt:

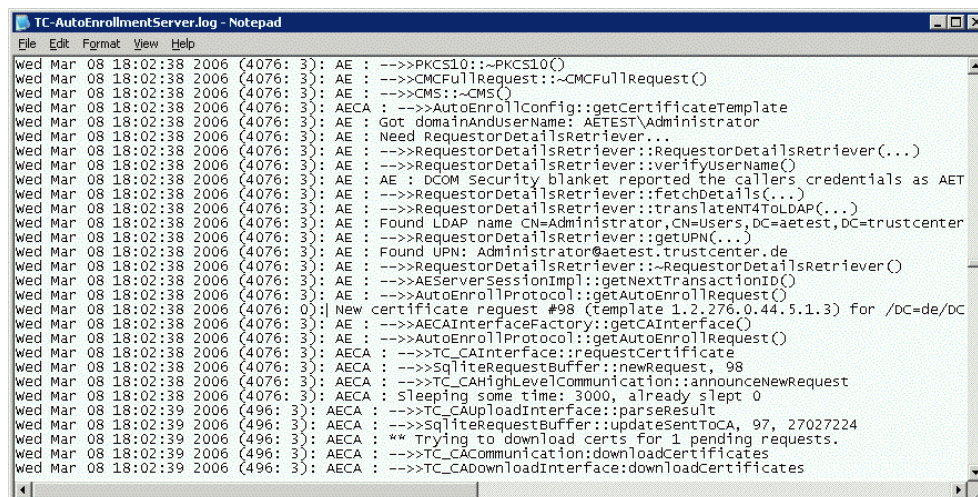


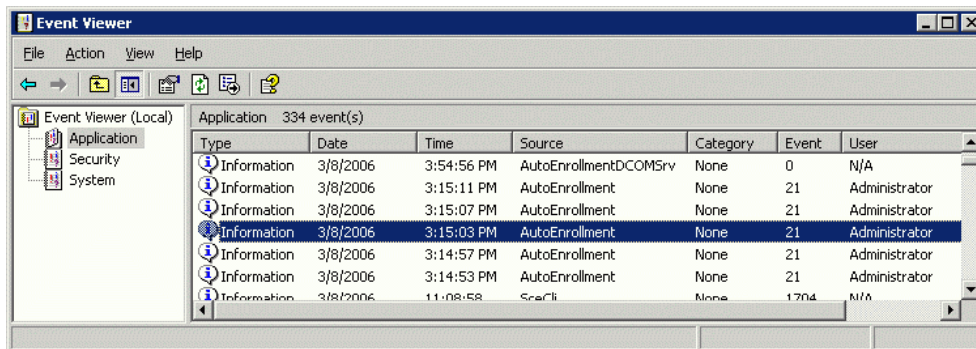
Figure 50: Checking the log file for errors

5.6.3 Using the Windows Event Viewer

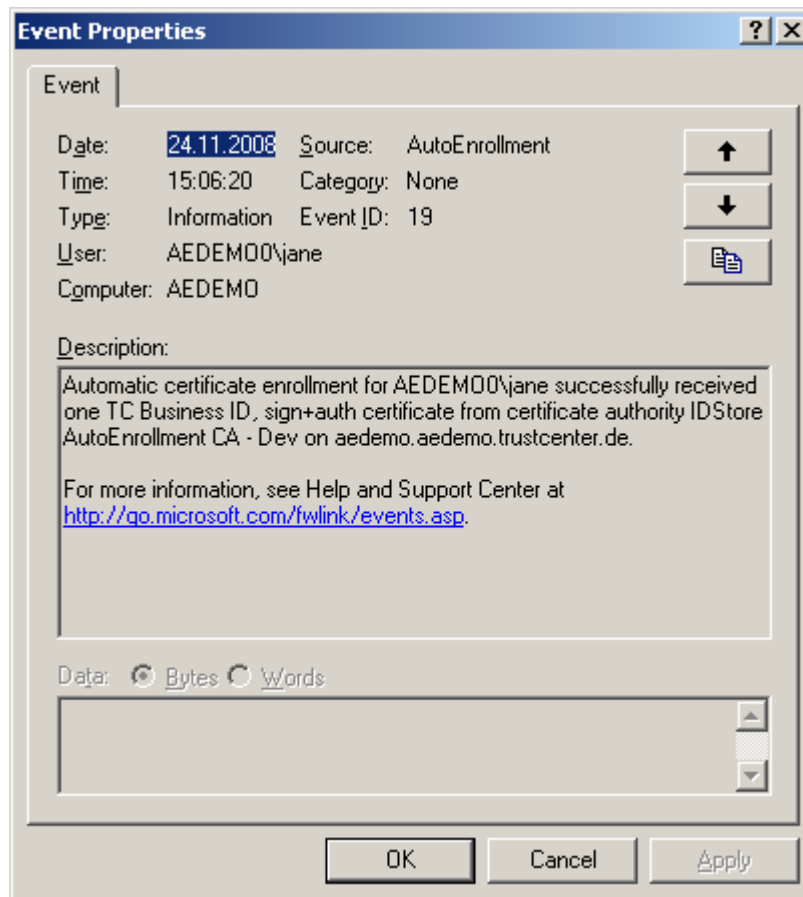
As a third means to track the autoenrollment process's events and activities use the Windows Event Viewer to display information about certificate requests created during the autoenrollment process.

To display Windows system events:

1. Click on **Start | Administrative Tasks | Event Viewer**.
2. Highlight the **Application** node and search for entries containing **Autoenrollment** in the **Source** column.



3. Double-click on such an entry to display its details.



4. In the above example the details show that the Administrator of the system attempted to autoenroll for a **TC Key Recovery Agent** certificate. The request could not be processed by the CA immediately: The request is pending.

5.7. Software update of TC AutoEnrollment Server

This section describes how to update the TC AutoEnrollment Server.

Updating the TC AutoEnrollment Server should be done as follows:

1. Stop the AutoEnrollmentDCOMSvc service.
2. Backup the relevant data, i.e. **TCRequestBufferFile**.
3. Uninstall the TC AutoEnrollment Server software package.
4. Install the updated software using the MSI installer package.
5. Set the security settings as compared to figure 15 (on page 22).

6. Set **CA Server Name** and the port (see figure 22).
7. Restart the service.

6. Frequently Asked Questions

This Chapter provides a list of frequently answered questions about the TC AutoEnrollment Server Software. If you encounter a problem with the software this is the first place to look for a solution to your problem.

If you can not find a solution here please contact TC TrustCenter support staff for assistance.

The Chapter is divided into the following sections:

- Problems related to publishing to ADS
- Problems related to certificate requests
- Miscellaneous problems

6.1. Problems related to Publishing to ADS

The TC AutoEnrollment Server publishes certificates and certificate revocation lists (CRLs) into the Active Directory. This publication requires appropriate permissions for the TC AutoEnrollment Server.

6.1.1 Certificates cannot be published (permission denied)

Error message: ERROR in PublishCertificate: Cannot commit data to Active Directory: permission denied 0x80070005

Cause: The AE server does not have sufficient privileges in Active Directory.

- Solution:**
1. Add the domain computer running the AE server to the Active Directory **Group Cert Publishers** (German: **Zertifikatherausgeber**).
 2. Open the Active Directory Users and Computers MMC Snap-in and open the **Computers** node.
 3. Rightclick on the computer running the AE server and choose **Properties**. Open the **Members of** tab. Click **Add** and add the computer to the **Cert Publishers** group.
 4. Alternative: Right click **Cert Publishers** under **Users** and choose **Properties**. Add the computer running the AE server to the list of group members.
-

6.1.2 CRLs cannot be published (cannot get object)

Error message: ERROR in PublishCRL: cannot get object in Active Directory.
'LDAP://[...]' : 0x80072030
ADsError (0x0x208d): 0000208D: NameErr: DSID-031001CD,
problem 2001 (NO_OBJECT), [...] (LDAP Provider)
WARNING : (PublishCRL): Please make sure that the
cRLDistributionPoint object exists [...]

Cause: The LDAP CDP does not exist in Active Directory.

- Solution:**
1. Create the LDAP CDP in Active Directory using **adsiedt.msc** as described in “Allow publishing to Active Directory” on page 26 of this guide.
 2. Grant the group **Certificate Publishers** write access to this object.
 3. Restart the AE server to force the CRL to be published.
-

6.1.3 CRLs cannot be published (permission denied)

Error message: ERROR in PublishCRL: Cannot commit data to Active Directory:
permission denied 0x80070005

Cause: The AE server does not have sufficient privileges in Active Directory.

- Solution:**
1. Add the domain computer running the AE server to the Active Directory Group **Cert Publishers** (German: **Zertifikatherausgeber**).
 2. Make sure that the LDAP CDP in Active Directory is writable for the **Cert Publishers** group.
 3. After that, restart the AE server to publish the CRL.
-

6.2. Problems related to certificate requests

The Microsoft enrollment clients read out information regarding certificate templates from the Active Directory before submitting the certificate request to the appropriate DCOM service.

6.2.1 Template not registered

Error message in server log file: WARNING : Certificate template is not registered with the server - rejecting request (AEException: Certificate template is not registered with the server: Template 'NotRegisteredTemplate' is not registered)

Cause: The requested certificate template has not been registered with TC TrustCenter.

Solution: Only certificate requests for registered certificate templates can be issued. Contact TC TrustCenter to resolve the problem.

6.2.2 Unknown profile

Error message in server log file: WARNING : Request failed: CODE: ERROR_IN_CSV_DATA, TEXT: TDL-ERROR: unknown profile, A: 67, C: 1.3.6.1.4.1.311.21.8.713069.12016719.5656194.13313939.13861784.249.5088053.4106067

Cause: The requested certificate template has not been registered with TC TrustCenter.

Solution: Only certificate requests for registered certificate templates can be issued. Contact TC TrustCenter to resolve the problem.

6.2.3 Certificate Request Wizard cannot be started

Message box: The wizard cannot be started...

Possible causes and solutions:

- The certificate of the enrollment service is not trusted by the client. The issuer certificate of the service's certificate is added to the root store during the initial configuration, so normally this error should not occur.
 - The enrollment service has no certificate templates configured or the configured templates do not exist in Active Directory. Check the **certificateTemplates** attribute of the enrollment service.
 - There are no certificate templates available for the client. Check the security settings of the templates using the Certificate Templates mmc snapin.
-

6.2.4 Request hit CA_ERROR

Error message: AECA : WARNING : Request hit CA_ERROR: #<aeid>, req_no: <reqno>

Cause: Problem at the remote CA.

Solution: Contact the remote CA. Please provide the following information:

- reqno (i.e. Request Number)
 - Name and/or OID of the template in question (search for New certificate request #<aeid> messages in the log file).
-

6.2.5 How to find detailed information about the enrollment process

To retrieve more information about the enrollment process, you can do the following:

Increase the log level of the autoenrollment server

1. Increase the log level using the configuration tool.
2. Please note that you need to restart the service to make the changes effective.

Use Microsoft Enhanced Event Logging

Follow the instructions given by Microsoft to enable enhanced logging of autoenrollment processes:

- [Troubleshooting \(Certificate Autoenrollment in Windows Server 2003\)](#)¹¹
- [Certificate Autoenrollment in Windows Server 2003](#)¹²

To enable enhanced logging of autoenrollment processes to include warning and informational messages, the following registry values must be created.

For user Autoenrollment:

Create the registry key

```
HKEY_CURRENT_USER\  
Software\  
Microsoft\  
Cryptography\  
AutoEnrollment
```

and create a new DWORD value named `AEEventLogLevel`.

Set its value to 0.

For Machine Autoenrollment:

Create the registry key

```
HKEY_LOCAL_MACHINE\  
Software\  
Microsoft\  
Cryptography\  
AutoEnrollment
```

and create a new DWORD value named `AEEventLogLevel`.

Set its value to 0.

6.3. *Miscellaneous problems*

6.3.1 Problems with SC Logon and/or domain controller authentication

Description: The user experiences problems logging on to the system using a smartcard or when authenticating to the domain controller on the network.

Possible cause: NT authentication store not present or not readable.

- Solution:**
1. Open adsiedit.msc in the MMC.
 2. Browse to
CN=Public Key Services,CN=Services, CN=Configuration, DC=<your domain>
 3. Check if there is an entry CN=NTAuthCertificates.
 4. The entry should be readable by **Everyone**.
-

7. Known Issues

This Chapter lists all currently known issues you could encounter when using the TC TrustCenter AutoEnrollment Server. This list may not be complete and will get updated as soon as TC TrustCenter resolves current issues or learns about new ones. Please review these issues before contacting TC TrustCenter with your problem.

8. Troubleshooting

8.1. *Repeating an action with a higher log level*

The autoenrollment server process keeps a log file to document its activities. When a problem occurs, e.g. a certificate can not be issued although apparently nothing is wrong with the corresponding request, you should always take a look into the autoenrollment process' log file. In most cases it will provide details about what exactly went wrong.

Sometimes the information in the log file may not be detailed enough to thoroughly investigate and resolve a specific problem.

In this case it can be useful to retry the failed action, but this time with a higher log level. The higher the log level the more information is stored in the log file about a particular action or error.

To increase the log level follow the instructions in section 4 “Configuring the TC AutoEnrollment Server” on page 28.

9. Appendix

9.1. Understanding the different log levels

Both AEConfig and the autoenrollment service write messages to the configured log file. There are four different predefined log levels each one representing a different level of log file verbosity:

<i>Loglevel</i>	<i>outputs messages of type ...</i>				
	Audit	Error	Warning	Info	Trace
Audit	x	x			
Warning	x	x	x		
Info	x	x	x	x	
Trace	x	x	x	x	x

Table 4: Predefined log levels

9.1.1 Format of Log file Messages

Log file messages conform to the following format:

```
<Date> (<PID>: <Level>): <Message>
```

Example:

```
Tue Apr 11 12:05:51 2006 (5036: 0): Service stopped.
```

A message may contain additional information such as request numbers, serial numbers etc. The placeholders used in this guide are as follows:

<i>Placeholder</i>	<i>Explanation</i>
<serial number>	CRL serial number
<id>	transaction id
<reqno>	TC request number (this value is needed for support calls on the status of requests) You may have to set the log level to “Trace” to see this value for pending requests.
<guid>	value of the GUID of the requestor
<DN>	DN of the requestor in ADs
<email>	email address of the requestor
<UPN>	UPN of the requestor
<template-oid>	Identifier for the requested template

Table 5: Place holders in log file messages

The lines or parts of the log messages that are of special interest or which should draw your attention to them are marked by ➔.

9.1.2 Audit messages (Level 0)

Here are some examples for messages of type *audit*:

```
Tue Apr 11 09:17:50 2006 (5036: 0): Service started,
waiting for requests.
```

```
Tue Apr 11 09:17:55 2006 (5072: 0): SUCCESS: Published CRL
<serial number> to ADs: CN=AECA3, CN=aeca3, CN=CDP,
CN=Public Key Services, CN=Services,
cn=Configuration,dc=aetest,dc=trustcenter,dc=de
```

```
Tue Apr 11 09:41:29 2006 (5036: 0): New certificate request
#<id> (template <template-oid>) for
/DC=de/DC=trustcenter/DC=aetest/CN=Users/CN=Administrato
r/Email=muenstermann@trustcenter.de
```

```
Tue Apr 11 09:42:37 2006 (4832: 0): Request COMPLETE: #<id>,
req_no: <reqno>
```

```
Tue Apr 11 09:42:38 2006 (5072: 0): SUCCESS: Published
certificate to LDAP://<GUID=<guid>>
```

```
Tue Apr 11 12:05:51 2006 (5036: 0): Service stopped.
```

```
Thu Apr 13 14:54:42 2006 (5272: 0): Configuration as read
from CA -->
AE server hostname = <hostname>
LdapCDP = CN=AECA3, CN=aeca3, CN=CDP, CN=Public Key
Services, CN=Services,
cn=Configuration,dc=aetest,dc=trustcenter,dc=de
check requestor = true
CA processing wait time (sec.) = 300
AutoReloadFuzziness (sec.) = 300
ConfigRefreshTime (sec.) = 86400
CrlRefreshInterval (sec.) = 43200
List of templates we can handle:
- TC_User (1.2.276.0.44.5.1.0)
- TC_SmartcardLogon (1.2.276.0.44.5.1.1)
- TC_DomainControllerAuthentication
(1.2.276.0.44.5.1.2)
- TC_SmartcardUser (1.2.276.0.44.5.1.4)
- TC_EFS (1.2.276.0.44.5.1.5)
- TC_Webserver (1.2.276.0.44.5.1.6)
List of template CNs registered for this enrollment
service in Active Directory:
- TC_User
- TC_SmartcardLogon
- TC_DomainControllerAuthentication
- TC_SmartcardUser
- TC_EFS
- TC_Webserver

<-- end configuration
```

9.1.3 Error Messages (Level 0)

Here are some examples for messages of type *error*:

```
Sat Apr 15 09:24:32 2006 (272: 0): AECA : ERROR: Could not
download configuration from [...]
➔ The remote CA could not be contacted.
```

When this error occurs, you can do the following:

- Check the machine's internet connectivity.
- Make sure the root certificate for the https server is trusted by both the current user *and* the local machine.

9.1.4 Warning Messages (Level 1)

Here are some examples for messages of type *warning*:

```
Thu Apr 13 15:52:16 2006 (4388: 1): AE : (PublishCRL
failed): Please make sure that the cRLDistributionPoint
object exists under LDAP://<CDP>
➔ The CRL could not be published. You need to create
the path in Active Directory.
```

See section 3.4 “Allow publishing to Active Directory” on page 26 for details.

```
Thu Apr 13 16:12:16 2006 (8946: 1): AE : Problem downloading
CRL, will try to reload CRL at <time>
➔ CRL could not be retrieved from the CA, will retry
later
```

```
Thu Apr 13 08:48:11 2006 (9384: 1): AE : The certificate
that signed the request is not trusted - rejecting
request #<id>
➔ Renewal of a certificate was denied
```

9.1.5 Info Messages (Level 2)

Here are some examples for messages of type *info*:

```
Thu Apr 13 14:54:36 2006 (5272: 2): AE : Loaded last
transaction id: <id>
```

```
Thu Apr 13 14:54:36 2006 (5272: 2): AE : DB schema revision
is 1
```

```
Thu Apr 13 15:21:22 2006 (5272: 2): AE : Stopping service...
```

```
➔ Information about a request taken from ActiveDirectory:
Thu Apr 20 9:41:12 2006 (480: 2): AE : Found LDAP name
<DN>
Thu Apr 20 9:41:12 2006 (480: 2): AE : Found email
address: <email>
Thu Apr 20 9:41:12 2006 (480: 2): AE : Found GUID:
<GUID>
Thu Apr 20 9:41:12 2006 (480: 2): AE : Found UPN: <UPN>
```

```
➔ Infos about local configuration:
Tue Apr 11 12:06:18 2006 (220: 2): AE : AEServer
Configuration:
=== AERegKey ===
EnrollServiceName:      'AECA3'
EnrollServiceDisplayName: 'TC Class2 AutoEnroll CA'
CAHostname:             'www.trustcenter.de'
CAPort:                 '2444'
➔ URL https://www.trustcenter.de:2444
DBName:                 'C:\Program Files\TC TrustCenter\TC-
AutoEnrollmentServer\TCRequestBufferFile'
RA_PSE_Fingerprint:    'C:\Documents and
Settings\Administrator.AETEST\Desktop\AETest-
SSL_Authentication-CDP-20090308.p12'
LogFile:                C:\Program Files\TC TrustCenter\TC-
AutoEnrollmentServer\logs\TC-AutoEnrollmentServer.log
LogLevel:               2
```

9.1.6 Trace Messages (Level 3)

Trace Messages are only relevant for TC TrustCenter support. There is no need that you understand those messages but TC TrustCenter might ask you to perform an action with a log level that outputs such messages in order to investigate and resolve a specific problem.

9.2. List of Figures

Figure 1: Data Flow of the Autoenrollment Process.....	3
Figure 2: Setting the machine's DCOM Access Permissions.....	9
Figure 3: Adding the Domain Computers and Domain Users groups.....	10
Figure 4: Setting DCOM Launch Permissions.....	11
Figure 5: Windows Firewall Settings.....	12
Figure 6: Setting Group Policies.....	13
Figure 7: Navigating to the autoenrollment settings.....	14
Figure 8: Setting Group Policy Autoenrollment Options.....	15
Figure 9: Add Certificate Templates SnapIn on Windows 2008 Server	16
Figure 10: Installing the software - Welcome screen.....	18
Figure 11: Installing the software - Selecting the installation folder.....	18
Figure 12: Installing the software - Confirming the installation.....	19
Figure 13: Installing the software - Installation is completed.....	19
Figure 14: Setting enrollment permission for the new server.....	20
Figure 15: Setting enrollment permissions - the Security tab.....	21
Figure 16: Setting enrollment permissions - Launch and Activation settings.....	22
Figure 17: Setting enrollment permissions - Access permissions.....	23
Figure 18: Opening the autoenrollment service's properties.....	24
Figure 19: Setting the service's startup type.....	25
Figure 20: Publishing to Active Directory.....	26
Figure 21: Starting the configuration tool.....	28
Figure 22: Running AEConfig for the first time.....	29
Figure 23: Choosing a PSE from a .p12 file.....	30
Figure 24: Choosing a PSE from the CSP list.....	31
Figure 25: Checking the PSE's validity using AEConfig.....	31
Figure 26: AEConfig is now ready to download the configuration data.....	34
Figure 27: Fetching the configuration data with AEConfig.....	35
Figure 28: Certificate Templates provided by TC TrustCenter.....	36
Figure 29: Saving AEConfig's settings.....	37
Figure 30: Starting the autoenrollment service.....	42
Figure 31: Stopping the autoenrollment service.....	42
Figure 32: Some controls are disabled while the service is running.....	43
Figure 33: Starting or stopping the autoenrollment service.....	44
Figure 34: Adding Snap-Ins to the MMC.....	47
Figure 35: Select Certificate Template for Manual Enrollment.....	48
Figure 36: Defining DACL properties for a specific certificate template.....	49
Figure 37: Setting the certificate snap-in to manage the current user's certificates.....	52
Figure 38: Requesting a test certificate.....	53
Figure 39: The Certificate Request Wizard.....	53
Figure 40: Selecting the certificate type.....	54

Figure 41: Providing a Friendly Name for the test certificate.....	55
Figure 42: Summary page of the Certificate Request Wizard.....	56
Figure 43: The test certificate has been issued.....	56
Figure 44: Displaying the test certificate using the certificates snap-in.....	57
Figure 45: Displaying certificate properties.....	57
Figure 46: Certificate Enrollment notification.....	58
Figure 47: Starting autoenrollment of certificates.....	58
Figure 48: Autoenrolling certificates status.....	59
Figure 49: Checking the number of pending requests.....	60
Figure 50: Checking the log file for errors.....	60
Figure 51: Opening the Event Viewer.....	61
Figure 52: Autoenrollment event details.....	62

9.3. List of Tables

Table 1: Supported Windows operating systems.....	6
Table 2: Relevant LDAP Attributes.....	38
Table 3: Description of Registry Settings.....	40
Table 4: Predefined log levels.....	72
Table 5: Place holders in log file messages.....	73

Online References

- 1 <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspix>
- 2 <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspix>
- 3 <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03pkg.mspix>
- 4 <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/operations/default.mspix>
- 5 <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspix>
- 6 <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/5712B108-176A-4592-BCDE-A61E73357930.mspix>
- 7 <http://technet2.microsoft.com/windowsserver/en/default.mspix>
- 8 <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/7f6df44c-06c3-4b92-ba32-63d895a7924b.mspix>
- 9 <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspix>
- 10 <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspix>
- 11 <http://technet2.microsoft.com/WindowsServer/en/Library/8b1e8736-1574-44a0-802f-974f7aeedd9c1033.mspix>
- 12 <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspix>