Guide to the Secure Configuration and Administration of Microsoft Exchange 2000®

Systems and Network Attack Center (SNAC)

Author: Trent Pitsenbarger

Updated: 8 Aug, 2002
Version 1.12

SNAC.Guides@nsa.gov

This Page Intentionally Left Blank

Warnings

- Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Microsoft Windows 2000 systems and should not be applied to any other Windows 2000 versions or operating systems.
- This document contains possible recommended settings for the system Registry. Windows 2000 system operation can be severely impaired or disabled with incorrect changes or accidental deletions when using a Registry editor (`Regedt32.exe` or `Regedit.exe`) to change the system configuration. There is no "undo" command for deletions within the Registry. Registry editor prompts user to confirm the deletions if "Confirm on Delete" is selected from the options menu. When user deletes a key, the message does not include the name of the key being deleted. Check selection carefully before proceeding.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- This is a living document and revisions will be constant; the change control area will state modifications. See Microsoft's web page for the latest changes or modifications to the Windows 2000 operating system and applications.

This Page Intentionally Left Blank

Acknowledgements

The foundation of this document is based on Exchange security guidance developed by the Mitre Corporation under contract to the NSA.

Some parts of this document were drawn from Microsoft copyright materials with their permission.

Our thanks.

Trademark Information

Table of Contents

Table of Figures

Table of Tables

Introduction

This document describes how to securely install, configure, and administer the Exchange 2000 server[1]. It is intended for the reader who is already familiar with Exchange 2000 Server but needs to understand more on how to make it more secure. This document is intended as a complement to the Windows 2000 Security Recommendation Guides available at http://www.nsa.gov.

In writing this guide the authors found that in many cases it is difficult to recommend specific, concrete actions due to the wide variety of operational environments in which Exchange can be used. Instead, a summary is offered which describes the concerns and recommends solutions that a user must tailor to his/her own environment. Major points or recommendations will be noted at the end of each section in a bulleted list for ease of reading and implementation.

WARNING: This guide does not address security issues for the Microsoft Windows 2000 operating system that are not specifically related to the Microsoft Exchange Server.

PLEASE NOTE THAT THESE DOCUMENTS ASSUME THAT THE READER IS A KNOWLEDGEABLE WINDOWS 2000 ADMINISTRATOR. A knowledgeable Windows 2000 administrator is defined as someone who can create and manage accounts and groups, understands how Windows 2000 performs access control, understands how to set account policies and user rights, is familiar with how to set up auditing and read audit logs, etc. These documents do not provide step-by-step instructions on how to perform these basic Windows 2000 administrative functions – it is assumed that the reader is capable of implementing basic instructions regarding Windows 2000 administration without the need for highly detailed instructions. In addition, most Microsoft products still require an administrator's ability to view, compare, and change Registry settings. To do this properly and safely (with regard to the systems continued operation) requires experience and care and should not be attempted by someone not experienced in doing it properly.

Getting the Most from this Guide

The following list contains suggestions to successfully configure and administer the Microsoft Exchange 2000 Server:

WARNING: This list does not address site-specific issues and every setting in this book should be tested on a non-operational network.

- Read the guide in its entirety. Omitting or deleting steps can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.
- Perform pre-configuration recommendations:
- Perform a complete backup of your system before implementing any of the recommendations in this guide.

[1] There are two versions of the server – the Exchange 2000 Server and the Exchange 2000 Enterprise Server. Unless specifically noted, the discussions are applicable to both.

- Follow the security settings that are appropriate for your environment.

Commonly Used Names

Throughout this guide the network names and the subnets will be used in the examples, screenshots, and listings.

WARNING: It is extremely important to replace the network names and subnets with the appropriate network name and subnet for the networks being secured.

About the Guide to Securing Configuration and Administration of Microsoft Exchange 2000 Server

This document consists of the following chapters:

Chapter 1, "**Exchange 2000 Installation,**" provides an overview of the pertinent security issues related to the installation of the Exchange 2000 server.

Chapter 2, "**Outlook 2002 Security,**" describes Outlook 2002 security configuration options for installation and operation. It also describes the configuration of the Outlook Security Template.

Chapter 3, "**Administrative Permissions,**" describes the configuration of permissions that can be assigned to Windows 2000 users/groups for Exchange objects within the Exchange System Manager. It also summarizes tools for managing permissions within Exchange.

Chapter 4, "**Administrative and Storage Groups,**" describes the administrative models that can be implemented with administrative groups and presents an overview of the security relevant settings associated with administrative and storage groups.

Chapter 5, "**Multi-Server Configurations,"** explains message transfer and routing between servers. It also covers routing groups, connectors and their associated security.

Chapter 6, "**SMTP Virtual Server,**" describes the security relevant settings for the SMTP Virtual Server.

Chapter 7, "**HTTP Access,**" describes security relevant topics of using Outlook Web Access on to access an Exchange system.

Chapter 8, "**Certificates and Advanced Security,**" discusses the methods that Exchange offers for secure communication.

Chapter 9, "**Network Protocols,**" describes the virtual servers associated with the Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3), Hypertext Transfer Protocol (HTTP), and Network News Transfer Protocol (NNTP) Internet protocols, as well as Internet Message Access Protocol version 4 (IMAP4).

Chapter 10, "**Developing Custom Applications,**" presents programming security considerations for developing custom applications for an Exchange 2000 server.

Chapter 11, "**Extending the Exchange Environment,**" presents different security solutions for extending the Exchange 2000 environment to less trusted domains.

Chapter 12, "Chat Services" looks at the Exchange chat server and client.

Chapter 13, "Instant Messaging" presents the security considerations related to Exchange Instant Messaging server and client.

Chapter 14, "Final Thoughts" covers malicious code detection, backup procedures, and other topics.

An Important Note About Operating System Security

Exchange 2000 Server security is tightly coupled to the operating system. For example, EXCHANGE 2000 SERVER logon can be coupled to the operating system logon so that a user does not have to log-on separately to Exchange 2000 Server.

File permissions, Registry settings, password usage, user rights, and other issues associated with Windows 2000 security have a direct impact on Exchange 2000 Server security.

The recommended source of information for how to securely configure the Windows 2000 server and Professional is the set of Windows 2000 Security Recommendation Guides available at http://www.nsa.gov. It is important to implement these guides on the Windows 2000 networking supporting the Exchange and Outlook infrastructure.

This Page Intentionally Left Blank

Chapter 1

Exchange 2000 Installation

This section defines the steps needed to install an Exchange 2000 server on a Windows 2000 network. The installation process has been separated into three areas: preparing for installation, installation and post-installation. The intent of this chapter is not to provide a complete administrative guide for installing Exchange; instead it focuses on those installation issues that are particularly relevant from a security perspective.

Preparing for Installation

Administrative Rights and Prep Utilities

Certain administrative rights are needed to install an Exchange 2000 Server. The account under which the installation takes place must have administrative rights to the machine that Exchange is being installed on. This account is automatically given administrative rights to Exchange as part of the installation process.

DomainPrep and ForestPrep are two preparatory Setup Utilities that must be run either during installation (it runs automatically) or before installation. DomainPrep is run once in each domain that has an Exchange 2000 server and in any domain that hosts Exchange users. It performs the Exchange setup tasks that require Domain Admins permissions; it should be run by a member of the Domain Admins group. This utility creates the groups and permissions necessary for Exchange servers to read and modify user attributes. DomainPrep is run on the Exchange target machine.

The ForestPrep utility is run once per forest; it extends the Active Directory schema to include specific Exchange information. ForestPrep also creates objects in Active Directory and gives permissions on those objects to the account designated as the Exchange 2000 administrator. In order to run ForestPrep, an account must be a member of the Enterprise Admins and Schema Admins groups. If ForestPrep is run before the Exchange 2000 installation, you will be prompted for an Exchange administrative account. This account will get full administrative rights to Exchange. The Exchange administrative account should be used for the subsequent installation. If the installation account is a member of all these groups, then these processes are run automatically during installation. The administrator of a domain controller is a member of all the mentioned groups by default. Otherwise, they must be run by accounts with the proper administrative privileges before installation. These routines are on the Installation CD-ROM.

Since the installation account is given full administrative rights to Exchange, you should create a special Exchange installation account to keep these rights separate from other rights. Any additional rights used for the installation could be removed later if desired. For installation of additional Exchange servers, the Exchange installation account must be a member of the Enterprise Admins group, or a member of both the Domain Admins group for the domain in which you are installing Exchange 2000 and an Exchange

Administrator with all rights. This account must also belong to the target machine administrator group.

Installation Directory

It is recommended that the operating system reside in its own partition for integrity reasons. For this reason a new partition should be set up for Exchange 2000. Installing on a separate physical drive is also useful for integrity reasons. The default permissions are set by Windows 2000 to full control for the EVERYONE group. The permissions on the Exchange installation directory should be changed by removing EVERYONE and giving full control to the following groups:

- SYSTEM
- CREATOR OWNER
- Domain Admins
- < All Exchange Administrative Groups> (covered in detail in Chapter 3)

If using Outlook Web Access, also give Authenticated Users *read and execute* access.

Finally, is also recommended not to install Exchange Server on a domain controller.

Installation

During installation there are two items of note from a security perspective. The first relates to the component installation screen shown in Figure 1.

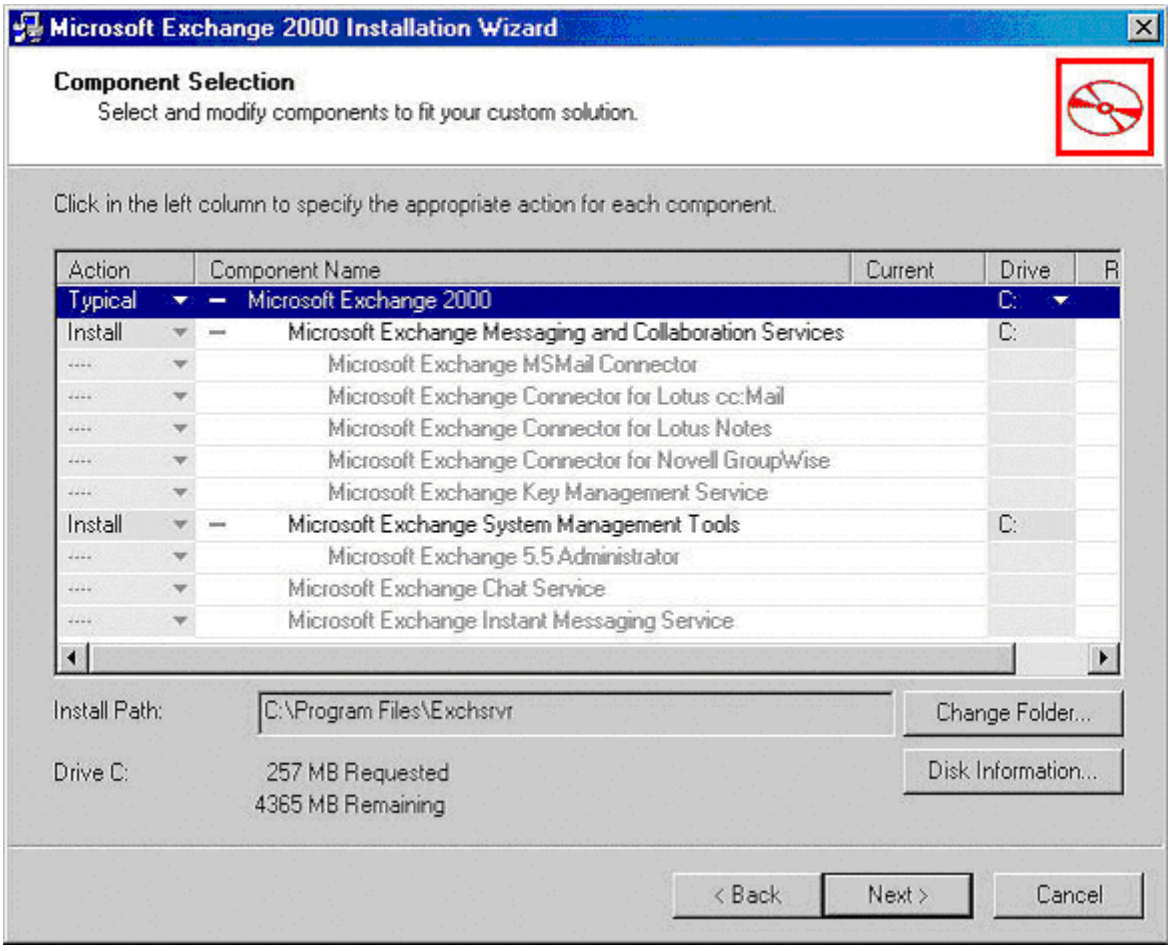

Figure 1. Exchange 2000 Server Component Installation Screen

By clicking on the Change Folder button, the installation path on that drive can be specified. This path should be set to the new partition/directory that was created for the installation. The second item of note is only relative under certain conditions. If a domain controller in the domain of installation was installed with the Pre-Windows Compatible Access setting, the dialog box in Figure 2 will be displayed. It is warning that a security group exists whose members can access hidden members of a distribution list. In this case, this group should be examined and members removed who should not have this access.

Figure 2. Installation Warning Box

Post Installation

Service Packs and Hot Fixes

It is important that the administrator install the latest service packs and security related hotfixes for Exchange Server, Windows 2000, Internet Information Server, and any other services running on the Exchange Server computer. Microsoft's HotFix & Security Bulletin Service, available at the following URL, is a very useful tool for keeping track of applicable patches:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp

Administrative and Routing Group Display

A default Administrative Group was created by the installation process. This group is named First Administrative Group. It will not be displayed until Administrative groups are enabled. To enable Administrative groups, use the System Manager to display the Organization Properties (General Tab under Properties).

The installation process also created a default Routing group named First Routing group. Routing groups must also be enabled before they can be displayed. If the installation were for additional Exchange servers into an organization with multiple Administrative or Routing groups, an option would be available during installation to select the desired groups. In a multi-server installation it may be useful, from a security perspective, to keep administration of the servers separate by creating separate Administrative groups. At this point, additional administrative accounts can be created and administrative privileges assigned; this will be discussed in Chapter 3, Administrative Permissions. Mailboxes can now be added to Windows 2000 accounts; this will be discussed in Chapter 2, Outlook 2002 Security.

OS Guideline Compatibility

There are three actions required to ensure that Microsoft Exchange works in concert with the operating system guidelines described in *An Important Note About Operating System Security.*

First, applying the OS guidelines can cause an "unknown user name or bad password error" when logging into an Exchange Server via IMAP or POP3. There are two ways that the problem can be fixed:

- Set the client to use *Secure Password Authentication* (preferred).

or

- On both the Exchange Servers and Domain Controllers, set the LAN Manager Auth Level to "send NTLMv2 response only/refuse LM". This is a change from the recommended setting of "send NTLMv2 response only/refuse LM & NTLM."

Second, ensure that the *Exchange Enterprise Servers* group is given the right to *manage audit and security logs* on the security policy applied to Domain Controllers.

Third, Microsoft Exchange 2000 requires remote registry access which is controlled by the access control list on the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
SecurePipeServers\winreg

On Exchange servers and domain controllers within the domain, add the Exchange Domain Servers group with Full Control access on this key.

Shared Directory Permissions

During installation, three Exchange related shares are created. The local computer account should be given full control over these directories (including subdirectories and files) in addition to the permissions listed above[2].

Important Security Points

- Apply the operating system security guidance as described in *An Important Note About Operating System Security*. Three actions are required to ensure that Microsoft Exchange 2000 works in concert with the operating system guidelines, as documented above.
- Install Exchange 2000 on a separate physical drive or at minimum create a separate partition/directory for the installation. Remove all permissions from EVERYONE group and assign the following permissions:
  - SYSTEM – Full Control
  - CREATOR OWNER – Full Control
  - Domain Admins – Full Control
  - < All Exchange Administrative Groups> – Full Control
  - If using Outlook Web Access, give Authenticated Users *read and execute* access.
  - The local computer account should also be given full control over the shared directories created during the installation (including subdirectories and files)[2].
- Do not install Exchange 2000 on a domain controller.
- Create a separate Exchange 2000 administrative account for the installation.
- Consider partitioning the Exchange 2000 administration into separate Administrative Groups. See Chapter 4 for a discussion of Administrative Groups.
- Install the latest service packs and security related hotfixes for Exchange Server, Windows 2000, Internet Information Server, and any other services running on the Exchange Server computer.

[2] In a mixed mode environment, the site services account would have full control permission for Exchange 5.5 servers.

This Page Intentionally Left Blank

Chapter 2

Outlook 2002 Security

Exchange supports a wide variety of clients. These include Outlook, Outlook Express, Outlook Web Access, and standard Internet e-mail clients. The most widely used client for Exchange 2000 servers is Outlook. The Exchange 2000 server supports Outlook versions starting with Outlook 97. This chapter discusses Outlook 2002 security configuration options for installation and operation and is primarily focused on installations using MAPI connectivity to the Exchange server. Connectivity to the Exchange server via protocols such as POP3 and IMAP4 are covered in Chapter 9.

The discussions within this chapter are also generally applicable to Outlook 2000 although there are some minor differences with regards to the dialog boxes.

Security For Outlook 2002

Outlook 2002 has security configuration options that can:

- Delegate access to personal folders and information while protecting personal information.
- Protect against malicious code attacks in e-mail message attachments and harmful Visual Basic for Application (VBA) macros contained within Outlook forms.
- Provide authentication and privacy for e-mail messages.
- Protect users from HTML messages with malicious content.
- Provide message security label information to the message header.
- Grant permissions to public and private folders.
- Customize client security settings.

These security configuration options are detailed in the following subsections.

Outlook 2002 Installation

There are four security critical considerations when installing Outlook 2002. First, the operating system should be installed in its own partition for integrity reasons. Second, it is important to realize that operating system security is critical to the secure operation of Outlook 2002 and the Exchange server. The recommended guidelines for securing

Windows 2000 operating systems is the series of guides published by the NSA and available at http://www.nsa.gov. Third, directory and file permissions should be set for the users and groups shown in Figure 3. These permissions should apply to all subfolders and files under the installation directory.

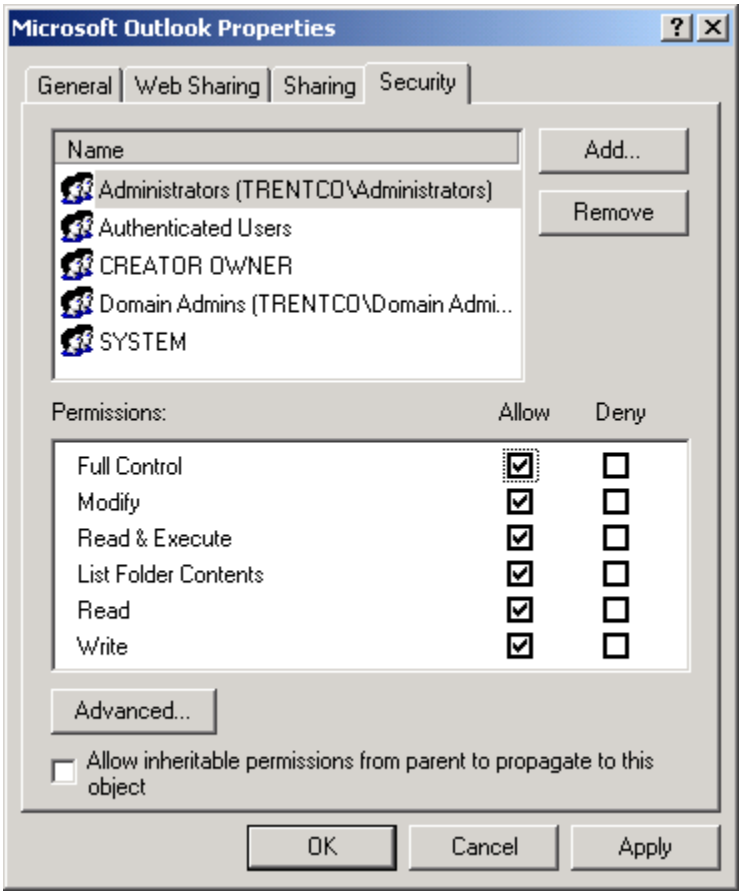

Figure 3. Outlook 2002 Access Control List

Table 1. Outlook 2000 Access Control List

Administrators	Full Control
Authenticated Users	Read & Execute
Creator Owner	Full Control
Domain Admins	Full Control
System	Full Control

Finally, as always keep up-to-date with service pack and security related hotfixes.

Outlook 2002 Configuration Setup

The first time Outlook 2002 is run, a Startup Wizard helps configure the application and setup an e-mail account. Additional e-mail accounts and other configuration settings can also be set by right clicking on the desktop Outlook icon.

Outlook security for an Exchange Server account is managed under the **Advanced** tab, as shown in Figure 4. The **Encrypt Information** option enables the encryption of the Remote Procedures Calls (RPC) use to connect to the Exchange Server over the network or when using dial-up networking; the information is encrypted only during transmission but is stored unencrypted. The **logon network security** has three available logon security options available. These include none, distributed password authentication, and password authentication. Password authentication is the recommended method. It allows single sign-on—once the user is logged onto the Windows 2000 domain, it is not necessary to log on a second time to access Exchange. Note, however, that logon credentials are subject to password guessing attacks; it is vital to implement a strong password policy as recommended in the *Guide to Securing Windows 2000 Group Policy: Security Configuration Tool Set*. This document is part of the family of Windows 2000 security guidance documents available at http://www.nsa.gov.

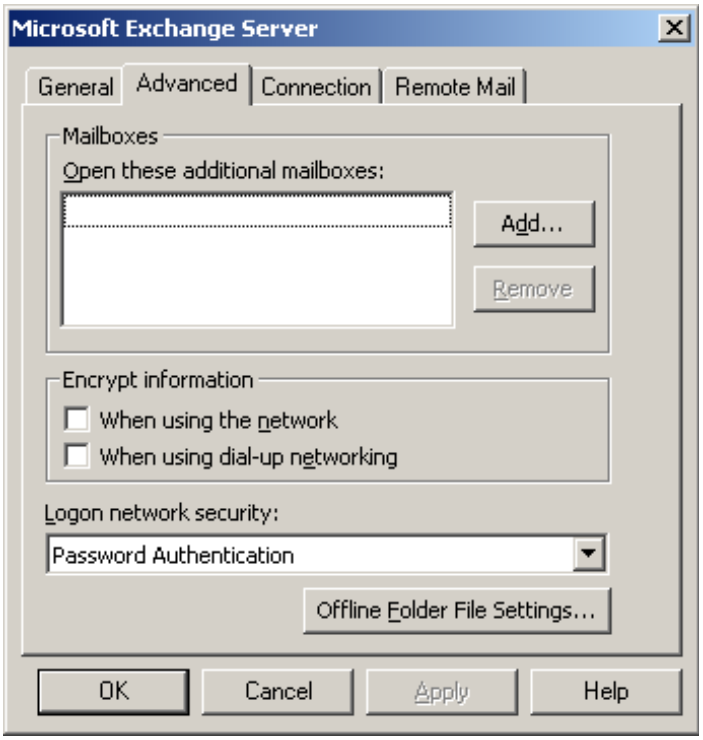

Figure 4. Advanced Setup for Outlook 2002 Client

Also included under the **Advanced** tab is a button for setting *Offline Folder Files*. *Offline Folders Files* allow users to save Outlook items when they are not connected to the server. This user file contains Outlook folders that are a copy of the user's Outlook folders in the Exchange store. The Outlook folders contained in the user's Offline Folders File can be synchronized with the Outlook folders contained in the Exchange store so both contain the most up to date information.

Figure 5. Offline Folder File Settings

The offline folder file settings are shown in Figure 5. To create an offline folder file, choose either the default file name shown or replace it with the user's e-mail account name. Note that a variety of encryption settings can be selected when creating the offline folder file. These settings are not effective as a means of preserving data confidentiality; however, Outlook provides protection for offline folders as described in the Microsoft knowledge base article Q163589 available at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q163589. Data confidentiality can be augmented by several means. First, saving the offline folders file to the user's home path will result in the inheritance of a restrictive set of access controls that limit access to the user and to the administrators. Another option is the use of the encrypting file system (reference NSA's guide entitled *Guide to Securing Microsoft Windows 2000 Encrypting File System* at http://www.nsa.gov). Finally, data confidentiality for e-mail content can be achieved via the use of S/MIME (reference Chapter 8, Certificates and Advanced Security).

Outlook Folders

Outlook saves information created and received in folders. These folders are information containers that are within a Personal Folders file or in the Exchange store. There are several different types of folders: standard default folders, personal folders, and Offline folders. When using Outlook 2002, the Exchange Server information store holds the folders so that Outlook users can easily share information. Personal folders are stored in a Personal Folders file on the hard drive of the Outlook client; these folders might contain information the users wish to backup from the information store. The offline folders contain a copy of the user's folders on the Exchange server; these were discussed in the previous subsection.

A Personal folders file is created when the Outlook client is installed, or it can be added later as a modification to a user's profile. A password can be assigned to a Personal folder; however, these passwords are not effective as a means of preserving data confidentiality, as tools are available on the Internet to strip off the passwords. Use the techniques described in the previous subsection to help preserve data confidentiality.

Just as with offline folders, Personal folders can be encrypted but this is not an effective means of provided data confidentiality.

Outlook Folder Permissions

Outlook provides the capability to share information through the use of public folders and shared private folders. Public folders share information based on the permissions granted to users. Private folders can be shared by either granting permission to specific users or by giving a user delegate access. These two methods are described in the following paragraphs.

Shared information can be manipulated by users based on the permissions that the user has been granted on the folder. These permissions are described in Table 2 and include: Owner, Publishing Editor, Editor, Publishing Author, Author, Contributor, Reviewer, Custom and None.

Table 2. Folder Permission Levels

Permission Level	Capabilities
Owner	Create, read, modify, and delete all items and files. Create subfolders and change the permission levels others have for the folder.
Publishing Editor	Create, read, modify, and delete all items and files, and create subfolders.
Editor	Create, read, modify, and delete all items and files.
Publishing Author	Create and read items and files, create subfolders, and modify and delete items and files created.
Author	Create and read items and files, and modify and delete items and files created.
Contributor	Create items and files only. The contents of the folder do not appear.
Reviewer	Read items and files only.
Custom	Perform activities defined by the folder owner.
None	No permission; can't open the folder.

Folder permissions are set from the folder list in Outlook. To view or set folder permissions on either a public folder or a shared private folder, right-click the private or public folder, and click **Properties** on the shortcut menu. After clicking the **Permissions** tab, the window shown in Figure 6 will be displayed. The user name and permission level is listed. Users can be added and removed from the list by using the **Add** and **Remove** buttons. The permission level is set in the **Permissions** section of the window. A custom permission level can be designated by checking the boxes of the options needed. After setting new permissions on the folder, click the **Apply** button to activate the new settings. Permissions on public folders can only be set by a user that has owner permissions on the folder. To designate all users, choose **Default** in the Name box. It is recommended that **Default** be set to **None** (which is the default) for a user's private folder; only specific users should be added with appropriate permissions. The private folder settings are perhaps most easily manipulated using the delegate access features which will be discussed shortly.

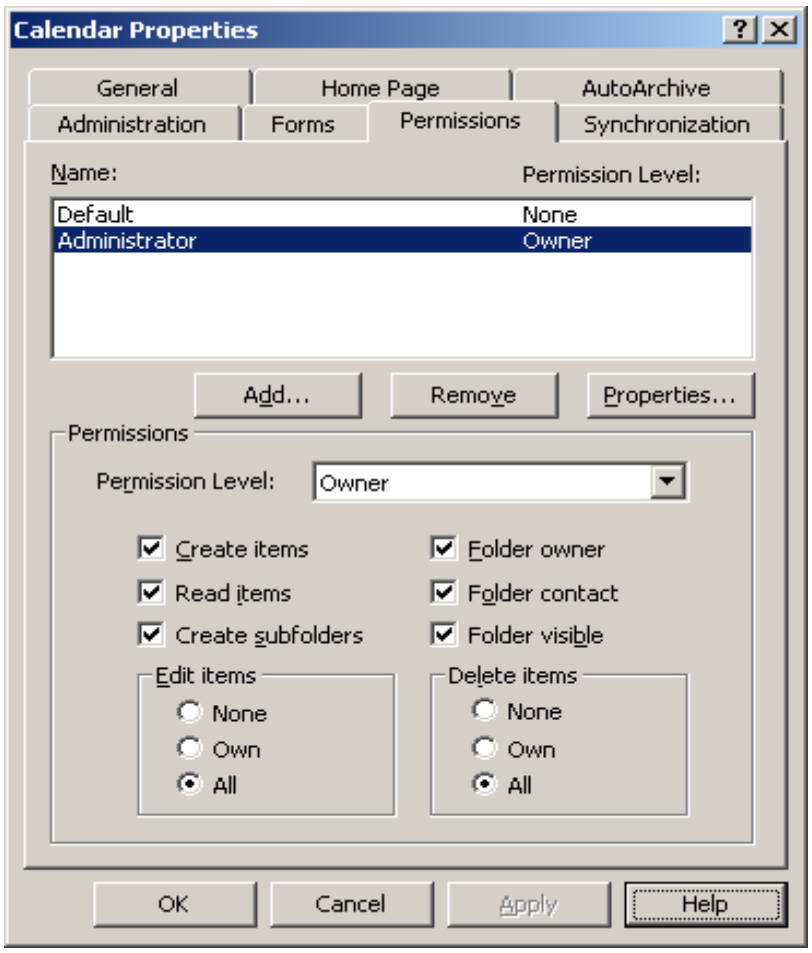

Figure 6. Calendar Folder Permissions

As discussed in Chapter 4, the administrator can control who has the ability to create public folders from the system manager. This chapter also contains information regarding why it is important to limit who has this ability.

Outlook folder properties also have a security relevant option listed under the **Administration** tab of the folder properties. The **This folder is available to** option limits user access to the folder to only **Folder owner** or to anyone with appropriate permissions.

Private folders can also be shared by granting users permission to open other users' folders, and permission to read, create and respond to items. This process is called **Delegate Access**. A user can delegate access to another user to read, create, modify and delete personal folder items. The user granting the permission determines the level of access. Delegate access settings have the effect of manipulating the private folder permissions discussed earlier.

Delegate access is only available when the user is connected to the server and the user's mail is delivered to the user's mailbox, not to a personal folders file. To add or remove delegates and assign permissions to delegates follow the steps outlined below:

- On the Outlook **Tools** menu, click **Options**, and then click the **Delegates** tab. The window shown in Figure 7 will be displayed.

- Delegates can be added or removed by choosing the appropriate button.

- To set permissions for the delegate choose the **Permissions** button. The available permissions include: Author, Editor and Reviewer; these are summarized in Table 3.

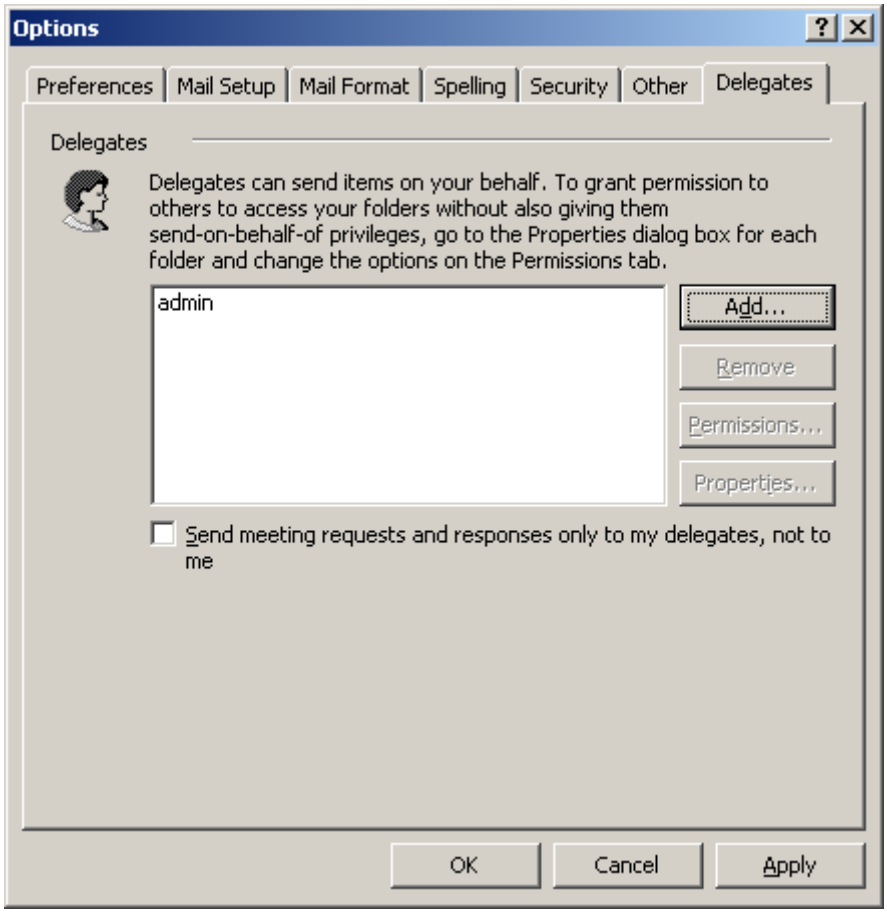

Figure 7. Delegate Access

Table 3. Delegate Access Permissions Levels

Permission Level	Capabilities
Editor	Everything an Author can do, plus modify and delete the items the manager created.
Author	Read, create items, and modify and delete items created.
Reviewer	Read items.
None	No access to this item.

The delegate permissions are set individually on a per folder basis. The user's folders, including calendar, tasks, inbox, contacts, notes, and journal are designated. The user can choose to have the delegate see their private items. These permissions are shown in Figure 8. Sent messages contain both the manager's and delegate's names.

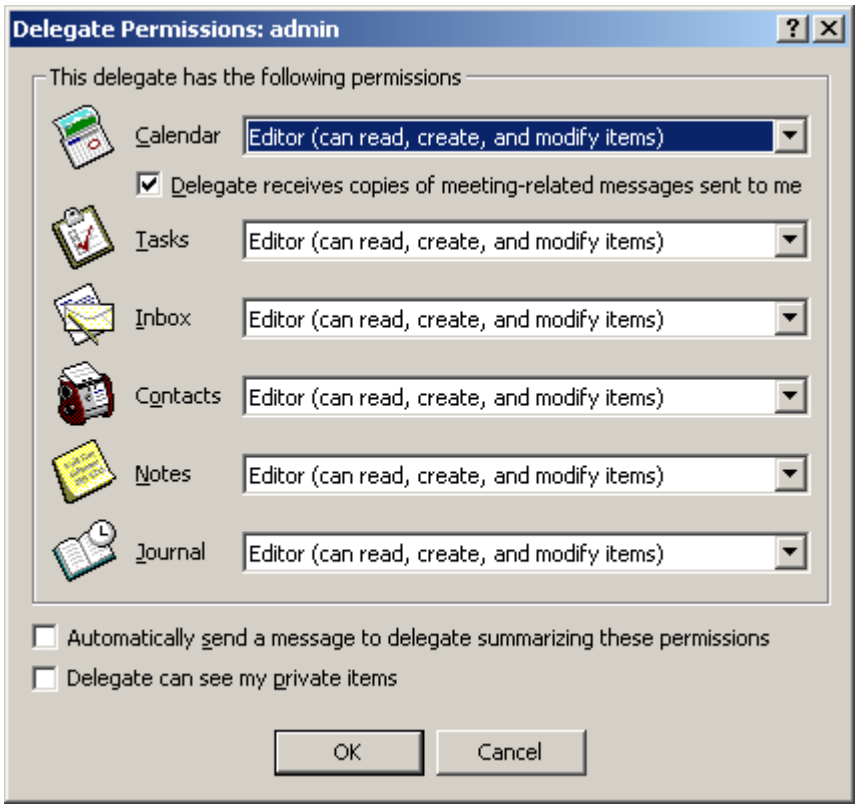

Figure 8. Delegate Permissions

Outlook E-mail Security

Outlook provides the following areas e-mail security options:

- Protecting against malicious code attacks in e-mail message attachments and harmful VBA macros.
- Providing authentication and privacy for secure e-mail messages.
- Protecting users from HTML messages with malicious content.
- Providing message security labels information to the message header.

Attachment Security

Outlook 2002 protects against malicious code attacks in e-mail attachments by checking the file type of each attachment in a message that is either received or sent. There are two levels of attachment security: level 1 file types and level 2 file types. Access to level 1 files is blocked. Level 2 file type attachments will prompt the user to save the file on the hard drive. The level 1 and level 2 file types are listed in Table 4. There are no file types

listed under the Level 2 for a default installation. The Exchange administrator can add and remove level types if the user is utilizing either the mailbox or offline folders as the mail delivery location[3]. This can be implemented by customizing the Outlook Security Template, discussed in the subsection, "Outlook Security Administrative Package", later in this chapter.

When a level 1 file is received the user's inbox will display the paperclip icon in the attachment column. The user will see a list of the blocked attachment files in the infobar at the top of the message. When a user sends a level 1 file type attachment, a warning message will be displayed stating that the recipient may not be able to access the file. If the file type is level 2, the attachment icon is shown; the user is prevented from launching the attachment directly from the e-mail message but is instead prompted to save the attachment to the hard disk. The attachment can be run from there.

Table 4. Level 1 and Level 2 File Type Description

Level	File Extension
Level 1	.ade, .adp, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .exe, .hlp, .hta, .inf, .ins, .isp, .js, .jse, .lnk, .mda, .mdb, .mde, .mdz, .msc, .msi, .msp, .mst, .pcd, .pif, .reg, .scr, .sct, .shs, .url, .vb, .vbe, .vbs, .wsc, .wsf, .wsh
Level 2	None

Macro Security

Like all members of the Microsoft office suite, Outlook provides the capability to create custom macros using the Visual Basic for Application programming environment.

Outlook protects against malicious code attacks in Outlook macros by setting the macro security level to High by default. There are three available settings: Low, Medium, and High:

- High — Only signed macros from trusted sources will be run. This is the recommended setting
- Medium — The user chooses whether or not to run macros.
- Low — No protection from macros; this is not recommended.

By default, these settings are controllable by the user. The macro security setting is set on the Outlook Tools menu; click Macro and then click Security. To view the macro security settings, click the **Security Level** tab. To view the trusted sources, click the **Trusted Sources** tab. Trusted sources can be removed using the Remove button. Trusted sources can be added by opening the item or add-in that contains macros from the source to be added to the list. When the Security Warning dialog box is displayed, select the **Always trust macros from this source** check box. If the security warning dialog box does not display this, then the macros are not digitally signed and cannot be added to the trusted source list.

Under the default condition, these security settings are stored in the registry under the HKEY_CURRENT_USER branch. Users can modify these settings because each user has write access to the applicable keys under this branch. It is difficult for the typical user to determine if a source should be trusted. It is recommended that the administrator

[3] For other users, such as those connecting to the Exchange server by IMAP or POP, Outlook 2002 will block all level 1 attachments but does not allow for the definition of level 2 attachments.

make this determination based on organizational policy. Outlook allows the administrator to specify the security level and the trusted sources in manner that will stop non-administrator changes. When the security settings are stored under the HKEY_LOCAL_MACHINE branch, Outlook will read these settings before checking HKEY_CURRENT_USER branch. This prevents the user from writing to them as long as the access control list for HKEY_LOCAL_MACHINE does not allow write access by general users. This method will stop a virus or other attack from modifying these settings.

For maximum security, it is recommended for the administrator to specify the high security setting and the trusted sources for the organization under HKEY_LOCAL_MACHINE. The registry locations are as follows:

For the security level: HKEY_Local_Machine\Software\Policies\Microsoft\Office \10.0\Outlook\Security\Level. Set this value to 3 for high security.

For the list of trusted sources: HKEY_Local_Machine\Software\Microsoft\VBA \Trusted. One way to do this is to begin with a single machine and choose to trust the approved macro developers for your organization. Once this is completed, populate this key using the values from HKEY_Current_User\Software\Microsoft \VBA \Trusted[4].

Note that the list of trusted sources is shared with the other Office applications. Also note that these settings only apply to VBA macros; they do not apply to VBScript embedded within custom forms. In this instance, Outlook limits execution based upon where the form is published. Organizational forms libraries and public folders are considered trusted locations, and VBScript contained in forms stored in these location is not subject to the macro security settings and can always be executed. Chapter 4 discusses this in more detail.

Secure Messages

Outlook provides options for authentication and privacy by digitally signing and encrypting messages. Digitally signing a message is proof for the recipient that the message is really from the sender because the message is digitally signed using a digital certificate. Encrypting messages ensures that only the intended recipient can read the message. Both these methods are done using digital IDs (certificates). A Digital ID establishes a user's identity to others that they communicate with. Digital IDs contain a unique digital code, which can be used to verify a digital signature or encrypt messages.

The digital ID is obtained from the Microsoft Exchange environment or from an external Certificate Authority (CA); it contains a certificate (public key) and a private key. Secure messaging for Outlook is set on the Outlook **Tools** menu; click **Options** and then click the **Security** tab. This security window is shown in Figure 9.

To enable secure messaging the user must first get a digital ID by clicking on the **Get Digital ID** button. The user will be prompted to choose the method of getting a digital ID; choose the Exchange Server if the digital ID will be obtained using the advanced security features of Exchange; click **S/MIME certificate** if the certificate will be obtained over the Internet. The choice is based upon local policy. If the S/MIME certificate is chosen, an external CA will issue the certificate. If the Exchange Server is chosen as the CA, the user will be prompted to enter in the token that was received from the administrator issuing the certificate; following this the user will enter in the password that will be used with the digital ID. For complete instructions on obtaining a digital ID refer to Chapter 8,

[4] Refer to the article, "Protecting Office Documents", found at http://www.microsoft.com/office.

Certificates and Advanced Security, in this document. After installing the digital ID the secure e-mail settings can be set. The options for secure e-mail are:

- **Encrypt contents and attachment for outgoing messages** – encrypts the contents and attachments for all outgoing messages.
- **Add digital signature to outgoing messages** – adds the digital signature to all outgoing messages.
- **Send clear text signed message when sending signed messages** – allows recipients who don't have S/MIME security to be able to read the message. The disadvantage of enabling this option is that some mail servers may slightly modify the message (wrapping lines, for example). This will cause false indications of tampering on the receiving end. To avoid these misleading indications, it is preferable not to enable this feature unless necessary.
- **Request secure receipt for all S/MIME signed messages** – verifies that the digital signature is being validated by recipients. When a message with a secure return receipt request is sent a notification is returned to the user's Inbox when the signature on the message is validated by the recipient's security system.

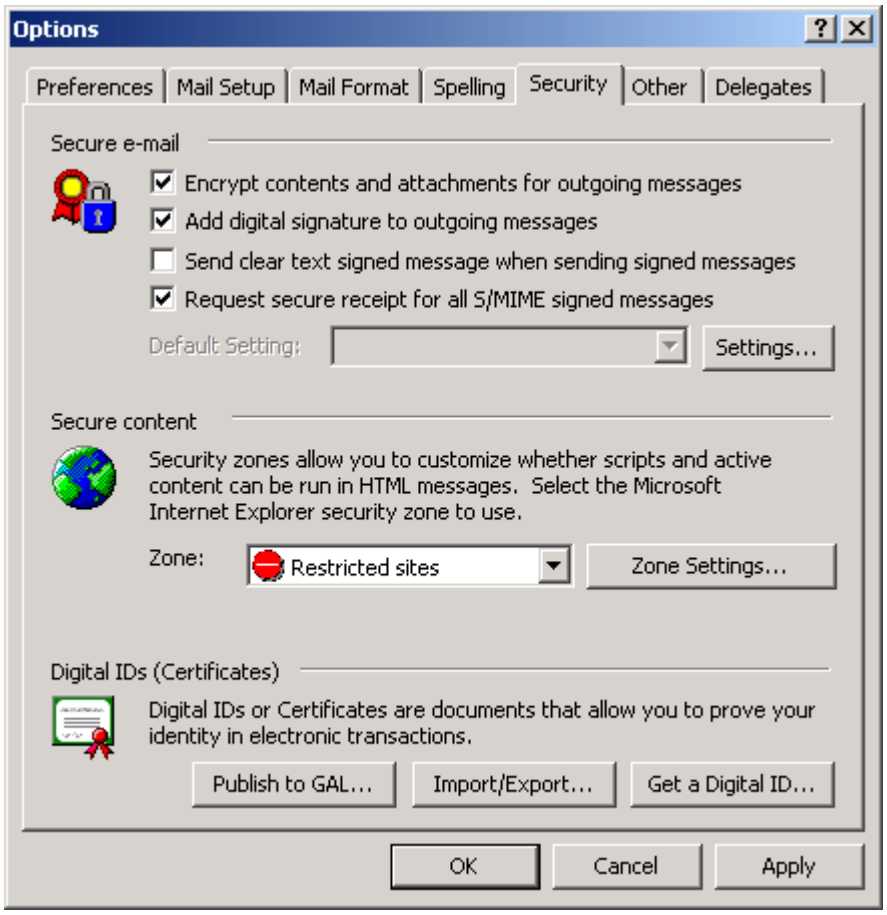

Figure 9. Outlook Security Options

The options chosen for secure e-mail are left to the discretion of the user. To ensure data confidentiality, all messages should be encrypted but it should be noted that if a recipient of the message has not set up the appropriate security options, the message cannot be sent securely. To send an encrypted message a copy of the recipient's digital ID must be available in Active Directory (for users in the same Exchange environment) or stored along with the recipients address in the **Contacts** folder or Address Book. To authenticate the message, all messages should be sent with a digital signature. Digital signature and encryption can be applied on a per message basis. This can be done by using the **Options** button and selecting **Security Settings** within the message being sent.

Each digital ID has security settings. These settings can be viewed and changed by clicking the **Settings** button shown in Figure 9. This allows the user to choose the certificate to use, the secure message format, set as default and select a name for these security settings. This is useful if the user has more than one digital ID and needs more than one set of security settings. Also selected from this screen is the **Security Labels** button. *Security labels* are used to add information to a message header about the sensitivity of the message content. To utilize security labels the administrator must set up a security label policy, the user must be using S/MIME and the message must be digitally signed.

Also shown in Figure 9 are the **Import/Export** button, the **Publish to GAL** button and the **Zone Settings** button. The **Import/Export** button is used to either import or export the digital ID to a file. The **Publish to GAL** button allows the user to publish their default security certificates to the Global Address List; this makes it easier to exchange encrypted messages with other users in the organization[5]. The **Zone Settings** button will be discussed below.

Script Protection

Outlook protects against malicious content in HTML based e-mail by utilizing *Security Zones*. *Security Zones* are used to control what happens when messages are received or web pages are accessed that contain scripts. By choosing the appropriate zone, potentially damaging content is prevented from being downloaded.

Outlook 2002 utilizes these zones in that one can select which of two zones Outlook messages fall into -- the Internet zone or the Restricted Zone. The settings for the selected zone are then applied by Outlook to all messages.

Security Zones can be set from the **Zone Settings** button shown in Figure 10. Each type of security zone is shown along with the security level for this zone. The settings can be changed by clicking the **Custom Level** button. The custom settings are displayed as shown in Figure 11.

[5] Note however that when obtaining the digital ID from the Exchange server it is automatically published to the GAL.

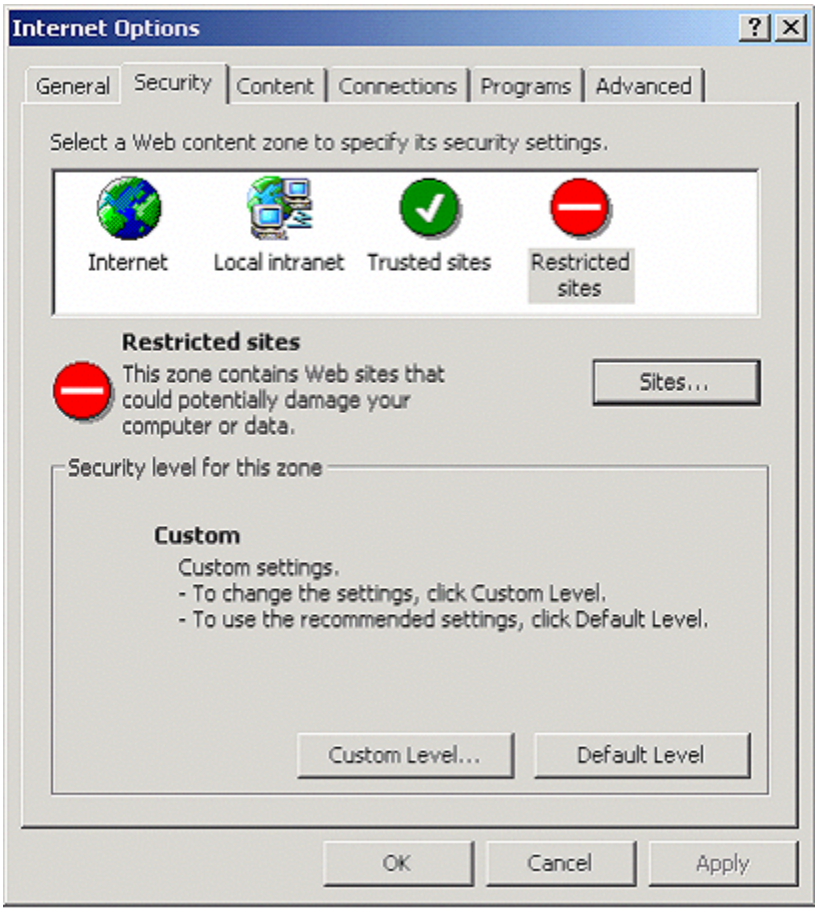

Figure 10. Security Zones Settings

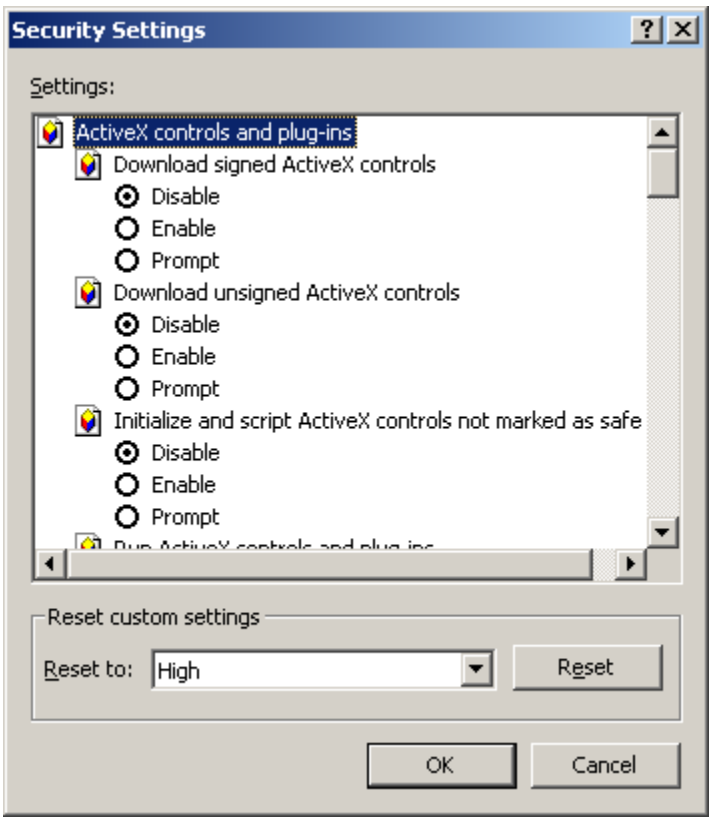

Figure 11. Custom Security Zone Settings

It is recommended for Outlook to run in the Restricted Zone with custom settings. These settings are listed in Table 5.

Table 5. Restricted Zone Custom Settings

☐	Download signed ActiveX controls	**DISABLE**
☐	Download unsigned ActiveX controls	**DISABLE**
☐	Initialize and script ActiveX controls not marked as safe	**DISABLE**
☐	Run ActiveX controls and plug-ins	**DISABLE**
☐	Script ActiveX controls marked safe for scripting	**DISABLE**
☐	Allow cookies that are stored on your computer	**DISABLE**
☐	Allow per-session cookies (not stored)	**DISABLE**
☐	File download	**DISABLE**
☐	Font download	**DISABLE**
☐	Java permissions	**DISABLE JAVA**
☐	Access data sources across domains	**DISABLE**
☐	Don't prompt for client certificate selection when no certificates or only one certificate exists	**DISABLE**
☐	Drag and drop or copy and paste files	**DISABLE**
☐	Installation of desktop items	**DISABLE**
☐	Launching programs within an IFRAME	**DISABLE**
☐	Navigate sub-frames across different domains	**DISABLE**
☐	Software channel permissions	**HIGH SAFETY**
☐	Submit non-encrypted form data	**DISABLE**
☐	Userdata persistence	**DISABLE**
☐	Active Scripting	**DISABLE**
☐	Allow paste operations via script	**DISABLE**
☐	Scripting of Java Applets	**DISABLE**
☐	Logon	**Anonymous logon**

Note that changes made here will also apply to the Restricted Zone when web surfing with Internet Explorer. Keep in mind that the Restricted Zone is intended to include those sites that are not trusted - one should restrict what those sites can do and in fact these recommended settings are only slightly more restrictive than the default settings for this zone.

Read as Plain Text

While using the restricted zone settings as outlined above will offer protection against scripts embedded in a HTML message, at least one vulnerability allowed a means to bypass this protection. This vulnerability is described at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-021.asp. Office XP Service Pack 1 offers the ability for all non-signed and non-encrypted messages which use HTML formatting to be read as plain text. This could cause some HTML messages to become difficult to read, but offers the advantage of offering additional protection against scripts embedded into a message. It is recommended to take advantage of this feature by setting the following key:

Key: [HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Outlook\Options\Mail]
Value Name: ReadAsPlain
Data Type: REG_DWORD
Value Data: 1

Respecting Least Privilege

The concept of least privilege means *giving a user only those rights that s/he needs to do their job*. *Least privilege* practices include making certain that administrative accounts are kept to a minimum, that administrators use a regular account as much as possible instead of logging in as administrator to do routine things such as reading their mail, and setting resource permissions properly. This limits the access of any malicious executables that may be inadvertently launched.

Outlook Security Administrative Package

The Outlook Security Administrative package contains the security administrative tools that implement optional customized security for Outlook 2002. Outlook default security features provide a level of protection but limit some functionality. These security limits can be modified using the security administrative tools.

To enable customized security settings, the clients must be using Outlook 2002 with the Exchange Server using either the mailbox or offline folders as the default mail delivery location.

Custom security settings are stored in messages in a top-level folder in the public folders tree. Each user that needs customized security must have a special registry key set on their computer. This registry key allows the client to download the custom security settings stored on the Exchange server. These features are provided through the use of an Outlook security administrative package, Admpack.exe, which is available on the Office XP Resource Kit or can be downloaded from the Microsoft web site. The administrative package is installed on the client machine by copying Admpack.exe and running the executable. This executable will copy the Outlook Security Template onto the client computer. [6] The Outlook Security administrative package helps with trusted code control, programmatic settings and Outlook security Settings.

Trusted Code Control

Trusted code control is the first step in the administrator security customization process. This will enable the administrator to see all the options that are available on the Outlook Security Template. The following steps outline the installation of the *Trusted Code Control:*

- Copy **Hashctl.dll** from the client computer to the following location on the computer administrators will use to modify the security settings**: \%systemroot%\system32[7]. ** Run the command**: regsvr32 hashctl.dll**

[6] OutlookSecurity.oft, Hashctl.dll, Comdlg32.ocx, Readme.doc are the four files copied onto the client computer after running this executable.
[7] %systemroot% is typically c:\winnt

- Copy **Comdlg32.ocx** from the client computer to the location **\%systemroot%\system32** on the computer administrators will use to modify the security settings. Run the command regsvr32 **comdlg32.ocx**

After running each command a dialog box will show that this operation was completed successfully.

Outlook Security Settings Customization

The Outlook Security template (OutlookSecurity.oft) is modified by the administrator to provide security for users with permission to access the template. To begin this process, a public folder must be created on the **Exchange Server**, where the security settings can be stored. The public folder must be named: "Outlook 10 Security Settings" or "Outlook Security Settings". This folder must have either of these exact names and must be created in the root of the public folder tree. The folder permissions must be set so that all users can read all items by setting the permissions for default user to reviewer. Also change the role of the anonymous user to none. Only users trusted to administer the security template settings should be given the permission to create, edit or delete items in this folder.

On the Outlook client computer open the file, OutlookSecurity.oft. When prompted for a folder, select the folder created on the Exchange Server in the previous step. The default template is shown in Figure 12.

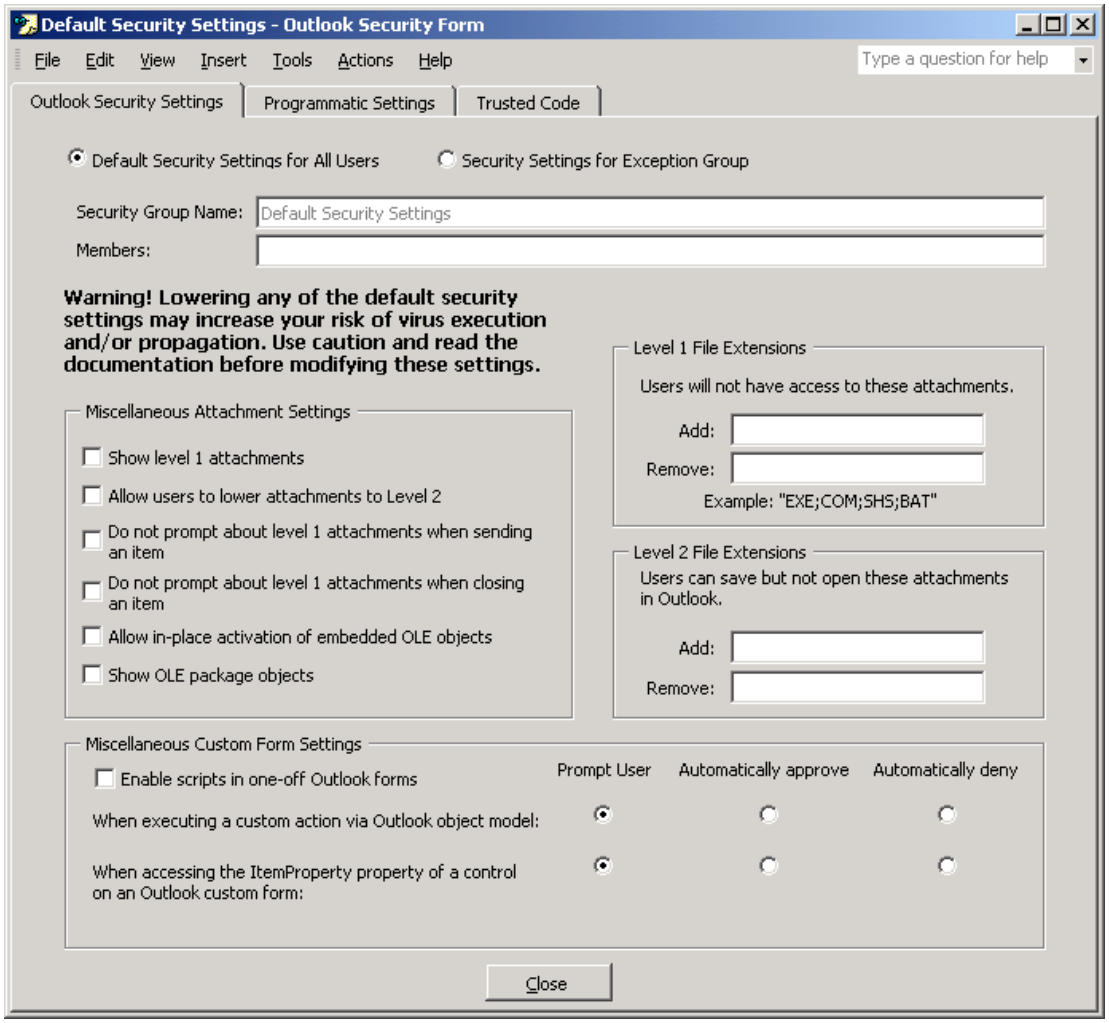

Figure 12. Default Security Settings on Outlook Security Template

On the **Tools** menu go to **Forms** and click **Publish Form** and select the folder created in the previous step, "Outlook 10 Security Settings" or "Outlook Security Settings". Name the form **Outlook Security Form,** publish the form and close the form without saving it. Using Outlook, open the form by choosing **File/New** and select the **Choose Form** command to open the template.

The security settings can be created so that they will be used by all users or they can be customized for a specific set of users. This is chosen at the top of the template as shown in Figure 12. If custom settings are being created for a specific set of users, the name of each user must be entered into the **Members** box along with the **Security Group Name** that describes that group. Following this selection, the rest of the form can be edited. Each area of the form is described in the following paragraphs.

As shown in Figure 12, there are three tabs available for customization. These tabs are: **Outlook Security Settings** tab, **Programmatic Settings** tab, and the **Trusted Code** Tab.

Outlook Security Settings

The **Outlook Security Settings** tab enables the configuration of settings in relation to attachments, the types of files user can access, and scripting. The **Outlook Security Settings tab** contains control boxes for *Miscellaneous Attachment Settings, Level 1 File Extensions, Level 2 File Extensions,* and *Miscellaneous Custom Form Settings*. These areas are described in the following paragraphs.

The miscellaneous attachment settings are described in Table 6.

Table 6. Attachment Settings

Item	Description
Show Level 1 attachments	Enables users to gain access to attachments with Level 1 file
Allow users to lower attachments to Level 2	Enables the end user to demote a Level 1 attachment to Level 2 via addition of a registry key [HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\10.0\Outlook\Security] "Level1Remove"=[semicolon delimited list]. While Windows 2000 non-administrative users do not have write access to this key, this setting is useful for mixed environments.
Do not prompt about Level 1 attachments when sending an item	Prevents users from receiving a warning when sending a Level 1 attachment.
Do not prompt about Level 1 attachments when closing an item	Prevents users from receiving a warning when they close a mail message, appointment, or other item containing a Level 1 attachment.
Allow in-place activation of embedded OLE objects	Allows users to double-click an embedded object and open it in the program. If using Microsoft Word as the e-mail editor, clearing this check box will still allow OLE objects to be opened when the embedded object is double-clicked.
Show OLE package objects	Displays OLE objects that have been packaged. Caution should be used in displaying OLE package objects, because the icon can easily be changed and used to disguise malicious files.

These default settings should be left as is (disabled); changing these settings can lead to virus propagation.

The types of files that can be accessed are configured in the Level 1 and Level 2 File Extensions boxes. The level 1 file types will be blocked from the user; these files types are listed in Table 4. Level 1 file types can be added or removed from this list using the Level 1 File Extension box. Level 2 file types can be added to this list by using the Level 2 File Extension box. The addition of Level 2 file types should be carefully considered based upon the operational environment. For example, if Perl interpreters are installed on a network, it may be prudent to add the .pl extension as a level 2 file.

The Miscellaneous Custom Form Settings specifies the action taken when controls are added to a custom Outlook form. The table shown in Table 7 describes the settings for scripts, custom controls and custom actions.

Table 7. Custom Form Settings

Option	Option Description
Enable scripts in one-off Outlook forms	Run scripts contained in forms where the script and the layout are contained in the message itself.
When executing a custom action via the Outlook object model	Specifies action when a custom action is run using the Outlook object model. One of the following actions must be selected: **Prompt user** – ask the user whether to allow programmatic send access. **Automatically approve** – always allows programmatic send access without displaying a message. **Automatically deny** – always denies programmatic send access without displaying a message.
When accessing the ItemProperty property of a control on an Outlook custom form	Specifies action when a user adds a control to a custom Outlook form and then binds that control directly to any of the Address Information fields. By doing this, code can be used to indirectly retrieve the value of the Address Information field by getting the Value property of the control. One of the following actions must be selected: **Prompt user –** ask the user whether to allow programmatic send access. **Automatically approve -** always allows access to Address Information fields without displaying a message. **Automatically deny -** always denies access to Address Information fields without displaying a message.

The custom form settings are set to **Prompt User** by default. Consider changing this to **Automatically Deny** if these features are not utilized by the organization's legitimate applications. The **Enable scripts in one-off Outlook forms** should not be selected.

Programmatic Settings

The **Programmatic Settings** tab enables the configuration of settings related to the Outlook Object model, Collaboration Data Objects (CDO) and the Simple Messaging Application Programming Interface (Simple MAPI). The **Programmatic Settings** tab is shown in Figure 13. These capabilities are defined as:

Outlook Object Model – allows programmatic manipulation of data stored in Outlook folders.

Collaboration Data Objects (CDO) – libraries are used to implement messaging and collaboration functionality in custom applications. CDO can be called from any language that supports automation and implements most MAPI functionality.

Simple MAPI – allows the addition of simple messaging functionality to Windows based applications.

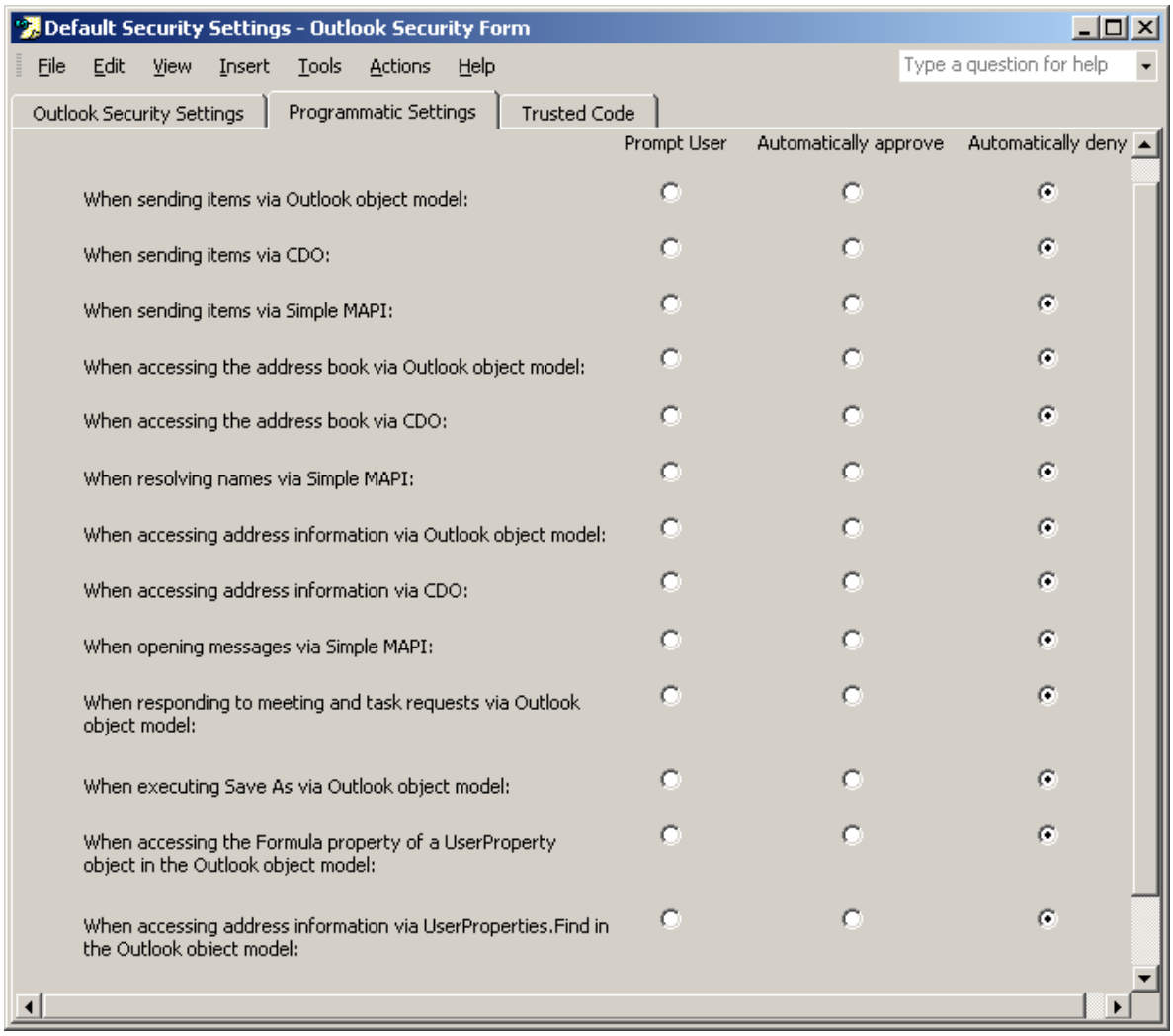

Figure 13. Programmatic Settings Window

Under the Programmatic Settings tab there are thirteen options that can be configured to control the Outlook Object model, CDO and Simple MAPI. Each option can be set for **Prompt User**, **Automatically approve**, or **Automatically deny.** These options are described in Table 8.

Table 8. Programmatic Settings

Option	Option Description
When sending items via Outlook object model	Specifies action taken when a program attempts to send mail programmatically using the Outlook object model.
When sending items via CDO	Specifies action taken when a program attempts to send mail programmatically using CDO.
When sending items via Simple MAPI	Specifies action taken when a program attempts to send mail programmatically using Simple MAPI.

Option	Option Description
When accessing the address book via Outlook object model	Specifies action taken when a program attempts to gain access to an address book using the Outlook object model.
When accessing the address book via CDO	Specifies action taken when a program attempts to gain access to an address book using CDO.
When resolving names via Simple MAPI	Specifies action taken when a program attempts to gain access to an address book using Simple MAPI.
When accessing address information via Outlook object model	Specifies action taken when a program attempts to gain access to a recipient field using the Outlook object model.
When accessing address information via CDO	Specifies action taken when a program attempts to gain access to a recipient field using CDO.
When opening messages via Simple MAPI	Specifies action taken when a program attempts to gain access to a recipient field using Simple MAPI.
When responding to meeting and task requests via Outlook object model	Specifies action taken when a program attempts to send mail programmatically using the Respond method on task requests and meeting requests.
When executing Save As via the Outlook object model	Specifies action taken when a program attempts to programmatically use the **Save As** command on the **File** menu to save an item.
When accessing the Formula property of a UserProperty object in the Outlook object model	Specifies action taken when a user adds a Combination or Formula custom field to a custom form and binds it to an Address Information field.
When accessing address information via UserProperties. Find in the Outlook object model	Specifies action taken when a program attempts to search mail folders for address information using the Outlook object model.

The *Programmatic Settings* should be set with the **Automatically deny** selection unless these settings are vital for operational reasons.

Trusted Code

The Trusted Code tab is used to load the COM add-ins that are trusted and can be run without encountering the Outlook object model blocks. Add or remove specific COM add-ins as trusted code by clicking the Add button, as shown in Figure 14. A list of authorized COM add-ins should be reviewed for inclusion as trusted code.

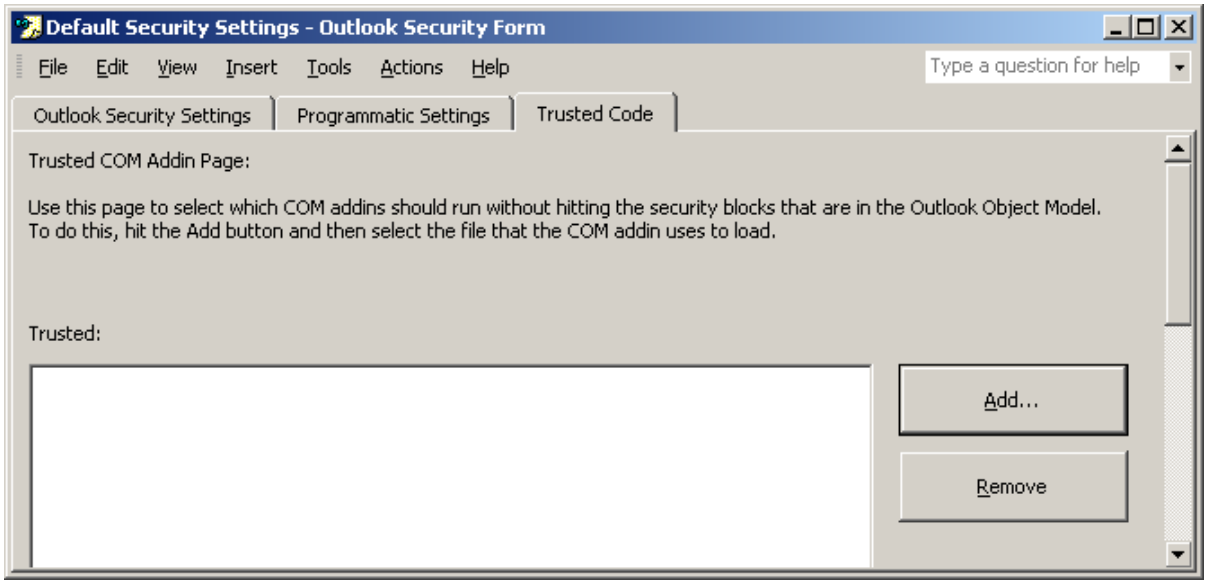

Figure 14. Trusted Code Window

Deployment of Customized Security Settings

These customized security settings defined via the Outlook Security template must be enabled for the client computers before they will be effective. To enable these settings a new registry key must be deployed to all clients that were not deployed with Office system policies. The registry key for enabling these custom settings is:

HKey_Current_User\Software\Policies\Microsoft\Security\CheckAdminSettings
DWORD value

The key settings are described in Table 9.

Table 9. Key Settings

Key state	Description
No key or key set to anything but 0,1 or 2	Outlook uses default administrative settings.
Set to **0**	Outlook uses default administrative settings.
Set to **1**	Outlook looks for custom administrative settings in the Outlook Security Settings folder.
Set to **2**	Outlook looks for custom administrative settings in the Outlook 10 Security Settings folder.

A value of 1 or 2 is required.

End User Customizations

A registry key is provided which is intended to preclude the user from demoting file types from level 1 to level 2. This registry key is located at:

HKey_Current_User\Software\Policies\Microsoft\Office\10.0\Outlook
String Value: DisallowAttachmentCustomization

Practically speaking, this setting is somewhat superfluous. In Windows 2000 non-administrative users can not create the registry key necessary to demote file types to level 2 and, for mixed environments, this setting is best controlled by the security template as previously discussed.

Administrative Control of Outlook Security Settings

The document "Outlook 2002 Security Model" is available at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/xpreskit/html/outg01.asp. It describes how an administrator can control many of the security options discussed in this chapter through registry settings. Other options are provided in the Office XP resource kit.

Important Security Points

- Install the client to a partition different from the operating system location.
- Keep up-to-date with service packs and security related hotfixes.
- Set Outlook 2002 file permissions as follows: Administrators: Full control, Authenticated Users: Read & Execute, Creator Owner: Full Control, Domain Admins: Full Control, System: Full Control.
- Use **password authentication** as the authentication method.
- Specify the high security setting for macros and specify the trusted sources for the organization under HKEY_LOCAL_MACHINE registry keys identified above.
- If data confidentiality is required, consider the use of RPC encryption to provided data confidentiality for Exchange messages as they transverse the wire between the client and server. Alternately, use S/MIME to enable e-mail content confidentiality over the complete path from writer-to-reader.
- Save the offline folders file to user's home directory and/or encrypt using the Encrypting File System to provide data confidentiality for the messages that are not otherwise protected at rest.
- Use folder permissions to protect personal information if delegating access to personal folders.
- Use the **Outlook Administrative Security package** to protect against malicious code based attacks.
- Protect users from HTML messages that contain malicious content by using the **Restricted Zone** with the described customized settings.
- Set Outlook 2002 to read HTML messages as plain text.
- Customize client security settings using the Outlook Security Template and utilize the settings detailed in this chapter.
- Review and approve the list of trusted code COM add-ins.

Chapter

3

Administrative Permissions

Exchange Server contains a wide variety of permissions that can be applied to various objects within the Exchange Systems Manager to facilitate restricting and partitioning administrative access.

This section describes the various permissions that can be assigned to Windows 2000 users/groups for the various Exchange objects within the Exchange System Manger and summarizes the tools available to the Exchange administrator for managing permissions.

System Manager

Exchange 2000 can be administered with two main tools: *System Manager* and *Active Directory Users and Computers*. These tools can be setup as snap-ins in the Microsoft Management Console (MMC).

System Manager is the Exchange administration tool that is installed during installation when Microsoft Exchange System Management Tools is selected on the Component Selection screen of the Microsoft Exchange 2000 Installation Wizard. If SMTP is installed, the System Manager can be installed on any computer running Windows 2000 that is used to manage the Exchange organization. This includes any computer running Windows 2000 Professional if Windows 2000 Administration Tools is installed.

Servers, connectors, public folders, address lists, protocols, and policies can be administered in System Manager. Under the organization node in System Manager, there are containers representing the areas that can be managed. Some of these containers contain other containers and objects. The specific containers that are displayed are dependent on whether or not the display of administrative and/or routing groups is enabled. This is controlled via the General tab of the organizational container properties page. An administrative group is a collection of Active Directory objects that are grouped together for the purpose of administering permissions. Administrative groups can contain policies, routing groups, public folder hierarchies, servers, and chat networks. Administrative groups can be used, as needed, to delegate and subdivide administration of the Exchange organization. A Routing group is a collection of servers that have permanent, high bandwidth connectivity. Routing groups contain Connectors and will be covered in Chapter 5.

Exchange Permissions

Exchange 2000 permissions control access to resources. Permission provides specific authorization to perform an action. Exchange permissions are based on the Windows 2000 permission model. Permissions on an object and on the object's child objects can be assigned to a user or group. When an object is created in Windows 2000,

the object inherits permissions from its parent object. Inheritance can be overridden either by assigning permissions directly to the object or by specifying that the object should not inherit permissions. Windows 2000 has provided a number of options for how inheritance can be set. These options are:

- This object only
- Inherit only
- This object and subcontainers
- This object and child objects
- Subcontainers only
- Child objects only
- This object, subcontainers, and child objects
- Subcontainers and child objects

In addition to the standard Windows 2000 permissions there are a number of Exchange specific permissions, most of which are described quite nicely in the Exchange Server help file and are included in the following:

- Add public folder to admin group. This permission is used to indicate which users are allowed to add a public folder to an administrative group.
- Administer Information Store. This permission is used by the Information Store service to determine if a user has permissions to perform various operations.
- Create named properties in Information Store. This permission is used by the Information Store service to determine if a user has permissions to create named properties. A named property is a store attribute that can be accessed by name. Examples include display name, locale, deleted item flags, and activation schedule.
- Create public folder. This permission is used to indicate which users are allowed to create a public folder under the given folder.
- Create top level public folder. This permission is used to indicate which users are allowed to create a top level public folder.
- Full store access. This permission is used to indicate which users are allowed full access to Information Store.
- Mail-enable public folder. This permission is used to indicate which users can make a public folder mail-enabled.
- Modify public folder ACL. This permission is used to determine a user has permission to modify a public folder Access Control List (ACL).
- Modify public folder admin ACL. This permission is used to determine if a user has permission to modify a public folder administrative ACL.

- Modify public folder deleted item retention. This permission is used to indicate which users are allowed to modify the length of time (in days) that items deleted from the public folder are retained.
- Modify public folder expiration. This permission is used to indicate which users are allowed to modify the expiration date of content in the public folder.
- Modify public folder quotas. This permission is used to indicate which users are allowed to modify the size limit of the public folder.
- Modify public folder replica list. This permission is used to indicate which users are allowed to modify the replica list. An administrator must be given this permission on the administrative group to which the given public folder points and the public database to which the replica should be added.
- Open mail send queue. This permission is used by Information Store to determine if a user has permission to open the Mail Send queue that is used for queuing messages to and from Information Store. Only the Exchange Servers account is typically granted this permission.
- Read all metabase properties. This permission is used to indicate which users are allowed to read the Internet Information Services (IIS) metabase, the database that stores configuration values for IIS.
- Remove public folder from admin group. This permission is used to indicate which users are allowed to remove a public folder from an administrative group.
- Receive As. This permission is used to grant a user account permission to receive messages using a mailbox.
- Send As. This permission is used to grant a user account permission to send messages using a mailbox.
- View information store status. This permission is used by the Information Store service to determine if a user has permission to view Information Store data, such as logon information and resources.

Permissions can be viewed in the System Manager by right clicking on a root or leaf node. From the pop-up menu, select Properties and then click on the **Security** Tab in the Properties dialog box.[8]

Fortunately one does not always have to deal directly with this plethora of permissions. The Exchange Delegation Wizard allows assignment of these permissions based upon roles as will be discussed shortly.

Windows 2000 Security Groups

There are various types of Windows 2000 security groups that are used to assign permissions. These types include Global Groups, Domain Local Groups and Universal Groups. Use groups to assign permissions since it simplifies the assignment and

[8] In order to enable the security tab on all Exchange object types, see Microsoft Knowledge Base Article Q259221.

revocation of permissions that can be accomplished by simply adding or deleting group members. Hence, only the permissions on the group need to be administered. Global Groups contain resources from one domain but can be used to assign permissions in any domain. Domain Local Groups are used to assign permissions only in the domain where they are defined. Universal Groups are used to assign permissions anywhere in the forest.

There are a number of pre-existing Windows 2000 security groups which have rights to Exchange 2000. These groups include *Domain Admins*, *Enterprise Admins*, *Exchange Domain Servers*, *Exchange Enterprise Servers* and *EVERYONE*. These groups are defined as follows:

- *Domain Admins* is a group with administrators of the domain as members. Members of this group can manage user accounts, contacts, groups, mailboxes, computers, messaging features, delivery restrictions, and storage limits. By default, this group is a member of the Administrators group on the Exchange 2000 Server, and its only member is the local user, Administrator.

- The *Enterprise Admins* group has as its members administrators of the enterprise. This group is for administering in any domain of the enterprise. Its members have full control over Exchange 2000 Server and are not restricted in any way. By default, this group is also a member of the Administrators group and its only member is the local user, Administrator.

- The *Exchange Domain Servers* group can manage mail interchange and queues. All computers running Exchange Server 2000 are members of this group. This group is a member of the domain local group, Exchange Enterprise Servers.

- *Exchange Enterprise Servers* is a domain local group. By default, this group has Exchange Domain Servers as its only member.

- *EVERYONE* is a group that contains as members all interactive, network, dial-up, and authenticated users. Members of this group can, by default, create top-level public folders, sub-folders within public folders, and named properties in the information store.

Administrative Roles and the Delegation Wizard

The Delegation Wizard, contained in the Exchange System Manager, is an Exchange 2000 tool that simplifies assigning permissions to Exchange objects. Rather than assign permissions to administrators individually, groups of administrators can be created and the Delegation Wizard can be used to assign a set of administrative permissions to each group. Creating security groups and adding specific users to those groups simplifies managing permissions across the organization.

A finer level of control can be obtained by using Roles in the Delegation Wizard; then, permissions can be modified as necessary directly on Exchange objects by using the System Manager.

When you start Delegation Wizard, you can assign the following roles to groups and users:

- **Exchange Full Administrator**. This role can administer all Exchange system information and modify permissions on Exchange objects.

- **Exchange Administrator**. This role can administer all Exchange system information.

- **Exchange View Only Administrator**. This role can view Exchange configuration information.

The permissions assigned to these roles depend on where in the Exchange hierarchy the Delegation Wizard is invoked. The Delegation Wizard can be invoked at the Organization level or at the Administrative Group level. The following tables offer an illustration of the permissions that result from implementing the Delegation Wizard at each of these levels. Remember that the permissions for many of the plethora of System Manager objects can be further refined via the properties page of the object.

Delegation Wizard Invoked at the Organization Level

If the Delegation Wizard is invoked at the Organization Level, the permissions shown in Table 10 apply to the following roles:

Table 10. Permissions with Delegation Wizard Invoked at Organization Level

Roles	Objects	Permissions
Exchange Full Administrator	Organization Object	All permissions except Send As and Receive As
Exchange Full Administrator	Administrative Group	All permissions except Send As and Receive As
Exchange Administrator	Organization Object	All permissions except Send As, and Receive As, Change Permissions, and Take Ownership
Exchange Administrator	Administrative Group	All permissions except Send As, and Receive As, Change Permissions, and Take Ownership
Exchange View Only Administrator	Organization Object	Read, Execute, Read Permissions, List Contents, Read Properties, List Object, View Information Store Status permission
Exchange View Only Administrator	Administrative Group	Read, Execute, Read Permissions, List Contents, Read Properties, List Object, View Information Store Status permission

Delegation Wizard Invoked at the Administrative Group Level

If the Delegation Wizard is invoked at the Administrative Group level, the following permissions shown in Table 11 apply.

Table 11. Permissions with Delegation Wizard Invoked at Administrative Group Level

Roles	Objects	Permissions
Exchange Full Administrator	Organization Object	Read, Execute, Read Permissions, List Contents, Read Properties, List Object
Exchange Full Administrator	Administrative Group[9]	All permissions except Send As and Receive As
Exchange Administrator	Organization Object	Read, Execute, Read Permissions, List Contents, Read Properties, List Object
Exchange Administrator	Administrative Group[9]	All permissions except Send As, and Receive As, Change Permissions, and Take Ownership
Exchange View Only Administrator	Organization Object	Read, Execute, Read Permissions, List Contents, Read Properties, List Object
Exchange View Only Administrator	Administrative Group[9]	Read, Execute, Read Permissions, List Contents, Read Properties, List Object, View Information Store Status permission

Administrative Account Structure

There are a number of considerations in setting up Exchange 2000 administrative accounts. First is the principle of *least privilege* that dictates giving Exchange administrators only those access rights that are necessary to do their jobs. By using Exchange administrator accounts that do not have Windows 2000 administrative rights, for example, potential damage is limited should that account become compromised. This concept of least privilege can be further extended to the partitioning of Exchange administration roles. For example, some Exchange administrators may require Exchange Full Administrator rights, while others may only require Exchange Admin or View Only access.

Another consideration is related to the structure of administrative groups. If multiple administrative groups exist in an organization, then it might be prudent to confine an administrator to only those Exchange resources in a particular group

Selection of the proper administrative model will be heavily dependent of the structure of the organization running the Exchange server. Small organizations tend to use more centralized management out of fiscal necessity that dictates the placement of administrative functions in the hands of a few individuals. It is also important to note that some Exchange Administrative functions, such as starting and stopping services and accessing certain portions of the registry, require local Windows 2000 administrative rights. Larger organizations tend to be more distributed, which lend themselves to the delegation of administrative rights as described here. In striking the appropriate balance between economic and security factors, keep in mind that respecting the concept of least privilege is a basic tenet of computer security.

[9] The permissions listed for the Administrative Group refer specifically to the administrative group for which the Delegation Wizard was run. Other administrative groups inherit the permissions from the Organizational Object.

Important Security Points

- Do not use Windows 2000 administrative accounts for Exchange 2000 administration when practical.
- Create security groups and assign permission to Exchange objects based upon those groups in lieu of individual accounts.
- Consider partitioning the Exchange 2000 administration into separate groups of administrators, remembering the concept of least privilege.
- Assign administrative roles using the Delegation Wizard to partition the administration of Exchange 2000.
- Understand inheritance ramifications when assigning permissions.

This Page Intentionally Left Blank

Chapter 4

Administrative and Storage Groups

An Administrative Group is a collection of Exchange 2000 servers and administrative objects that are logically grouped together for common administrative purposes. An administrative group can be used as a way of partitioning administrative access among different administrators. An administrative group can contain objects such as policies, routing groups, public folder trees, and servers.

This chapter will present an overview of the various administrative models that can be implemented with administrative groups. It will also present an overview of the security relevant settings associated with administrative and storage groups and will review related security settings associated with mailboxes that are accessed via the Active Directory Users and Computers MMC snap-in.

Administrative Models

In the centralized administrative model, one group maintains complete control over all of the Exchange 2000 servers in the organization. This may be the model of choice for organizations with a limited number of administrators, or those who wish to simplify administration. In the decentralized administrative model, each location has its own team of Exchange administrators, and administrative control is allowed over any objects placed inside their administrative group. These groups are often based on geographical locations or on the departmental needs of the organization. Each of these groups can contain policies, servers, public folder trees, and other objects specific to the group. This model delegates more customized control over the server. The mixed administrative model is best for restricting certain administrative functions to certain people, but not for specializing every administrative function. In this model, you create administrative groups by function rather than by geographical location or departmental boundaries. For example there might be a group that only administers policy objects.

When developing the administrative model, apply the concept of *least privilege*—giving a user only the access rights necessary to perform his or her tasks. The Delegation Wizard discussed in Chapter 3 can be of utility in implementing the administrative model.

Server Objects

The first object beneath the Administrative Group Container is the server container. There are several items associated with this container that are particularly security relevant including diagnostic logging, message tracking, monitoring, and server policies.

Diagnostics Logging Tab

Exchange 2000 services log events to the Windows 2000 application log. Diagnostics Logging can be configured from the **Diagnostic Logging** tab of the Properties page for

the server. Diagnostic logging can be quite useful for debugging problems or investigating security incidents.

Exchange 2000 Server events are assigned an *event level* representing the degree of event criticality. Four levels of increasing criticality—5, 3, 1, and 0—characterize the seriousness of each event (5=least critical; 0=most critical). The *logging level* determines which event levels are logged. Four distinct levels of logging can be set. The levels are:

- **None** - Only events with a logging level of 0 are logged. These events include application and system failures.
- **Minimum** - All events with a logging level of 1 or lower are logged.
- **Medium** - All events with a logging level of 3 or lower are logged.
- **Maximum** - All events with a logging level of 5 or lower are logged. All events concerning a particular service are logged.

Figure 15 shows the Exchange components that can be selected:

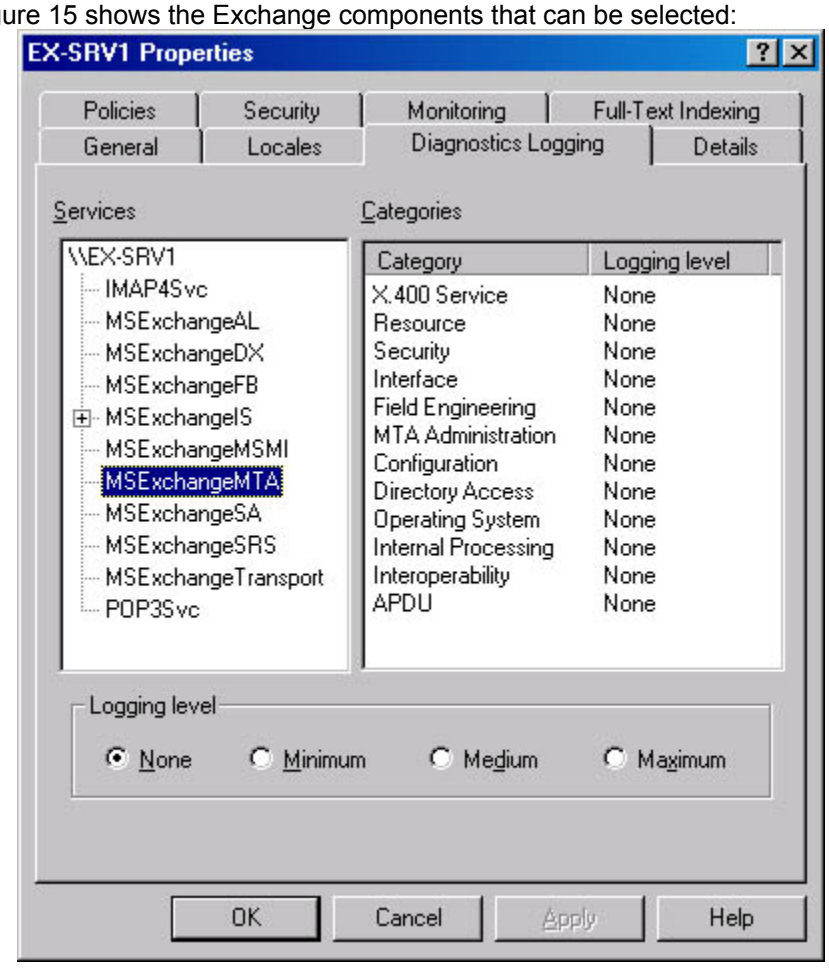

Figure 15. Diagnostic Logging Tab of the Server Properties Page

The minimal recommended Diagnostics Logging settings for the Exchange components are:

MSExchangeMTA at the **maximum level**:

- Security

MSExchangeIS (both Public Folder and Mailbox) at the **maximum level**:

- Logons
- Access Control
- Send On Behalf Of
- Send As

IMAP4Svc and **POP3Svc** at the **maximum level**:

- Authentication

General Tab - Message Tracking

Message tracking is used to monitor the flow of messages in an Exchange 2000 organization. These logs are another useful tool for the administrator in investigating security incidents. Message tracking is enabled from the **General Tab** of the **Properties** page of the server. Exchange 2000 server maintains daily log files with a history of all the messages transferred within an organization. The status of a message—such as whether it has been sent, received, or is waiting in a queue to be delivered—can be determined from the log. Postings to public folders can also be monitored with message tracking.

Standard message tracking allows searches by standard header information, date, time, message ID, as well as sender and recipient. Extended logging allows searches, including the subject line of the message. Standard logging is turned on when the message logging box is selected. Extended logging is turned on when the subject logging box is also selected. Both these options are on the General Tab of the server Properties page. There is also a parameter determining how many days of logs should be retained. The message logs can be searched using the *Message Tracking Center Tool* in the **System Manager**. Since the log files are tab-delimited text files, they can also be searched using standard text editors.

Policies Tab

The message tracking options described above can be set individually on each server or can be controlled for multiple servers via the use of a server policy. Policies will be discussed in more detail later in this chapter.

Monitoring Tab

Exchange Server 2000 allows the monitoring of various resources on the Exchange sever such as CPU usage, disk utilization, Exchange services, and more. These are configurable using the **Monitoring** tab. Notifications can also be configured for automatic delivery when a utilization threshold is reached. For example, a monitor could be set up to send the administrator an e-mail alert when the CPU utilization goes over 90% for a time period of more than five minutes. This could be indicative of a denial of service attack or simply an indication that usage patterns are loading down the server – in either event, an occurrence worthy of administrative attention. It is recommended to minimally monitor CPU utilization and disk capacity for those disk volumes containing user data to

help prevent resource depletion and to set a corresponding alert. To set an alert, navigate to the **Tools/Monitoring and Status/Notification** container within **System Manager**. The alerts can be configured to send an e-mail message or to run a script when a threshold is reached. Running a script can be a particularly valuable feature should the Exchange Server go off-line. One could create a script to use the Net Send command to provide a notification, for example.

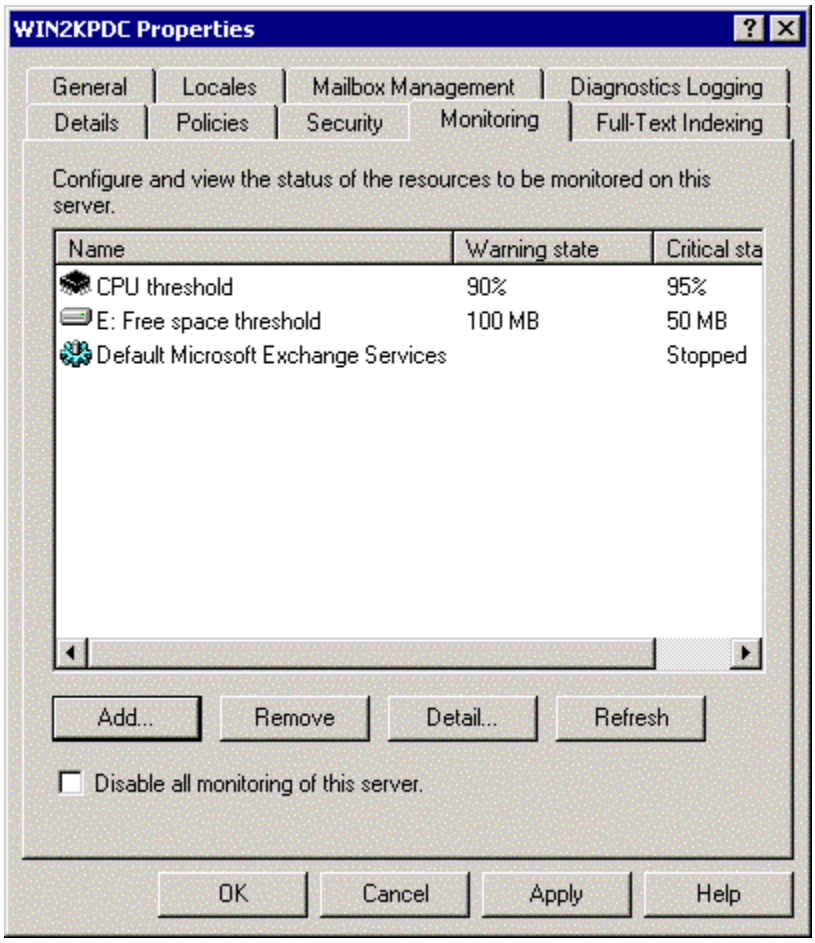

Figure 16. Server Monitoring

Storage Groups

Information stored in Exchange 2000 Server is contained in up to four *Storage Groups,* while Exchange 2000 Enterprise Server is contained in up to 16 storage groups. Upon installation, a default Storage Group named *First Storage Group* is defined. Storage groups contain the *Mail Box Stores* and *Public Folder Stores* that contain the mailboxes and public folders of Exchange 2000 users. Figure 17 shows a properties page of a storage group.

Three items are noteworthy on this property page. The first is the location of the transaction logs. Exchange does not write directly to its database files. Instead, all message transactions are written first to transaction log files and then to the database files. This is done for performance and to improve recoverability should the database

become corrupt. Since log files are written sequentially, Microsoft Exchange clients experience a higher level of performance. Writing data directly to the randomly-accessed database files would entail greater overhead and therefore diminished performance.

For recoverability, transaction log files can be used to recover message transaction data in the event of corruption of the Exchange database files provided that the logs have been backed up or the logs remain intact. As an added layer of protection, log files should be kept on a separate physical disk drive from the Exchange database files. If the database files are damaged, a backup of the database files can be restored and any data that has not been backed up but that has been recorded in the transaction logs can be "played back" by an Exchange compliant backup utility to complete the restore.

The second item of note is the *Circular Logging* option, which is off by default. When this option is enabled, as new log files are created they overwrite old log files provided those log files have been fully committed (written) to the database file. This approach saves disk space but leave the Exchange server more vulnerable to data loss. If a database is corrupted and some of the transaction logs created since the last backup have been overwritten, it will be impossible to fully recover the data. *Circular Logging* should not be enabled due to this drawback.

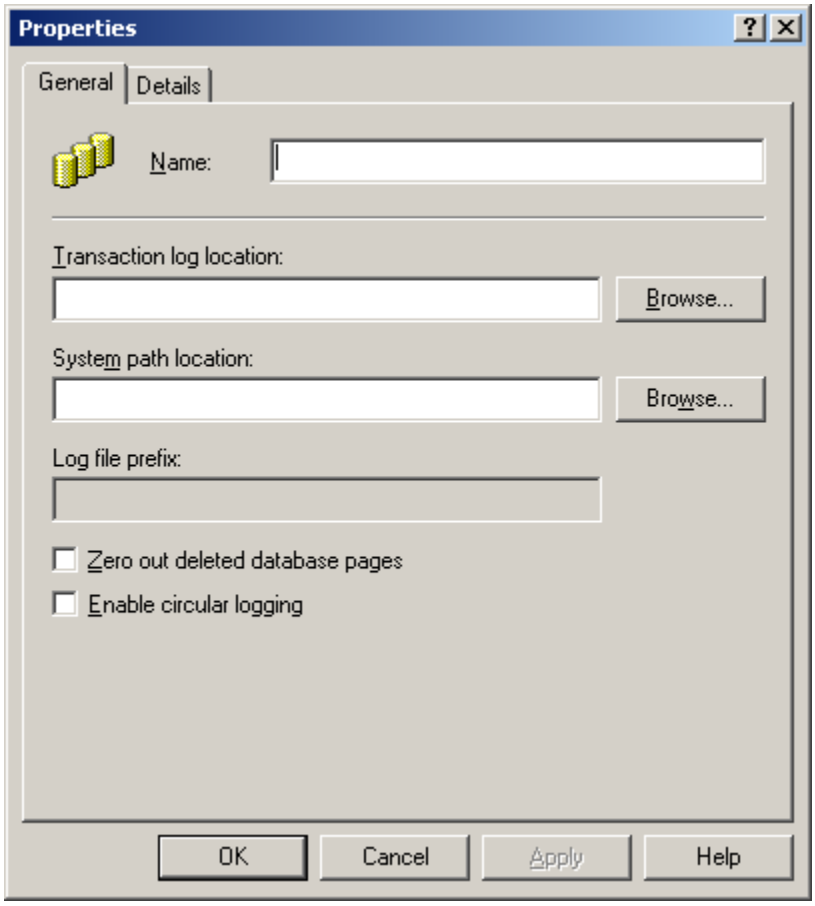

Figure 17. General Tab of Storage Group Properties Page

Third, an option exists to zero out disk pages after deletion, enhancing security at the cost of some additional overhead.

Mailbox Store

The Mailbox Store is a database that contains all the mailboxes of Exchange 2000 users. The Mailbox Store manages the mailboxes and tracks messages. The Mailbox Store contains the private folders within the mailboxes. A user must have an Exchange account and a password with proper access rights and permissions to access a particular private mailbox. There are a number of security relevant options associated with the properties of a Mailbox Store.

General Tab

There is a checkbox option under the **General** tab that allows the archiving of all messages sent to or received by the mailbox store. The archive is stored in a designated mailbox, which belongs to a user. This mailbox is selected by checking the archiving option and then clicking on the **Browse** button. The mailbox can then be selected. If allowed by applicable policy, this option can be enabled by administrators to facilitate the investigation of any security incidents. The use of the archiving option should be carefully controlled as it offers a very convenient method of eavesdropping on Exchange user message.

Figure 18 shows the **General** Tab of the **Mailbox Store Properties** Page:

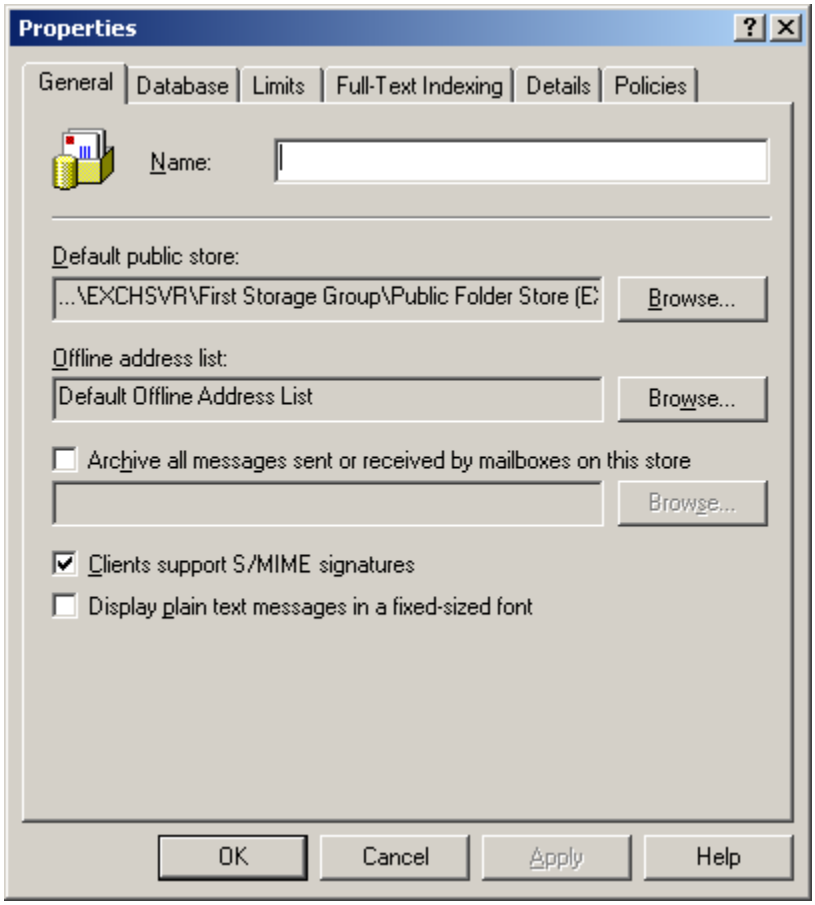

Figure 18. General Tab of Mailbox Store Properties Page

Exchange 2000 Server supports the Secure Multi-purpose Internet Mail Extension (S/MIME) for message confidentiality and integrity. As part of the S/MIME standard, clients can add a signature to a message that is used by the recipient to verify the identity of the user. In order to preserve these signatures as messages pass through the Internet Mail Service, it is necessary to enable the **Clients support S/MIME signatures** option; this is enabled by default.

Limits Tab

Figure 19 shows the **Limits** Tab of the **Mailbox Store Properties** page.

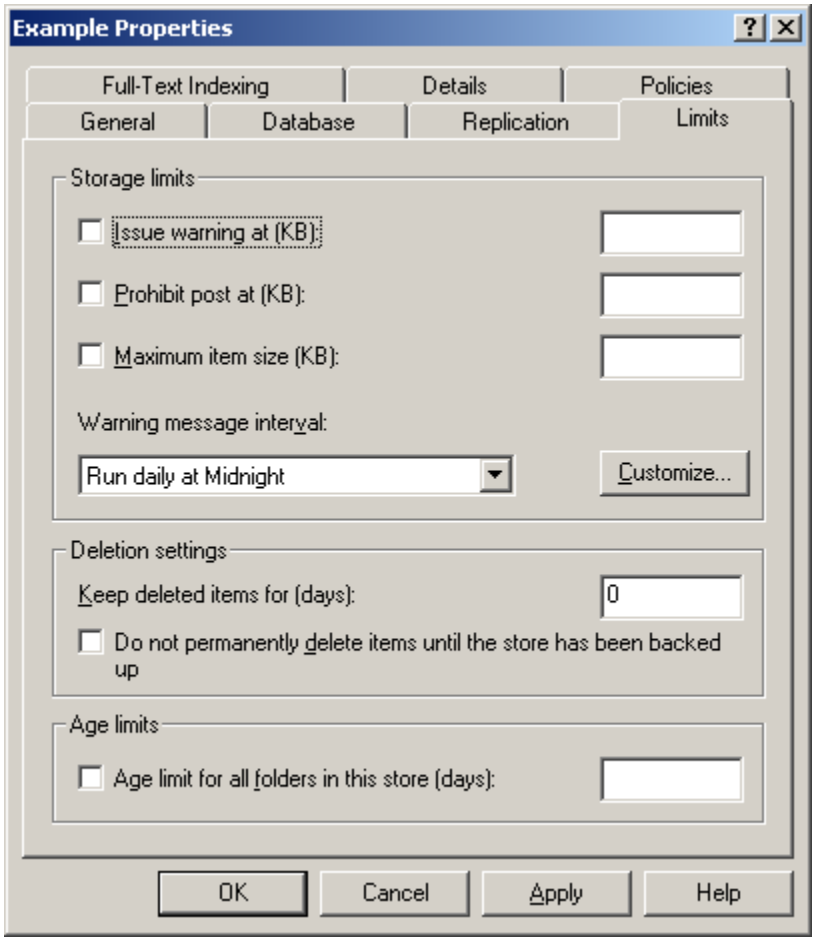

Figure 19. Limits Tab of Mailbox Store Properties Page

The limits defined on the **Limits** Tab apply to individual boxes. These limits can be used to issue warnings to users using excessive storage for messages and block sending and receiving for these accounts. The warning check interval can also be customized. Deleted messages and mailboxes can also be used and retained for varying periods. These limits are useful aids in mitigating and identifying denial of service attacks predicated upon depletion of storage space.

This property page also includes an option to retain deleted items for a given number of days or to retain deleted items until the store has been backed up. This feature relates to the ability of Outlook users connected via MAPI to recover items that have been deleted from the deleted items folder via the **Recover Deleted Items** option under the tool menu.

To maximize data recoverability, it is recommended to select the option to **Do not permanently delete items until the store has been backed up**.

Policies Tab

A *Mailbox Store Policy* is a set of properties, which can apply to a group of mailbox stores. This can be a useful tool for administering mailbox stores, as simply changing the policy will apply the changes to the associated group of mailbox stores. It is a useful single point of administration. Mailbox Store Polices are set under the **Administrative Groups/[administrative group name]/System Policies** container and will be discussed in more detail later in the chapter.

Logons Container

The Logons container is contained under the mailbox store. Contained within it is information about current logons to mail boxes within the store, information which could be useful in the investigation of security incidents. For each mailbox, the following default information is listed:

- **User Name** – The name (display name) for the user logged on to this mailbox.
- **Windows 2000 Account** – The Windows 2000 Account of the user currently logged on to this mailbox.
- **Logon Time** – The date and time the user logged on to Exchange 2000.
- **Last Access Time** – The last user to access the mailbox, as well as the date and time of the access.
- **Client Version** – The version of the client used to log on to this mailbox.

There are no security settings associated with the logons container; it simply serves as a convenient way for an administrator to note who is currently connected to the mailbox store.

There are a number of optional information items which can also be displayed.

Mailboxes Container

Similar to the Logons Container is the Mailboxes Container, which gives similar information related to each users mailbox. The following default information, important for security audits and incident investigation, is listed for each mailbox:

- **Mailbox** – Display name for the mailbox.
- **Last Logged On By** – The name of the user who last logged on to this mailbox.
- **Size (KB)** – The total amount of disk space that this mailbox occupies.
- **Total Items** – The total items stored in the mailbox.
- **Last Logon Time** – The last time a user logged on to this mailbox.
- **Last Logoff Time** – The last time a user logged off from this mailbox.

There are also a number of optional columns which can be displayed.

Mailbox Permissions

The majority of security related settings associated with mailboxes are not accessible via the *Exchange System Manager*. Instead, these settings are accessed through the *Active Directory User* and *Computers MMC* snap-in.

There are a number of permissions, which are important to security. These can all be accessed from the **Properties** pages for the user associated with the mailbox through the *Active Directory Users and Computers MMC* snap-in. Figure 20 shows the **Exchange Advanced** Tab of **Properties** for a particular user. This tab will not display unless the **Advanced** option under the **View** menu item is activated.

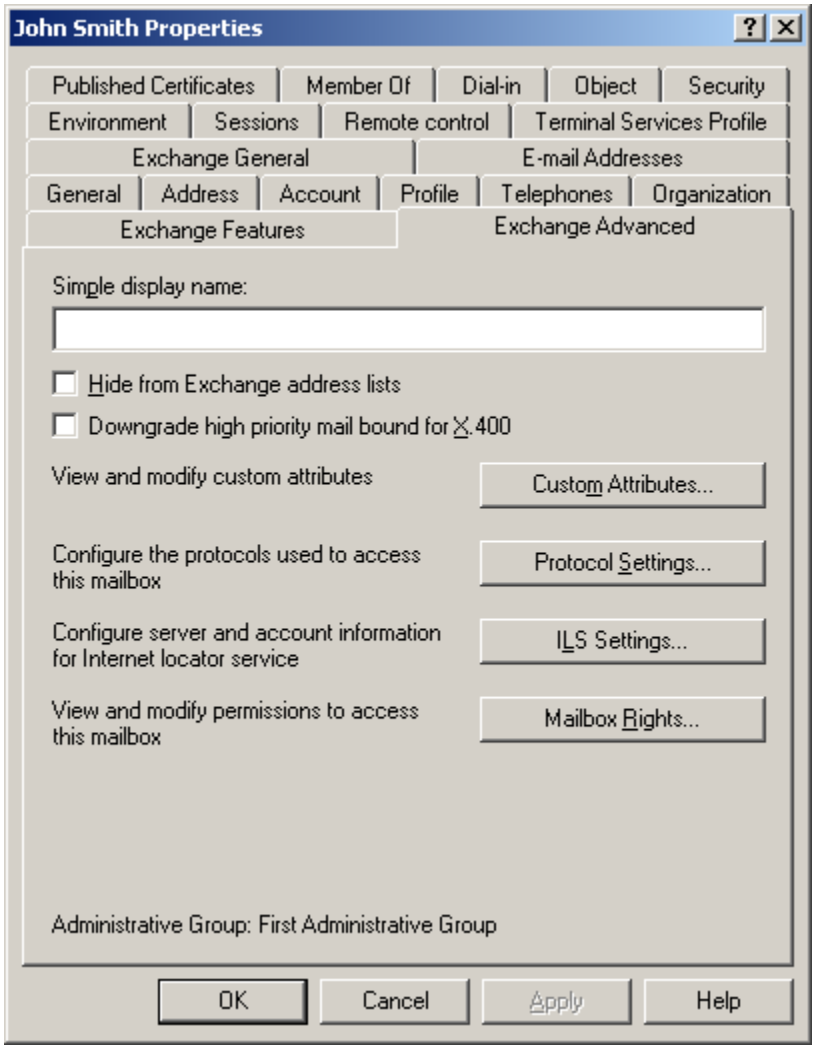

Figure 20. Advanced Tab of Mailbox Properties Page

By selecting the **Mailbox Rights** option on this page, the **Mailbox Right**s are displayed as shown in Figure 21.

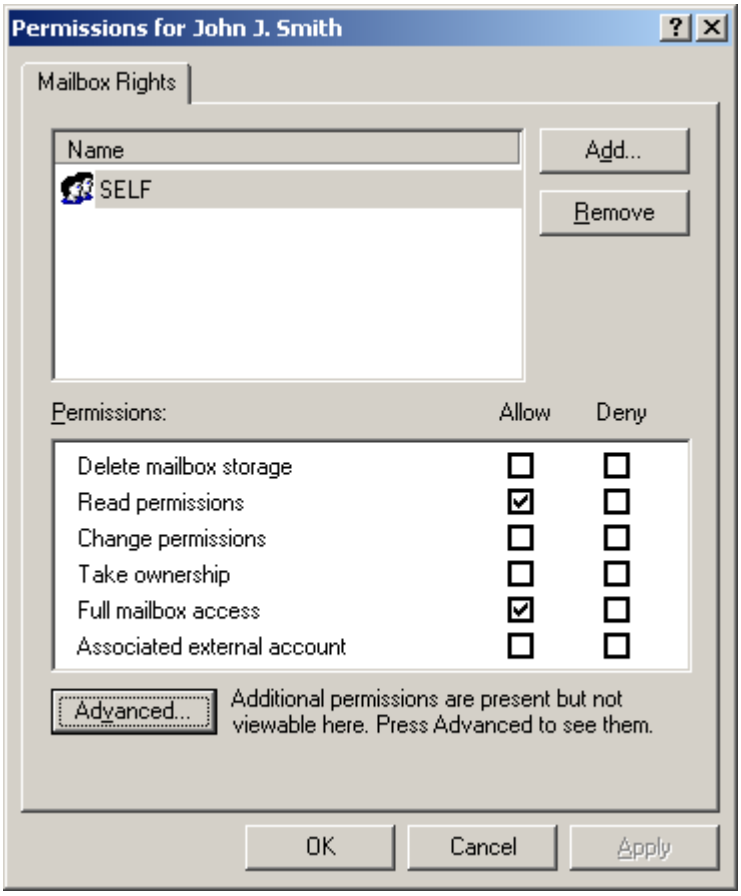

Figure 21. Mailbox Rights Page

Shown are the default rights, which a user has to his own mailbox. The different mailbox rights are as follows:

- **Delete Mailbox Storage** – If allowed, the user or group may delete the mailbox itself.
- **Read Permissions** – The user or group can read the permissions granted to the mailbox.
- **Change Permissions** – The user or group can change the permissions granted to the mailbox.
- **Take Ownership** – The user or group can take ownership of the mailbox.
- **Full Mailbox Access** – The user or group can access the mailbox and all of its contents, including the subfolders.
- **Associated External Account** – The account, which is a Windows 2000 server account outside of the Windows 2000 forest where the Exchange server resides, may access the mailbox.

Typically these settings do not require any manipulation on the part of the administrator; however, it is useful to point out these settings as they represent one way which the integrity of the Exchange environment could be compromised – a person with Windows

2000 administrative rights or Exchange administrator rights (obtained legitimately or covertly via a compromised account) can grant himself (or any other user) full mailbox access to another user's mailbox. This would compromise any hope of data confidentiality unless the Advanced Security options of Chapter 8 are invoked.

Send As, Receive As, and Send On Behalf of Permissions

Certain other mailbox permissions can also be manipulated via other tabs associated with the user properties page. Figure 22 shows the Windows 2000 permissions associated with a user under the **Security** tab:

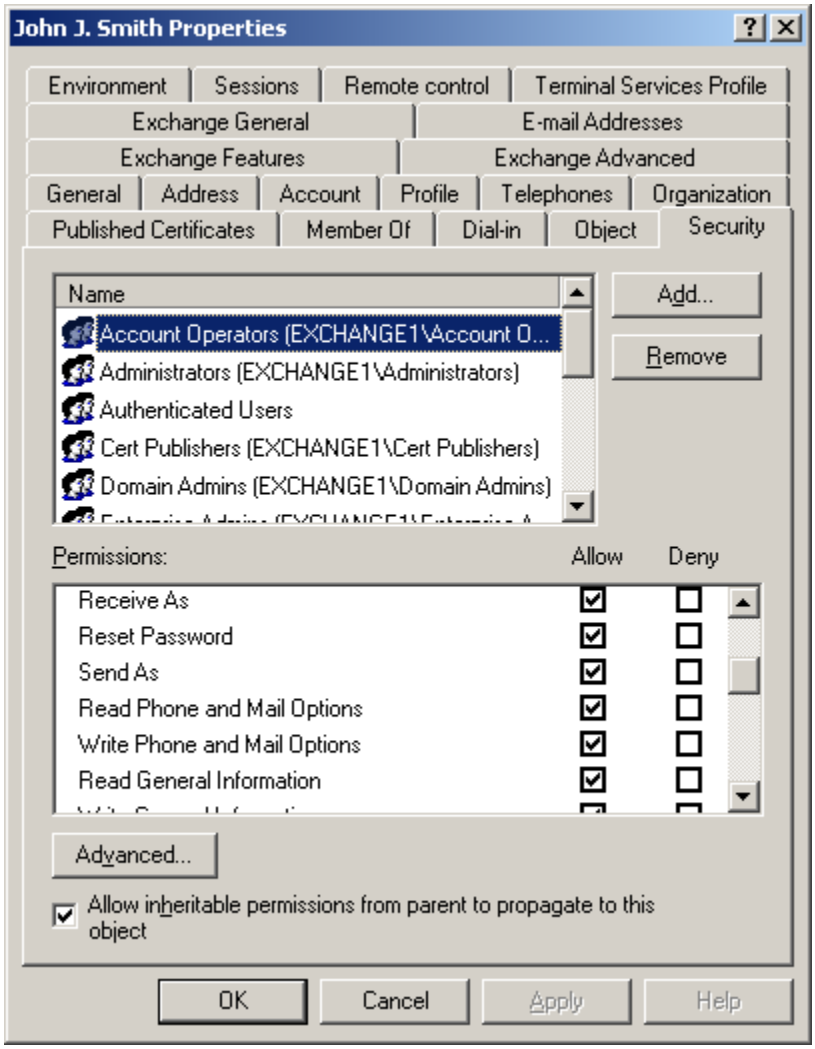

Figure 22. The Security Tab of the Properties Page of a User

The *SEND AS* permission allows a user or group to send messages from other mailboxes that will appear as if they came from the *SEND AS* mailbox. This right is used via the Outlook client mailbox using **View, From Field** option. *SEND AS* is a very powerful option and its use should be avoided. Note that *SEND AS* is one of the items

recommended for logging. Administrators should check the log for any unexpected occurrences of this event.

The *SEND ON BEHALF* permission is accessed from the **Exchange General** Tab of the *Permissions Pages* using the **Delivery Options**. When a message is sent by User1 using this permission, the FROM field of the message will state User1 *ON BEHALF OF* User2 so that the actual sender can be known. If both *SEND AS* and *SEND ON BEHALF* are both set, then *SEND AS* will prevail, as it is the stronger permission. Note that this permission is also set when a user is specified as a delegate in the **Delegates** Tab of the **Options** dialog box in Outlook 2002. This means that the user can have control over who is granted this right which can be which is noteworthy because, while the messages will be marked *sent on behalf of*, this is not apparent if the message is simply read from the preview pane. For this reason it was recommended earlier to log occurrences of messages send on behalf of another person so that any abuse of the privilege can be addressed.

Public Folder Store

A Public Folder Store is an Exchange database for storing public folders. A Public Folder Store also indexes public folder contents and assists in the replication of public folders to other Exchange servers. As implied by the name, public folders are intended to be access by multiple users but the administrator can limit access in various ways. A Public Folder Store must be associated with a Public Folder Tree. Upon installation, there is a default Public Folder Tree named Public Folders and a default Public Folder Store named with the name of the server. This pair, Public Folder Tree and Public Folder Store, are unique in that they are the only pair that is MAPI-enabled, or accessible via MAPI clients such as Outlook 2002. Other Public Folder Trees can be defined which can be accessed via other clients such as WebDav or NNTP clients.[10]

General, Limits, Policies Tabs and Logons Container

These properties page tabs have almost identical meanings to those given for Mailbox Stores (except they refer to Public Stores) so they will not be detailed here. The same discussion given previously applies here.

Public Folders

Public folders are created as part of public folder trees. The public folder is part of some public folder store for a particular Exchange server. An administrator can create public folders either in the Outlook 2002 client or within the System Manager. If a public folder is created as part of the default Public Folders tree, then the folder will automatically be MAPI accessible. If there are other public folder trees, then a public folder created underneath them can still be made MAPI accessible. To mail-enable a folder, select the folder in Exchange System, right click, and choose **All Tasks** and **Mail Enable**. When a user creates a public folder that user becomes the owner of that public folder. The Properties page of the folder must be accessed in either Outlook 2002 or the System Manager to perform management of that folder.

[10] Refer to Chapters 9 and 10 for more information on these topics.

Limits

The **Limits** tab gives options very similar to those for Public Folder Store and Mail Store. One different feature is that the option to inherit the retention parameters from the associated public folder store is given. The Limits tab defines messaging limits for the public folder. *Any setting made at the public folder level overrides the setting made for the public folder store*. You can define the following limits on this tab:

- **Storage Limits -** Indicates the amount of disk space, in kilobytes, that a folder can take up before a warning is issued to the folder's owner. This setting works like the setting at the public folder store level.

- **Deleted Item Retention -** Defines the number of days that deleted messages are retained in the folder before being permanently removed. This default defined for the public folder store can be used or overridden by a new setting.

- **Age Limits -** Specifies the maximum number of days that a message remains in this public folder before it expires. If not specified, the default set at the public folder store level applies.

The setting of appropriate limits, taking into account the amount of public storage available and the particular intended purpose of public storage, are important to mitigate the damage done by denial of service attacks.

Client Permissions

The **Permissions** tab allows the assignment of permissions to users on the current public folder. Each user can be assigned one of several roles, and each role has a set of permissions associated with it. The available permissions are as follows:

- **Create Items** - Allows the user to post items in the folder.

- **Read Items** - Allows the user to open any item in the folder.

- **Create Subfolders** - Allows the user to create subfolders within the folder.

- **Edit Items** - Specifies the items in the folder that the user can edit. The *None* option indicates that a user cannot edit items. The *Own* option indicates that the user can edit only items that he or she created. The *All* option indicates that a user can edit any item in the folder.

- **Folder Owner** - Grants the user all permissions in the folder, including the ability to assign permissions.

- **Folder Contact** - Specifies that the user is to receive copies of any status messages regarding the folder, including nondelivery reports.

- **Folder Visible** - Permits the user to see the folder in the public folder hierarchy.

- **Delete Items** - Specifies the items in the folder that the user can delete. The *None* option indicates that a user cannot delete items. The *Own* option indicates that the user can delete only items that he or she created. The *All* option indicates that a user can delete any item in the folder.

The following table shows the default permissions of the roles that can be assigned to users accessing the public folder. The standard default permissions for a particular role can be modified, as that role is assigned to a particular user.

Table 12. Administrative Roles

Role	Create	Read	Edit	Delete	Sub folders	Owner	Contact	Visible
Owner	Yes	Yes	All	All	Yes	Yes	Yes	Yes
Publishing Editor	Yes	Yes	All	All	Yes	No	No	Yes
Editor	Yes	Yes	All	All	No	No	No	Yes
Publishing Author	Yes	Yes	Own	Own	Yes	No	No	Yes
Author	Yes	Yes	Own	Own	No	No	No	Yes
Nonediting Author	Yes	Yes	None	Own	No	No	No	Yes
Reviewer	No	Yes	None	None	No	No	No	Yes
Contributor	Yes	No	None	None	No	No	No	Yes
None	No	No	None	None	No	No	No	Yes

There are some default group permission assignments made to a public folder. The creator of the folder is given the Owner role. Default is given the Author role. Default specifies the rights given to everyone who has an Exchange account, unless otherwise specified. Authors can create items in a folder and edit and delete only their own items. Anonymous is given the Contributor role. Contributors can only create items. These default permissions should be carefully considered, subject to the security policy of the organization, and further restricted if necessary.

The Exchange-specific permissions for the administration of a public folder are detailed in Chapter 3, Administrative Permissions. For a particular public folder, these are accessed from the **Administrative Rights** Option of the **Permissions** Tab of the **Properties** Pages accessed via **System Manager**. Note that the Client Permissions have to do with the content of the public folder, whereas the Administrative Rights have to do with manipulating the public folder permissions.

Public Folder Creation Rights Default

The default public folder permissions give the Everyone group the right to create top-level folders and the right to create public folders from the Outlook client. This right needs to be restricted to the maximum extent possible. A user who creates a public folder is the owner of that folder and, as the owner, can create custom forms which contain executable code. These custom forms are treated by Outlook as a trusted code base – *it bypasses the macro code detection mechanism discussed in Chapter 2 and therefore will execute without any opportunity to disable it.* This problem is exacerbated by the fact that the owner has complete control over the permissions associated with the folder and could extend ownership to any number of additional individuals. *Only trusted individuals who understand the implications and responsibilities associated with public folder creation should be given that privilege of creating them.* The following rights are required in order for a user to be able to create public folders: Create Top-Level Public Folders, Create Public Folders, and Create Named Properties.

System Policies

A policy is a set of configuration parameters that applies to one or more Exchange objects in the same class. For example, a policy can be created that affects certain settings on some or all of the Exchange servers in an organization. If a setting has to be changed, then simply modifying the policy will effect the change on each server to which the policy has been applied. System Policies apply to a server, a mailbox store, or a public folder store. These policies appear in the Policies container under the administrative group responsible for administering the policy. Creating a policy involves navigating to the appropriate Policies container, right-clicking the container, and then selecting the kind of policy to be created. Policy containers in administrative groups give you the option of creating any type of system policy: a server policy, a mailbox store policy, or a public folder store policy.

When working with system policies, it is important to create the policy object in the administrative group that will be responsible for administering the policy. Failure to do so may cause an inadvertent group to have administrative control over the policies. The following discussion describes how to create each type of system policy. A server policy enforces message tracking and log file maintenance settings. It is not used to enforce security or other settings on the servers in the administrative group. To create a server policy, right-click the **System Policies** container, point to **New**, and then choose **Server Policy**.

Public folder store policies include a number of configuration options, including maintenance schedules, limits, and full-text indexing. They are applied on a per-store basis across public folder tree boundaries. The procedure for creating a public folder store policy is similar to the one for creating a server policy.

A mailbox store policy allows the configuration of a number of settings for mailboxes, including the default public folder store, the maintenance schedule, a message archiving recipient that receives copies of all e-mails, and full-text indexing.

The use of system policies is an important administrative tool that can be used to enforce secure setting for certain system objects.

Important Security Points

- Design Administrative Groups to reflect the organizational and geographic structure of the Exchange Organization. Choose an administrative model best suited to your organization.
- Assign rights to the administrators according to the principle of Least Privilege.
- Enable diagnostic logging for the various elements identified above.
- Monitor CPU utilization and disk capacity for those disk volumes containing user data to help prevent resource depletion and set a corresponding alert.
- Enable the option to Zero Out Deleted Database Pages on the Storage Group property page if there is high concern about inadvertent information disclosure in deleted messages.
- Store transaction log files on a separate physical drive.
- Do not enable circular logging.

- Do not disable the Clients Support S/MIME Signatures check box if the Mailbox Store has to support Secure/Multipurpose Internet Mail Extensions (S/MIME).
- Use Message Tracking, Diagnostic Logging and the Logons and Mailbox Containers to assist in security incident detection and handling.
- Apply Limits to Public Folder Stores and Mailbox Stores to mitigate Denial of Service attacks.
- Select the option to not permanently delete items until the store has been backed up in order to maximize the ability to recover deleted data.
- Restrict the right to create public folders to the maximum extent possible.
- Examine and restrict the default permissions on Public Folders to be consistent with the security policy of the organization.
- Use System Policies to enforce security settings for certain system objects and prevent these settings from being changed by unauthorized users.

Chapter

5

Multi-Server Configurations

This chapter explains message transfer and routing between servers. It also covers routing groups and connectors and their associated security.

Routing Groups – A Brief Overview

A *Routing Group* is a collection of servers that have permanent, high bandwidth connectivity. During Exchange 2000 installation, a default routing group, which includes the server as a member, is created.[11] When an Exchange Server is added to a routing group, the connection between the new server and other servers in the group are automatically configured.

Connectors are used to connect routing groups. Connectors must be manually configured. The major connectors in Exchange 2000 are:

- **Routing Group Connector**
- **SMTP Connector**
- **X.400 Connector**

There are some common attributes that are specified in all connectors. One or more designated bridgehead servers must be specified. Bridgehead servers can be local or remote. A local bridgehead server is the originator of messages. A remote bridgehead server is a recipient of messages. All servers in the group can originate messages, but the local bridgehead server is the relay point for transferring messages over the link. Similarly, the remote bridgehead server is the relay point for receiving messages for its group.

Routing Group Connector

Routing group connectors are used to connect routing groups to each other. The default protocol in routing group connectors is SMTP. If the organization is operating in mixed mode, however, RPC is used to communicate with Exchange 5.X servers. More than one server can be designated as local bridgehead servers, and this is a good policy for availability reasons. Multiple remote bridgehead servers can be specified, and these will be tried in a priority order when delivering messages. The connector is one way, outgoing. There are no real security choices to configure, so the default security

[11] If co-existence with Exchange 5.0 and 5.5 is required, that is, the organization runs in mixed mode, a pre-Exchange 2000 site becomes part of the default administrative group and the servers become part of the default routing group. In this case, all servers in a routing group must come from the same administrative group so they can never be moved to a new routing group.

configuration choices are obtained. Configuration changes can be made by right-clicking on the Connectors container located under the Routing Group Container. Since there is no encryption used with the *Routing Group Connector*, *IPSec* or an *SMTP connector* should be used if encryption is desired.

SMTP Connector

The *SMTP connector* can be used to connect two routing groups or to connect a routing group to the Internet or a non-Exchange server. The *SMTP connector* can also be used to connect two different Exchange Organizations. The SMTP connector is also uni-directional like the *Routing Group connector*. Multiple local bridgehead servers can be specified, but remote bridgehead servers are handled differently than in the routing group connector. Either a single smart host—an SMTP server that functions as a relay point—is specified, or DNS MX records are used to find mail servers in the remote routing group.

The *SMTP Connector* has a number of security options as shown in Figure 23.

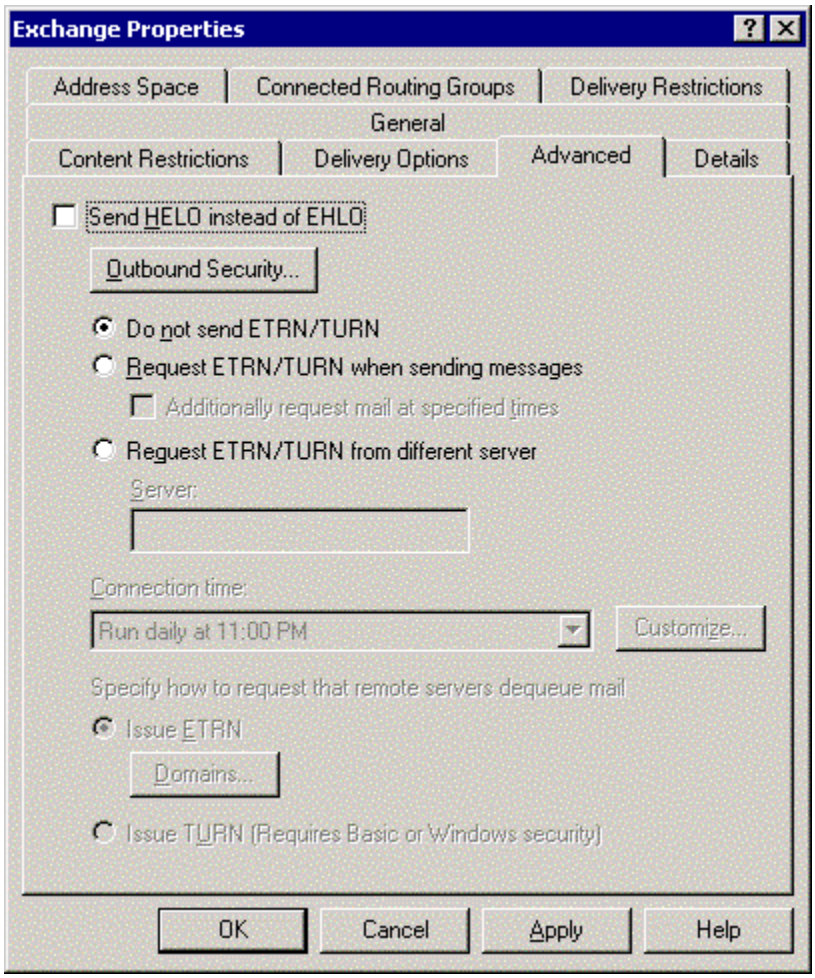

Figure 23. SMTP Connector Advanced Tab under Properties Page

These can be accessed with the **Advanced** Tab under the SMTP connector's property page.

The **Outbound Security** button gives access to encryption and authentication options. By default, remote connections are not authenticated. There are three authentication options that can be configured.

- **Anonymous access** – This option gives no authentication.
- **Basic authentication** – This option passes name and password in the clear.
- **Integrated Windows Authentication** – This option provides authentication based on a Windows 2000 account.

There is also a **TLS Encryption** box, which can be checked. This will encrypt message traffic flowing through the connector. TLS (Transport Layer Security) is a later version of SSL that was designed to be an Internet standard. TLS encryption can be combined with the Basic or Integrated Windows Authentication. The use of *TLS encryption with Basic authentication* is necessary to protect the passwords in transit.

Given that routing groups consist entirely of Exchange Servers running in Windows environments, the use of integrated Windows authentication is recommended as the authentication mechanism. If traffic is sensitive, TLS encryption should be used.

X.400 Connector

X.400 is a messaging standard that is used by many messaging systems. You can use the *X.400 connector* to connect Exchange 2000 Server to any foreign messaging system that supports X.400 standard. The *X.400 connector* has a single local bridgehead server and, if connecting to a routing group, a single remote bridgehead server. Because of this, multiple connectors have to be configured for availability or other multi-link purposes. In order to configure an *X.400 connector,* a *Service Transport Stack* has to be configured. There are two choices:

- **X.25** – Dial-up and direct communication in compliance with Open Systems Interconnection (OSI) X.25 standard.
- **TCP/IP** - Exchange 2000 Server uses Windows 2000 TCP/IP services.

X.400 systems have the ability to specify passwords for authentication. This is essentially basic authentication with passwords transmitted in the clear. These passwords are specified as part of the configuration of the connector.

X.400 connector authentication may either use no passwords or passwords transmitted in the clear, both of which pose immediate security risks. Evaluate where *X.400 connectors* need to be used and isolate their use to avoid security issues.

Multiple Servers Within a Routing Group

Each routing group in an Exchange 2000 organization consists of a collection of well-connected Exchange 2000 servers for which full-time, full connection access is guaranteed. Connectivity among servers in a routing group is based entirely on Simple Mail Transfer Protocol (SMTP)[12].

[12] However, when Exchange 5.0 or 5.5 servers are present in a mixed-mode organization, communication with these servers will be with Remote Procedure Calls (RPC).

Unlike Exchange 5.5, where intra-site and inter-site RPC communications are encrypted, SMTP communications in Exchange 2000 are not encrypted. Each server does, however, use SMTP authentication with Kerberos. There are two encryption options available in this case, neither of which is used by default. Internet Protocol Security (IPSec) is available in Windows 2000 as a standard service, and Transport Layer Security (TLS) encryption is a standard part of the SMTP service.[13]

Common Connector Administrative Restrictions

There are some functions that are common to all connectors that can be used to enhance the security of the connection. On the Properties Page of the Connector under the **Delivery Restrictions** Tab, the access can be set to be either accept or deny access to specific users, contacts, and groups for this connector. Under the **Content Restrictions** Tab on the Properties Page, the **Only Messages less than (KB) box** can be checked to restrict the size of messages that can pass through this connector. This is shown in Figure 24.

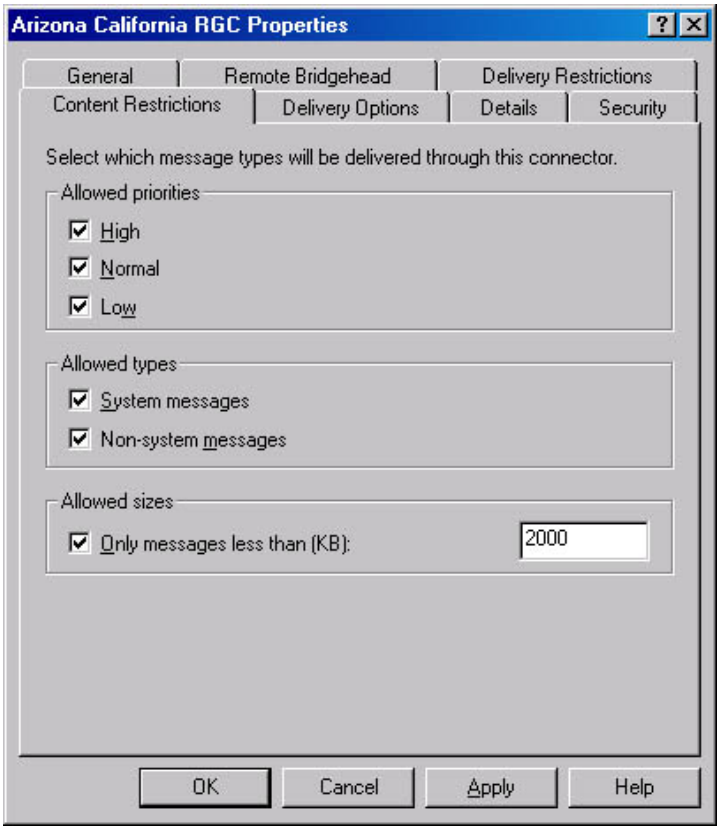

Figure 24. Content Restrictions Tab of Properties Page

Note that some of these restrictions will not take effect until the following registry key is set:

[13] For information concerning IPSec, please reference the OS guide entitled, *Guide To Securing Microsoft Windows 2000 IPSec*. For information regarding the use of TLS with SMTP, refer to Chapter 6, SMTP Virtual Server.

HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/Resvc/Parameters/

Add the following value to this key:

Value Name: CheckConnectorRestrictions
Data Type: REG_DWORD
Value: 1

Reference Microsoft Knowledge Base article Q277872 for more details which is available at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q277872

Other Connectors

There are a number of other connectors that can be used to connect to "foreign" mail systems. There are connectors for Lotus Notes, Lotus cc:Mail, Novell GroupWise and Microsoft Mail. These are beyond the scope of this document. These other connectors and foreign mail systems should be reviewed for security considerations prior to use.

Important Security Points

- When using *Routing* or *SMTP Connectors,* multiple bridgehead servers should be specified for availability.
- When using an *X.400 Connector,* configure multiple connectors for availability.
- When connecting routing groups, use *IPSec* or the *SMTP connector* with encryption in place of the *Routing Group connector* if traffic is vulnerable to interception.
- Given that routing groups consist entirely of Exchange Servers running in Windows environments, the use of *Integrated Windows Authentication* is recommended as the authentication mechanism when using the SMTP connector.
- For connections within a Routing Group, *IPSec* or *SMTP TLS encryption* should be used if traffic is vulnerable to interception.
- On the Properties Page for each connector type, **Delivery Restrictions** and **Content Restrictions** can be set to deny access to specific users, contacts, and groups and restrict maximum message size to mitigate denial of service attacks. Note that a registry key, referenced above, must be set before some of these restrictions are effective.
- Review all other implemented connectors and foreign mail systems for security considerations.

This Page Intentionally Left Blank

Chapter 6

SMTP Virtual Server

This chapter is concerned with the *SMTP Virtual Server*. In Exchange 2000 Server, SMTP is the native mail protocol for mail submission and mail transport. The *SMTP Virtual Server* replaces the *Internet Mail Connector (IMC)* and *Internet Mail Service* (IMS) in previous versions of Exchange Server. In Exchange 2000, multiple virtual servers can be configured on the same physical server to provide different configurations for different messaging services. A default SMTP server is defined when Exchange 2000 is installed, but more than one SMTP virtual server can be defined for hosting different domains, for different authentication requirements, or simply for availability. Each virtual server has its own IP address, port number, and authentication settings.

Security Features For Incoming Connections

The security of incoming connections can be controlled in four ways:

- Access can be granted or denied by IP addresses or Internet domain names.
- Authentication can be configured for incoming connections.
- Secure incoming connections can be specified.
- Restrictions can be set on which computers can relay messages through this server.

Start the **System Manager**, locate the server desired, expand the **Protocols** container, and choose **SMTP** to access these features. Right clicking on the SMTP virtual server gives access to the properties that control these options.

Access Control

By default, virtual servers are accessible to all IP addresses. Control of the IP addresses that have access to a server can be by domain, subnet, or IP address. This feature can be found by choosing the **Access** tab and then clicking on the connection button. The **Access** Tab is shown in Figure 25.

Granting access gives a computer access to the virtual server, but users may still have to authenticate themselves to submit or retrieve mail if authentication is required. Denying access, however, would not allow users from that computer to submit or retrieve mail regardless of authentication. Access can be allowed or denied for a specific IP address or list of IP Addresses. Access can be allowed or

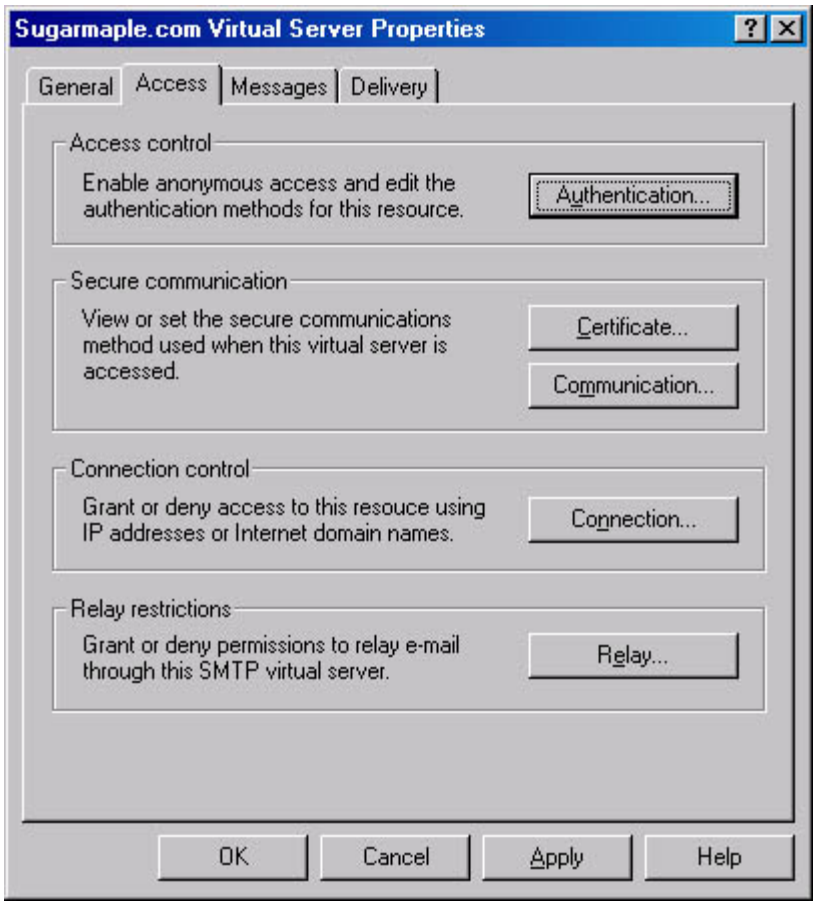

Figure 25. Properties Page Access Tab

denied by subnet address. Access can be allowed or denied by a fully qualified domain name. Identify all the computers, if possible, that require connectivity, and explicitly allow access to those computers by listing them by specific IP address or subnet mask.

Authentication

The **Authentication** button gives access to the authentication page. There are three authentication options available. All three authentication options are selected by default. These three options are:

- **Anonymous** – Anonymous Authentication gives access to computers, either servers or clients, which do not have to provide a username or password.

- **Basic** – Basic Authentication allows access to this virtual server by sending in a password in the clear. There is a TLS Encryption option, which encrypts names, passwords, and message content. A key certificate must be generated for the server to use TLS.[14] When basic authentication is specified, a default domain must be given for the authentication which indicates to the server which domain to use in verifying the user supplied password.

[14] Refer to the NSA *Guide to the Secure Configuration and Administration of Microsoft Windows 2000 Certificate Services* found at http://www.nsa.gov.

- **Integrated Windows Authentication** – This is the standard Microsoft Windows authentication based on Windows 2000 account names and passwords. Passwords are not sent in the clear.

Since most SMTP hosts use **Anonymous Authentication** by default, this option should be enabled if access by any host on the Internet is required. On the other hand, if this virtual server will operate in a tightly controlled environment with a small number of known hosts, then **Basic** (with TLS encryption) or **Integrated Windows Authentication** should be selected.

Secure Connections

If the **TLS Encryption** box has been selected, a certificate must be installed which the server will use in establishing TLS sessions. Clicking on the **Certificate** button will activate the *Certificate Wizard*. On the **Access** page, the **Communications** button must be selected and the **Require Secure Channel** option must be selected in the **Security dialog** box. There is an additional option in the Security dialog box to require 128 bit encryption (recommended).

Relay Restrictions

After selecting the **Access** tab and clicking on **Relay**, the **Relay Restrictions** dialog box is activated. Restriction on which computers can relay messages through the virtual server can be controlled here. As in the Access Control section, the restriction here can be by single or a list of computers. Control can also be by subnet or domain. Access can be either granted or denied. To avoid being a conduit for unknown server mail activity, this privilege should be specifically granted, if practical, only to known computers that have a real need for this function.

Global Filters

Restrictions can also be applied to incoming e-mail addresses under the global settings for the organization. Select the **Global Settings** container under the Organization and then select the **Message Delivery** container to set these. After setting the filter under the global settings, filtering has to be enabled in the specific virtual server before it is applied. This can be accomplished on the **SMTP Virtual Server Properties** Page. Select the **General** Tab and then click on the **Advanced** Box. The IP Address to be filtered must be selected, and then particular individual filters can be activated.

Security Features For Outbound Connections

The **Outbound Security** button on the **Properties** page is accessed from the **Delivery** Tab. This button controls the **Outbound Connections** dialog box. These options control the connections that are initiated by the server with other servers. The same authentication options detailed above for inbound connections also appear here with some differences. Here, further details on the server's authentication information must be supplied for the *Basic* and *Integrated Windows* options. In addition, only one option can be chosen as opposed to inbound security, where multiple options may be selected. For *Basic*, a Username and Password must be supplied for this server. For the *Integrated Windows* option, an account and password must be supplied for the Windows Security support. Note that if

authentication is desired for some specific servers but not for others, SMTP connectors can be setup with authentication for those servers.

Message Restrictions

There are a number of message restriction options. These can be found under the **Messages** tab in the **SMTP Virtual Server Properties** pages. The **Messages** tab is shown in Figure 26.

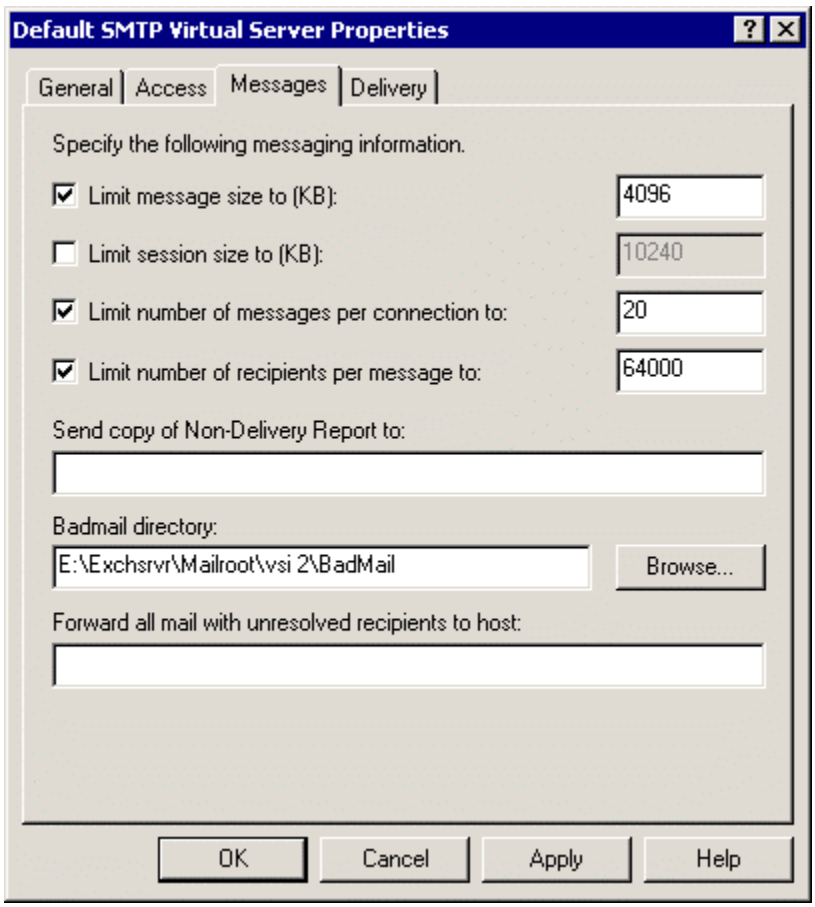

Figure 26. Messages Tab

Of these, one is noteworthy from a security perspective. This option to **Limit Message Size to (KB)** can be used to limit message sizes accepted from other SMTP hosts. When the limit is exceeded, the virtual server does not write any data beyond the set limit. This prevents large messages from filling up the disk space on the server and therefore helps to constrain denial of service attacks. The default value of 4096KB may not be adequate in today's environment where large attachments may be the norm, but in order to constrain denial of service attacks this limit should be examined and set to a reasonable value.

Global Message Restrictions

There are a number of settings in the **Global Settings** for the organization related to SMTP autoresponses. To access them, open the **Properties** page for the **Global Settings/Internet Message Formats/Default** object and select the **Advanced** tab. These autoresponse function boxes include:

- **Allow Out of Office Responses**
- **Allow Automatic Replies**
- **Allow Automatic Forward**
- **Allow Delivery Reports**
- **Allow Non-Delivery Reports**
- **Preserve Sender's Display Name On Message**

If the *SMTP Virtual Server* is being used to connect to a less trusted network, all of these should be turned off since they may provide sensitive information to an attacker.

The first three options are disabled by default.

SMTP Protocol Logging

There are a number of different logging facilities in Exchange 2000 Server. These include *Message Tracking*, *Diagnostics logging*, and *SMTP Protocol logging*. *Message Tracking* can be used to record a history of messages processed by the Exchange Server. These tracked messages can then be searched using the message tracking facility, as discussed in Chapter 4. Diagnostics logging writes records to the application log on a service basis and was discussed in Chapter 4. Protocol logging, used in conjunction with Diagnostics logging, can be used to investigate common security events such as authentication failures. *SMTP Protocol logging* is enabled on a virtual server basis. Four different format options exist for SMTP Protocol logging. These formats include:

- **W3C Extended Log File Format** – ASCII text with each field space-delimited with a new line for each entry**.**
- **Microsoft IIS Log File Format –** IIS log file format in ASCII with each field tab-delimited and each entry on a new line.
- **NCSA Common Log File Format** – ASCII text in NCSA log file format with fields space-delimited and each entry on a new line.
- **ODBC Logging –** ODBC (Open Database Connectivity) compliant with each entry as a record.

W3C Extended Log File format (the default) or **ODBC Logging** is the preferred choice. The administrator has the option of selecting the information that goes into the log records.

Table 13 shows these options.

Table 13. Log File Format Options

Property Name	Log Field	Description
Date	Date	Connection date.
Time	Time	Connection time.
Client IP Address	c-ip	IP address of client making the request.
User Name	cs-username	Account name of an authenticated user.
Service Name	s-sitename	Name of the service processing the command.
Server Name	s-computername	Server on which the log entry was generated.
Server Port	s-port	Server Port
Server IP Address	s-ip	IP address of the server on which the log entry was generated.
Method	cs-method	Protocol command sent by the client
URI Stem	cs-uri-stem	URI Stem
URI Query	cs-uri-query	URI Query
Protocol Status	sc-status	Protocol reply code.
Win32 Status	sc-win32-status	Microsoft Windows 2000 status or error.
Bytes Sent	sc-bytes	Bytes sent by the server.
Bytes Received	cs-bytes	Bytes received by the server.
Time Taken	time-taken	Length of time the action took in milliseconds
Protocol Version	cs-version	Protocol Version
Host	cs-host	Host
User Agent	cs(User Agent)	User Agent
Cookie	cs(Cookie)	Cookie
Referer	cs(Referer)	Referer

For tracking typical security problems, log at least *date, time, client IP address, user name,* and *method*. To access these settings, open the **Property** page for the *SMTP Virtual Server* and select the **General** Tab.

SMTP Banner

By default, the SMTP service will display a banner identifying the SMTP service as being based upon the Microsoft mail service. A potential hacker can get at this information by simply creating a telnet connection to the SMTP port. Since this

presents a leakage of information that could give an attacker an advantage, it is generally recommended to modify this banner. This is accomplished via a change to the IIS Metabase using a tool such as Microsoft's MetaEdit. Complete details are available in Microsoft Knowledge Base article Q281224 available at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q281224.

Figure 27 and Figure 28 illustrate the banner before and after it was modified on a test installation.

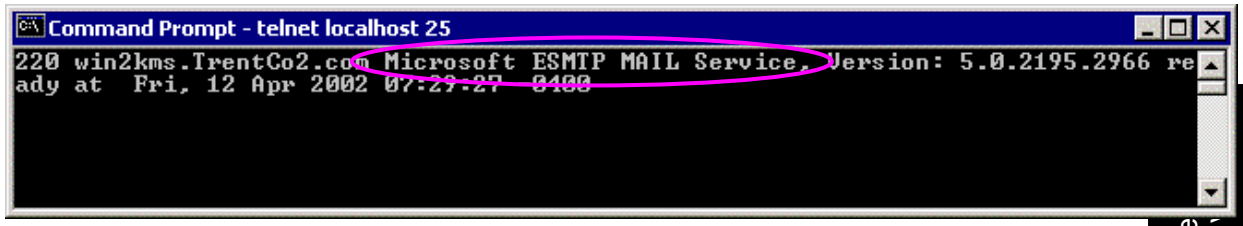

Figure 27. SMTP Default Banner

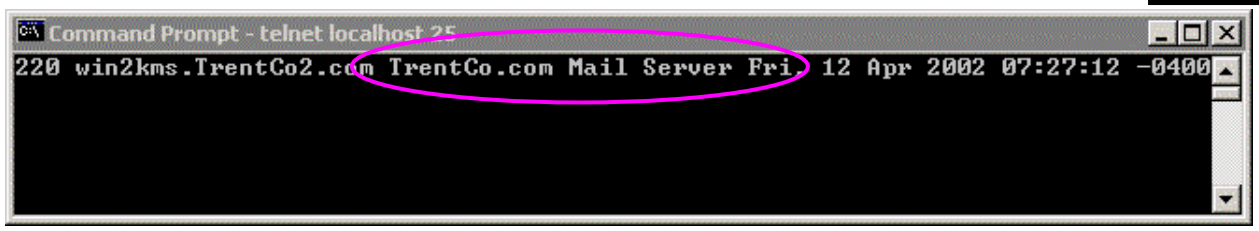

Figure 28. SMTP Banner After Modification

Relationship Between Virtual Machines Vs. Connectors

Now that the *SMTP Connectors* (in Chapter 5) and *SMTP Virtual Servers* (Chapter 6) have been covered, it is important to discuss the interaction between the two. SMTP Virtual Servers are the foundation of *SMTP Connectors* – note that the **General** tab of the SMTP connector properties page allows one to specify the applicable virtual server. The SMTP connector enhances the features offered by the SMTP virtual server by offering additional security and connectivity options. SMTP connectors are most commonly used to support customized connectivity between a SMTP Virtual Host and specific other SMTP hosts. The most notable of these enhanced features include:

- **Placing restrictions on which users can send Internet-bound messages**. When the connector is used to support connectivity to the Internet (or any other less trusted network), it may be desirable, dependent on the local security policy of the organization, to limit who can send e-mail to that network. To set these restrictions, navigate to the **Connectors** container, open the properties page for the connector, and select the **Delivery Restrictions** tab. Note that once again the **CheckConnectorRestrictions** registry key must be set as detailed in chapter five.
- **Setting additional limits on the types and sizes of messages that can be sent via the SMTP Virtual Server**. These settings are accessed via the **Content Restrictions** tab. Most interesting from a security perspective is the ability to disable the ability of system messages to flow through the

connector. If the connector is being used for connecting Routing Groups, then this should be enabled; otherwise, disable it.

- **Controlling the flow of messages from an ISP or Smart Host using ETRN/TURN**. ETRN and TURN are two SMTP commands that control the flow of messages from an SMTP host to the other end of a part time connection. For example, consider the case where an SMTP connector is being used as an organization's conduit for Internet mail messages which are sent via an Internet Service Provided (ISP). The connector can send its outgoing messages and then issue the ETRN or TURN command to instruct the ISP's mail server to reciprocate and send any messages it has in its queue that are addressed to the organization. The roles are *turned* – first the organization's SMTP connector is in send mode, then the ETRN or TURN command is sent and the roles are reversed.

These commands should be disabled from the Advanced tab of the connector if they are not needed. If they are required, keep in mind the distinction between the two commands. The TURN command requires basic or Integrated Windows security (set via the Outbound Security button). Both options have shortfalls. Basic security results in passwords being sent essentially in the clear unless TLS is also utilized and Integrated Windows security only works in homogenous Windows networks. The ETRN command does not use any form of password-based authentication. Instead, it requires the host issuing the ETRN command to provide a fully qualified domain name to the host that is expected to respond. That host then establishes a new connection using that fully qualified domain name. This provides a level of protection that mail is being delivered to the proper mail server, but it is only as reliable as DNS.

Alternately, the SMTP connector can be set up to wait for another SMTP host to contact it to pick up messages ready for delivery. In this case, the other host issues the ETRN/TURN command. To set this up to use TURN, one must specify the account that will be used for authentication. This is accomplished via the **Delivery Option** tab.

If ETRN/TURN support is required, the use of TURN with *basic authentication* plus TLS is recommended instead of ETRN.

Important Security Points

- Since most SMTP hosts use *Anonymous Authentication* by default, this option should be enabled if access by any host on the Internet is required. On the other hand, if the virtual server will operate in a tightly controlled environment with a small number of known hosts, then *Basic* (with TLS encryption) or *Integrated Windows Authentication* should be selected.
- Use Integrated Windows Authentication or TLS encryption (128 bit) in conjunction with Basic Authentication whenever possible.
- Use message size limits to constrain denial of service attacks.
- Disable all autoresponse options.
- Enable protocol logging to help in investigating security relevant events such as authentication failures. *Date, Time, Client IP address, User name,* and *Method* should be logged at a minimum.
- Modify the SMTP banner so that it does not so readily indicate the type of SMTP server being run.

- *If practical*, identify all the computers that require connectivity and explicitly allow access to just those computers by listing them by specific IP address or subnet mask.
- If ETRN/TURN support is required, the use of TURN with *basic authentication* plus TLS is recommended instead of ETRN.

This Page Intentionally Left Blank

Chapter 7

HTTP Access

Exchange offers a feature that allows users to connect to their mailboxes or public folders via the web using the Hypertext Transfer Protocol (HTTP). This feature is called *Outlook Web Access (OWA)*. Exchange Server 2000 comes with Outlook Web Access installed by default. Any web browser can be used to view mail, but Microsoft Internet Explorer offers the most options.

Since OWA utilizes the HTTP protocol it should come as no surprise that IIS plays an important role. When Exchange 2000 is installed it creates the necessary entries under the default web site to provide for OWA functionality. Some of the administrative functions related to OWA are accessible via both the IIS Internet Services Manager and the Exchange System Manager. Where possible it is recommended to use the Exchange System Manager for manipulating these settings. The System Manager stores its configuration settings within the Active Directory, but it will replicate OWA settings to the IIS Metabase as necessary. If one was to administer OWA setting via the Internet Services Manager, it could create a situation where changes could be overwritten by the System Manager at a later time.

Security Concerns With OWA

There are two security considerations associated with the use of OWA. First is the selection of the appropriate authentication mechanism. Second, the advanced security features do not work from within OWA; other techniques must be used to ensure data confidentiality.

Authentication

The authentication method selection is controlled from the System Manager. Navigate to the **server container/Protocols/HTTP** and expand the **Exchange Virtual Server** container. The authentication method should be set for the *Exchange* and *public* folder within the Exchange Virtual Server container. From the container properties, select the **Access** tab, and then click **Authentication**. The options available are:

- **Basic Authentication** – A browser independent clear-text user name and password authentication method.
- **Integrated Windows Authentication** – An Internet Explorer (IE) specific authentication method that leverages the native Windows authentication, such as NTLM or Kerberos.
- **Anonymous Access** – Allows unauthenticated access.

Figure 29 illustrates the authentication methods dialog box.

Figure 29. HTTP Access - Authentication Options

The preferred method of authentication is Integrated Windows Authentication. However, if browsers other than Internet Explorer are used, basic authentication in conjunction with Secure Socket Layer (SSL) should be utilized.

Data Confidentiality

OWA does not support the use of S/MIME and, in fact, does not support any means of reader-to-writer security. It is possible, however, to protect messages in transit between the web server and the browser using SSL. Using SSL also protects the authentication name/password when using basic authentication, offering a protected means of authentication that is not limited to Internet Explorer. The downside of using SSL is the overhead required to create an SSL session is large. Since there is such a big overhead associated with SSL, its usage will reduce the performance of the system unless used in conjunction with hardware accelerators. Also keep in mind that SSL only protects the messages in transit but does nothing to protect the message in storage.

The SSL settings are not exposed via the System Manager and therefore must be enabled from the Internet Services Manager. For more information, refer to the NSA guide "Guide to the Secure configuration and Administration of Microsoft Internet Information Services 5.0" available at http://www.nsa.gov.

Important Security Points

- Use Integrated Windows or Basic authentication with SSL to authenticate users.
- Use SSL to protect e-mail messages in transit between the web browser and server.

This Page Intentionally Left Blank

Chapter 8

Certificates and Advanced Security

One of the methods that Exchange offers for secure communication is *Advanced Security*. *Advanced Security* provides writer-to-reader security – messages are protected while in transit as well as when they are in storage on the Exchange Server or local file. *Advanced Security* provides security through the use of public and private key pairs in conjunction with a symmetrical algorithm such as DES. The public key is associated with a user through a certificate. Certificates are stored in the *Active Directory* for access by users within the Exchange environment. *Advanced Security* provides authentication, e-mail message integrity, and the ability to encrypt and decrypt e-mail messages.

There are two ways that a user can obtain these credentials in the Exchange environment. One method is to obtain these credentials from a commercial provider. The other method is through the *Advanced Security* features of the Exchange server. This chapter focuses on obtaining credentials through the Exchange Server. When the Exchange Server distributes credentials to the user, these credentials can be specified to be X.509 v3 compatible; this allows users to send messages to other users via the S/MIME standard. This chapter assumes that the Outlook client is connecting to the Exchange Server via MAPI (as opposed to IMAP4 or POP3). *The user is only given the option of obtaining credentials from the Advanced Security feature when connecting via MAPI.*

Advanced Security uses the *Key Management Service* (KMS) to manage keys. *KMS* is not installed by default with Exchange. *Certificate Services* must be installed and *Exchange Certificate Templates* must be setup in the Exchange organization before *KMS* can be installed. For more information on securely configuring *Certificate Services,* see the *Guide to the Secure Configuration and Administration of Microsoft Windows 2000 Certificate Services* which is available at http://www.nsa.gov. To set up Exchange *Certificate Templates* on the Domain Controller*:*

- **Start menu->Programs->Administrative Tools->Certification Authority**
- In the console tree, double click the name of the **Certificate Authority** (CA).
- Right click **Policy Settings** and select **New** then select **Certificate to Issue**.
- In the **Select Certificate Template** box that pops up, hold down CTRL and click the following:
  - **Enrollment Agent (computer)**
  - **Exchange User**
  - **Exchange Signature Only**

Figure 30 shows the **Certificate Template** dialog box that appears when selecting the appropriate certificate templates.

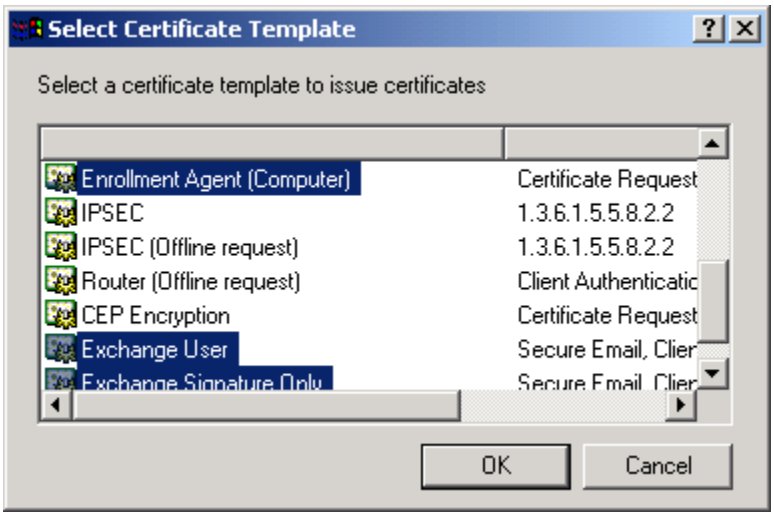

Figure 30. Certificate Templates

Now add the KMS component to Exchange from the original Exchange installation media. During installation the KMS service startup password is generated. There are two password options: enter the password manually or retrieve the password from a disk. The recommended option is to retrieve the password from a disk. The password should be stored on a floppy disk and kept in a safe place. This floppy disk will be needed every time the KMS service is started. Figure 31 shows the KMS password options.

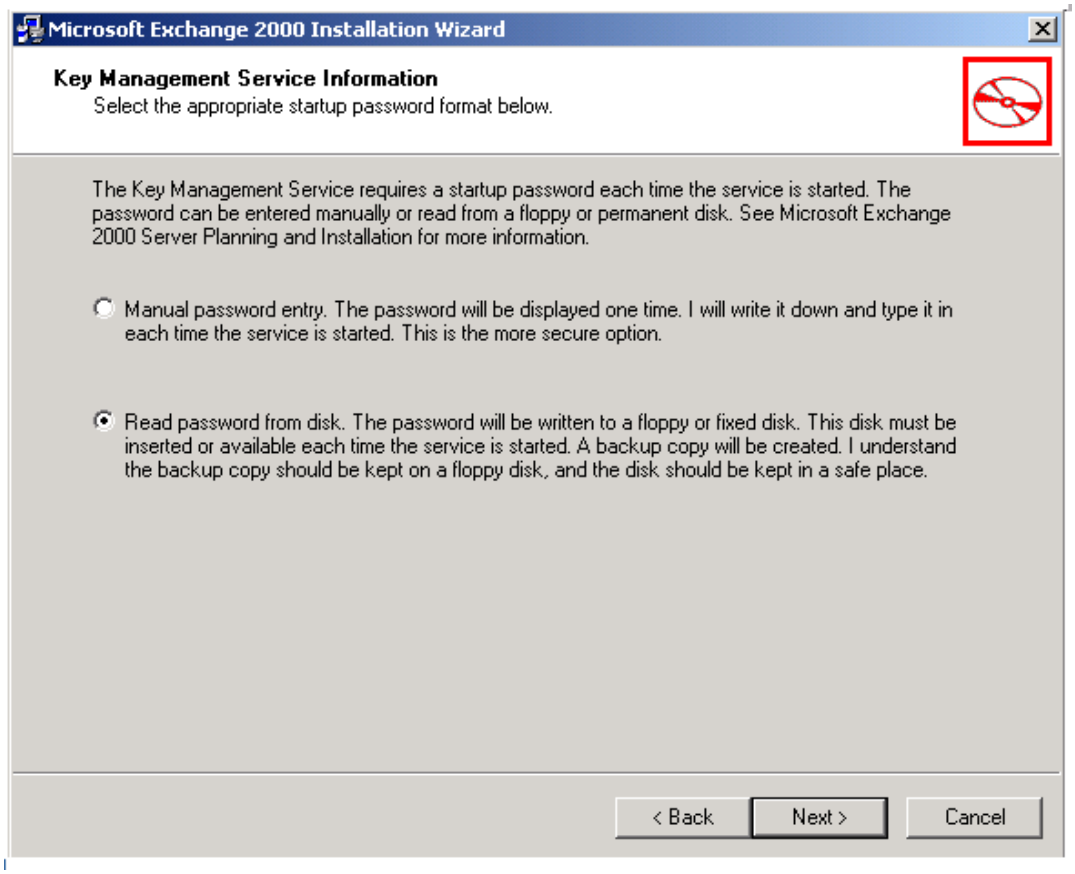

Figure 31. KMS Password Option Selection

With KMS installed, Exchange can provide the keys used for encrypting, decrypting, and signing messages. After the credentials have been created for a user, the user's public certificate is stored within the *Windows 2000 Active Directory,* giving all Exchange users access to them.

It is always recommended to reapply the latest service pack after adding components from the original source media.

Security Concerns with "Advanced Security"

Advanced Security and the *KMS* can improve the security of the Exchange environment, but certain factors must be considered in order to achieve the maximum benefit. The first consideration is the strength of the algorithm to be used. The second consideration is that *KMS* is installed with a default administrative password of "password" while the third relates to the manner in which the token that is used to enroll users in *Advanced Security* is distributed. And finally, it is important to remember when dealing with the KMS that administrators can be required to coordinate certain key management functions which provides an additional layer of security for these critical tasks via what is commonly referred to as multi-person control. Each of these concerns will be discussed in turn.

To choose the preferred algorithm to use for encryption:

- **Start menu-> Microsoft Exchange -> System Manager**
- In the console tree, select **Advanced Security.**
- In the right pane, right click **Encryption Configuration** and select **Properties**.
- Once in the **Properties**, click the **Algorithms** tab.

Figure 32 shows the **Encryption Configuration Properties** Dialog box.

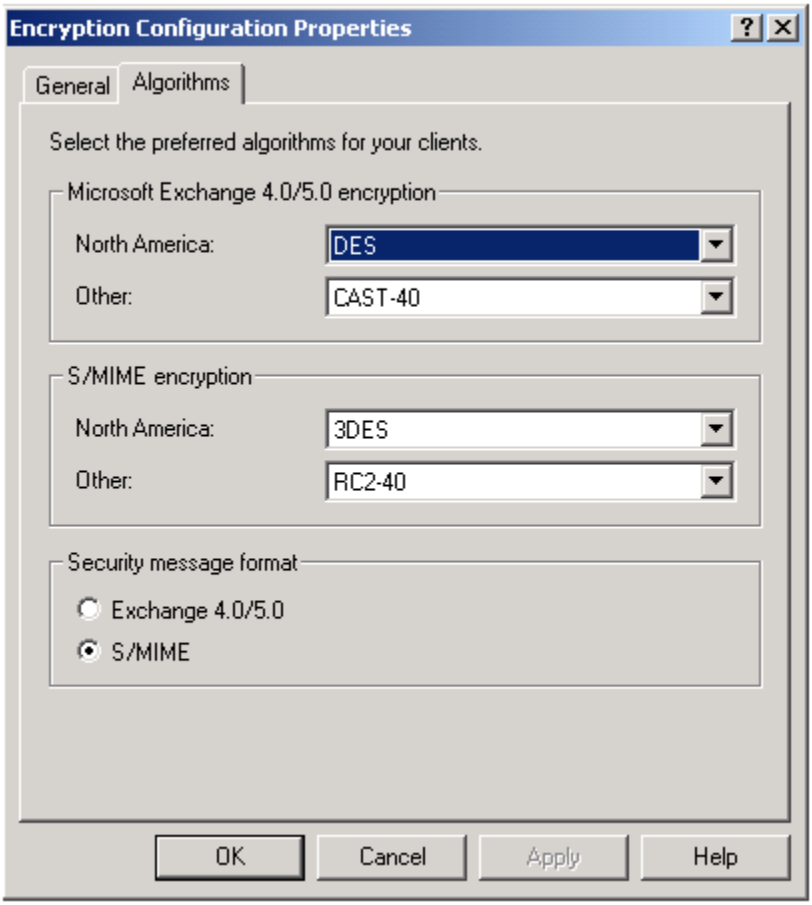

Figure 32. Encryption Configuration Properties

The Exchange Administrator can choose from several encryption algorithms:

Algorithms compatible with Outlook 97 and older:

- **DES** – The Digital Encryption Standard. This is the default selection. DES provides a 56-bit key.
- **CAST-64** – Provides a 64-bit key and is only available in the North American version of Exchange.
- **CAST-40** – Provides a 40-bit key and can be used outside of North America.

Algorithms compatible with Outlook 98 or newer:

- **3DES** – Known as “triple DES” and provides an enhancement to the DES algorithm by utilizing three DES algorithms in series. This algorithm is only available in North America and is the default selection for S/MIME encryption.
- **DES** – The Digital Encryption Standard as described above.
- **RC2-128** – Provides a 128-bit key. Only available in North America.
- **RC2-40** – Provides a 40-bit key that can be used outside of North America.

- **RC2-64** – Provides a 64-bit key and is only available in the North American version of Exchange.

The *Security message format* depends on the clients supported. If the clients are Outlook 98 or newer, administrators should select the **S/MIME** option and select the preferred encryption algorithms from the S/MIME encryption portion of the dialog box. It is generally better from a security perspective to use a longer key length such as provided by 3DES or RC2-128.

Different organizations may have different minimum Exchange key lengths and algorithms. In addition, users on a distribution list may select their preferred encryption methods. These different key lengths and algorithms could impact security by limiting encryption strength to the shortest key length used by any user appearing on an e-mail distribution list.

There is a registry key that can be set on the client computer so that Outlook will notify the user when a minimum key length is not being utilized. This key is:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\10.0\Outlook\Security

- **MinEncKey DWORD** value needs to be added; and the value should be set to the minimum key length desired for the organization. Valid key lengths are 40, 64,128, and 168. Setting this key will not preclude a user from sending a message encrypted with a shorter key, but it will provide an alert as illustrated in Figure 33:

Figure 33. Minimum Key Length Violated

As mentioned earlier, longer keys are more secure. A minimum of 128 bits is generally recommended for sensitive data.

The second security consideration is the default password of the KMS. The KMS controls all the administration functions of keys and certificates. After installation, the default password should be changed immediately because it is published in the Exchange help files. Use the password policy recommendations contained within *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set* (http://www.nsa.gov) to set the KMS password.[15]

The third security consideration is the token distribution method. To enroll in Advanced Security, the users must receive a token from the Exchange server. There are two ways to distribute the token to the user: it can be delivered to the user through some out-of-band technique or it can be e-mailed to the user. To select a method:

- **Start menu->Programs-> Microsoft Exchange -> System Manager**
- In the console tree, click on **Advanced Security**.

[15] The KMS password is not subject to the password policy set by the group policy.

- In the details pane, right click **Key Manager** and select **Properties**
- In the dialog that pops up, click the **Enrollment** tab

Figure 34 shows the dialog box that appears when the **Enrollment** tab is selected.

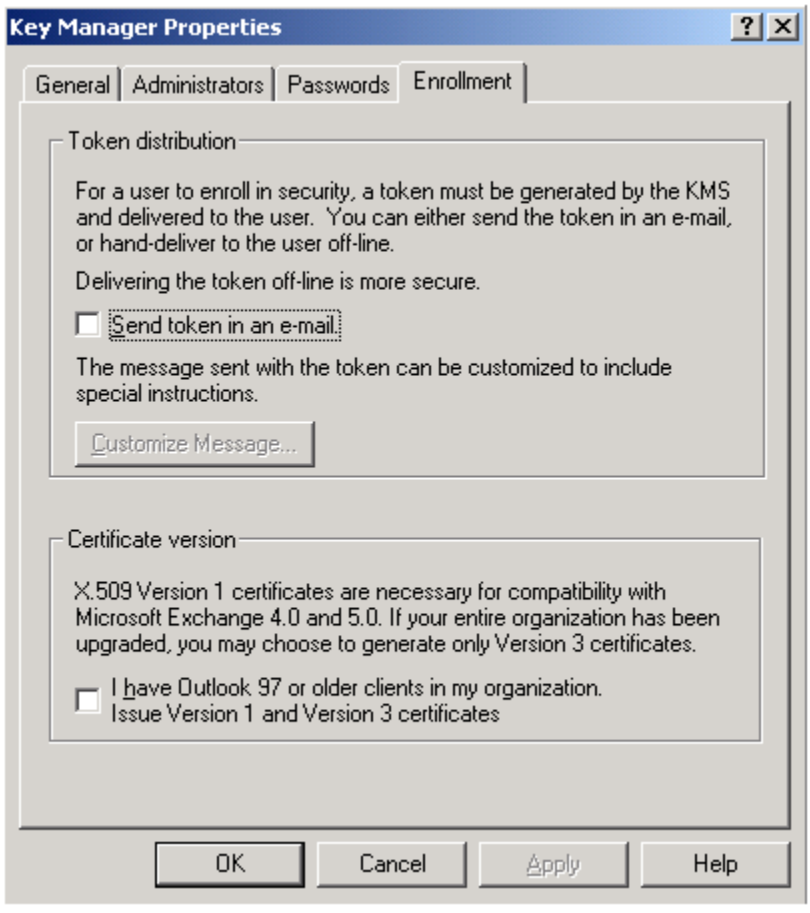

Figure 34. Enrollment Tab

If possible, the administrator should hand deliver the token to the user or use another out-of-band, trusted method. Hand-delivery is the default option. Sending the token via e-mail could allow an unauthorized person to make a copy.

The tokens can be generated from the *Active Directory Users and Computers* MMC snap-in. Select the **Exchange Features** tab under the properties page for the user and click on **E-mail Security** and **Properties**. The **Enroll** option generates the token. Every time the **Enrollment** tab is accessed, the administrator needs to put in a password. To get around entering the *KMS* password for each user enrolled in advanced security, there is a bulk enrollment option. This option allows the administrator to enroll multiple users at one time, only having to supply the *KMS* password once. This feature is accessed by right clicking on the **Key Manager** container within the Exchange System Manager and selecting **All Tasks**/**Enroll Users**. Unfortunately, this feature does not expose the user token to the administrator – it will only function if the option to mail tokens is enabled. For this reason its use is not generally recommended.

Finally, the *Key Management Service* allows advanced security administrative tasks to be placed under the control of multiple administrators. This can be used in particularly sensitive environments to place additional safeguards on more sensitive events. For

example in many environments the two most sensitive operations are recovering a user's key and importing/exporting records. One could require two-person control over these functions. *KMS* administrators are specified under the **Administrator's** tab. Assignment of multi-person control is made under the **Passwords** tab.

Figure 35 shows the *KMS* dialog box to assign multi-person control.

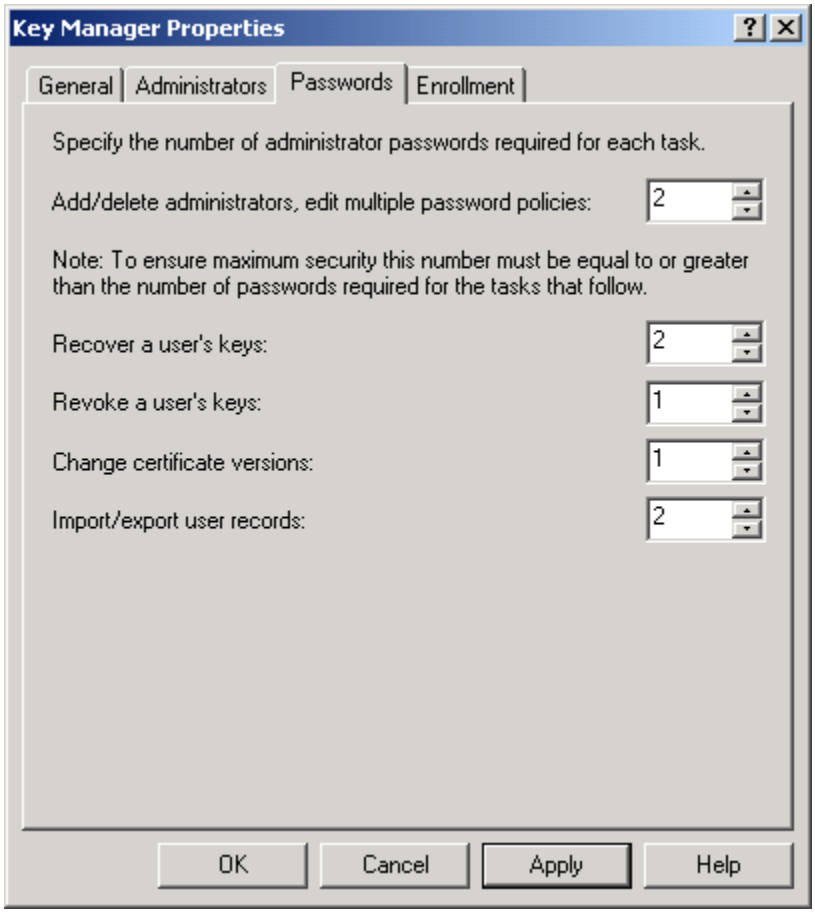

Figure 35. Passwords Tab

Client Advanced Security

Once the token has been distributed to the user, Advanced Security can be set up on the client, Outlook. In Outlook, the certificate is referred to as a *Digital ID*. To install the Digital ID used by Outlook, perform the following steps:

- **Tools** -> **Options**
- Select the **Security** tab
- Click the **Get Digital ID** button
- A dialog box pops up asking where to obtain the certificate from
- Select the **Exchange Server** Option

- Enter the token
- The password prompt is displayed [16]

Figure 36 shows the dialog box that appears when **Options**-> **Security** is selected.

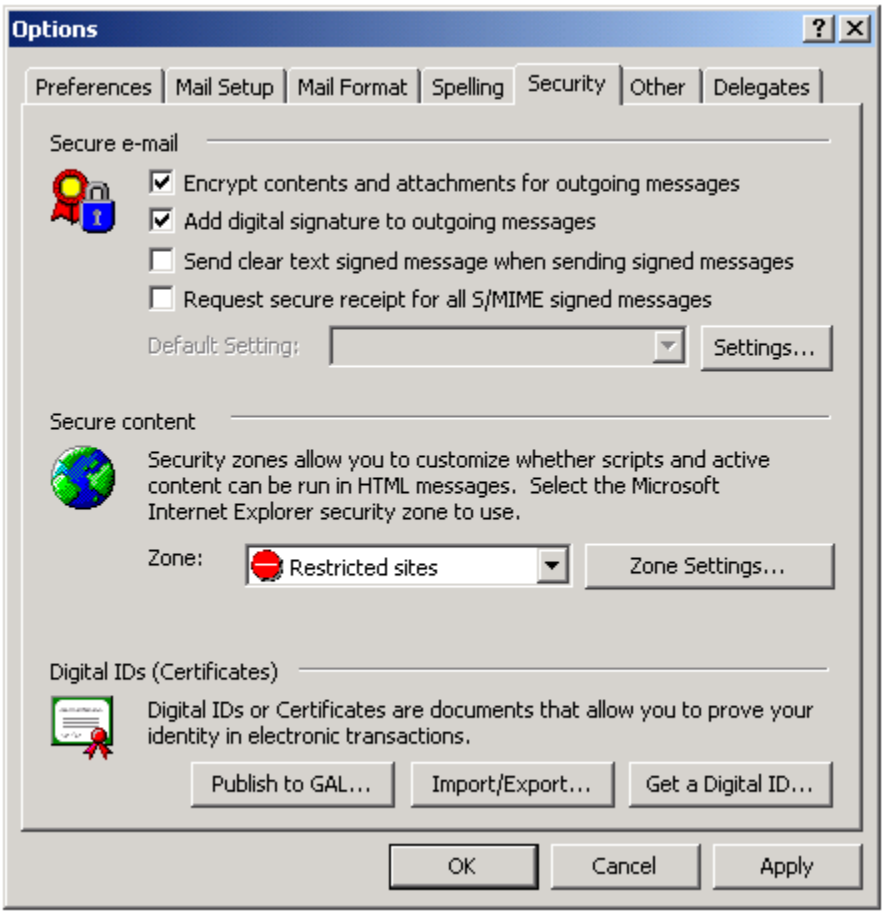

Figure 36. Security Options Dialog Box

Following this selection, an e-mail message is sent to the Exchange server and an encrypted reply is returned. Open the message and enter the password created earlier. This decrypted message informs the user that they have been enrolled in Advanced Security and gives the user the option to add the certificate to the store. The certificates should be added to the store at this point.

After enrolling in Advanced Security, signed and/or encrypted e-mail messages can be sent.

Certificate Revocation

Certificate revocation is used to deny a user further access to Exchange's Advanced Security features.

Before a user's certificate can be revoked, it is necessary to give the *Exchange Enterprise Servers* account the right to manage the certificate authority. To do so, open

[16] NSA's *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set* should be consulted for guidance on selecting a strong password.

the **Certification Authority MMC** and open the **properties page** for the certificate authority. Select the **security tab** and give *Exchange Enterprise Servers* the *manage* permission.

Once this is accomplished the *Active Directory Users and Computers* MMC snap-in can be used to revoke a certificate:

- Click the **Start** Menu and select **Programs**->**Administrative Tools**->**Active Directory Users and Computers**.
- In the console tree, click **Users**.
- In the details pane, right click the user and select **Properties**.
- On the **Exchange Features** tab in the features column, click **E-mail Security** and then click **Properties**.
- Type the KMS password.
- Click **Revoke** in the user's E-mail Security dialog box.

Bulk revocation can also be accomplished in a manner similar to the bulk enrollment feature described above.

The amount of time it takes for the Certificate Revocation List (CRL) to be re-published depends on the scheduled revocation publish interval. By default, this interval is one week. This property can be changed by using the following steps:

- Click the **Start** Menu and select **Programs**->**Administrative Tools**->**Certification Authority**.
- Expand the certificate authority by clicking on the plus sign.
- Right click on the **Revoked Certificates** container and select **properties**.

This is shown Figure 37.

Revocation may be necessary for any number of reasons including the compromise or possible compromise of a private key. In more sensitive environments it will be prudent to lower this value to accelerate the propagation of updated CRLs.

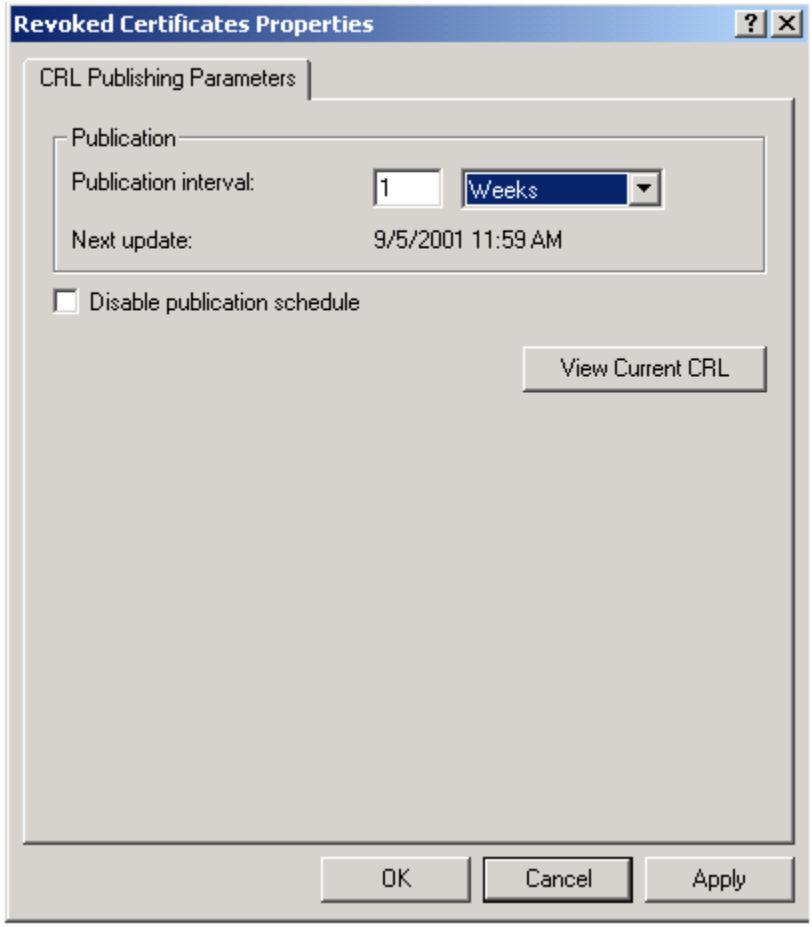

Figure 37. Revoked Certificate Properties

The publication of a CRL can also be forced by the following steps:

- Click on the **Start Menu** and select **Programs**->**Administrative Tools**->**Certification Authority**.
- Expand the root certificate by clicking on the plus sign.
- Right click the **Revoked Certificates** folder, select **All Tasks**->**Publish**.

This is shown in Figure 38.

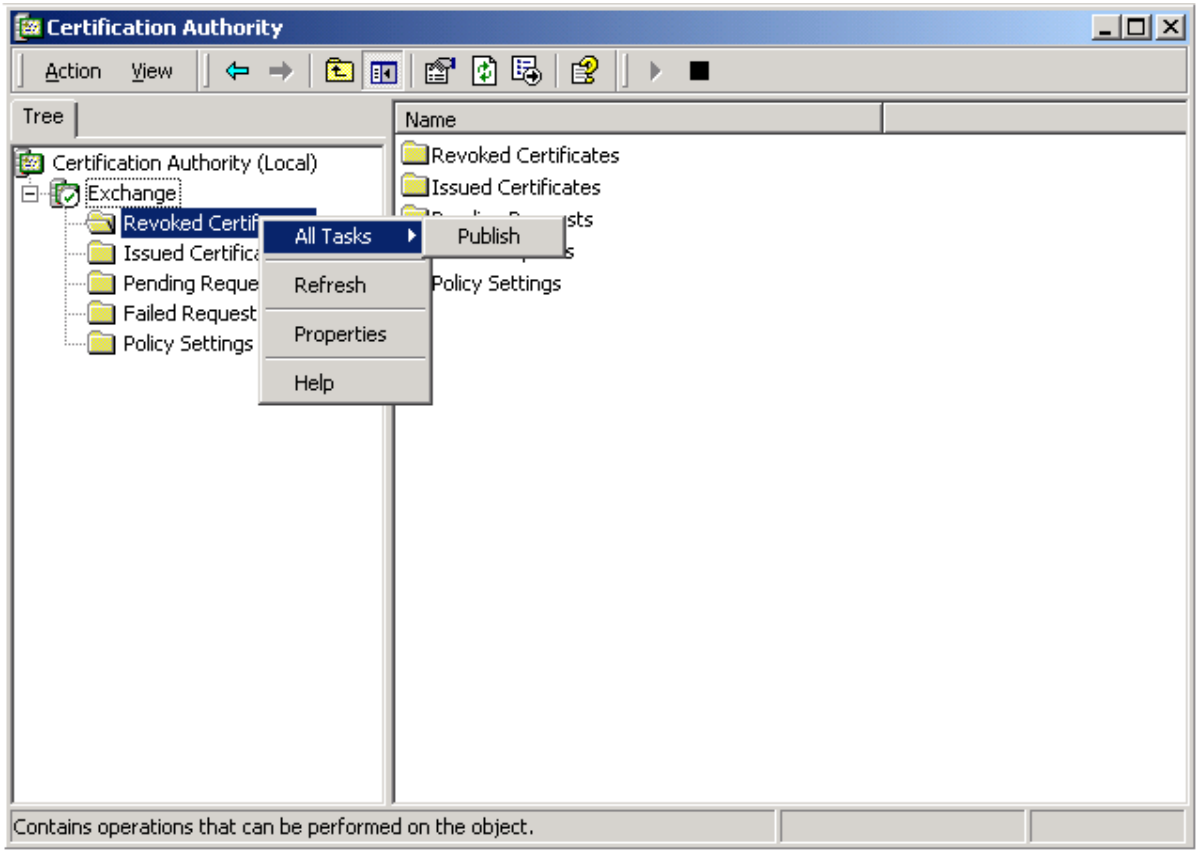

Figure 38. Revocation List Publishing

It is recommended to force publishing of the revocation list after any updates; however, note that the change will not take place for any client that still holds a valid CRL.

When a user attempts to send a signed or encrypted e-mail message, the Outlook client will check the CRL. If the senders certificate is on the CRL, the user will be prohibited from sending the message as illustrated in Figure 39.

Figure 39. User Prohibited From Sending Messages by the CRL Check

Likewise, if a user attempts to send an encrypted message to a user on the CRL, the dialog box of Figure 40 is displayed.

Figure 40. Attempting to Send an Encrypted Message to a User on a CRL

Revoking a certificate has a similar effect upon messages send prior to revocation by that user. When an Outlook client opens a message it will check the CRL for an entry matching the signer of that message – if a match is found the message illustrated in Figure 41 is displayed.

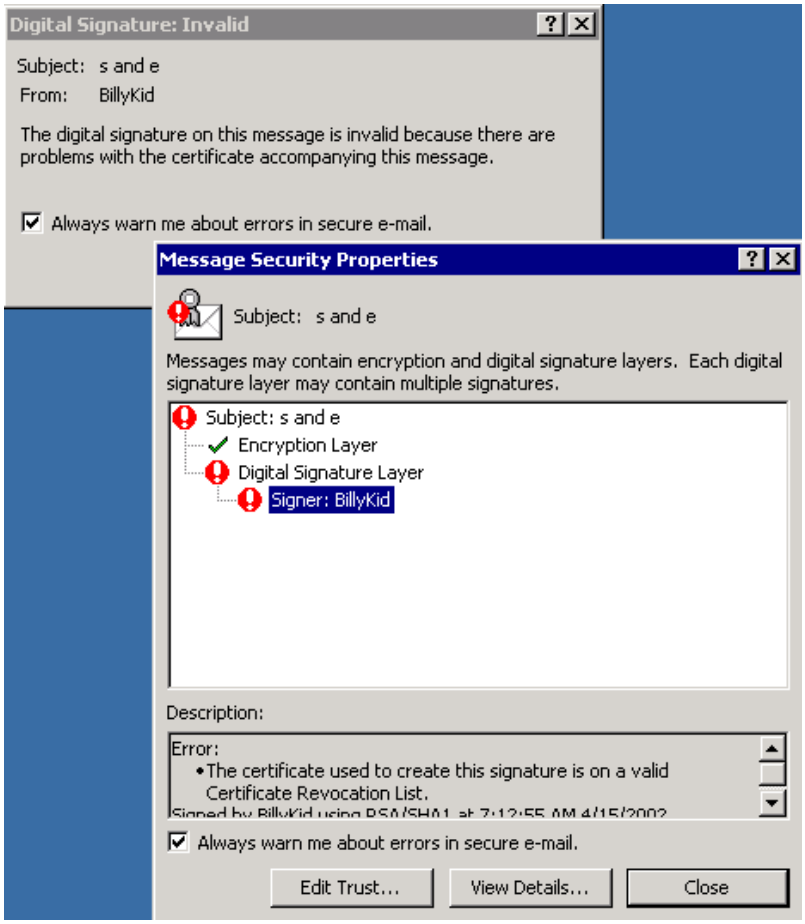

Figure 41. Signed Message Received From User on a CRL

Note that revoking a user's certificate does not prevent that user from sending and receiving unsecured mail. If a user has "gone bad" or for any other reason needs to be kept out of the Exchange environment, simply disable the Windows 2000 account.

Key Recovery

The Advanced Security facility also provides the option to recover the keys if they have been corrupted or the user forgets his password. To recover the keys follow the steps detailed above for revoking a certificate, but click **Recover** on the user's **E-mail Security** dialog box**.**

Important Security Points

- Use Exchange's Advanced Security features to provide writer-to-reader security.
- Choose the encryption algorithm, taking into consideration key length and strength.
- Change the KMS password immediately after installation.
- Do not e-mail KMS tokens to the user.
- Use multi-person control for KMS administrative functions in particularly sensitive applications.
- Set the password for KMS and client certificate storage in accordance to the password policy recommendations contained within *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set*.
- Store the KMS password on a floppy disk and store securely.
- Use certificate revocation if it is necessary to deny a user further access to Exchange's Advanced Security.
- Remember that certificate revocation does not prevent that user from sending and receiving unsecured mail. If a user has "gone bad" or for any other reason needs to be kept out of the Exchange environment, simply disable the Windows 2000 account.
- Consider lowering the CRL publishing interval.

This Page Intentionally Left Blank

Chapter 9

Network Protocols

Exchange supports Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3), Hypertext Transfer Protocol (HTTP), and Network News Transfer Protocol (NNTP) Internet protocols, as well as Internet Message Access Protocol version 4 (IMAP4). Each protocol has an associated virtual server; these virtual servers are discussed in this chapter with the exception of the SMTP virtual server which was discussed previously in Chapter 6.

Security For Protocol Virtual Servers

Each protocol—POP3, IMAP4, NNTP, and HTTP—has a virtual server associated with it. For each protocol more than one virtual server can be defined. This can be done for several reasons: for hosting different domains, for different authentication requirements, or simply for availability. Each virtual server has its own IP address, port number, and authentication settings. The security of the virtual servers can be controlled using the following methods:

- Access Control can be configured to grant or deny access by IP address or Domain name.
- Client Authentication can be configured.
- Secure Channel communication (SSL) can be configured.
- Duration and number of connections can be configured.
- Protocol and Diagnostics logging can be set.
- Several of the virtual servers -- SMTP, HTTP, and NNTP -- allow logging that yields audit trails of commands received from clients.

POP3

Post Office Protocol version 3 (POP3) is the protocol that dynamically enables users to retrieve mail from the mail server. It was designed for workstations that don't have enough resources to maintain both SMTP services and a message transfer system. POP3 clients access only server inboxes and can not access other public or private folders. This protocol is fast and is used only for mail retrieval.

A POP3 virtual server is provided when the Microsoft Exchange 2000 Server is installed. It is automatically enabled so that users can download their mail as soon as the server and client are configured. To ensure that the server can support the POP3 clients, several areas must be configured. These areas include: assigning an IP Address, TCP Port, and

SSL Port; controlling access to the server; specifying message formats; and setting connection limits. These configuration areas are discussed in the following paragraphs. To configure the POP3 virtual server, follow the steps outlined below.

Using the Exchange System Manager, open the **Protocols** container; this is found by navigating down through **Administrative Groups**, **Administrative group**, **servers**, **server name**, **protocols**. This is shown in Figure 42. After selecting the POP3 folder, review the properties of the POP3 virtual server as shown in Figure 43. The properties are found by right clicking on the POP3 server icon.

The POP3 Virtual Server properties are divided into three areas: **General**, **Access** and **Message Format**. Listed under the **General** tab are the IP address assignment and connection limitations. To assign an IP Address, TCP Port, and SSL Port to the POP3 virtual server enter the **Advanced** button. This defaults to the IP address as unassigned, the TCP port as 110 and the SSL port as 995. To enable the SSL capability on the POP3 virtual server, a certificate must be requested (discussed below). The number of connections can be set in order to constrain denial of service attacks; this number should be set at a reasonable value given the environment in which the POP3 service is running. While an attacker may be able to launch a denial of service attack against the POP3 service by exceeding this limit, other services should remain available if a reasonable limit is set.

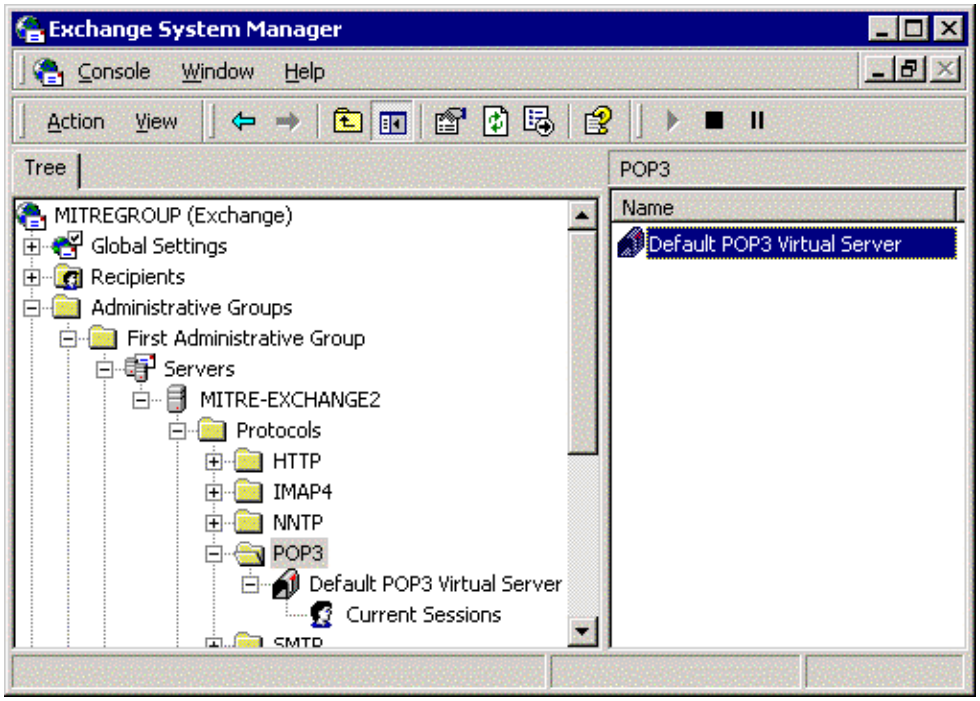

Figure 42. Exchange System Manager Protocols Container

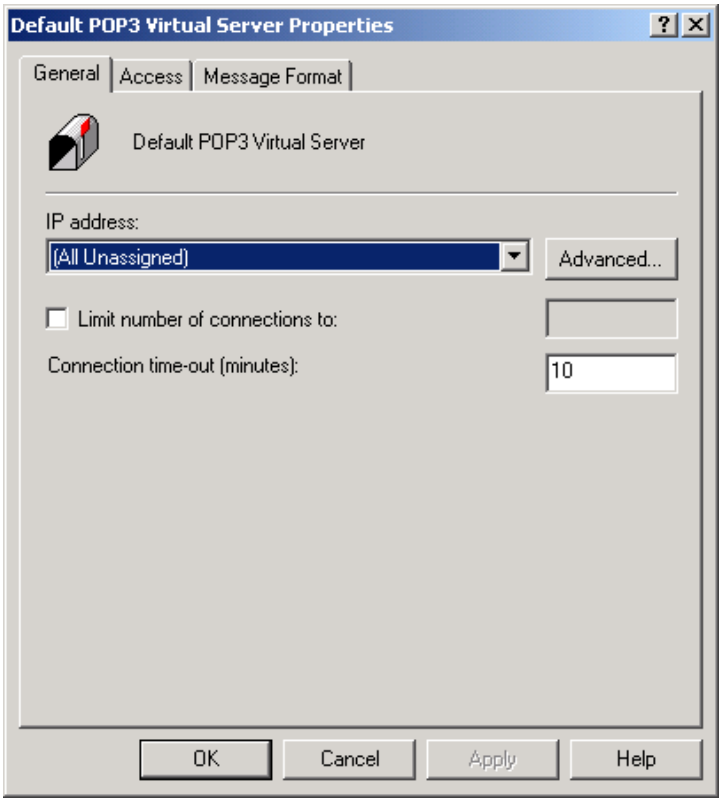

Figure 43. POP3 Virtual Server Properties

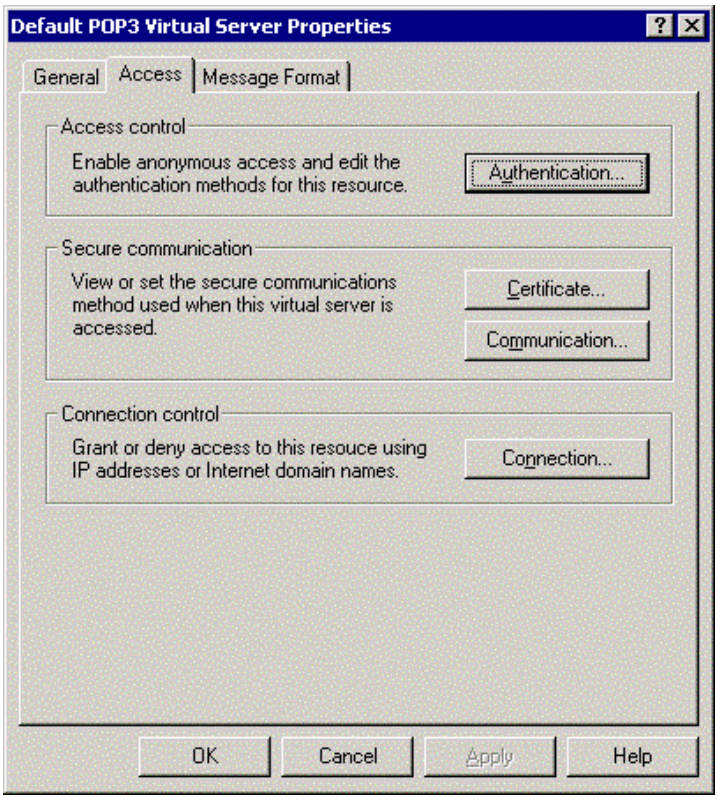

Figure 44. POP3 Virtual Server Access Properties

The dialog box shown under the **Access** tab of the server properties is shown in Figure 44. This dialog box allows for the configuration of Authentication mechanisms, Connection control, Certificate requests/install, and Secure Channel Communication.

The POP3 virtual server in Exchange can be set to use one of several authentication mechanisms. These authentication mechanisms include Basic Authentication, Basic Authentication with SSL and Integrated Windows Authentication. These methods are detailed below.

- **Basic authentication**. This method requires the user to provide a valid Windows user name and password. The user's information is sent as unencrypted clear text across the network. Avoid this authentication method.

- **Basic Authentication Over SSL**. This method requires the user to provide a valid Windows 2000 user name and password. The user's information is sent over an encrypted SSL channel.

- **Integrated Windows authentication**. This method requires the user to provide a valid Windows 2000 user account name. It authenticates by relaying the user's Windows credentials directly to the server, without requesting information from the user or transmitting unencrypted information across the network.

Basic authentication is chosen as the default configuration. It is recommended to use Basic authentication over SSL or Integrated Windows Authentication. To enable Basic authentication over SSL, set SSL port and request a certificate as detailed in subsequent paragraphs. To disable the basic authentication capabilities (with or without SSL) uncheck

the Basic Authentication box shown in Figure 45. Use either **Basic authentication with SSL** or **Integrated Windows Authentication**; both options can be selected.

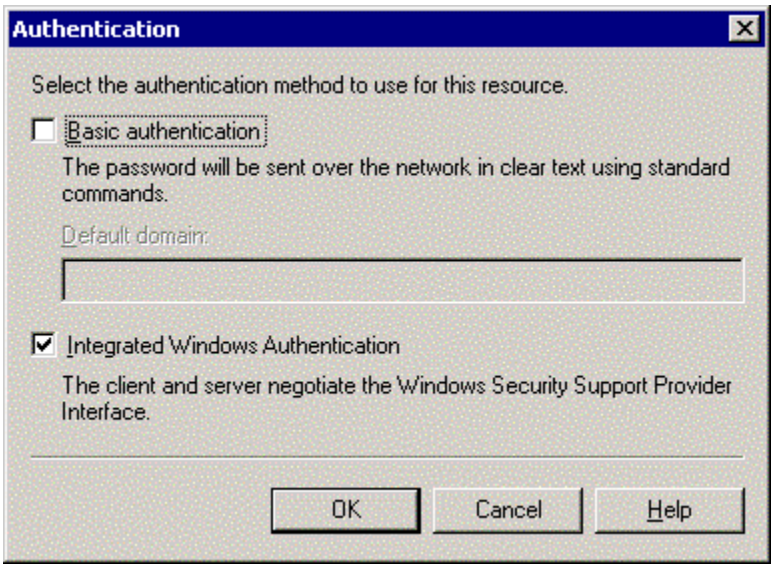

Figure 45. POP3 Virtual Server Authentication Properties

For SSL certificate request and installation, return to the Access tab and choose the Certificate box listed under Secure Communication. Continue through the Web Server Certificate Wizard to request and install the SSL certificate for secure communication between the virtual server and a POP3 client.

The next option for Secure Communication is the Communication box. This option can be enabled after the SSL certificate has been installed. Upon choosing the Communication box, the dialog box shown in Figure 46 is shown. To restrict access to only clients supporting SSL connections, select the **Require secure channel** check box. It should be noted that enabling SSL could substantially increase server load. However, if it is enabled, it is recommended to restrict access to clients supporting 128-bit encryption.

Figure 46. Require Secure Channel Dialog Box

The connection control option listed under the **Access** tab is used to restrict or deny access to the virtual server based on IP address. Use **Connection** to prevent computers from connecting to the virtual server. Although it may not be practical in all cases to restrict access based on IP address, it is recommended to restrict access to critical servers as much as possible. The **Connection** box used to restrict or allow access by particular IP address or subnet mask is shown in Figure 47. Access can also be allowed or denied by a qualified domain name. Be aware that if clients are configured for DHCP, unauthorized users could inadvertently be allowed to access the virtual server. Similarly, authorized users could be denied access.

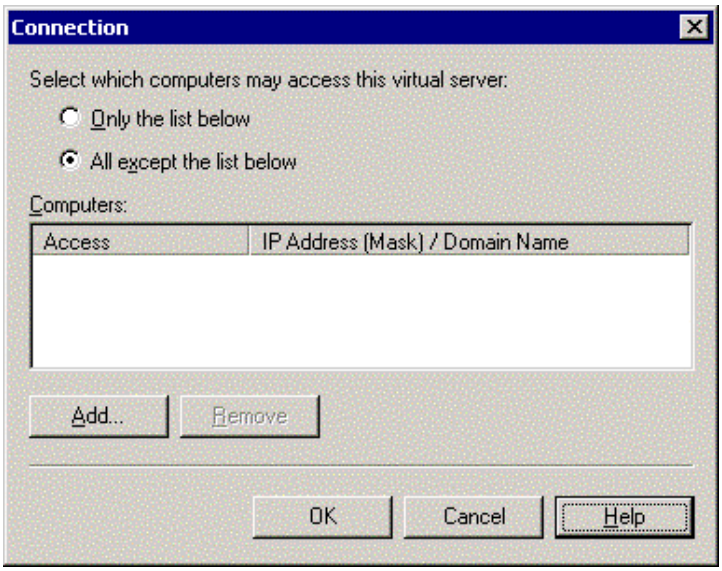

Figure 47. Connection Restriction Dialog Box

Client setup is also required. Clients cannot log on to Exchange via POP unless complementary settings are utilized, particularly in relation to authentication methods. Figure 48 illustrates the appropriate dialog box from a user's e-mail profile. Note that the **Log on using Secure Password Authentication** option is selected, analogous to the server setting **Integrated Windows Authentication** discussed above. Chapter 2 details how to access the profile in Outlook 2002.

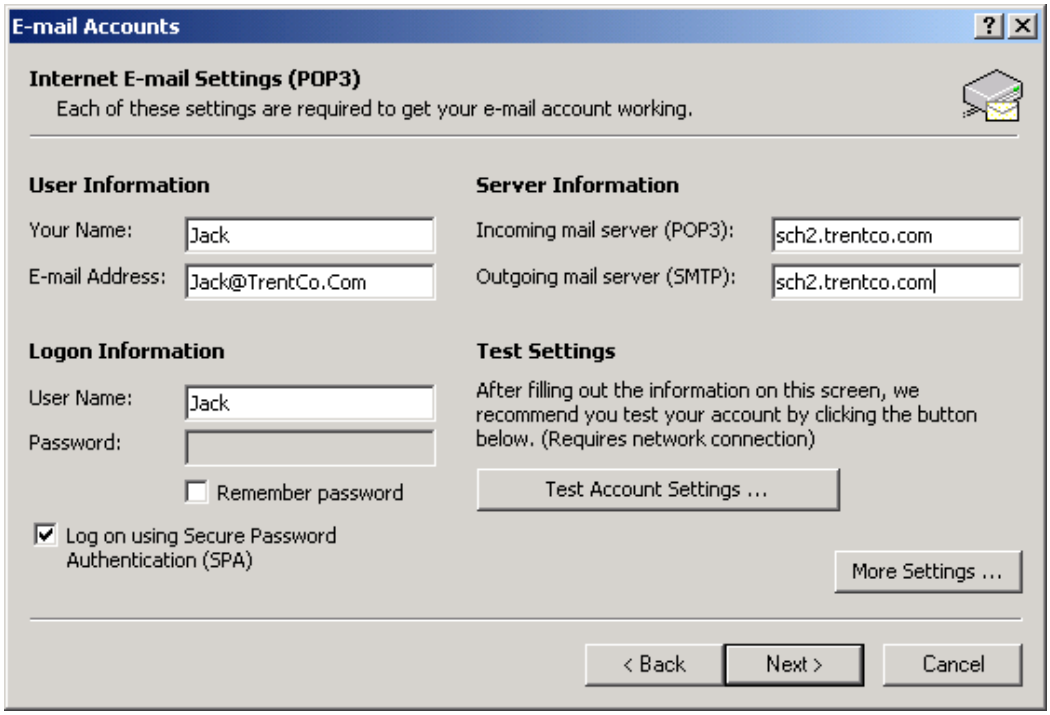

Figure 48. Client-Side POP3 Authentication Settings

If utilizing plain-text passwords with SSL in lieu of Secure Password Authentication, then it is also necessary to configure the client to use the POP3/SSL port. To access these settings, click on **More Settings** from the dialog box illustrated in Figure 48 and select the **Advanced** tab. Both the Exchange Server and the Outlook 2002 will default to port 995 when using POP3/SSL.

IMAP4

Internet Message Access Protocol version 4 (IMAP4) is a protocol that enables a client to access mail on a server instead of downloading it to the user's computer. This protocol is used in situations where a user logs onto the server from different workstations and different locations. Once the user is connected to the server they can access the mail as though it is stored locally. This gives the user the ability to access other folders on the mail server. IMAP4 does not handle sending mail; SMTP provides this functionality.

An IMAP4 virtual server is provided when the Microsoft Exchange 2000 Server is installed. It is automatically enabled so users can access their mail as soon as the server and client are configured. To ensure that the server can support the IMAP4 clients, several areas must be configured. These areas include assigning an IP Address, TCP Port, and SSL Port; controlling access to the server; specifying message formats; and setting connection limits. Many of these configuration areas are identical to the configuration areas previously discussed for the POP3 server; only configuration areas that are different will be discussed.

Using the Exchange System Manager, open the **Protocols** container; this is found by navigating down through **Administrative Groups**, **Administrative Group**, **Servers**, **server name**, **Protocols** as shown previously in Figure 42. After selecting the **IMAP4**

folder, review the properties of the IMAP4 virtual server as shown in Figure 49. These properties are divided into three areas: **General**, **Access** and **Message Format**.

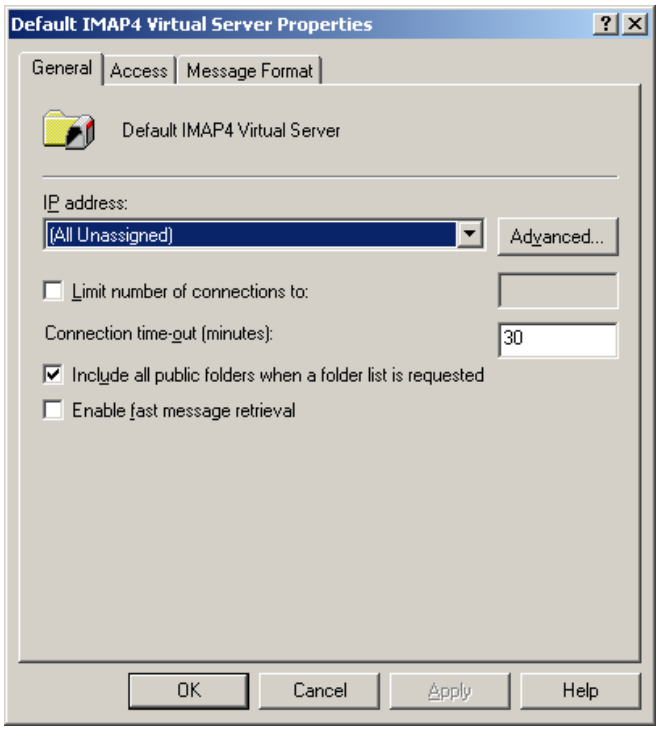

Figure 49. IMAP4 Virtual Server Properties

The **General** tab of the IMAP4 server contains the IP address assignment and the **Advanced** button for setting the TCP port and the SSL port. These are configured as described for the POP3 virtual server. It also contains additional settings, *Include all public folders when a folder list is requested* and *Enable fast message retrieval.* Although these settings are not security related, they can affect the performance of the clients. If there are a large number of public folders, some clients may not function properly. If the former option is not selected, then public folders are not included when a client requests a list of folders from the virtual server. The latter option, fast message retrieval, will speed the retrieval of messages that do not require exact message sizes; however, some clients will not function if this option is enabled.

The **Access** tab of the IMAP4 server allows for the configuration of **Authentication mechanisms**, **Connection control**, **Certificate requests/install**, and **Secure Channel Communication.** These configuration settings are identical to the settings described for the POP3 server. Use Basic Authentication with SSL or Integrated Windows Authentication for authentication. Implement these options as described for POP3. Apply connection control to restrict or deny access to the IMAP4 server based on specific IP addresses if practical.

Client side setup options are also similar to that discussed for POP3.

POP3 and IMAP Banners

By default, the Exchange POP3 and IMAP services will display banners identifying the server as being based on Microsoft Exchange upon the establishment of a connection and again as the connection is broken. A potential hacker can get at this information by simply

creating a telnet connection to the POP3 or IMAP ports. Since this presents a leakage of information that could give an attacker an advantage, it is generally recommended to modify this banner. This is accomplished via a change to the IIS Metabase using a tool such as Microsoft's MetaEdit. Complete details are available in Microsoft Knowledge Base article Q303513 available at:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;q303513

Unfortunately, in testing conducted by the author using Exchange Server 2000 with Service Pack 2 and as reported by several others in Exchange newsgroups, *this does not presently work*. If this feature is fixed by Microsoft is recommended to change the banners.

LDAP

The Lightweight Directory Access Protocol (LDAP) is commonly used in conjunction with IMAP or POP access to query the Active Directory for user names and e-mail addresses. The Active Directory requires users to authenticate before access is allowed. Unfortunately, the default condition in Outlook 2002 is to send the user name and password in the clear and THERE IS NO OPTION FOR SECURE PASSWORD AUTHENTICATION. This is illustrated in the network sniff detailed in Figure 50 which shows user *Jack* and his password (which was temporarily set to *[password]* for the purpose of this illustration). It is therefore very important to utilize SSL in conjunction with LDAP.

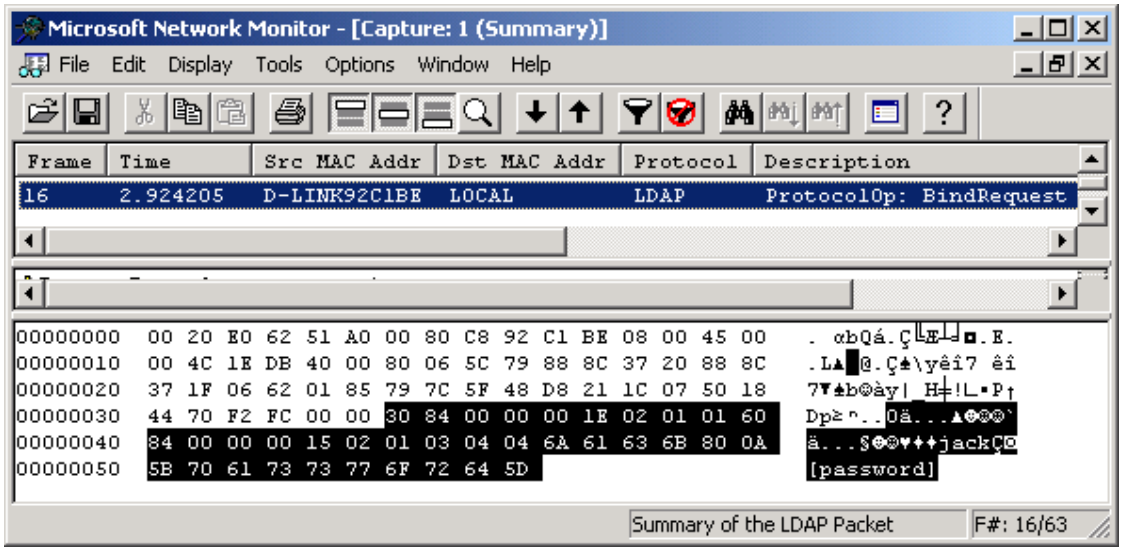

Figure 50. Passwords Sent in the Clear - LDAP

Setting up LDAP to use SSL begins with the issuance of a certificate on the domain controller that is used in the establishment of SSL sessions between the client and server. Assuming that an certificate server has already been be established in the Windows 2000 domain, the certificate is issued via the Group Policy MMC snap-in. Under the **Default Domain Policy** container, navigate to **\Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Automatic Certificate Request Settings**. Right click and select **New\Automatic Certificate Request**. Run through the resulting wizard, selecting the **Domain Controller** template in the second dialog box. This

results in the issuance of a certificate that will allow LDAP to respond to SSL queries. Non-SSL queries will still be serviced as well, so it is important to specify the use of SSL from the client.

To setup Outlook 2002 to use SSL for its LDAP queries, Select **Tools/E-mail Accounts**. Navigate to the **Directory Service (LDAP) Settings** page and click on **More Settings**. Change the **Connection Details** portion of the dialog box to enable **Use Secure Sockets Layer** and change the port number to 636. This is illustrated in Figure 51.

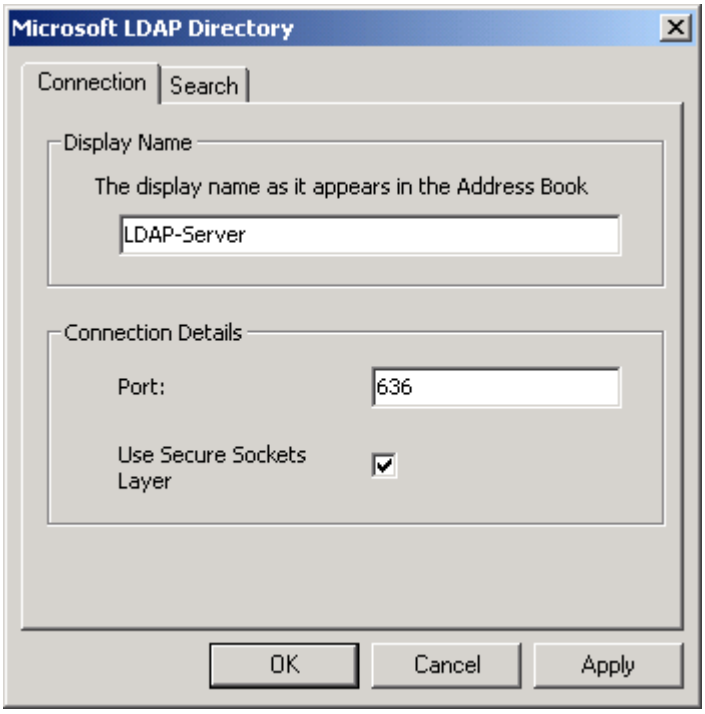

Figure 51. Outlook 2002 Configured for LDAP/SSL

The search tab, which is also shown in Figure 51, allows one to enter a search base which serves as the starting point for the LDAP queries. By default this is blank which results in LDAP searches that can return system objects for which the user would have no need to send e-mail. To clean up the query results, enter a search path in the form of:

cn=users,dc=[domain name part 1],dc=[domain name part2],dc=[domain name part 3]…

Or more specifically, in the author's test lab the following was used which reflects a domain name of TrentCo.com:

cn=users,dc=trentco,dc=com

It is also necessary to establish a user certificate before LDAP/SSL access is granted. The procedures for obtaining a user certificate will be dependent on local policy, but for the sake of illustration assume for a moment that a Microsoft Certificate Server is being utilized which is located within the Windows 2000 domain. To obtain a certificate via this method, the user would go to http://[certificate server computer]/certsrv and follow the wizard to obtain the certificate. Once the certificate is generated, the wizard includes an option to install it. Once the certificate is installed, LDAP queries will be protected by a SSL tunnel.

HTTP

Hypertext Transfer Protocol (HTTP) is the protocol used by the World Wide Web and is used by Exchange Server 2000 to allow access to mailboxes and folders via a web browser. The HTTP Exchange virtual server is found in the Protocols folder using the Exchange System Manager as described for POP3. Although the HTTP virtual server is listed in the Exchange System Manager, it cannot be managed from this point. It must be administered from the Internet Services Manager that manages the Internet Information Services (IIS).

Using the **Internet Services Manager**, the **HTTP Exchange Virtual Server** can be administered using settings applied to the **Default Web Site**. This is shown in Figure 52. After selecting the **Default Web Site**, open the properties page.

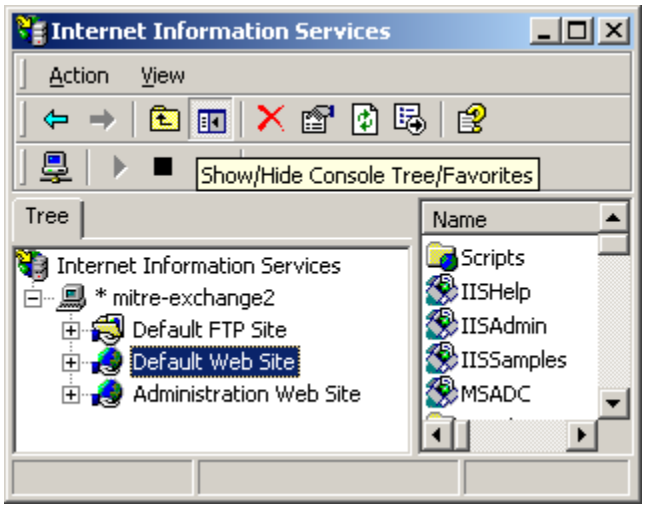

Figure 52. HTTP Virtual Server in IIS

The security properties relevant to the HTTP virtual server are contained in the **Directory Security** tab. These properties are shown in Figure 53. The security properties should be set for authentication, access control and secure communication.

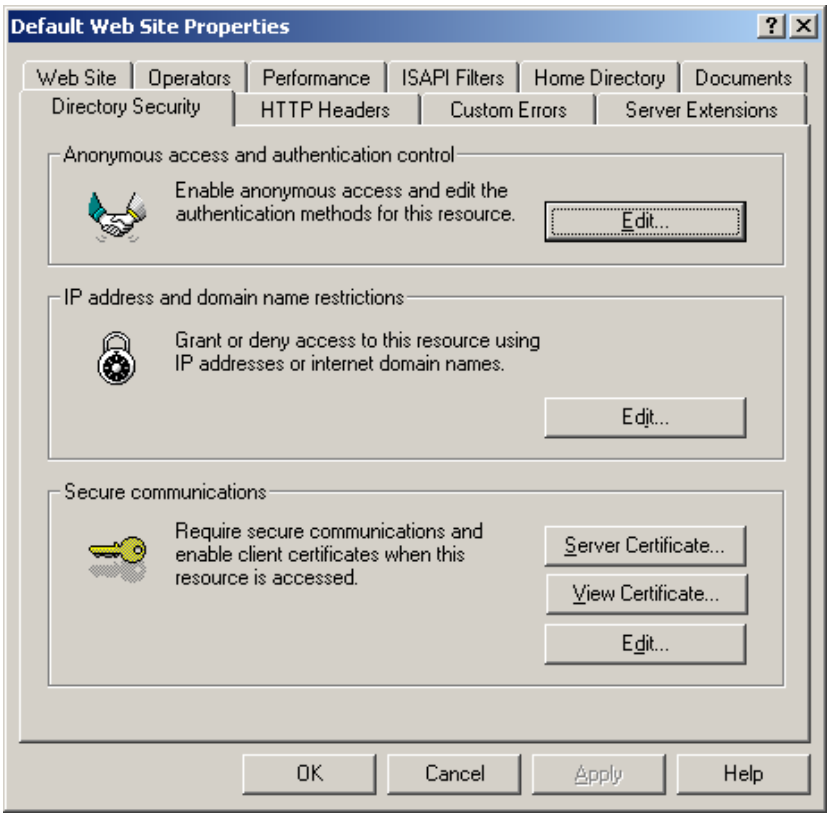

Figure 53. Directory Security Settings for HTTP Virtual Server

The Authentication settings have been discussed previously. The recommended authentication methods can be set using the **Edit** button listed under the *Anonymous access and authentication control* box. Access can be restricted or granted based on IP address or Internet domain names. SSL communication can be configured using the **Edit** button in the secure communications box. All child nodes of the HTTP virtual server will inherit these settings. If there are child nodes of this server that should not inherit these values, select only those children that should not inherit when the *Inheritance Override* dialog box appears after applying the security settings.

For additional security considerations related to IIS, refer to the *Guide to the Secure Configuration and Administration of Microsoft Internet Information Server 5.0* available at http://www.nsa.gov

NNTP

Network News Transfer Protocol (NNTP) is a protocol used over TCP/IP networks that defines client and server commands used to access newsgroups. These newsgroups are represented as public folders in Exchange. Users can read and post messages and documents to NNTP newsgroups. These items can be replicated to Usenet host computers in news feeds. The NNTP virtual server administers newsgroup services by controlling authentication and client connections from a centralized location. These are controlled by configuration properties that are similar to the POP3 configuration properties. They include bound IP addresses, port number, and authentication type. Many of these configuration areas are identical to the configuration areas previously discussed for the POP3 server; only configuration areas that are different will be discussed.

Using the Exchange System Manager, open the **Protocols** container; this is found by navigating down through **Administrative Groups**, **Administrative Group**, **Servers**, **server name**, **Protocols** as shown previously in Figure 42. After selecting the **NNTP** folder, review the properties of the NNTP virtual server. These properties are divided into three areas: **General**, **Access** and **Settings**.

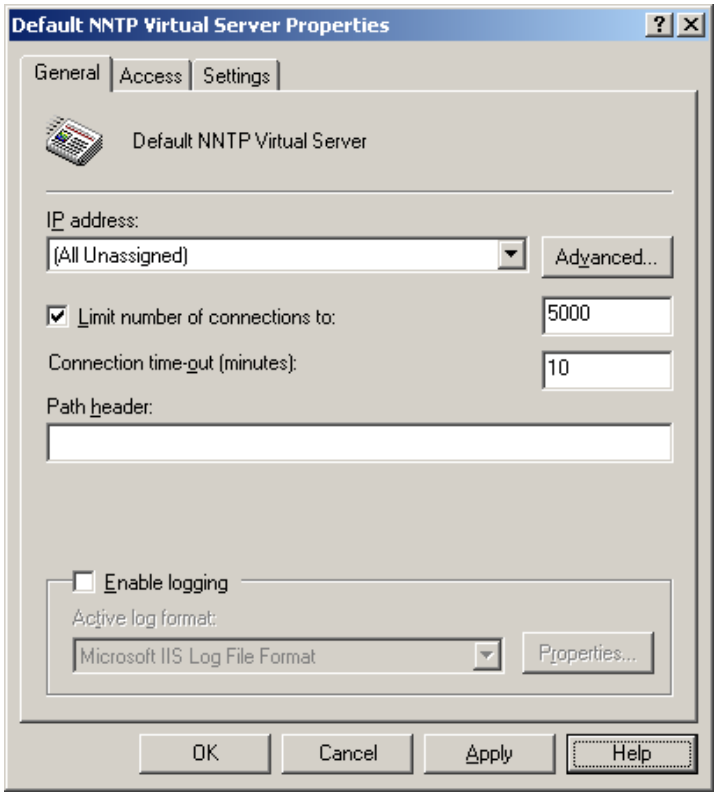

Figure 54. NNTP Virtual Server Properties

Under the **General** tab the IP address, TCP port and SSL port are configured as described previously. Consider enabling protocol logging via the Enable logging box. This can be used to track user activity when connected to the NNTP server and therefore may be useful in for such things as tracking the delivery of malicious code uploaded by a user. Be aware that these logs can grow very quickly; make certain that sufficient disk space is available to ensure that a denial of service condition is not created by log files that overwhelm the available storage.

The **Access** tab allows the configuration of Authentication method, secure communication, and connection control. The authentication methods available are Anonymous, Basic, Integrated Windows Authentication, and SSL authentication as shown in Figure 55. The authentication method should be chosen with care, remembering that basic authentication sends the password in the clear. If Anonymous authentication is allowed, a particular user account should be used for this purpose. This anonymous user is set as shown in Figure 56. It is acceptable to use these default settings.

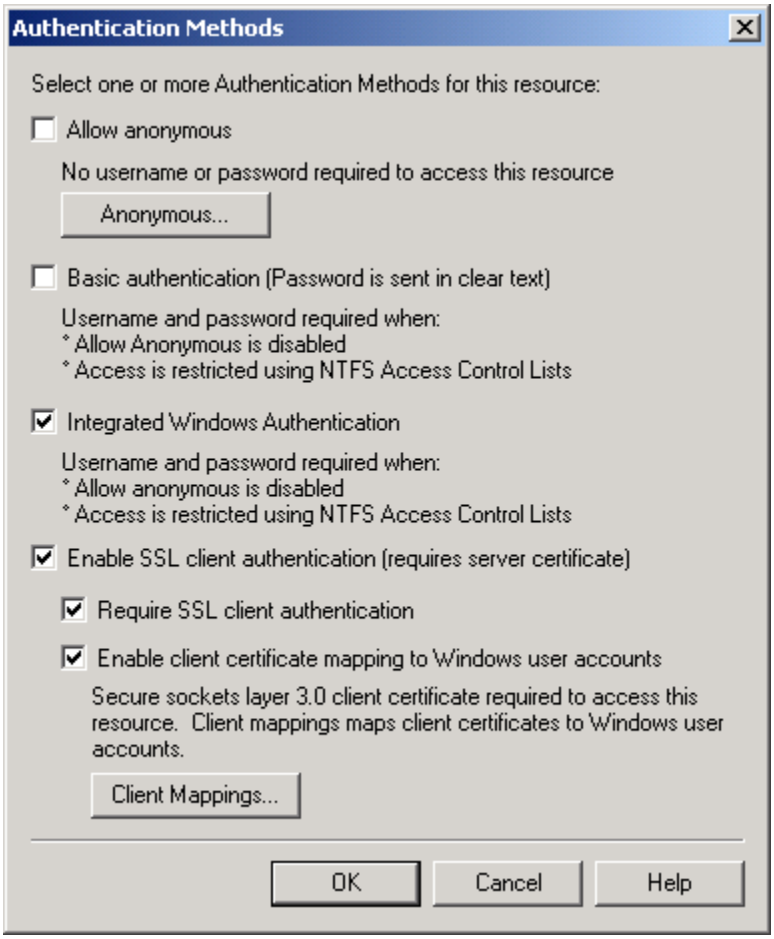

Figure 55. Authentication Methods for NNTP Virtual Server

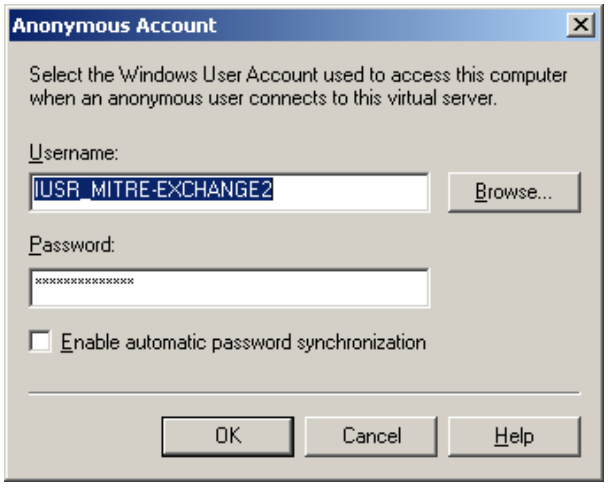

Figure 56. Anonymous Access Account for NNTP

The Settings tab is used to restrict the size of articles and connections and to choose if articles from the virtual server can be shared with other NNTP servers. These settings have appropriate values set by default. In order to constrain denial of service attacks, these limits should be examined and set to reasonable values.

Setting the Windows 2000 Server permissions for the directories that contain the newsgroups can also set access control for particular newsgroups.

Protocol Logging

Protocol logging may be useful for such things as tracking the delivery of malicious code uploaded by a user. Be aware that logs grow quickly and unless sufficient disk space is available, a denial of service condition could be created. Enabling protocol logging may also decrease service and system performance. Protocol logging can be enabled for SMTP, NNTP and HTTP. It can be used to track the commands a virtual server receives from users. When used with Windows 2000 event logs, the protocol log helps to identify problems with the virtual server. Protocol logging is enabled for SMTP and NNTP through the Exchange System Manager under the virtual server. It is listed on the **General** tab of the properties for the virtual server. Four protocol logging formats exist; these formats have been discussed previously in Chapter 6. The HTTP Exchange virtual server logging is enabled through the Internet Services Manager. The protocol logging is enabled by clicking on **Enable logging box** contained in the Default Web Site Properties; this is shown in Figure 57.

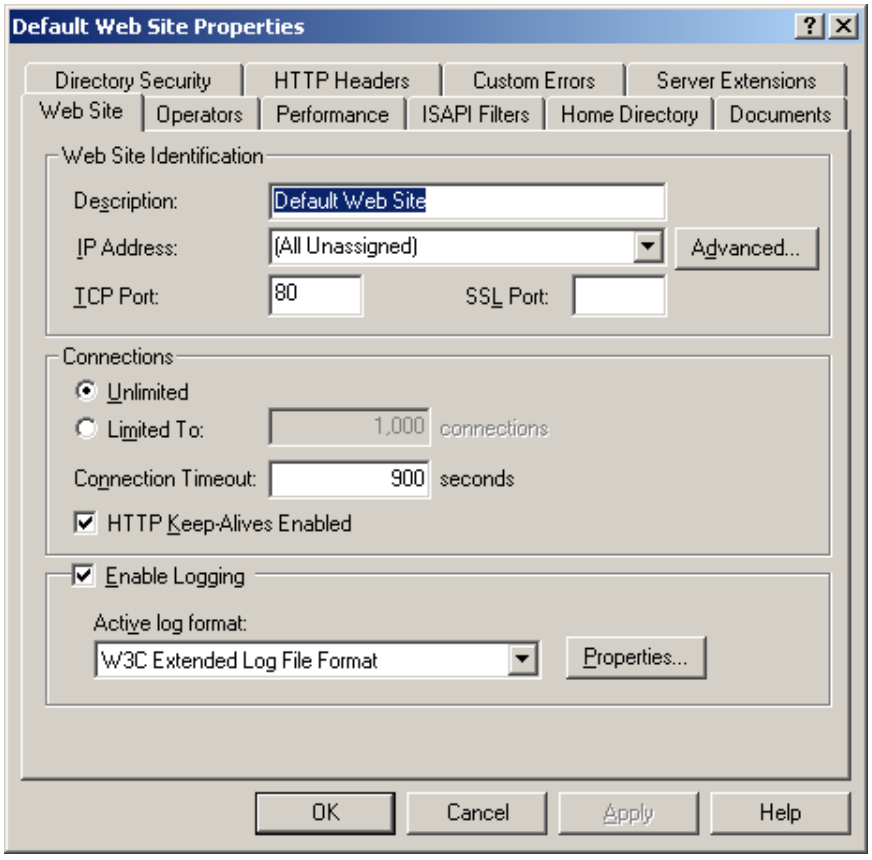

Figure 57. Default Web Site Properties

Diagnostics logging writes records to the application log on a service basis. Diagnostics Logging can be configured for the virtual servers that do not enable protocol logging. This includes the POP3 virtual server and the IMAP4 virtual server. Diagnostics logging can be enabled by right clicking on the Exchange server from the *Exchange System Manager* Window. The **Diagnostics Logging** tab contains the services that can be logged. For

POP3 or IMAP4 it is recommended to, at a minimum, enable logging for authentication. Select a logging level of **maximum**. This is shown in Figure 58.

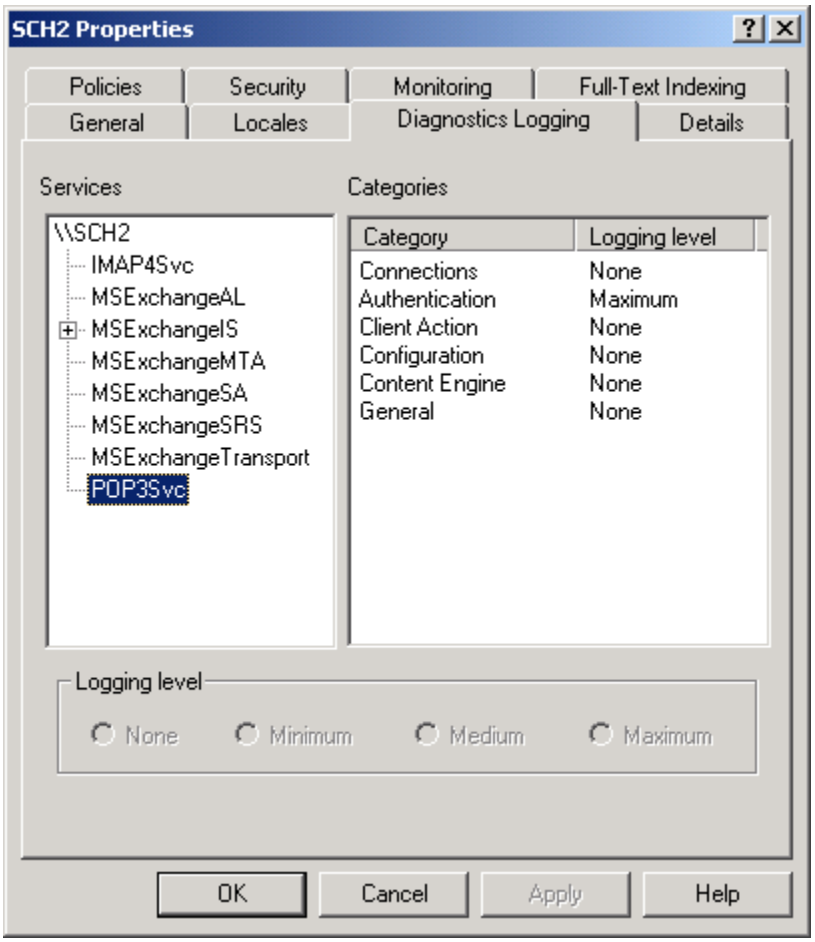

Figure 58. Diagnostics Logging for the Exchange Server

Mailbox Protocol Settings

Each mailbox-enabled user can have protocol settings configured for their mailbox. These settings are configured from the Active Directory Users and Computers Console. After selecting **Advanced Features** under the View menu, the **Exchange Advanced** tab will be shown for a chosen user. The **Protocol Settings** button allows the administrator to set which protocols are enabled for that user's mailbox. The protocols available are HTTP, POP3 and IMAP4.

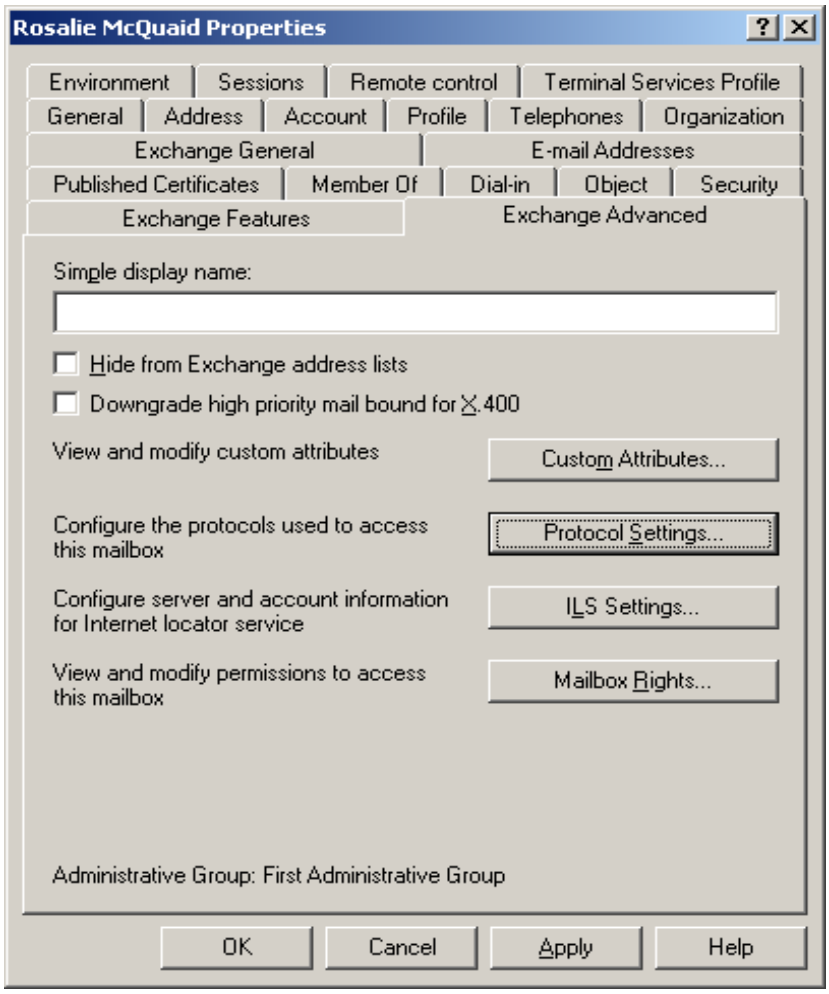

Figure 59. User/Mailbox Properties for Protocol Settings

These settings, as shown in Figure 59, are relevant from a security perspective in that they can be used to deny access to the protocols on a per-user basis, perhaps in response to misuse or simply because the service is not required.

Important Security Points

- Avoid using Anonymous Authentication.
- Grant or Deny access to virtual servers by IP address or Domain name if practical.
- Use Integrated Windows Authentication or Basic Authentication over SSL.
- If using SSL, restrict access to clients using 128-bit encryption.
- If using LDAP in conjunction with POP or IMAP access, protect authentication information via SSL.
- Use message and connection limits to constrain denial of service attacks.
- Use protocol logging and diagnostics logging to help troubleshoot and investigate security relevant areas.

- Use mailbox settings under the Active Directory Users and Computers Console to restrict access to HTTP, IMAP4, and POP3 on a per-user basis if necessary.

Chapter 10

Developing Custom Applications

This section provides an overview of the security-relevant aspects of developing custom Exchange 2000 applications. It includes a review of security-relevant Exchange 2000 API elements, as well as identifies high-level security implications for Exchange 2000 developers. It is intended to make developers aware of the security issues and considerations involved with Exchange 2000 application development; other reference material should be consulted for more in-depth application development security instruction.

Introduction

Exchange 2000 functionality can be tailored or extended through the use of custom applications. Custom applications are user-developed software programs that can access and manipulate Exchange 2000 data, modify the format and display of Exchange 2000 data, or add new features to an Exchange 2000 server. Its extensible web and collaboration capabilities offer richer and more flexible customization options than were available in Exchange 5.5. The Exchange 2000 security options available to custom applications are also more granular than those available in Exchange 5.5, where security focused on setting folder permissions.

Creating custom Exchange 2000 applications requires access to Exchange 2000 data stored in the Active Directory (user and group information) and/or the Web Storage System (WSS, which contains data about Exchange 2000 resources). New in Exchange 2000, the WSS is a loosely structured database of mailboxes, folders, documents and other Exchange 2000 resources that gives developers new ways to access Exchange 2000 information store data. In addition to the Exchange 5.5 interfaces, Messaging API and Collaborative Data Objects (CDO), Exchange 2000 information store data are also accessible via XML, WebDAV, or Exchange OLE DB providers such as ActiveX Data Objects (ADO). Each piece of store data in WSS is considered an object, and URLs can be used to obtain access to these objects.

This chapter presents general application development security considerations, as well as those specific to data access, application extensions, and web applications. For additional information on developing custom Exchange 2000 applications, see *Programming Collaborative Web Applications with Microsoft Exchange 2000 Server* by Mindy Martin.

General Security Considerations

Programmers should take security into account before beginning custom Exchange 2000 application development. In particular, programmers should be cognizant of the application's intended users and relevant access needs and restrictions. For instance, application users should not be given permissions to privileged folders or other user

mailboxes. Exchange 2000 offers permissions, security descriptors, and exchange roles to help define and implement application security.

Permissions

As discussed in Chapter 3, permissions are privileges associated with Exchange 2000 resources. Resource permissions are extended or denied to Exchange 2000 users and groups. In addition to the standard read, write, delete, and create permissions, Exchange 2000 also provides more granular permission settings, including viewing folder contents, editing items owned by other users, and creating new child folders.

When developing Exchange 2000 applications, programmers should ensure resource permission settings do not allow unauthorized access to information about other users. For instance, applications that query mailbox information should not inadvertently allow users access to other user mailboxes. Resource permissions, however, should also be sufficient to enable authorized users access to and implementation of custom applications. Additional information about properly configuring permission settings is contained herein.

In addition to explicitly assigned permissions, resources can inherit permissions from parent objects. By default, new folders inherit permissions of parent folder(s). New parent folders, however, do not propagate inherited permissions down to pre-existing child folders. Items automatically inherit permissions of new or pre-existing parent folders, although they can be overridden on a per-object basis by disabling inherited permission propagation or modifying the child object's permissions. Permissions can also conflict with one another. For instance, a user is granted permission to view folder contents but a group the user belongs to is denied permission to view folder contents. In this and all cases involving a denied permission, the denied permission takes precedence.

Security Descriptors

The Exchange 2000 WSS also implements and extends the Windows 2000 notion of security descriptors. Security descriptors are sets of security-related attributes that are associated with each WSS resource. The security descriptor includes access control information and is used to define and determine what users, groups, and/or exchange roles can or cannot access a particular WSS resource. The Exchange 2000 server automatically compares the requesting user's Active Directory credentials with the discretionary access control list in the object's security descriptor to enforce a specified security policy. In order to extend security descriptors to Windows 9x objects, they are defined using XML. Security descriptor values can be set through the Exchange System Manager. Application developers need to understand how to define, access, and interpret resource security descriptors to extend this functionality to their application.

Exchange 2000 Roles

Exchange 2000 introduces the concept of *exchange roles*, a set of users and/or groups that a developer can create and assign permissions to. Similar to groups, exchange roles include a collection of users. Unlike groups, however, exchange roles are user-created, affiliated with a particular application and/or folder, stored on the object itself (versus defined and managed in AD), and do not require privileged access to AD services. Exchange roles represent groups of Windows 2000 users and/or groups that are used to define application-specific roles and properties, such as Editor, Last Reviewer, etc. Exchange roles are specified during code design, validated during run time, and populated by application user(s) during implementation. Unlike permissions,

parent object role properties are not inherited by child objects, unless programmers explicitly implement a specific inheritance solution (e.g., using move/copy event sinks). Moving and copying folders or items with associated roles, however, retains existing role properties. Application developers can use exchange roles to create flexible user groups for extending application-specific permissions.

Data Access Applications

The first type of application are those that access and manipulate Exchange 2000 data. Example data access applications include calendar scheduling, sharing, and publishing. Applications obtain Exchange 2000 data from the WSS (information about Exchange 2000 resources) and from Active Directory (information about domain users and groups). The security considerations relevant to each data access approach are explored in this section.

WSS Data Access

As described earlier in this guide, Exchange 2000 stores all its resource information in the information store or *WSS*. To access this data, developers can use ActiveX Data Objects (ADO), Collaboration Data Objects (CDO), HTTP, or XML. This discussion focuses on ADO and CDO-specific application development security considerations. ADO and CDO are server-based APIs that interact with the Exchange OLE DB (ExOLE DB) provider to obtain access to WSS information. ADO and CDO support all COM-based programming and scripting languages, to include Visual Basic, Visual C++, and VB Script, as well as Java and JavaScript. ADO is primarily used to perform simpler operations, such as traversing, querying, and setting WSS properties, whereas CDO is intended to support more complex, collaboration-focused activities.

Because ExOLE DB uses a pre-defined security context, applications using ExOLE DB interfaces ADO and CDO will attempt to execute regardless of what user and associated permissions are logged on. If a user has access to the application folders, he can read, modify, and run the application code. To prevent this vulnerable scenario, application developers should embed ADO and CDO applications in an ActiveX DLL to take advantage of COM+ role-based access control (RBAC). While the WSS folder permissions could be altered to control what users or groups can access and edit applications, these changes will not prevent the code from executing. Therefore, the most prudent approach when using ADO and CDO is to use COM+ RBAC. For more information on protecting ADO and CDO applications with COM+ RBAC, see *Programming Collaborative Web Applications with Microsoft Exchange 2000 Server* by Mindy Martin.

Active Directory Data Access

As Exchange 2000 uses Active Directory to manage user and group information within a domain, applications also need access to this data. Application access to Active Directory objects is provided through Active Directory Service Interface (ADSI), similar to that provided with Exchange 5.5, as well as CDO and ADO. In general, ADSI provides the most extensive set of AD object access capabilities, while CDO and ADO provide more focused AD access (e.g., to manipulate users, mailboxes, and folders).

Valid authentication is required before access to an AD object is extended. Security contexts containing credentials that validate a user and his ability to perform a particular task against a secured object provide the necessary authentication. Access to AD objects, therefore, is accomplished by extending a security context with the AD object

request. While supplying default credentials—those of the default or logged on and program executing user—is the preferred approach to AD data access, ADSI does support access using alternative credentials through explicit credential specification. By using the ADSI OpenDSOObject method of the IADsOpenDSObject interface, users can provide credentials of choice to access AD objects.

Extending Application Capabilities

In addition to Exchange 2000 data access and manipulation, developers can create applications that extend Exchange 2000 server capabilities. New capabilities include those created using Event Sinks and Workflow Logic.

Event Sinks

An Event Sink is a COM component that is activated to run on the Exchange server by a particular event, such as the reception of a new message. Event sinks are used to design simple tasks, such as sending a message when a file is added to a public folder, or complex tasks, such as scanning incoming mail messages for viruses.

Event sinks run in a separate process on the server from the WSS. As a result, the Exchange server requires authentication before executing event sinks. To accomplish this, event sinks should run under their own user accounts. This account should be afforded, at a minimum, access to the folder where the event takes place. Accesses beyond those necessary to implement the event sink should be curtailed.

Workflow Components

Exchange 2000 also supports the development of workflow applications to manage state associated with specified objects and actions. For instance, a workflow application could track the progress of a document requiring approvals from multiple users. Exchange 2000 provides two Workflow component security modes, restricted and privileged. Restricted mode limits what the developer and component can do. It acts as an application sandbox and prevents object creation. Restricted mode also limits the damage an unintended or rogue application (e.g., malicious code) could inflict upon the server. In contrast, privileged mode does not levy access restrictions on the application or developer; they operate with full system permissions. In order to run a workflow component in privileged mode, the developer must be part of the privileged workflow authors role.

Restricted mode is the default and preferred workflow security mode.

Web Applications

Forms are the most commonly implemented type of Exchange 2000 web applications. Forms are web-based templates for displaying Exchange 2000 data. There are two kinds of Exchange 2000 forms, WSS forms and Outlook forms. WSS forms are server-based forms that link and display Exchange 2000 data—specifically WSS data—in web pages. Sample WSS forms include those provided through OWA that enables web-based access to Exchange 2000 mailboxes and other data. Outlook forms, conversely, are client-based forms that display Outlook or client-accessible Exchange 2000 data and are developed using Outlook client software such as Outlook 98, Outlook 2000, or Outlook 2002. Example Outlook forms include custom contact forms that contain additional data fields (e.g., pager number).

Both types of forms can include executable code, such as VBScript and Visual Basic. Therefore, care must be taken to ensure that custom forms available for widespread use do not include malicious code or leave exposures that may be exploited. Be sure to separate development environments from operational systems and limit developer tools and development system access to trusted developers. Insist on thorough testing of custom applications before making them available.

The following sections provide specific security considerations for each type of form.

WSS Forms

The WSS and related WSS forms infrastructure enable forms to be applied at "run time" instead of being hard coded to a set of data. This means that different forms can display the same data back to different users, depending on the user's browser settings. For instance, a browser on a hand-held device, an older browser, and a Java-enabled browser may all use different forms to display the same data. Microsoft refers to this as a data-driven instead of forms-driven approach. The main underpinnings of this approach are *content classe*s, the *forms registry*, and the *WSS schema*. Content classes are indices that correlate Exchange 2000 data items with WSS forms. The WSS forms registry is a data store that stores forms along with their requisite content classes and browser settings. WSS forms are *registered* in a WSS through a forms registry, which is not related to the Windows 2000 registry. As the WSS is a loosely structured database, the WSS schema is the database schema equivalent of the, namely the set of properties associated with a particular WSS and its contents. The WSS schema can be extended to support custom, user-defined features such as new properties, content classes, and data items.

Ultimately, these elements work together to provide requested content in a tailored format back to the user. When a user requests information from a browser, a forms rendering process correlates requested user data with corresponding content classes, WSS schema, form registry, browser settings, and form.

Folder Permissions

The WSS form security considerations, therefore, center around establishing the proper permissions for the forms and their underlying infrastructure. Permissions for the folders containing each of the WSS form elements must be configured to prevent unauthorized access to the different form parameters. Folder permissions should be set as specified in Chapter 4. The folders listed should be configured to deny access to anyone but the Web application and system administrators. It recommended that anonymous access not be granted to any of these folders. The affected folders include:

- Public store folders where the web forms or applications are stored.
- WSS form registry folders.
- WSS schema folders that store form registry properties and values.
- Folders containing custom content classes.

In addition, the *virtual directory* permissions must be set properly. The virtual directory is the WSS construct through which browser access to WSS data and applications is provided. It is effectively another path to the form-containing WSS folder. The virtual directory access must be configured to limit unauthorized access without constraining use of and authorized access to the web application or form, as follows:

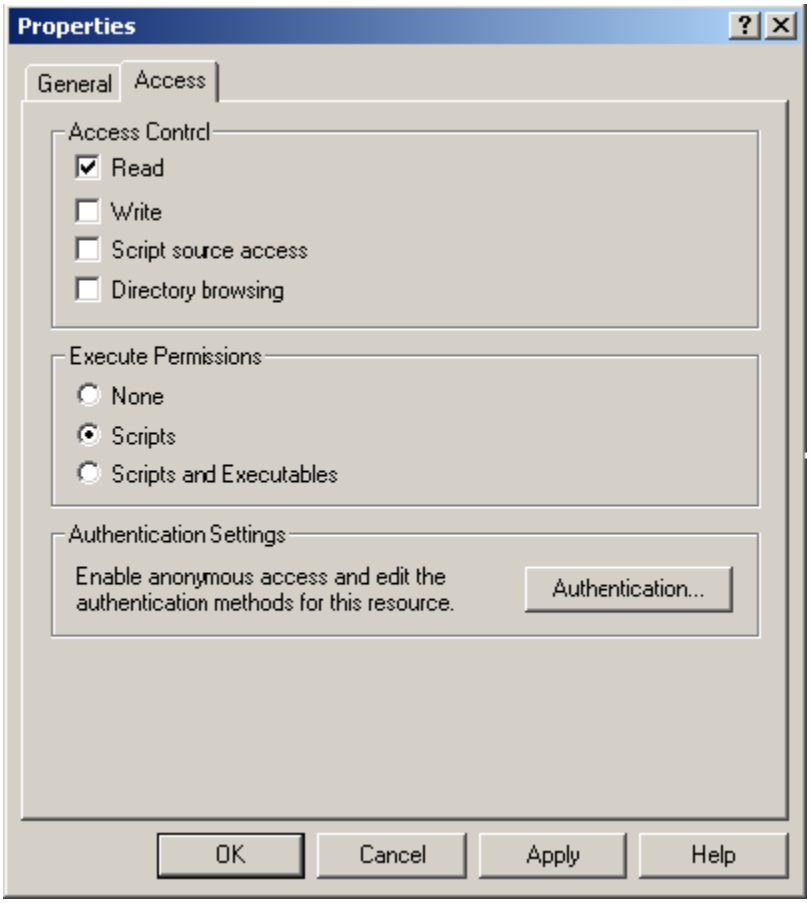

Figure 60. Virtual Directory Properties

To set browser access permissions for your web application or form:

- Open the Exchange System Manager.
- Go to the virtual directory folder, found under Protocols/HTTP/Exchange Virtual Server, and select the "Public Folder" folder or applicable sub-folder that corresponds to the public folder where your application is stored.
- Click on the *Access* tab.
- The top box in the pop-up window specifies what type of browser access to your web application is needed.
- If your application is a form, users should not need more than READ access to it, so check the READ box. For web applications that do not perform tasks requiring user interaction, user READ access may not be necessary; in this case, none of the access boxes should be checked.
- If your application, however, is a system administration tool or other privileged WSS interface tool, you may need to permit Write, Script Source Access, and/or Directory Browsing access as well. In this case, limit authentication options to Integrated Windows Authentication, as explained later in this section.
- The middle box in the pop-up window is called *Execute Permissions*.

- If your web application is a static web page that does not use ASP, other scripting language, or executable code, click None.
- If your web application uses ASP or other scripting language, click Scripts.
- If you web application uses scripts and executable code, click Scripts and Executables.

■ Keep the same pop-up window open to configure authentication options, as follows:

- Click on the Authentication button in the Authentication Settings frame. The Authentication Methods pop-up window appears as shown in Figure 61.

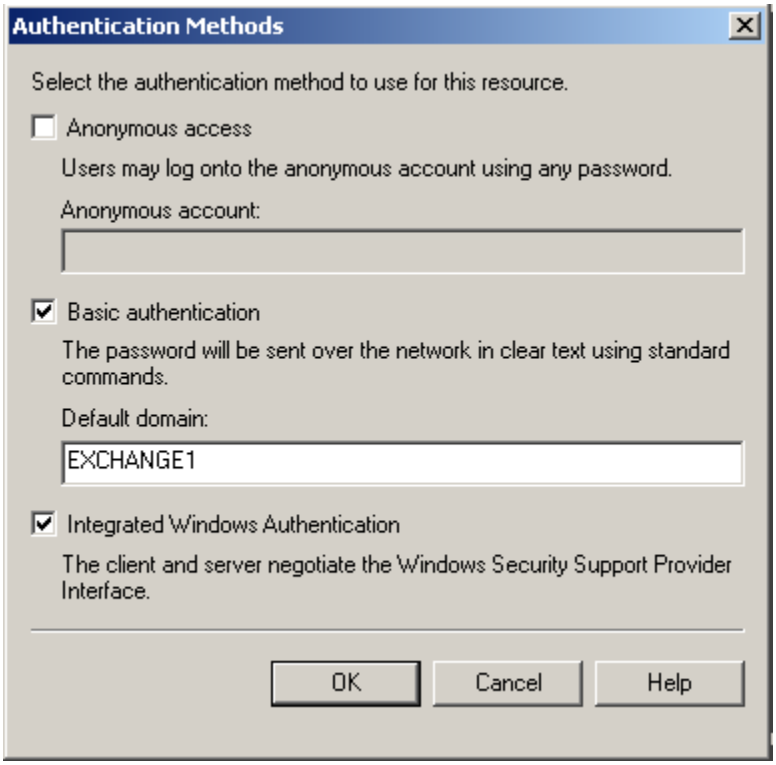

Figure 61. Authentication Methods

■ Restrict access to your web application to authorized domain users by unchecking the box next to Anonymous access.

■ Windows 2000 needs to authenticate each web application user in AD in order to turn anonymous access off.

■ Select Basic Authentication and/or Integrated Windows Authentication. For the former, enter a default domain name and use SSL if it is desired to protect the passwords in transit. Integrated Windows Authentication will also allow for authentication without passing passwords on the network.

If you are using COM+ roles with your application, Anonymous access must be disabled.

To extend access to non-Exchange 2000 users, check the box next to Anonymous access and specify a user account with standard access rights that the code in the web site executes as.

Outlook form security also focuses on folder permissions, as is explained in the following section.

Outlook Forms

Unlike WSS forms, Outlook forms are MAPI-based, are stored in MAPI-based folders. They can access WSS data, too, but require additional code to map some of the WSS resources to the MAPI namespace.

Folder Permissions

The main Outlook form security concern is setting permissions on the folders containing the forms. To be usable by others, Outlook forms are generally placed in public folders and/or published in an organizational forms library. Ownership rights to these folders should be limited to trusted developers and administrators inasmuch as owners have ability to add custom code to the forms that bypasses the macro security features described in Chapter 2.

To administer the organizational form libraries, select the **Public Folders** tree, click on **Action/View System Folders**, and navigate to the organizational forms library under the Eforms Registry container. By default, no organizational form libraries are configured. See Chapter 2 for more information on configuring Outlook folder permissions.

Password Protection

Password protection should be used to prevent unauthorized modification of custom web applications or forms. Passwords are assigned in the properties page when in form design mode by selecting the **Set Password** button on the **Properties** tab. Use of a robust password, a non-dictionary word that includes non-alphanumeric characters, is recommended.

Important Security Points

In conclusion, Exchange 2000 offers developers a lot of options for incorporating security into their applications. The main security points are summarized below.

- Use Exchange Roles to define and manage a set of application-specific users and/or groups who have the same access needs.
- Note that Exchange Roles do not inherit properties from parent roles unless explicitly specified using move/copy event sinks.
- Embed ADO and CDO applications in an ActiveX DLL to take advantage of COM+ role-based access control.
- Access to AD objects requires a valid security context with the AD object request.
- Use the restricted workflow component security mode to limit unintended consequences of application development, as well as prevent malicious code execution.
- Disable anonymous access to limit web application access to authorized domain users. Use Integrated Windows Authentication.

- Limit access to developer tools, such as Visual Basic and Exchange Forms Designer, to trusted developers to prevent development of malicious applications.
- Protect Outlook forms by using passwords.

This Page Intentionally Left Blank

Chapter 11

Extending the Exchange Environment

Introduction

While the other chapters of this document focused primarily on setting up the internal mail server (reference the *Microsoft Windows 2000 Network Architecture Guide*), this chapter will detail several methods for extending the Exchange environment to less trusted domains. This chapter presents a series of solutions which address a range of capabilities starting with the simple need to send and receive e-mail with users on the Internet and concluding with the much more involved solution of giving users located on external networks full access to the internal Exchange environment. Each of these solutions represents a tradeoff between security and functionality.

The reader needs to consider two points when reviewing this chapter. First, it is impossible to fully anticipate the range of network architectures to which the guide may be applied. For that reason this document can not be all-inclusive – there may be additional steps that are required related to DNS setup, firewall filtering, and a host of other issues that are not detailed in the solutions that follows. Please consider this as an outline of how Exchange should be configured, not as a complete prescription for setting up the network. Second, only local authorities can decide which of these solutions is best given the nature of data on the network and the features that are desired. Consider the advantages and disadvantages of each solution given the threat environment.

Solution 1 – Mail Forwarder

This solution allows users in an Exchange 2000 environment to send and receive SMTP e-mail to/from an external network such as the Internet.

There are several risks associated with the receipt of e-mail from potentially untrusted entities outside the site. Chief among these concerns are attacks against the recipient's e-mail environment. Examples of this include attempts to exploit buffer overflows and content driven attacks in the form of malicious code.

The mail forwarder is simply a mail server that sits in a demilitarized zone and forwards e-mail messages intended for internal users to the internal mail server. It likewise accepts mail destined for the external network for delivery. As the mail forwarder is the only mail server that is exposed to the external network, the risks associated with e-mail are somewhat reduced by limiting the exposure of the internal mail server to the untrusted environment. This mail forwarder must not be a member of any internal Windows 2000 domains so as to help limit the damage that could result from its compromise. The mail forwarder simply accepts messages from the internal mail server for delivery to the Internet and vice-versa. Content checking, initial virus scanning, and filtering ideally should also be performed here to guard against malicious code.

Figure 62 illustrates this solution.

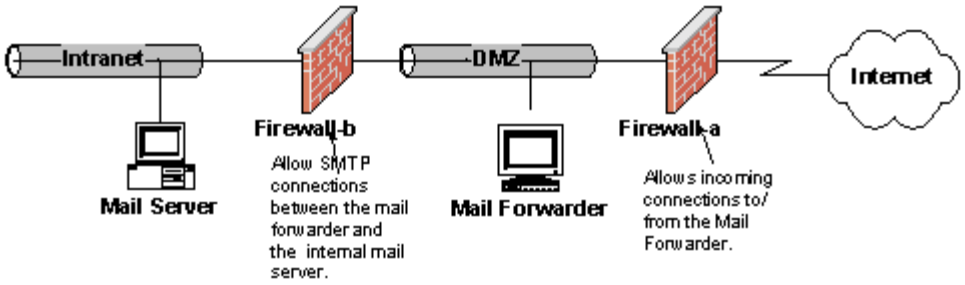

Figure 62. Mail Forwarder Solution

The Exchange Server on the internal network (labeled *Intranet* in the figure) is configured to use the mail forwarder as its *smart host*. To access this setting open the *SMTP Virtual Server Properties* page, select the *Delivery* tab, and click on *Advanced*. Figure 63 illustrates the proper settings[17]. Note that the option to attempt direct delivery before sending to smart host is selected. This allows users on the Intranet to send SMTP messages to both the Intranet and Internet.

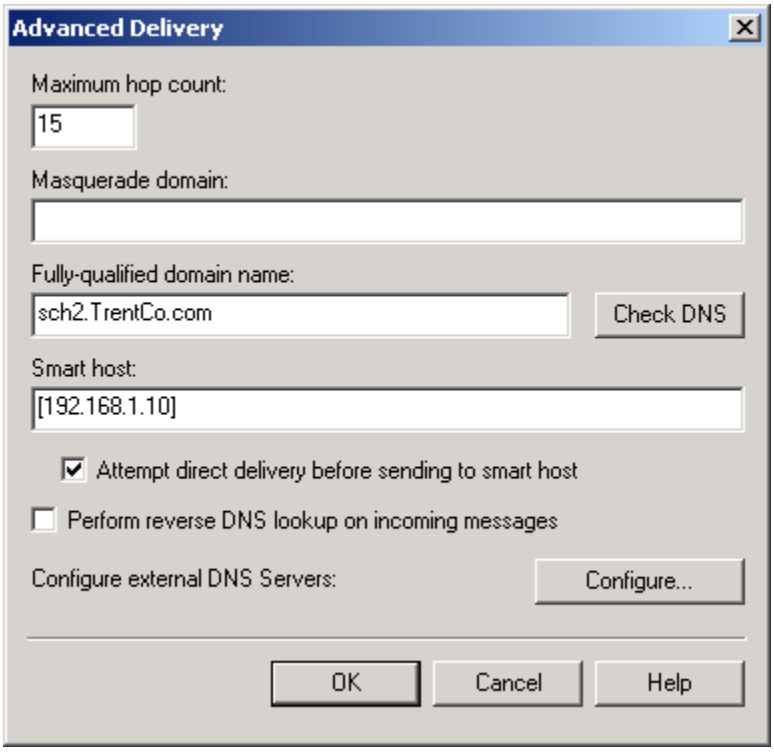

Figure 63. Advanced Delivery Options

Firewall-a is configured to allow SMTP connections in both directions. This will allow the mail forwarder to both send and receive e-mail on behalf of the organization. Firewall-b is configured to allow STMP connections in both directions as well, but only between the internal mail server and the mail forwarder.

[17] As an example of the various approaches that could be used to implement this concept, connectivity could also be achieved through use of a SMTP connector in lieu of applying the settings to the SMTP virtual server. The approach one would take depends on the overall network architecture.

The mail forwarder is likewise configured to forward messages destined for the Intranet to the internal mail server[18]. It is this mail forwarder that is advertised via the Domain Name Server (DNS) as the mail server for the organization. Mail sent from the Internet to the organization will be received by the mail forwarder and subsequently sent to the internal mail server. Content checking such as virus scanning should be performed in the DMZ and the mail forwarder should be made as secure as possible by applying the applicable OS guidelines and disabling all unnecessary services.

Any time e-mail from an untrusted source is allowed into an organization there is a risk that an attacker can take advantage of that path. The advantages of this approach are in its simplicity. Full e-mail connectivity is provided with minimal additional hardware and the impact to the firewall rule set is very limited – only the SMTP port has to be opened. Additional benefit is derived from the fact that the mail forwarder offers an excellent place to focus malicious code countermeasures; however, it should be noted that this can not be a replacement for malicious code countermeasures on the client machines as encrypted messages can not be effectively scanned in transit. Finally, the option of reader-writer encryption is preserved with this solution through the use of S/MIME.

The disadvantage of this approach is that is strictly intended to allow internal users to send and receive mail to/from the Internet or other external network. It does not provide a means for users to access their Exchange mail store from the external network as might be required, for example, to support users who are traveling.

Solution 2 – Front-end/Back-end Servers

The second solution deals with a scenario where it is necessary to give users access to the Exchange environment from an external network such as the Internet. This situation could arise in support of employees who are traveling or to support an external partner, for example.

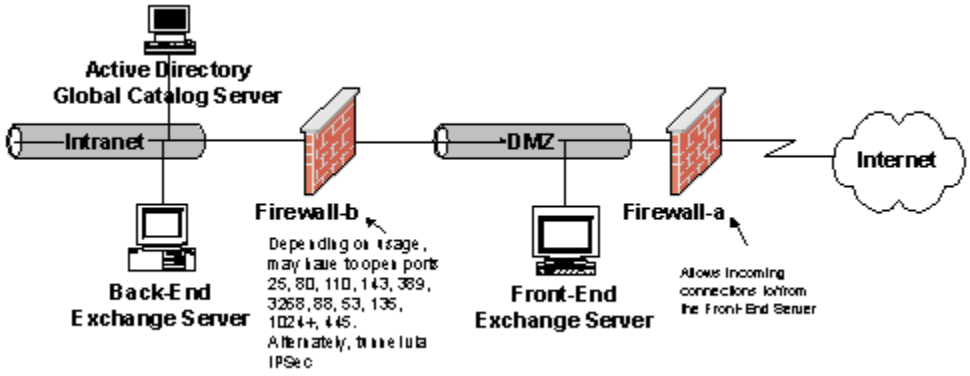

Figure 64. Front-end/Back-end Servers

The basic tenet of this solution is the concept of a back-end, front-end server. Microsoft has provided this capability in Exchange 2000 primarily as a means of loading sharing tasks between Exchange Servers. Under this architecture users can connect via POP3, IMAP4, or HTTP to a front-end server. This front-end server does not hold any mail accounts but simply forwards the request to the Exchange server where the users mail folders and public folders reside. It determines which Exchange server to forward the request based upon an Active Directory query.

[18] The mail forwarder could be another Exchange server or any of a number of other SMTP servers.

This architecture can be implemented with the front-end server placed within the DMZ in order to offer the internal network a measure of protection. This would allow external users to connect to the front-end server from the external network with the request forwarded to an internal back-end Exchange server. SSL can be used between the front-end server and the user to protect the data in transit. This architecture is illustrated in Figure 64 and is described in detail in a Microsoft white paper, *Exchange 2000 Front-end and Back-end Topology,* available at http://www.microsoft.com/exchange/techinfo.

The advantage of this solution is that it gives users more complete access to the Exchange environment than was available under the mail forwarder solution. Users can send and receive mail and, if using Outlook Web Access, access their calendars. This solution has a very notable drawback in that it requires the opening of a large number of ports on the internal firewall (firewall-b). If an attacker compromised the DMZ, this could place the internal network in jeopardy. This solution is generally not recommended if sensitive data exists on the internal network, but as always a final decision in this regard would be under the purview of local authorities.

Solution 3 – Terminal Server

Microsoft Terminal Server offers an interesting mechanism for extending the Exchange environment in a more secure manner. Terminal Server allows users to log into a Windows 2000 server and to execute their desktop on that machine. Only mouse movements and keyboard entries are sent from the client machine to the Terminal Server and only screen refreshes are returned – all execution occurs on the Terminal Server computer.

This ability to restrict where the user is executing programs can be used to reduce the risk of the extending the Exchange environment outside of the trusted network. In this example, users on the internal network log into a terminal server machine in the DMZ to execute their mail clients. The mail client executes exclusively on the terminal server

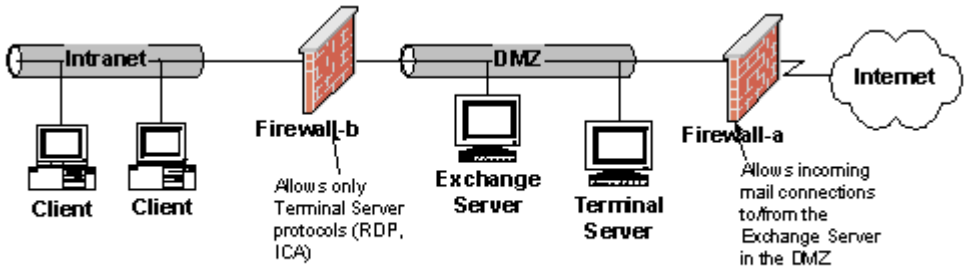

Figure 65. Terminal Server Solution

computer with only screen refreshes being passed back to the client machine. While malicious code could still do damage to the terminal server computers and the data that resides on them, if the firewall is sound damage should be limited to the DMZ. Also, it is administratively easier to concentrate countermeasures on the terminal server machines vice having to apply them to a plethora of client machines. The figure below outlines the concept. Note that the firewall between the terminal server and the user workstations (firewall-b) only allows terminal server protocols to pass. These are the protocols necessary for screen refreshes to pass to the client. By blocking all other protocols, any malicious code is limited in its potential "reach" to the terminal server computers where countermeasures could be strenuously applied. As is always the case when configuring

a DMZ, the computers within the DMZ should not be part of any internal Windows domain.

Access to users on the external network (Internet) can be granted by allowing them to connect to the Terminal Server via Firewall-a. This would allow roaming users complete access to Exchange data including their calendars, to-do lists, and etc.

This approach has several advantages. First, it can be scaled to simply allow internal users to share e-mail with users on the Internet or it can be used as a way of supporting users who need access to the Exchange environment from the external network. Second, when used in conjunction with a sound firewall policy it restricts the ability of malicious code to compromise data on the internal network. Finally, having all e-mail execute within a fixed number of terminal server machines can reduce the administrative burden of applying malicious code countermeasures.

There is one notable disadvantage. Under this scenario all Exchange data is stored in the DMZ and would be subject to compromise in the event that the DMZ is successfully attacked. If this is a concern the risk can be mitigated by giving users two Exchange accounts – one which resides in the DMZ and reserved for non-sensitive data and another on the Internal network which would be used for data requiring greater protection.

The use of the Terminal Server solution has it's own unique set of security concerns; reference NSA Guide, *Guide to Securing Microsoft Windows 2000 Terminal Services*.

Solution 4 – Remote Access

The Remote Access Service (RAS) can be used to allow users to dial into the network and obtain complete access to the internal network. This kind of access should not be used unless absolutely required for operational reasons; however, if remote access is required there is information available on securely connecting to networks using the Remote Access Security Program (RASP) which can use devices such as FORTEZZA modems for dialing into networks. More information on this technology is available at http://ias.itserealm.com/rasp.

Important Security Points

- Consider that extending the Exchange Environment cannot be accomplished without increased security risk. One should weigh the operational benefits verses the risk carefully before proceeding.
- Consider the use of a mail forwarder or terminal server architecture if it is necessary for users to send mail to/from the Internet.
- Consider the use of a terminal server architecture if it is necessary to extend the Exchange environment so those external users have full connectivity to their message store. A front-end, back-end architecture or dial-in access can be used as well but is generally not preferred.

This Page Intentionally Left Blank

Chapter 12

Chat Services

Microsoft Exchange Chat Service provides an environment for online group discussions. One Chat server can handle up to 20,000 concurrent users in one chat room. Each administrative group in the Exchange System snap-in can have only one Chat Communities container in which multiple virtual chat communities can be created. Each chat community can host multiple chat rooms, or channels, and can be governed by its own administrative controls.

The Chat Service of Exchange 2000 Server is based on the Internet Relay Chat (IRC) protocol, which supports real-time conversations between two or more users. With IRC, people meet on channels to communicate in public or in "private". In this usage, privacy relates only to restricting who can join a chat; it is not a reference to robust data confidentiality. It is very important to note that the chat service does not provide any native means of providing data encryption; messages are always transmitted in the clear unless protected by another form of virtual private network. Chat should never be used for sensitive traffic unless encryption is employed.

Chat Service operates independently of other servers running Chat Service, using separate user and channel lists. Users contact Chat Service over TCP port 6667, which is usually the port number assigned to the first chat community although other port numbers can be used if necessary. Any IRC-based client that is RFC 1459 compliant, such as mIRC, will work.

Communities

When the Chat Service is installed, a chat community named Default-Chat-Community is automatically created in the First Administrative group. This community can be renamed if necessary, and additional chat communities can be created under other administrative groups. To create a chat community, start the Exchange System snap-in, right-click **Chat Communities**, point to **New**, and then choose **Chat Community**.

Figure 66 illustrates the property page for the Default-Chat-Community.

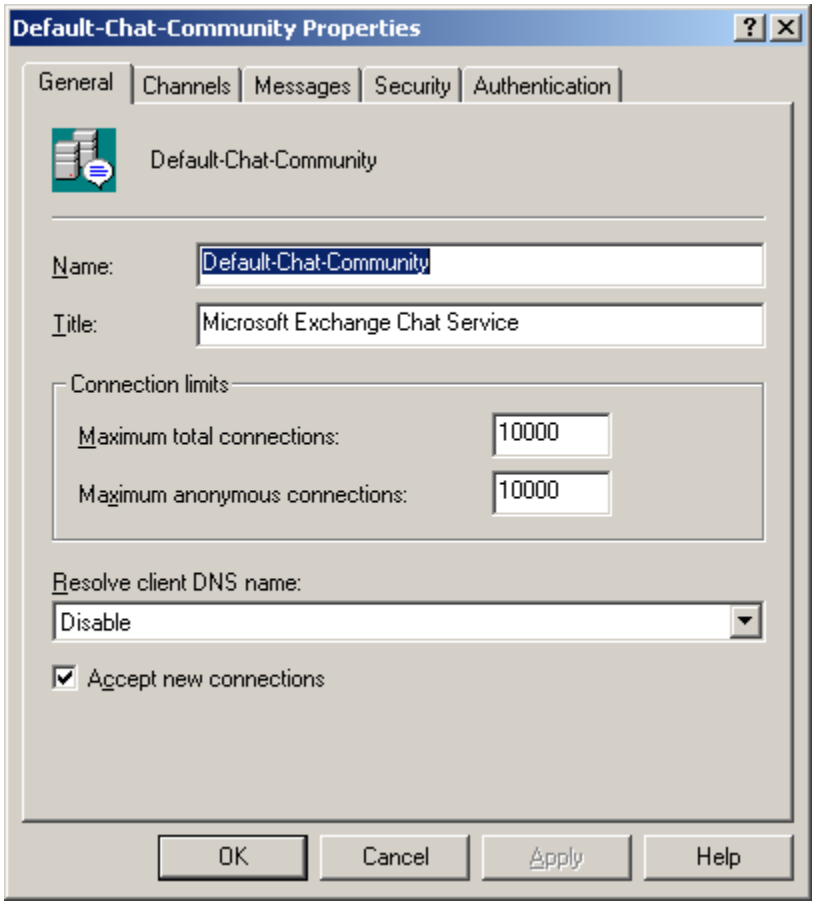

Figure 66. General Tab of the Chat Communities Property Page

General Tab

Under the **General** Tab, the connection limits can be set. The value set for **Maximum Anonymous Connections** must be less than or equal to the one for **Maximum Total Connections**. The default for both is 10,000, and the range for both is 0 to 99,999,999. These should be set consistent with their use and should not be set to arbitrarily high values to mitigate denial of service attacks.

There is a setting to specify if client DNS names should be resolved. This is a security measure. The choices are *Disable*, *Attempt*, and *Require*. The Disable option directs the server not to attempt IP-to-host-name resolution of the chat client. This is the least secure option, especially if the community is available to clients on the Internet. The Attempt option directs the server to try host-name-to-IP resolution. If a valid DNS name is returned, the server allows the client to connect to the chat community. Finally, the Require option directs the server to look up and resolve the IP address of an incoming chat client. If no valid DNS name is returned, the client connection is refused. This is described as the most secure option in the Exchange help file, but it is not a substitute for more rigorous access control measures. The Require option could serve as a limited means of access control to ensure only legitimate clients on a closed network are able to connect. It is of little utility in Internet environments, as the ability to successfully resolve a client DNS name is hardly an indicator of benign intent.

Channels Tab

The **Channels** tab is shown in Figure 67. This tab is used to configure channel defaults and to allow dynamic channels for a chat community.

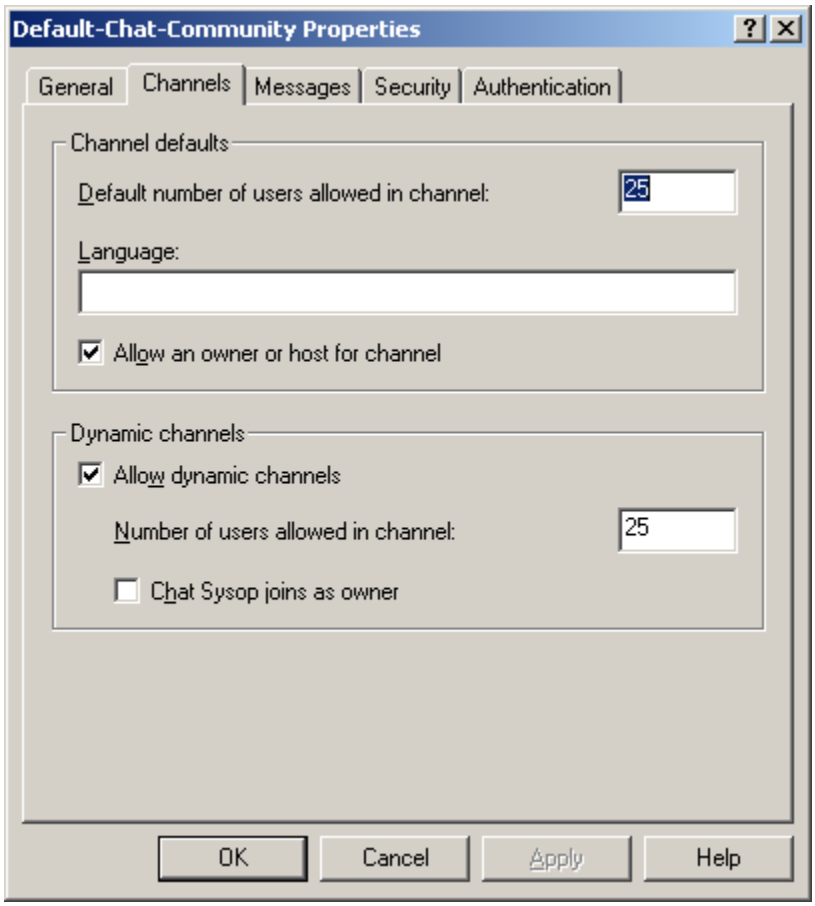

Figure 67. Channels Tab of Chat Communities Property Page

When selected, the **Allow an owner or host for channel** check box permits any user who creates a persistent or dynamic channel to become the channel owner or host.

The **Number of users allowed in channel** field controls the maximum number of users allowed on any dynamic channel in the chat community. The default is 25. The value must be between 0 and 99,999. A value of 0 permits unlimited membership in the channel.

The **Chat Sysop joins as owner** check box grants owner status to chat users with sysop permissions when they join a dynamic channel. Registered channels are not affected by this setting.

Security Tab

The Security Tab is shown in Figure 68.

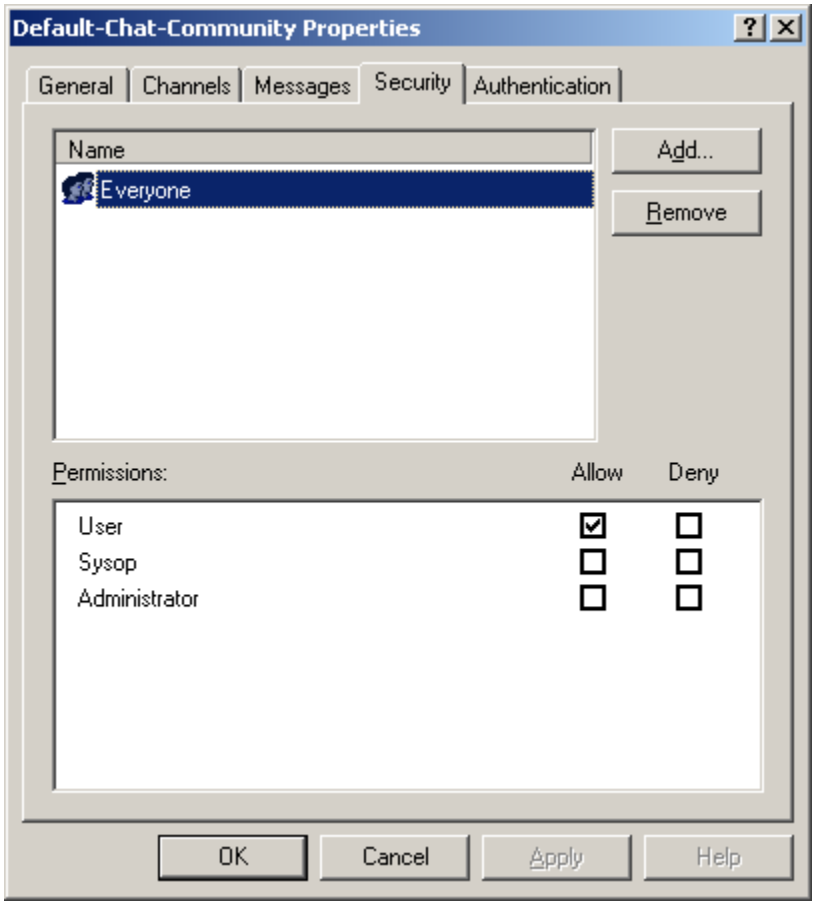

Figure 68. Security Tab of Chat Communities Property Page

The Security Tab shows the Chat roles that can be assigned to users and groups in a particular Chat community. These roles are:

User: A user can logon to the community from a chat client as an authenticated member. Assign this permission level to those who want to use the chat community.

Sysop: Sysops use a chat client to monitor and control a server's dynamic channels, in addition to any registered channels to which they have access. Sysop permissions allow the administration of the service using chat protocol commands (MODE, ACCESS, KILL, and so on) from a chat client. Sysops have no special permissions in a channel unless **Chat Sysop Joins As Owner** is selected in the **Modes** tab of the channel.

Administrator: Administrators become the owners of any channels they join and cannot be denied access to or removed from any channel. Administrators can also use administrative commands not accessible to other users and can override any action a sysop initiates, such as a user ban.

It is a good practice to assign permissions, such as Sysop, to groups rather than individuals to simplify administration. Individuals can simply be added to or removed from the group whenever required.

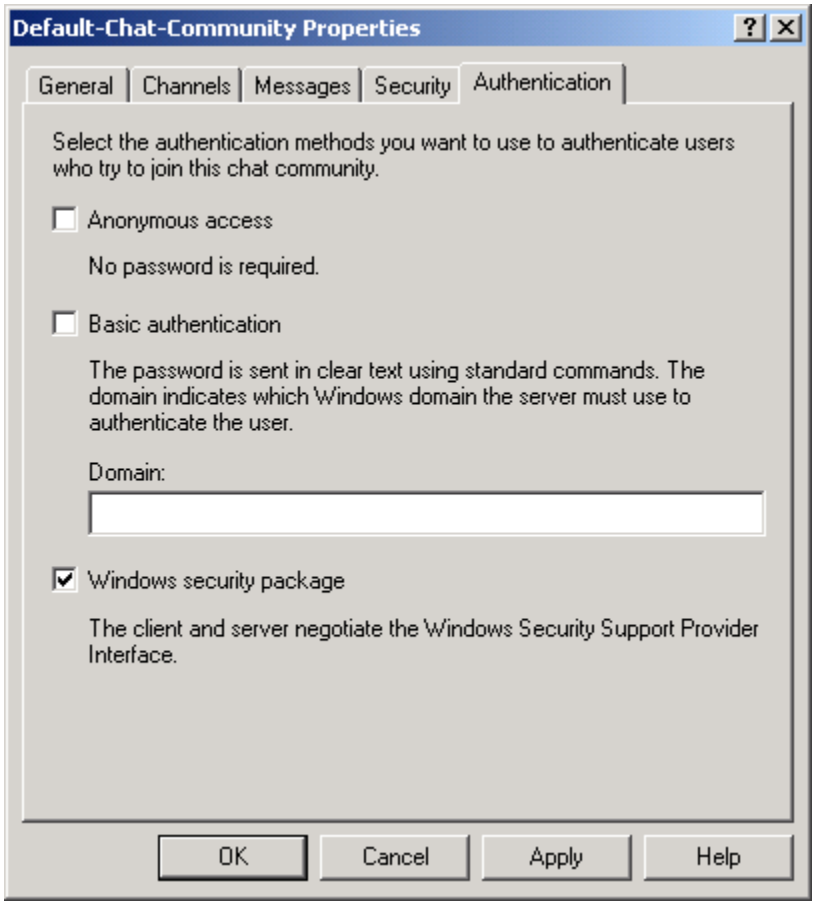

Figure 69. Authentication Tab of Chat Communities Property Page

Authentication Tab

Figure 69 shows the Authentication Tab of the Communities Property Page. The Authentication tab is used to configure the authentication methods for the chat community. These methods (as previously described) use Active Directory security features for all user accounts. The Windows security package is the most secure option, but only works in homogenous Windows environments.

Enabling Server Connectivity

A chat community must be connected to a server. This is accomplished in the Exchange System snap-in. Navigate to the IRCX container under the server object that will host the chat community, right-click IRCX, and choose Properties. On the property page, click Add. In the Add Community list, select the name of the chat community to be added to the server. Select the **Enable Server to Host This Chat Community** option. In the IP Address field, a unique IP address for each community is added. The default TCP port is 6667. Communities must have a different port or a different IP address.

Removing or Disabling a Chat Community

A chat community can be removed in three different ways. The first way is to remove a chat community's association with a server. This can be accomplished from the IRCX property sheet by selecting the community and clicking *Remove*. The second method disables a chat community temporarily, retaining the community's association with the server and also retaining the community and its configuration for future use. In this case, clear the **Enable Server to Host This Chat Community** check box in the property page for the chat community. The third method removes a chat community entirely from a server by deleting the community from the container for that chat community.

Channels

A channel (chat room) is a virtual place where users meet to exchange information. When a user joins a channel, the user can read anything that is typed to members of the channel. There are two types of channels, registered and dynamic. Registered channels are permanent channels that are created by a system administrator. Registered channels have two categories: those that start when a user joins the channel and those that start automatically when Chat Service starts. Any started channels that are not secret or hidden are visible and can be displayed in a chat client with the List or Listx command.

Dynamic channels are temporary channels that a user creates from the client by using the IRC Join command or the IRCX Create command. A channel host manages a channel from the chat client. Only dynamic channels have channel hosts. The first person to join a channel automatically becomes the channel host. This status can be shared with other chat users. The user who is the channel host is also referred to as a channel operator.

Security Background

Channels can be configured to be either secure, cloneable, or both. A secure channel is one to which access is restricted. As there are no encryption capabilities, the channel cannot be truly secure. A channel can be restricted to allow only authenticated users, invited users, or users who enter the correct password. In addition, channels can be restricted by identifying only a group of user accounts or a selected number of group accounts as channel users. Finally, channels can be moderated, meaning that only those who have been granted a "voice" can speak.

A cloneable channel is a registered channel that automatically duplicates itself when its member limit is reached. Any security settings that are configured for the initial channel will be duplicated in the new channel. A sysop is a user who monitors and controls a chat community's dynamic channels—as well as any registered channels to which the sysop has been given permissions—from a chat client. The sysop can also close a channel by using the IRC Kill command without having owner privileges on that channel. Sysops have no special permissions in a channel unless **Chat Sysop Joins As Owner** is selected on the channel's Modes tab.

Creating a Channel

To create a new channel, open the Exchange System snap-in, right-click the **Channels** container under the chat community, point to **New**, and then choose **Channel**. The property page for the new channel appears. On the General tab, the channel is named, and the topic and the content rating of the channel are entered.

The **Create This Channel When The Service Starts** check box makes the channel available whenever the Chat Service is running. If this box is not selected, the channel will become visible only when a user joins it.

Access Tab

Figure 70 shows the access tab of the channels property page:

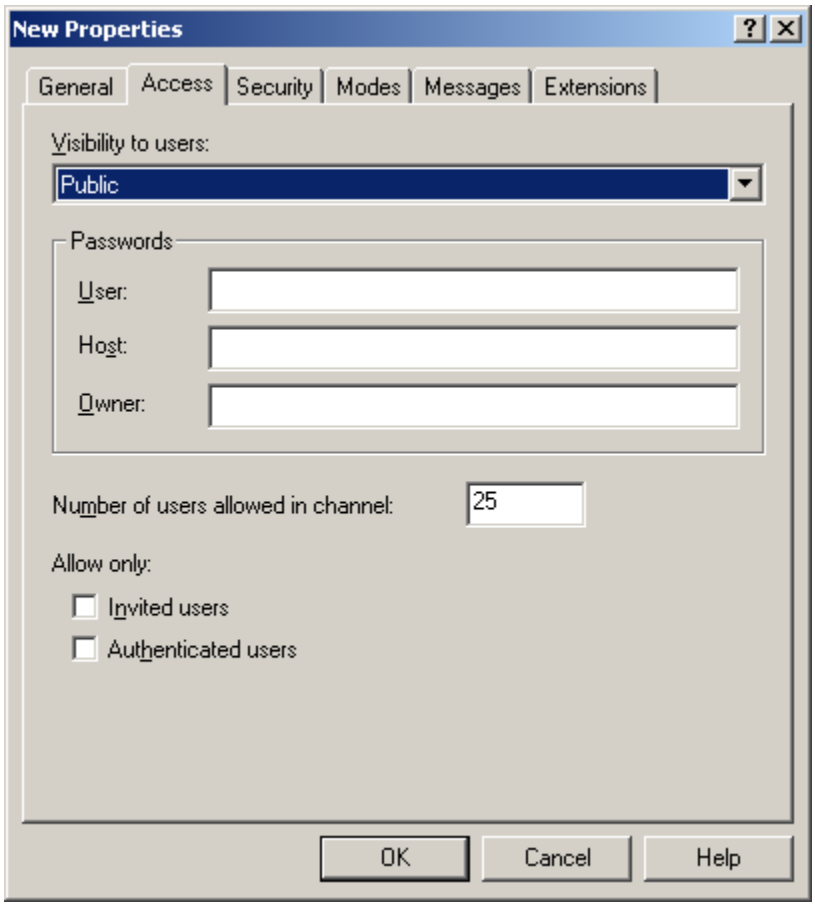

Figure 70. Access Tab of Channel Properties Page

Channel modes can be configured on the Access tab. These modes control a channel's visibility to users. They are as follows:

Public: Nonmembers can obtain all information about the channel (except for text messages) from a chat client by using the IRC List command.

Private: Nonmembers can obtain only the name, number of members, and PICS property of the channel from a chat client by using the IRC List command.

Hidden: A hidden channel is the same as a public channel except that it cannot be found by using a List or Listx command. If you know the exact channel name, however, you can obtain all of the properties of this type of channel from a chat client by using IRC and IRCX commands.

Secret Nonmembers cannot use queries to locate the channel.

Passwords can be set for users, host, and owner. These passwords, specific to the channel, are in addition to any account passwords used for authentication using the mechanism selected in Figure 69.

Options are provided to allow access by only invited and authenticated users. If **Invited users** is selected, users cannot join the channel unless specifically invited by the channel owner using the **/INVITE member [channel name]** command. If the **Authenticated users** checkbox is selected, only users who successfully authenticate using basic authentication or the Windows security package (selected as illustrated in Figure 69) can connect to the channel.

Security Tab

The **Security** Tab of the property page is shown in Figure 71:

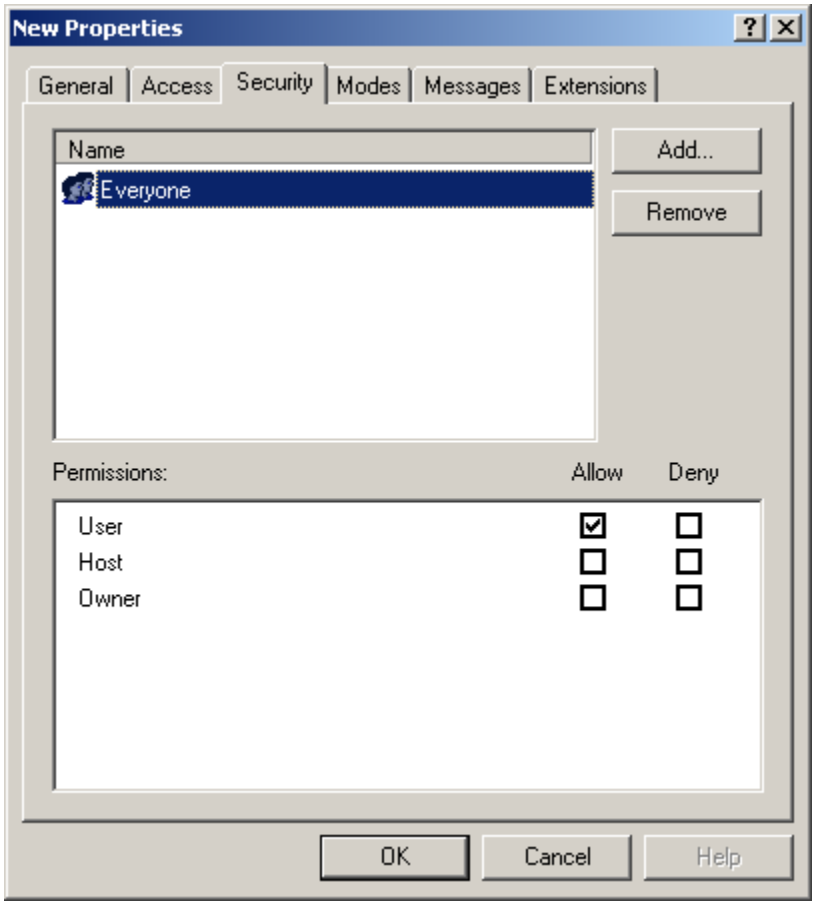

Figure 71. Security Tab of the Channel Property Page

On this page, channel permissions can be set for users and groups. The settings are:

User: A Chat User is a client connected to the server.
Host: A Channel Host, also referred to as a channel operator, manages a channel. Hosts may change access for their channel. Hosts may not remove access added by owners.
Owner: A Channel Owner manages a channel and the channel hosts. Owners may change access for their channel.

Modes Tab

The **Modes** Tab of the property page is shown in Figure 72:

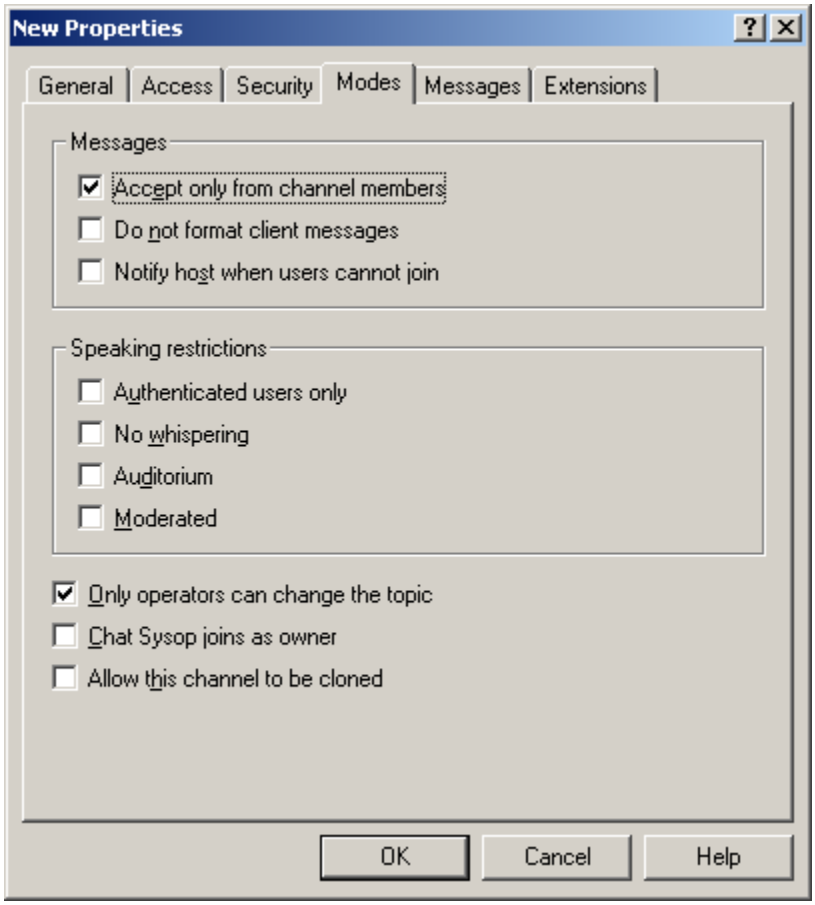

Figure 72. Modes Tab of Channels Property Page

There is an option **Allow this channel to be cloned** that allows cloning. A cloneable channel is a registered channel that duplicates itself when its member limit is reached. The limit is 99 clones. Each clone retains the properties of the original channel but is a separate channel. There are speaking restriction options, such as defining a moderated channel. A chat user joining a moderated channel cannot post messages to the channel without permission but can see messages posted by the designated speakers. Access to a channel can also be limited to invited users or to authenticated users, as detailed above. These settings allow for controlled access channels.

Extensions Tab

Under the **Extensions** Tab is an option for a transcription extension that transcribes conversations occurring on one or more registered channels and saves these transcriptions to a directory named after the community. Each transcript file is saved to a folder with the same name as the channel.

Each transcript file contains all messages sent publicly to a channel within a 24-hour period (12:00 a.m. to 11:59 p.m.). When a user first joins a channel that has transcription enabled, the user is informed of that fact immediately upon entering the chat room. The default location for transcripts is the C:\Exchsrvr\Chatdata\Transcript folder. The location of the transcripts can be changed in the channel transcript extension properties. Once the change has been made, the Chat Service must be stopped before the new

configuration will take effect. By default, only public messages are transcribed. This option can be useful in investigating possible security problems.

Classes

User connections to a chat community can be controlled with user classes and/or bans. User classes can be used to control connections by a group of users without the need to create a security group in Active Directory. When a user logs on to Chat Service, the service searches the existing classes in alphanumeric order by class name. The selection criteria for each class are applied against the user. Chat Service adds the user to the first matching class and applies that class's restrictions to the user. The user is added to the first class that it satisfies. This ends the search.

General Tab

To create a user class, start the Exchange System snap-in, right-click the **Classes** folder under the chat community, point to **New**, and then choose **Class**. Figure 73 shows the General tab of the property sheet for a new user class:

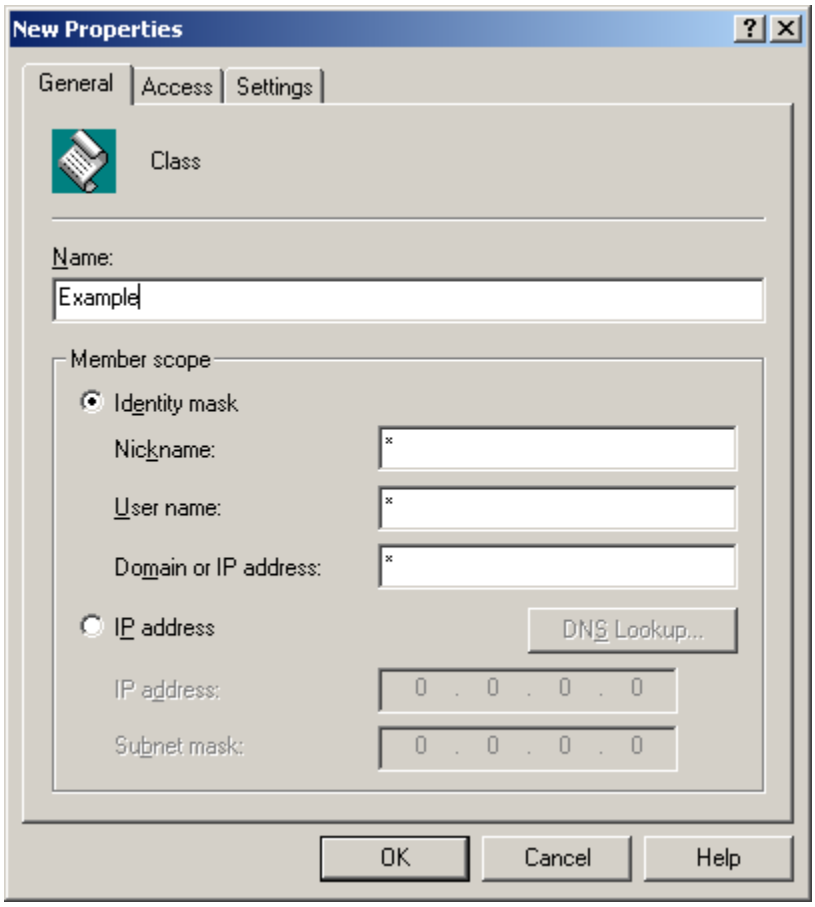

Figure 73. General Tab of User Class Property Page

Members of the class can be defined either by filling in the three fields in the identity mask or by specifying an IP Address and subnet mask. Wild card characters asterisk ("*") and question mark ("?") can be used in the identity mask fields. For example, an

asterisk in the nickname field would mean any nickname could be used. Bill* in the user name field would mean any user name starting with the characters “Bill”, while *.com in the domain field would mean any domain ending in “.com”. All three fields together are used to determine class membership.

Access Tab

The fields under the **Access** Tab can be used to restrict members of the class. The class members can be restricted to Anonymous or Authenticated logons, or they can be allowed both Anonymous and Authenticated access. Members can be restricted from logging on, owning or hosting channels, creating dynamic channels, or joining dynamic channels. The times of day a class can be active can also be set.

The **Hide class members’ IP addresses and DNS names** check box should be enabled to preclude this information from being shared unnecessarily. Doing so will deny a potential attacker a vital piece of information should they decide to launch an attack against a chat user. Figure 74 shows the **Access** Tab:

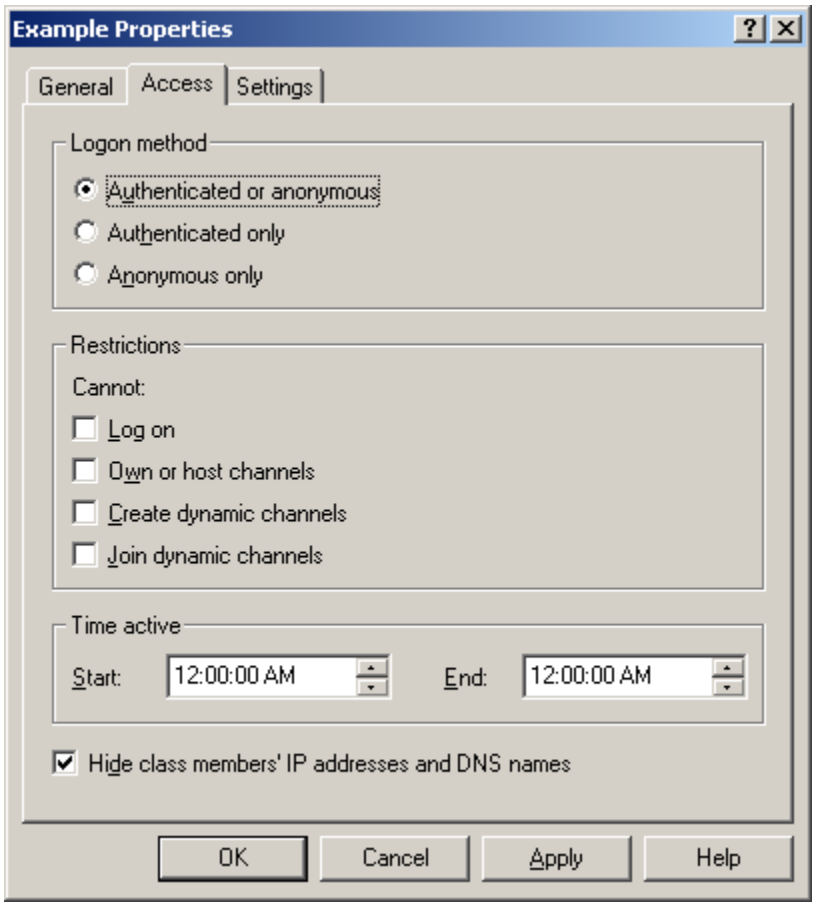

Figure 74. Access Tab of User Class Property Page

Settings Tab

Figure 75 shows the **Settings** Tab of the User Class Property Page.

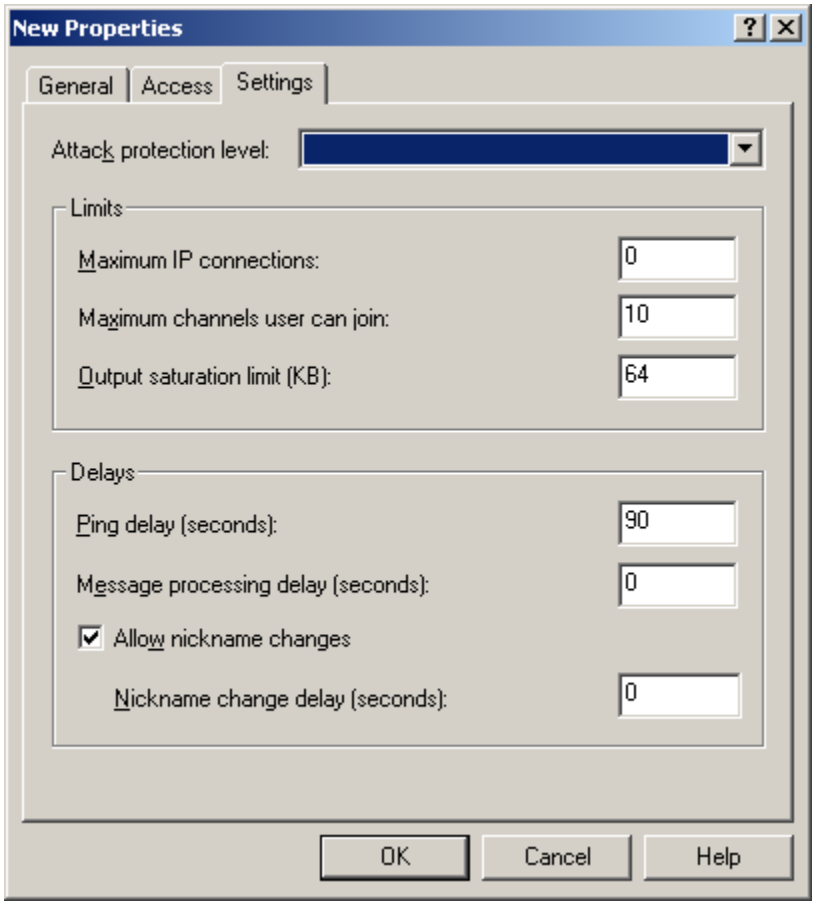

Figure 75. Settings Tab of User Class Property Page

The **Attack protection level** sets protection levels to prevent denial of service attacks. There are four choices for the attack protection level: None, Low, Medium, and High. If Chat Service detects any of the events shown in Table 14, it temporarily suspends the user's session. After the delay expires, the service resumes normal message processing. As shown in Table 14, each attack protection level corresponds to a delay time in seconds, based on the type of message or event. The attack protection delay is added to the message processing delay and the channel lag delay. The channel lag delay adds a delay to any message sent to a channel. This delay is added to any other delay that is in effect. This delay is set with the IRCX Prop command. The delay has a value of from 0 to 2 seconds. The default setting is 0 (no lag). The Prop command can only be set by a chat administrator or chat sysop.

Table 14. Attack Protection Levels (in seconds)

Message Type or Event	None	Low	Medium	High
Data	0	1	2	3
Invitation	0	2	4	5
Join	0	2	3	4
Wrong channel password	0	2	4	5
Standard message, such as a Privmsg, Notice, or Whisper command	0	1	2	3
Message from host to channel	0	1	1	2

In the Limits area, the following values can be entered:

Maximum IP connections controls the number of connections per IP address for this user class. This limit does not affect sysops and chat administrators. The default setting of 0 allows for unlimited connections.

Maximum channels user can join controls the number of concurrent channels that a user can be chatting on. The server tracks this number based on a user's nickname.

Output saturation limit (KB) indicates the maximum amount of data that the server will buffer for a client before dropping the client connection.

The **PING delay (Seconds)** parameter is concerned with the PING message used to test if an active client is present at the other end of a connection. The PING is sent from the server to the client after the configured number of seconds of inactivity. Any client that receives a PING message must respond with a message indicating to the server that the client is still active. If the client fails to respond, the server severs the connection to the client. This timeout value can be set to any value between 15 and 3599 seconds.

The **Message processing delay (Seconds)** option controls the amount of time the server waits before processing the next message from all clients. The default is 0, but it can be set to any value up to 10 seconds.

The **Nickname change delay (Seconds)** option controls how often (in seconds) a user can change his or her nickname.

Specific recommendations for these settings depend on the operating environment. In a closed environment, it may be reasonable to have very liberal limits. In less controlled situations, where denial of service attacks may be of greater concern, consider tightening these restrictions.

Bans

Further restrictions on the use of Chat Services can be done using bans. Figure 76 shows the **General** Tab of the User Ban Property page:

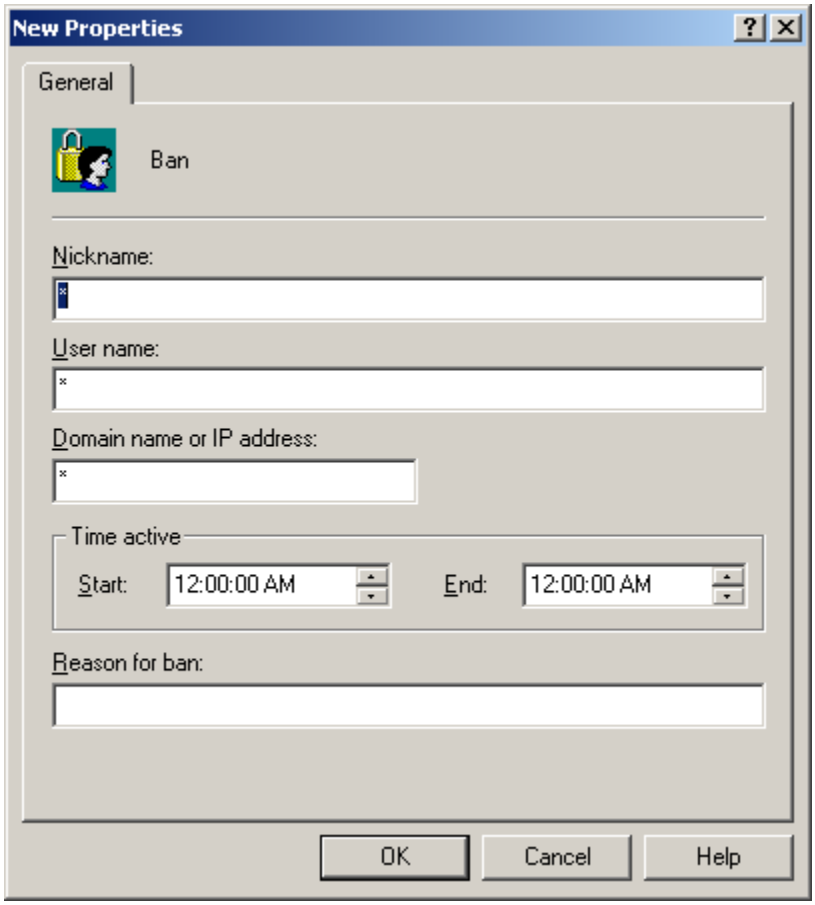

Figure 76. General Tab of User Ban Property Page

The identity fields have the same format as the identity mask in the User Class general tab, including the use of wild card characters. To define a ban, the Bans Containers within a Chat Community is selected within System Manager. Right click the **Bans** container and select **New**. The use of certain times of day can also be restricted.

Creating Dynamic Channels from the Client

Chat users can find out which rooms are available and occupied by choosing Room List from the Room menu of the Microsoft Client. The Chat Room List dialog lists all available rooms, shows how many members are currently in each room, and displays the room's topic, if available. From this box, a user can create a new room by clicking the Create Room button and then configuring the Create Chat Room dialog. This button is available only if dynamic channels have been enabled for the chat community. Figure 77 shows this dialog box:

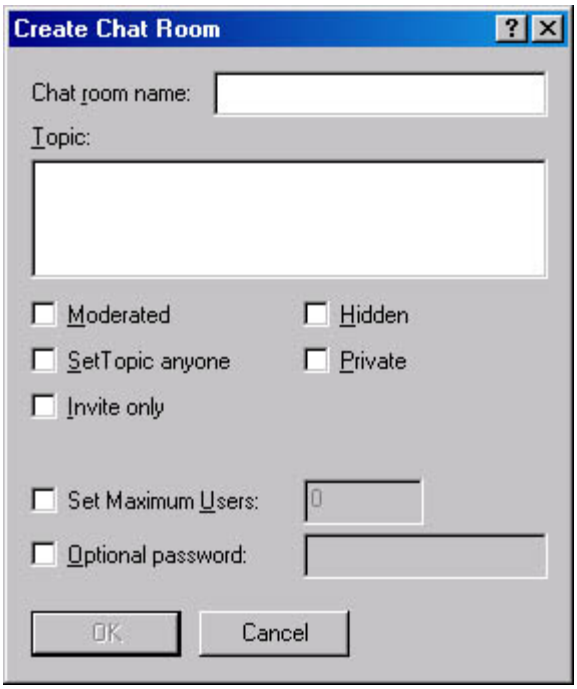

Figure 77. Creating a Chat Room

The creator can control this channel by limiting the number of users. A password can also be set for security purposes.

Important Security Points

- Do not use Chat for sensitive traffic unless encryption is employed.
- Limit the maximum total and anonymous total connections to a reasonable number.
- Assign permissions, such as Sysop, to groups rather than individuals to simplify administration.
- Limit the number of users in a channel.
- Use Channel modes to control a channel's visibility to other users.
- Assign user, host, and owner permissions to channels, as appropriate.
- Realize that the transcript option can be used to provide an audit log of selected chat discussions.
- Authenticate users whenever practical using the Windows security package option.
- Set an appropriate attack protection level on a class.
- Recognize that limits on a class and bans can be used as a means of restricting access.
- Hide class members' IP addresses and DNS names.
- Recognize that passwords can be set for the users, host, and owner of a channel as a means of restricting access.

- Limit the number of users and set a password for dynamic channels.

Chapter 13

Instant Messaging

Microsoft Exchange 2000 Instant Messaging (IM) is a real-time collaboration (RTC) communication service that provides system users with the ability to communicate instantly over TCP/IP networks using typed or voice messages. All IM communication occurs over the rendezvous protocol (RVP). RVP is an extended subset of the WebDAV protocol, which is an extension to the HTTP 1.1 protocol specification.

Instant messaging is generally intended as an alternative to e-mail where a more interactive and immediate correspondence is required. While Instant Messages certainly offers that advantage over e-mail, there are some other differences that could be viewed as disadvantages. First, Instant Messages are not recorded in the information store; they are not saved after they leave the screen. Once messages are gone, there is no way to recover them. Second, Exchange Instant Messaging does not provide any native means of providing data confidentiality; SSL is not supported, and messages are always transmitted in the clear unless protected by another form of virtual private network. IM should never be used for sensitive traffic unless these other means are employed.

Installation and Configuration

Installation

Exchange 2000 IM ships with the Exchange Server software CD as an optional installation. Refer to the Microsoft Exchange documentation for installation instructions.

Home and Routing Servers

Instant Messaging uses *Home* and *Routing* server types. A Home server hosts IM user accounts and passes all Instant Messages to the user. It is responsible for maintaining current user information for any user assigned to it and for issuing notifications of changes in a user's status to any subscriber of that user information. Messages sent to a user first pass through the user's Home server. The Instant Messaging client software represents the user to the Home server and acts as the inbox for that user messages. Home servers also cache information from Routing servers.

The Routing servers are used to forward or redirect messages and information to Home servers on the network. The Routing server is a virtual server that receives messages, determines their destination Home server, and forwards or redirects the messages to user accounts on the Home server.

Both Home and Routing servers need their own IIS web site host. The primary consequence of this from a security perspective is that certain security administrative functions are managed via Internet Information Server. Also, if multiple IM virtual servers are used on one machine, there must also be a new IIS Web site created for each IM virtual server. Hence, when an IM Routing server receives an Instant Message

addressed to a user, it locates the user in the Active Directory and uses the IM settings in the user account to forward the message to the user's Home server.

Firewalls

From a security perspective, Exchange IM is best used within a security boundary, such as an organization's intranet; however, Exchange does support the extension of the IM environment through a firewall.

Managing Exchange IM traffic through a firewall is configured in the **Firewall Topology** tab within the Global Settings' Instant Messaging Settings Properties Page, as shown in Figure 78:

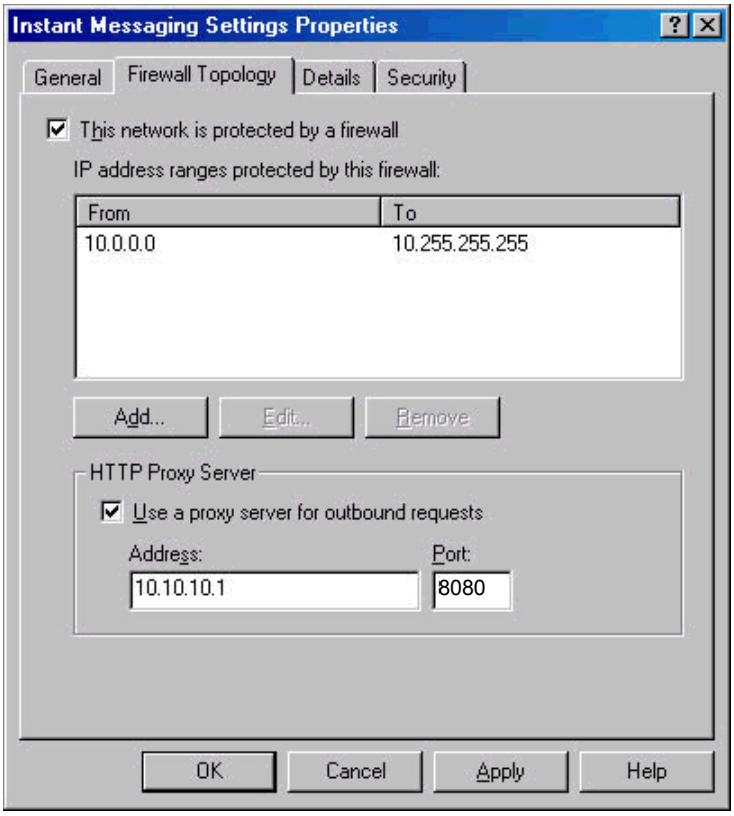

Figure 78. Firewall Topology Properties

The administrator should select the **This network is protected by a firewall** check box and then click the **Add** button to define the IP address ranges that should be protected by the firewall.

If enabling IM Internet connectivity, administrators should also use an HTTP proxy server for outbound communication. To configure IM to use an HTTP proxy server, the administrator should select the **Use a proxy server for outbound requests** check box, as shown in Figure 78, and then specify the proxy server's IP and port number.

However, Instant Messaging does not support proxy servers between clients and their home servers or users logging on from outside a network secured by a firewall. Home servers must be able to open connections to clients at any time, which cannot occur if firewalls separate clients from their home servers. Thus, a network deploying Instant Messaging cannot support users logging on from external networks to Home servers when incorporating firewalls.

The Instant Messaging Routing servers should be used to receive all inbound messages. These are the only servers that should be visible from the Internet and should always be placed within a demilitarized zone. Inbound Instant Messaging HTTP traffic must be allowed through the firewall on TCP port 80 to the Instant Messaging Routing servers. As IM Home servers contain user data, it is highly recommended that they are not allowed direct Internet connections.

Authentication and Password Policy

User authentication settings are controlled by the Internet Information Services snap-in. Open the property page for the Instant Messaging virtual server, select the directory security tab, and click on the edit button adjacent to *anonymous access and authentication control*.

By default, **Anonymous Access**, **Digest Authentication**, and **Integrated Windows Authentication** are all selected. It is recommended to clear the selection of Anonymous Access and Digest Authentication. Digest Authentication is intended as an alternative to Integrated Windows Authentication for non-windows clients; however, at the time of this writing, there were no Exchange IM clients available for non-Windows platforms.

Managing Users

Configuring Users

This section discusses how to configure a user's access to IM servers. Access to Exchange IM is controlled by the administrator through the Active Directory Users and Computer Snap-in. Select the **user object**, right click, and select **Exchange tasks** to access the various IM related actions. From here, one can enable or disable IM for the user, as well as set the user's IM Home server.

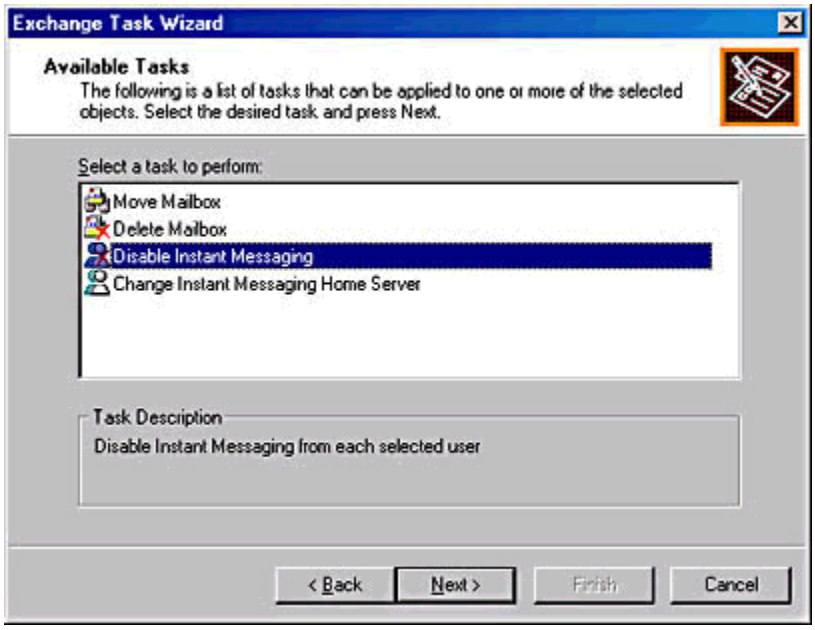

Figure 79. Disabling Instant Messaging For a User's Account

Controlling External Access

Instant Messaging has an option for controlling access to an IM user's presence information and controlling access to send and receive messages. Figure 80, displays the **Exchange Features** tab of the user's property page that is used for controlling message traffic. The Privacy tab of the IM property page, also shown in Figure 80, is used to control access to this user's account.

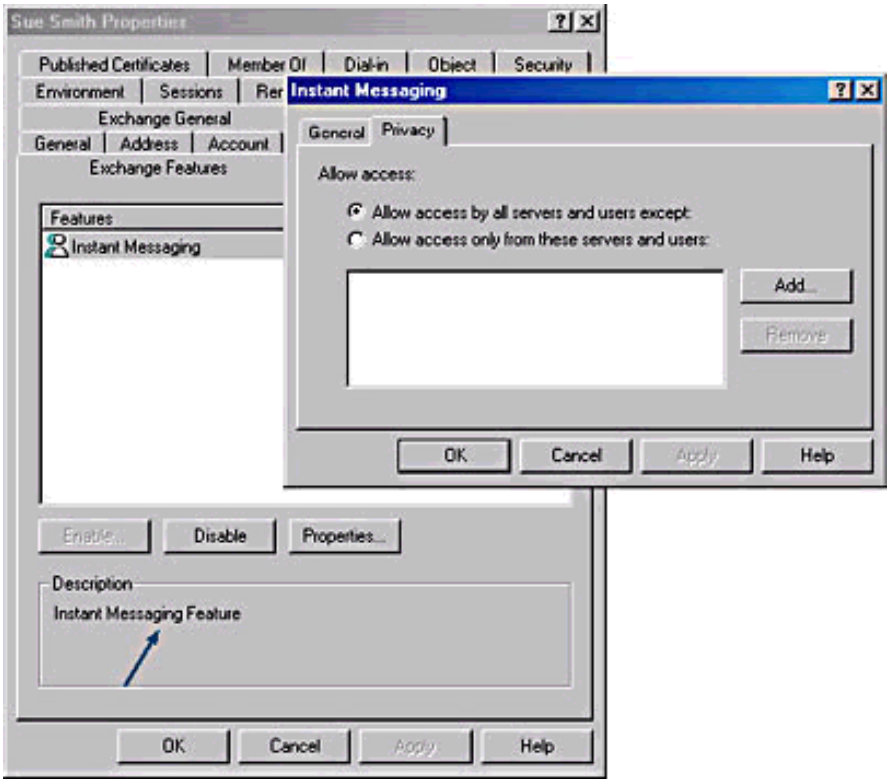

Figure 80. Privacy Tab of User Property Page for IM

This option allows limitations on IM services for user accounts. For instance, if the **Allow access only from these servers and users** option is selected, only the listed accounts will be able to send messages to the user or be able to see when the user is online. Alternately, to restrict only a few users from obtaining presence information and Instant Messaging privileges, select the **Allow access by all servers and users except** option, whereby only those users listed will be the only ones restricted for this user account.

Managing Servers

Removing a Server

Consistent with good security practices, IM servers should be removed from a system when no longer in use.

Removing an IM server is accomplished by removing the IM virtual server or by removing the IM service entirely. Figure 81 is the window used for removing a server. In Figure 81, the "move users" check box is selected. This is automatically checked by the application to help prevent loss of data and resources. If the server being deleted is an

IM Routing server that is not hosting IM user accounts, clear the check box before selecting delete.

To delete a virtual server, navigate to the **Instant Messaging (RVP)** container under the **Protocols** container in System Manager. Right-click the **IM virtual server** and select the **delete** option.

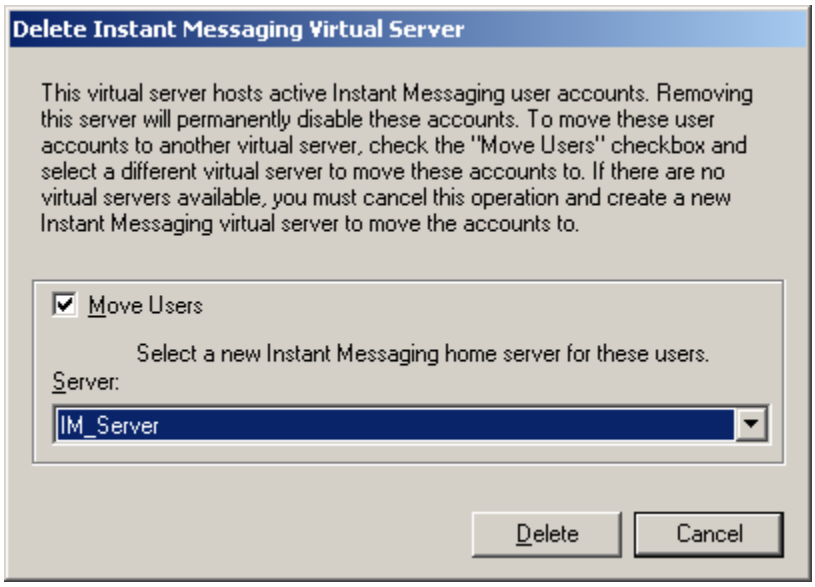

Figure 81. Removing an IM Virtual Server

Taking a Server Offline

To take an IM server off line without removing it, stop the corresponding IIS virtual server. This is done in the Internet Information Services snap-in by right-clicking the virtual IIS site and then choosing **Stop**. All IM services on the Web site will stop, and users will be notified via a message indicating the halt. To place the IM server back online after maintenance is completed, simply start the IIS virtual server again.

Limits and Logging

To prevent IM Server message load saturation, limiting the number of allowed users is recommended. This is done by using the Internet Information services snap-in, as displayed in Figure 82. Go to the Web Site tab of the Web site's property page. In the **Connections** area, select the **Limited To** button, enter the maximum number of simultaneous connections, and then click OK.

This tab can also enable logging to keep track of user activity on an IM server. The default format for the log files is the W3C Extended Log File format**.** Reference the *Guide to the Secure Configuration and Administration of Internet Information Services 5.0* available at http://www.nsa.gov for specific guidance regarding auditing in IIS.

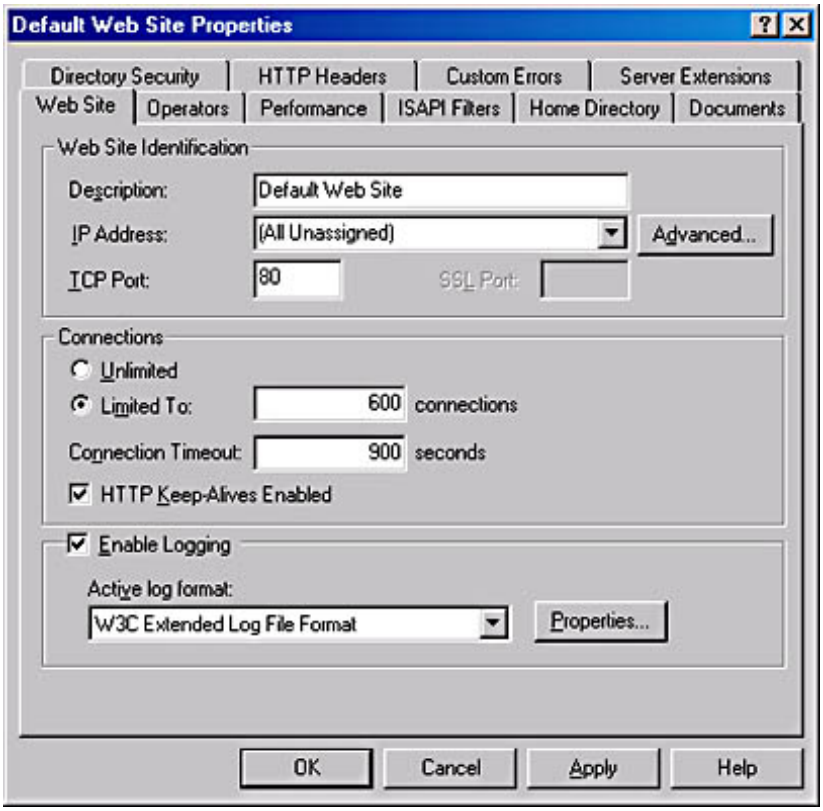

Figure 82. Limiting user connections and enabling logging

The name and directory location of the IIS log file containing IM data is set and shown by clicking the Properties button, as shown in Figure 82.

Database and Transaction Logs

To designate a new location for the IM data and the transaction log files, use the property page for Instant Messaging (RVP) as shown in Figure 83. Changing the location here, however, does not automatically move the existing databases and transaction log files. Instead, IM creates new databases and files in the new location. To continue using the same databases and transaction logs, copy the files to the new directory, and stop and restart the virtual Web site in IIS. As discussed in Chapter 4, it is recommended to place the database and transaction log files on separate physical drives. Set the access permissions on these directories as detailed in Chapter 1.

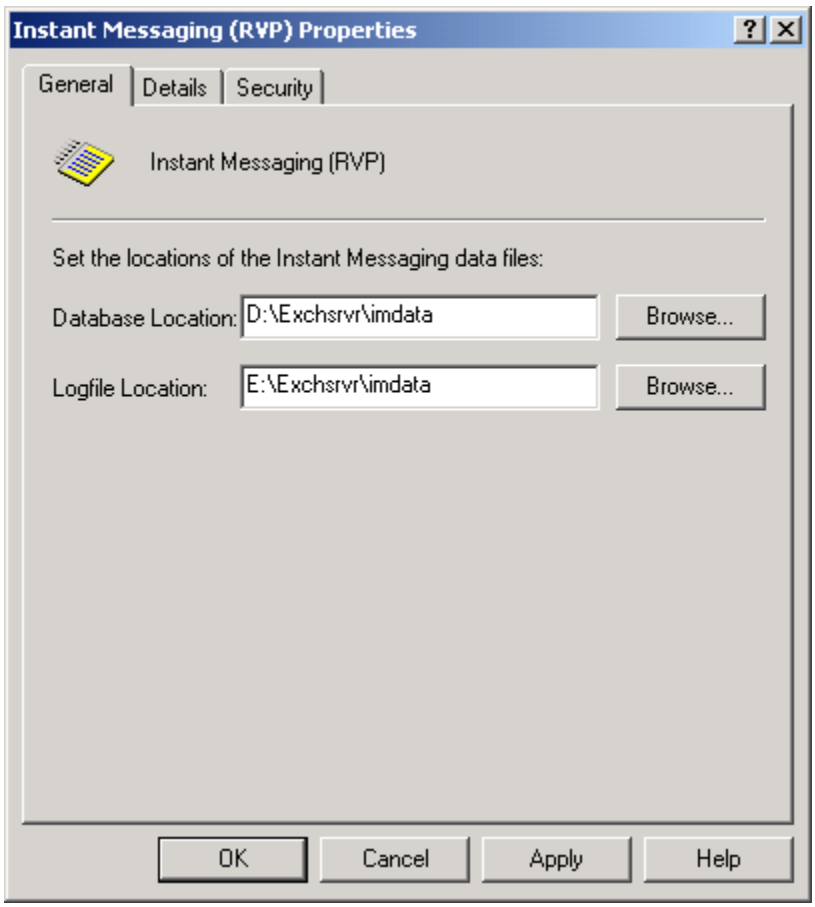

Figure 83. Designating a New Location for IM Database and Transaction Log Files

Managing Clients

Presence and Privacy

Instant Messaging enables users to check the online status of another user in their "contact list" and, if the contact is logged on, instantly send a message to that user. When a user logs on, a status notification is sent to the Instant Message server, which passes the status information to users who have subscribed for user presence information.

Users can display who will receive status information, as illustrated in Figure 84. The **Privacy** tab in the IM Client Options window shows the users who presence status is reported to and which users are prevented from seeing their presence information.

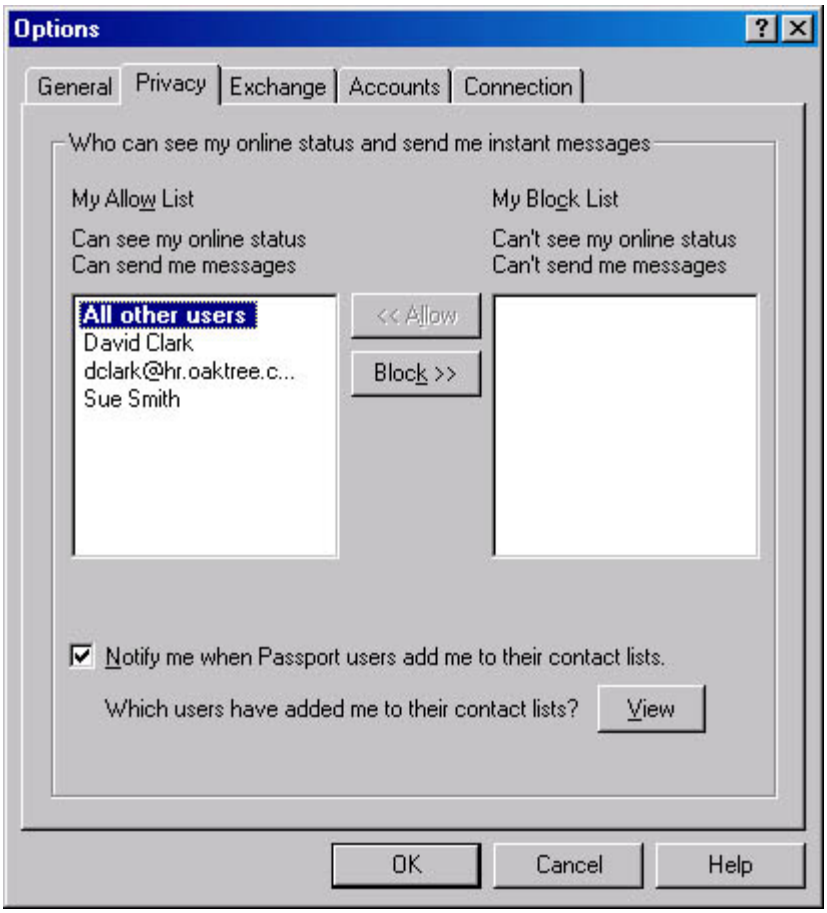

Figure 84. Privacy Tab of MSN Messenger Client Options

As described earlier in this chapter and seen in Figure 80, the Active Directory user account property sheet specifies the default set of users and groups that can send messages to that user or see the user's presence information. It is these settings that are reflected on the client, as illustrated in Figure 84. The user can further restrict the list of users who can send him messages by adding those users to the block list, but he can not override the Active Directory-specified privacy settings by adding users to the allow list.

Important Security Points

- Do not use IM for sensitive traffic unless means are employed to protect confidentiality. Exchange IM does not provide any native means of providing data confidentiality. SSL is not supported, and messages are always transmitted in the clear unless protected by another form of virtual private network.
- Limit Exchange IM use to a network security boundary, such as an intranet, if possible. If Internet access is needed, configure firewall and proxy access and use a VPN to encrypt sensitive communications.
- The Instant Messaging Routing servers should be used to receive all inbound messages. These servers, and not the Home servers, should be visible from the Internet and should always be placed within a demilitarized zone.

- Use Windows Integrated Authentication (WIA) for user authentication and disable digest authentication and anonymous access.
- Allow or block specific server and user access to user IM accounts, as desired. Users can further restrict access through their client privacy settings.
- Place the IM database and transaction log files on separate physical drives. Set the access permissions on these directories as detailed in Chapter 1.
- Limit the number of users for the IM service to prevent saturation.
- Enable IIS logging of user activity on an IM Server.

This Page Intentionally Left Blank

Chapter 14

Final Thoughts

This final chapter of the "*Guide to the Secure Configuration and Administration of Microsoft Exchange 2000*" deals with various miscellaneous topics of interest – third party malicious code countermeasures, backup procedures, and distribution group security.

Third Party Malicious Code Countermeasures

Malicious code is a leading threat to information systems and, while it can spread through any mechanism that entails the receipt of computer data, e-mail is the most common conduit today. While chapter 2 detailed recommendations that can help to counter this threat, numerous third party programs exist that are designed specifically for the Exchange environment and are a necessary part of any comprehensive Exchange security policy.

Using a product especially designed for Exchange can have numerous benefits. A well designed malicious code solution will integrate with Exchange so that new messages are automatically scanned. Other important features include the ability to scan attachments, including compressed files, the ability to selectively allow only those file attachments that are of operational necessity, and the ability to provide protection for the Installable File System (discussed later). Specific product recommendations are well beyond the scope of this document; however, this is a topic which is covered in depth on the Internet and other sources. It is recommended to implement malicious code countermeasures on the Exchange servers and any gateways to less trusted networks as detailed in chapter 11; however, it is important to remember that these countermeasures will be limited in that encryption will mask the presence of malicious code. Implementing countermeasures on the individual workstations will help prevent infestation via encrypted messages. If the chosen malicious code countermeasures are based upon pattern matching, it is important to keep signature files current.

Backup and Recovery Procedures

Robust backup and recovery procedures are vital for maintaining the integrity of the Exchange environment. Specific guidance will not be offered here as Microsoft has developed some excellent papers on the subject. Suggested references include:

- *Disaster Recovery for Microsoft Exchange 2000 Server* available at http://www.microsoft.com/Exchange/techinfo/deployment/2000/E2Krecovery.asp
- *Exchange 2000 Server Disaster Recovery: Worst-Case Survival Handbook* available at http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/exchange/support/exrecovr.asp

Distribution Group Security

As reported on the NTBugtraq mailing list (http://ntbugtrak.ntadvice.com), a possible denial of service attack can be levied against an Exchange server by an attacker who takes advantage of a general distribution group (such as all_employees@foobar.com). This denial of service attack can be launched by individuals internal to the Exchange environment or can be launched by external parties with connectivity to the Exchange Server (via the Simple Mail Transport Protocol, for example.)

In order to invoke this attack the attacker sends an e-mail to a general distribution group with a request for a read receipt. The attacker uses a spoofed returned e-mail address such that the distribution group is used as both the destination address and return address as shown the following illustration:

From: <all_employees@foobar.com>
To: <all_employees@foobar.com>
Subject: Important message!

Since a read receipt has been requested, a message will be send back to the originator (all_employees@foobar.com) each time a user reads the attacker's message. Since the receipt is addressed to the distribution group, the receipt will be sent to all members of that list. This can result in an extraordinary amount of traffic and result in a denial of service. For example, if the all_employees distribution group has 1000 members, 1000 read receipts could be generated, each of which will be sent to all 1000 members of all_employees. This means that one message from an attacker could result in the generation of over 1 million messages!

1 + 1000 + 1000 * 1000 = 1,001,001

(1 original message + sent to 1000 users + 1000 users send a read receipt to 1000 users)

While in all likelihood some of the members of the all_employees distribution group would elect not send a receipt the attacker could compensate by simply sending out a series of messages and quickly create a plethora of traffic as some subset of users respond.

Fortunately, there is a simple configuration setting which will significantly reduce the threat. Open the Active Directory Users and Computers MMC and set it to display advanced features by selecting **view/advanced features**. Open the properties page for the distribution group and enable the **Do not send delivery reports** option under the **Exchange Advanced** tab. This will preclude read receipts messages from being generated for messages sent to the distribution group.

Installable File System (IFS)

When Exchange is installed it creates a drive (M:\ typically) that exposes mailboxes and public folders via the file system. The intent is that these mailboxes and public folders can be accessed as any directory structure would be – via Windows Explorer, the command prompt, and etc. The security related issues with IFS relates primarily to the possibility of malicious code introduction, as discussed above, and controlling access. Modifying the ACLs on these objects via the operating system can cause difficulty. As one example of the difficulties that can be introduced by direct manipulation of these ACLs, reference Microsoft Knowledge Base Article Q309766 available at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q309766. It is best to manipulate these access controls via the Outlook client or System Manager.

Important Security Points

- Implement a program to reduce the threat of malicious code based attacks.
- Implement a backup and recovery strategy.
- Enable the option to not send delivery reports for distribution groups.
- It is recommended to manipulated access controls related to the IFS via the Outlook client or System Manager.

This Page Intentionally Left Blank

Addendum A - Exchange 2000 and Active Directory Integration

As organizations roll out Windows 2000 one of the most fundamental decisions they must make is the structure of their Windows 2000 domain trees and forests. This addendum presents a brief overview of the available options, with a focus upon the impact this decision has on the Exchange environment. Please note that this is not intended to be a complete dissertation on Active Directory design – the reader needing this background is encouraged to consult the document *Guide to Securing Microsoft Windows 2000 Active Directory* available at http://www.nsa.gov and the wealth of information developed by Microsoft and others on this topic.

Most commonly, the decision of how to structure the Windows 2000 forest revolves around the notion of having a single forest for the entire organization or separate forests for major units within the organization tied together with trusts. The two options are illustrated in Figure 85:

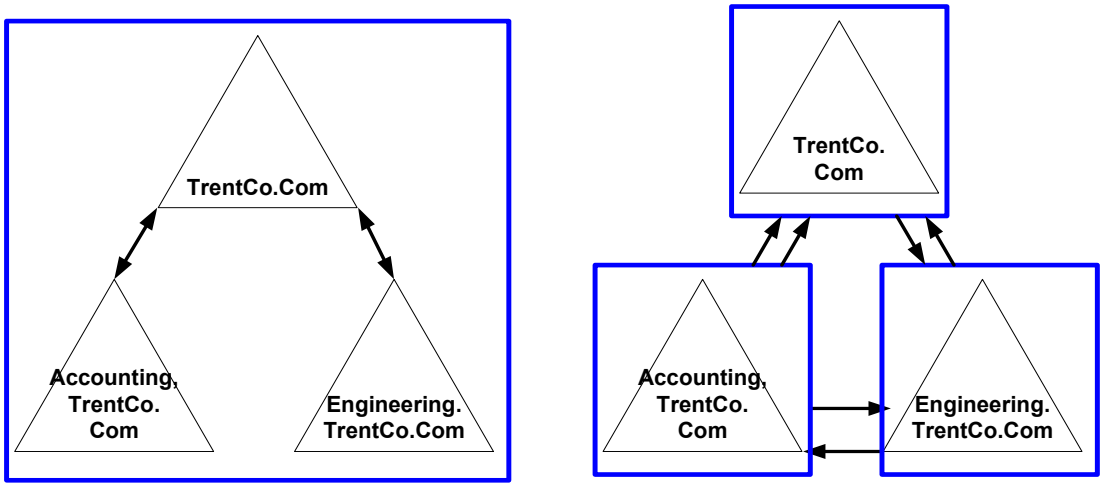

Figure 85. Active Directory Structure

The option on the left illustrates an active directory organization where a single forest encompasses the entire organization. It includes domains for two departments within this hypothetical company with a root domain *TrentCo.com* where corporate applications reside. Transitive trusts are automatically created by Windows 2000 such that users in each domain can access resources in any other domain, assuming of course that they have the appropriate access rights to those resources. The option on the right illustrates the three elements of the organization, each contained within their own forest, with a trust created by the administrators in both directions between the three forests.

There are numerous considerations when deciding which of these two structures are best suited to a given organization. The option of using a single forest for the organization offers a simpler administrative model in that Windows automatically creates the trusts between domains and a single Active Directory schema is utilized which can simplify the

implementation of corporate applications. The down side of this structure for some organizations is the existence of enterprise administrators who enjoy administrative rights across the entire forest. The second option of deploying multiple forests offers a higher degree of autonomy between the various units, but could result in an increased administrative burden. Trusts between domains must be created manually, and the provision of corporate applications that span all the domains in the organization could be more complicated as there is no notion of Active Directory synchronization between forests.

In considering the impact of this decision upon the Exchange Server environment it is important to note that while an Exchange organization can span all the domains in a forest, it can never extend beyond the forest. This is driven by the fact that the Exchange environment relies on the Global Catalog for generation of the Global Address List and for storage of other pertinent information such as routing configurations. The Global Catalog contains no information about other forests, even those that are linked by trusts.

In the case where a single forest is used for the organization, Exchange servers and Outlook clients have access to a Global Catalog which will contain pertinent information about every Exchange user and Exchange server within the organization. The most visible impact of this is the ability of each user in the organization to easily access the e-mail address of coworkers via Global Address List searches.

In the case where a separate forest is used for each division in the organization, the Global Catalog only contains information for that local forest, even if trusts were to be established between them. Connectors would be required to facilitate the transfer of mail between organizations, but these cannot be used for directory synchronization. Users could enter the addresses and other contact information for coworkers outside of their forest into their local address books, or synchronization of pertinent Global Catalog information could be accomplished via the use of a metadirectory or by using the LDAP Directory Interchange Format to share pertinent data between forests. LDIFDE.EXE, which is included with Windows 2000, can be used for this purpose[19].

[19] Reference *Using LDIFDE to Import and Export Directory Objects to Active Directory (Q237677)* at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q237677

Changes

Version 1.1:

- Added details about changing the SMTP, POP3, and IMAP banners.
- Beefed up the Service Packs and Hot Fixes section to emphasize the need for installing service packs and security related hotfixes.
- Added a series of graphics illustrating the effects of certification revocation.
- Modified the section on HTTP access (Outlook Web Access) to indicate that the System Manager should be used instead of the Internet Services Manager whenever possible to manage HTTP settings. Also clarified portions of this section.
- Added a short section on the security concerns related to the Installable File System.
- Solved a mystery as to why LDAP/SSL would not work and updated that section accordingly.
- Added Addendum A.
- Added a recommendation to take advantage of a new feature available with Office XP Service Pack 1 that forces Outlook to read unsecured HTML messages as plain text.

Version 1.11

- Corrected a typo.
- Clarified a statement under Deployment of Customized Security Settings

Version 1.12

- Removed an erroneous FOUO designation.