# Global Information Assurance Certification Paper

# Exchange 2000 Security an Overview

## GIAC Security Essentials Certification
## Practical Assignment Version 1.4b Option 1

**Charles V Polkiewicz**
**January 28, 2004**

# Table of Content

## Abstract

Exchange 2000 is a Microsoft premier messaging product, with over 100 million licenses sold throughout the world[1]. Securing this product is a challenge for any administrator. Proper administration requires both knowledge of the product and understanding of security policies involved.

Exchange 2000 product information is scatted and locating them becomes a time consuming tasks. The intent here is to facilitate the life of these administrators by offering them with a summary of settings, potential issues, and general security awareness that will best secure their environment. Policy, server design, and limitations of Exchange 2000 are also considered. Default settings such as “anonymous” access, clear text password, and default ACL granting full rights to everyone that can cause serious problems and they are carefully examined and detailed resolutions are provided. Most importantly, considerations of viruses’ breakout and methods of preventions are also illustrated with details.

Finally, cost effective implementations of Exchange 2000 security and policies are also reviewed. Risk management against cost analysis is recommended so that organizations give considerable attention and direct proper resources for protecting their assets.

*"Forewarned is for armed" - unknown*




[1] Microsoft Corp, “Microsoft Exchange Server Winning the Enterprise with 100 Million Seats sold” (Jan 23, 2002)
http://www.microsoft.com/presspass/press/2002/jan02/01-23MarketLeaderPR.asp (Jan 20, 2004)

## Objective and Scope

This document will cover basic security for exchange 2000 - emphasizing security server settings, and procedures to improve security and potential security pitfalls that can arise with implementation. This document will not include detail sections on Windows 2000 server or Internet Information Server (IIS) security. It assumes that the reader has basic knowledge of the windows 2000 active directory (AD) & Exchange 2000 and can use tools to administrate them.

# Installation Considerations

What you should know before installing Exchange 2000 on a Windows 2000 server.

**Administrative Groups**
Before installation it is best to create two security groups[2] in active directory (AD) for both normal exchange administrators (EA) and elevated privileges exchange administrators (EPEA). For normal day-to-day administrative work the EA account should suffice. Members of the EA group should be able to perform the following tasks: backup/recovery, exchange maintenance work, Exchange troubleshooting, remote administration, reviewing of logs and starting & stopping services. In contrast the EPEA members should only be used as needed for installation of exchange, installing/configuring enterprise aware antivirus solutions, and other one-off administrative tasks. EPEA accounts are not needed for everyday use and should be discouraged. For additional security, consider disabling these accounts and enabling them as needed. The group configurations are explained as follows:

1. Group - Exchange Administrators
Added to each Exchange2000 servers local administrators group
Not a member of the domain administrators group or any other elevated privileges group.
Once installation of your first exchange 2000 server has been completed use the system manager - *Exchange Administration Delegation Wizard* to give the group *Exchange Administrative Role*.

2. Group – Elevated Privileges Exchange Administrators
Added to the Schema Administrators Group
Added to the Enterprise Administrators Group
In multi domain systems added to each Domain Administrative Group
Once the installation of your first exchange 2000 server has been completed use the system manager – *Exchange Administration Delegation Wizard* to give the group *Exchange Full Administrator Role*.

[2] Pitsenbarger, Trent, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000" (v1.2) (10/13/2003) http://nsa2.www.conxion.com/ Download Zipped Archive for Windows 2000 Guides and open W2k21.pdf p5-7 (11/10/2003)

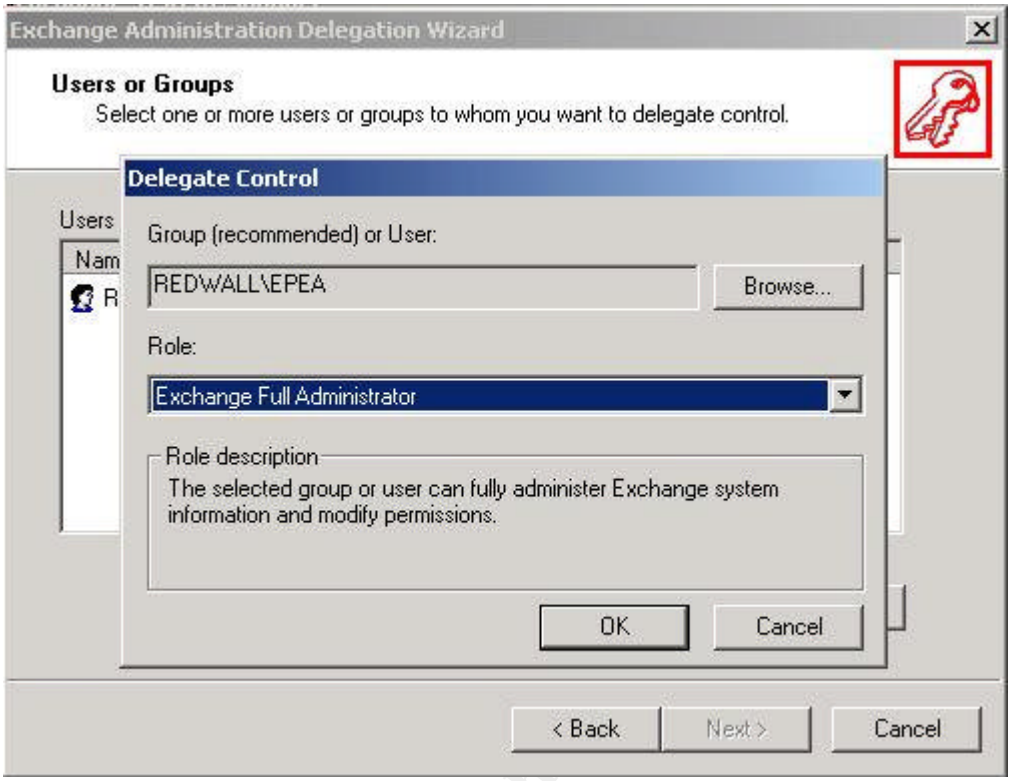



*Figure 1 – View of the Exchange Administration Delegation Wizard*

A special account should be added to both EA & EPEA groups and used for the installation of Exchange 2000 within the organization[3]. This account will be the ultimate powered account within the Exchange and Windows 2000 environment. For security reasons this account should have an ambiguous name (i.e. Thomas Smith).

**Specialized Administrative Groups**

For large organizations, additional administrative groups are required to perform specialized tasks - such as creating, deleting, and moving mailboxes[4]. These groups will be granted enough power to perform only the required tasks. Bear in mind that they follow the security principle, namely least permission required to perform a desired task. Such groups should not have administrative power as given to the EA & EPEA groups.

[3] Pitsenbarger, Trent, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000" (v1.2) (10/13/2003) http://nsa2.www.conxion.com/ Download Zipped Archive for Windows 2000 Guides and open W2k21.pdf p5-7 (11/10/2003)

[4] Microsoft Corp, "Minimum permissions Necessary to Perform Exchange-Related Tasks", (v8.0) (10/9/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;316792&Product=exch2k (1/17/2004)

Create Mailbox Group

Create a group and give that group Exchange View-Only Administrator role in Exchange System Manager. Then add the following write permissions to the user object as listed in appendix A - part 1.

Delete Mailbox Group

For a group to delete a mailbox, the following is required. First the group should be given the Exchange View-only Administrator Role in Exchange System Manager. Then add the following write permissions to the user object as listed in appendix A - part 2.

Move Mailbox Group

For this group to move mailboxes, first give this group the Exchange View-only Administrator Role in Exchange System Manager, then give the write permissions to the user object as listed in appendix A part 3.

Once these three additional groups have been created, you can add member(s) to them as needed. For instance, there could be a major move of users required for an upcoming server consolidation. With these groups you can give a small number of users just the minimum required permissions to perform the mailbox moves.

## Server Drive Configuration & Backups

Although server drive configuration is generally not a security consideration (it is a disaster recovery issue) it is worthy noting its potential impact on its users. Disasters issues include recovery from a virus out break or other illicit activity. To best protect from potential data loss, circular logging should be turned off and differential or incremental backups should be performed daily. It is important to remind administrators that circular logging requires full backup which can be costly and time consuming. Therefore, full backups take place on the weekends and differential or incremental backups occur on daily basis.

The default setting for Exchange is to have circular logging enabled. Circular logging works by first placing incoming data into log files. Then, the log files are read and finally its content is written to the IS database[5]. Only a small number of these uncommitted log files exits at any time. As they are committed to the database, they are flagged to be rewritten by the system. So as new data comes in to the server it can reuse an already committed log file. In the case of a virus breakout and if part of the information store is damaged or completely lost, you will have to restore the database from the last full backup. Unfortunately, all the data generated in the interim between the last full backup and the incident will be lost. To prevent it from happening is recommended that the circular logging is disabled and log files are allowed to grow in sequential order. Of course, with time these log files will fill up the whole volume of the hard drive and cause the system to halt. When a full backup is performed all committed log files are automatically deleted. On the other hand, whenever an incremental backup is performed the log files that have been committed can then be backed up to tape and deleted from the server, thus taking significantly less time to perform than a full backup would. Now, when a differential backup is done, the log files are copied to tape but not deleted from the drive. Each successive differential backup requires more time. When comes to restoring any of these three backup types, applicable procedures must be followed. For a restore to be successful, the last full backup will have to be recovered. If an incremental system is used, then these additional incremental tapes have to be restored so that log files are played back and committed to the database. Differential restore requires the last full backup and the last full differential tape are restored and replayed to the database. The last differential tape includes all the needed log files to be played back into the database.

Assuming that circular logging is turn off. For best performance and server disaster recovery considerations, the drives should have the following setup[6].

---

[5] Glenn, Walter & Chellis, James, "MCSE Exchange 2000 Server Administration", Alameda CA-USA, Sybex 2001, p591-592. ISBN 0-7821-2898-X

[6] Glenn, Walter & Chellis, James, "MCSE Exchange 2000 Server Administration", Alameda CA-USA, Sybex 2001, p594-596. ISBN 0-7821-2898-X

C:\ drive should be a mirrored setup with boot files and system files.
D:\ drive should be a mirrored setup with log files for the First Storage group.
E:\ drive should be a RAID 5 striped set with parity and should contain the first storage group databases.

If additional storage group is needed then additional mirrored set of drives should be added for its log files. All storage group database files could reside on a single RAID 5 striped set with parity.

The speed of exchange 2000 depends a great deal on the transaction file creation. This hard drive setup also allows for better backup of the system, since you can now do differential and incremental backups and have sufficient space for the log files.

For full backup of exchange the following is required to be backed for each Exchange 2000 system[7].

- Backup of all committed log files
- Backup of all database files - PRIVx.EDB, PUBx.EDB, and .STM databases.
- EXCHSRVR subdirectories - \Program Files\Exchsrvr
- Site Replication Service (SRS) – this database is used in mixed exchange 5.5 environments.
- Key Management Server (KMS) database – this database provides key management and advanced security. This should also include CA certificates and KMS startup password.
- System state backup should also be included – this would include IIS metabase (configuration database) and local server registry information.

Some third party backup products do not have the ability to backup system state data. To mitigate this issue, use the built-in Windows2000 backup utility to backup system state data to a file on the system and then backup it to a tape.

Proper setup of hard drive configuration and backup strategy can pre-determine your ability to recover from a disastrous situation.

[7] Glenn, Walter & Chellis, James, "MCSE Exchange 2000 Server Administration", Alameda CA-USA, Sybex 2001, p592-593. ISBN 0-7821-2898-X

## Server Setup and Exchange settings

The following setup and configuration should be done prior to Exchange 2000 installation. First installation of Windows 2000 with all drives formatted to NTFS. The settings for domain naming service (DNS) should be properly setup during the install. This is vital for proper Windows 2000 domain controller active directory (AD) querying. Server should then be added to AD as a member server. Only the minimum services should be installed for the operations of Exchange2000. The following is a list of these services.

Service[8]

- Internet Information Service 5.0 (IIS)
- Network News Transfer Protocol (NNTP)
- Simple Mail Transfer Protocol (SMTP)

The latest service pack should be installed and any post service pack hot fixes. Antivirus (AV) should be installed and updated to the latest virus definition. The AV should then be setup to scan all drives fully before proceeding with Exchange 2000 installation.

Post installation of Exchange 2000 should include the installation of the latest service pack and any post hot fixes. An antivirus that is "Exchange aware" should also be installed. In addition, some modification of the AV will be required for proper functionality. This is addressed in section *Antivirus for Exchange Server.*

Permission modification of the exchange directory is required since the "everyone" group is granted full control by default. It is prudent that the "everyone" group be removed and that full control be given to the following groups: System, Creator Owner, Domain Administrators, EA, and EPEA Group[9].

Message tracking should be enabled to enhance the ability for troubleshooting issues. To enable message tracking:

- Start Exchange System Manager
- Expand the server container and right click on the server – properties
- On the General tab select "Enable Message Tracking" check box[10].
- On the General tab select "Enable Subject logging and display" check box[11].

---

[8] Microsoft Corporation, "XADM: How to Set Up Exchange 2000" (8/14/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;262068&Product=exch2k (1/20/2004)

[9] Pitsenbarger, Trent, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000" (v1.2) (10/13/2003) http://nsa2.www.conxion.com/ Download Zipped Archive for Windows 2000 Guides and open W2k21.pdf p6 (11/10/2003)

[10] Microsoft Corp, "XADM: How to Enable Message Tracking in Exchange 2000 Server" (v1.1) (6/17/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;246856&Product=exch2k (1/19/2003)

The messages tracking feature relies on a share folder, which is grants the "everyone" read capability. To disable this on each server use Windows Explorer to find drive:\program files\Exchsrvr*Exchange Server Computer Name*.log and right click on permissions. Click the sharing tab and remove the "everyone" group and add in EA and EPEA groups with full permissions[12].

To enhance security, local server *Security Policy* must be modified so that built-in users group loses its ability to logon locally onto an Exchange 2000 server.

Exchange 2000 has no default message size. This can cause issue if your email system is attacked by a mail bomb – that is when an excessive number of emails with large attachments are sent to your organization to overwhelm its ability to handle mail. This can cause your email system to slow down or even halt. To less the potential of a "denial of service attack", configure the global message size limits to 10 MB or to an agreed limit for your organization. This setting will override any setting for SMTP virtual server or user mailbox[13]. Here are the procedures for such a configuration:

1. Start Exchange System Manager
2. Expand Global Settings
3. Right-click Message Delivery and click Properties
4. Click default Tab and configure the setting as needed

**Security Tab is Missing**
System manager has one glaring security issue. Out of numerous objects, the only ones to have the security tab by default are:

- Address Lists
- Global Address Lists
- Database (Mailbox stores and Public Folder Store)
- Top Level Public Folder Hierarchy

This can lead an Exchange administrator to disregard potential security issues simply because these tabs are not present. As one would say *"Out of Sight is out of Mind."* So, having these tabs available in all objects would raise flags to the administrator.



---

[11] Microsoft Corp, "XADM: Tracking log and Queue Viewer Allows Access to Message Subject" (v1.1) (6/17/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;246867&Product=exch2k (1/19/2004)
[12] Microsoft Corp, "How to change the share permissions on the Message Tracking share in Exchange 5.5 and in Exchange 2000" (v1.0) (8/25/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;825222&Product=exch2k (1/19/2004)
[13] Microsoft Corp, "Set Size Limits for Messages", (v6.0) (12/18/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;322679&Product=exch2k (1/18/2004)

In order to resolve this issue the following registry setting needs to be added[14].

1. Start a registry editor. (Regedt32.exe)
2. Locate the following registry key:
   HKEY_Current_user\Software\Microsoft\Exchange\ExAdmin
3. Menu EDIT, click Add Value, then add the following value:
4. Value Name: ShowSecurtyPage
5. Data Type: REG_DWORD -> Value: 1

This change takes effect immediately without the need for a system reboot. The drawback is that this only affects the currently logged in user.

## Protocols

In system manager, the protocols are listed underneath each server.

**SMTP Authentication**
The default in Exchange 2000 is for SMTP service to allow anonymous and basic authentication (clear text) to use the service. This should be turned off and only integrated Windows authentication should be allowed.

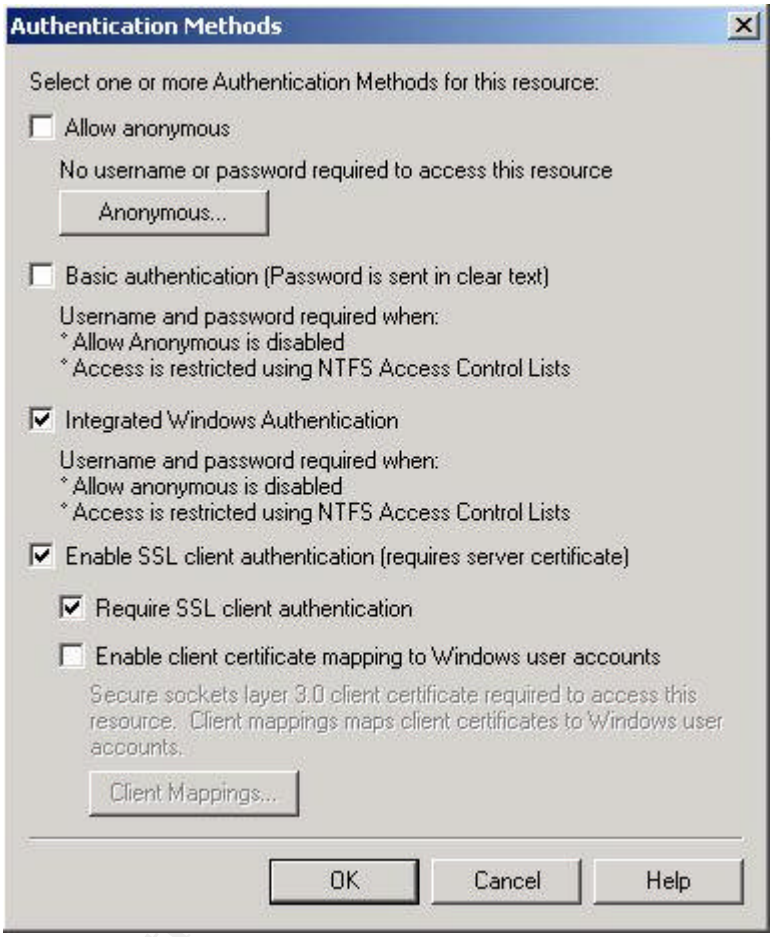
**Are any of these needed?**
There are three protocols that by default are installed and enabled. These are Network News Transfer Protocol (NNTP), Post Office Protocol (POP3) and Internet Message Access Protocol version 4 (IMAP4). The security concerns are twofold. First, which - if any - of these protocols should be enabled? Second, what security configuration should be used to control their access? Most protocols have some level of authentication – anonymous and basic clear-text, for instance, should be disabled and never used even for internal connection[15]. Basic security principle "if it's not needed it should be disabled or uninstalled", should be followed. Thus, lessening the potential of an disastrous attack by some worm or virus. For IMAP4 and POP3 the best solution is to replace such connection with Outlook web Access (OWA).

**NNTP**
This protocol is what the Usenet newsgroups use to deliver content worldwide. This information can be delivered to public folders and even pushed back out to the world for publishing purposes. For the most part, very few - if any - institutions will use this function. Security can be enabled just like any public folder can with ACL's - see section *Top Level Public Folder Creation and Folder Administration below.*

---

[14] Microsoft Corp, "XADM: Security Tab Not available on All Objects in System Manager", (v1.2) (7/8/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;259221&Product=exch2k (1/18/2004)
[15] Glenn, Walter & Chellis, James, "MCSE Exchange 2000 Server Administration", Alameda CA-USA, Sybex 2001, p624-627. ISBN 0-7821-2898-X

Content of which Usenet newsgroups should be included can be configured through the NNTP wizard. In addition, levels of authentication can be used, at a minimum SSL or Integrated Windows Authentication[16]. If this service is not needed is should be turned off on each server.




**NNTP Settings**

## POP3

This protocol is used by mail programs such as Outlook Express. A user can connect to the server through the Internet and download their mail from their Inbox folder only and send mail by relaying through the SMTP virtual server running on Exchange 2000. To increase security, 128 bit SSL certificate should be required and the required port 995 opened on any firewall[17]. For internal network, Integrated Windows authentication can be used. Most corporations no longer use this form of mail delivery relaying more on virtual private network (VPN) or dial up connection directly to the corporate network. So that outlook can

[16] Glenn, Walter & Chellis, James, "MCSE Exchange 2000 Server Administration", Alameda CA-USA, Sybex 2001, p624-627. ISBN 0-7821-2898-X

[17] Microsoft Corp, "How to: Help Secure Post Office Protocol Client Access in Exchange 2000", (v2.0) (6/25/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;319273&Product=exch2k (1/19/04)

be used directly. If this protocol is not needed, it should be disabled on each server within the organization.

**IMAP4**

This protocol is used by mail programs like outlook express. A user can connect to the server through the internet and read email and move it between folders within its mailbox. Sending email requires the SMTP virtual server on Exchange 2000 to relay the mail back out to the internet[18]. To secure this connection, the 128 bit SSL should be required. In order to use this service, the required port 993 should be opened on any firewall[19]. For internal network, the Integrated Windows authentication should be used. This protocol should be disabled if not needed on each server within the organization.

**Outlook Web Access (OWA)**

Most of the security settings available for OWA are administrated through IIS. To get to the authentication settings in system manager simply expand the protocols folder then the HTTP folder. Next, open the Exchange virtual server folder and right click on any of these two folders: “Exchange” or “Public”. Then, go to the access tab and click authentication. You can now control the level of authentication. By default basic authentication is enabled, so uncheck this box for both folders.


**Figure 2 – View of the OWA Authentication Methods**

[18] Glenn, Walter & Chellis, James, “MCSE Exchange 2000 Server Administration”, Alameda CA-USA, Sybex 2001, p624-627. ISBN 0-7821-2898-X

[19] Microsoft Corp, “How to: Secure Internet Message Access Protocol Client Access in Exchange 2000” (v1.3) (6/5/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;319278&Product=exch2k (1/24/2004)

In addition the IIS lockdown Wizard tool should be used to secure the virtual HTTP server. After that you should review MS knowledge base article 309677 "XSADM: Know Issues and Fine Tuning When You Use the IIS lockdown Wizard in an Exchange 2000 Environment". Also SSL should be enabled for OWA, this can be found under MS KB article 320291 "XCCC: Turning On SSL for Exchange 2000 Server Outlook Web Access".

## Securing Outlook Client

In both Outlook 2000[20] and Outlook 2002[21] you can configure the client to encrypt the remote procedure call (PRC) communications. This is done on the client by:

1. On the menu bar - clicking tools then select services
2. On the services page make sure you have MS Exchange server selected, and then click properties
3. Click the advanced tab
4. In the encrypt information section, select both when using the network and when using Dial-up networking options

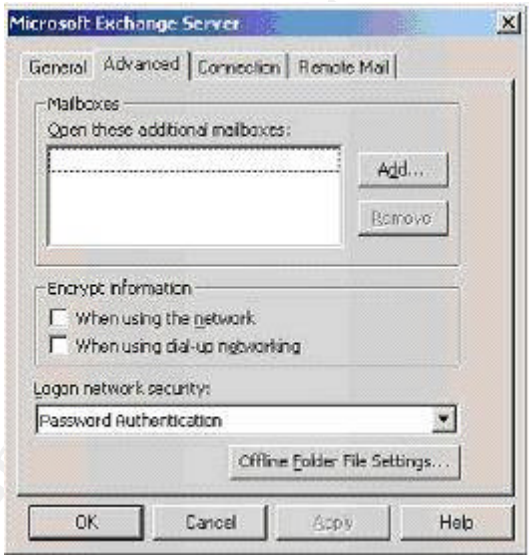



*Figure 3 – View of Encryption information*[22]

This will ensure the protection of your communications between the server and Outlook.

---

[20] Glenn, Walter & Chellis, James, "MCSE Exchange 2000 Server Administration", Alameda CA-USA, Sybex 2001, p663. ISBN 0-7821-2898-X

[21] Pitsenbarger, Trent, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000" (v1.2) (10/13/2003) http://nsa2.www.conxion.com/ Download Zipped Archive for Windows 2000 Guides and open W2k21.pdf p13 this included the picture of Microsoft Exchange Server (11/10/2003)

[22] Pitsenbarger, Trent, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000" (v1.2) (10/13/2003) http://nsa2.www.conxion.com/ Download Zipped Archive for Windows 2000 Guides and open W2k21.pdf p13 this included the picture of Microsoft Exchange Server (11/10/2003)

## Top Level Public Folder Creation and Folder Administration

The default is that the "everyone" group has full rights, which enables an ordinary user to create a top level public folder and changes its permissions. For example, when a user creates a folder ACL assigns him as the owner of it. This user then has the right to create additional sub-folder(s) and has full rights to set the permission for anyone as desired. This illustrates how undesirable ownership and permissions settings can be propagated. To resolve this potential security issue the top public folder creation should be limited only to administrators. In order to modify the settings a registry modification that was described in the section *Security Tab is Missing* will need to be implemented. An additional step is required, namely that you open the properties for the organization object in system manager and click the security tab. Clear the allow permission for the "everyone" group to create top level public folders[23]. Unfortunately this setting will have to be repeated each time a new server is added to the organization. Since the "everyone" group is added back each time a new server is added to the organization.

Once you have the top level locked down, each root folder can now be managed properly. First, each new root folder should have a new group associated with it. This group should be given ownership rights as the EA and EPEA groups do. This facilitates delegation of folder growth and security to business managers or data owners. As a matter of policy only these three groups should be owners of any public folder. Through this process of ownership non administrators can be given the Publishing Editor, Editor, Publishing Author, Author, Nonediting Author, Contributor, Reviewer, and None security settings.

Permissions on public folders are administrated through predefined roles. Each of them has some combination out of 8 permissions[24]. The permissions are:

- Folder Owner - full control over the folder, and can change permissions.
- Create Items – Can create new object within the folder.
- Create Subfolder – can create a new folder.
- Edit Item – can modify objects within a folder.
- Delete Items – can delete objects within a folder.
- Read Items – can open and view object within the folder.
- Folder Contact – Receives email notifications.
- Folder Visible – can see the folder within its hierarchy.

---

[23] Microsoft Corp, "Restricting Users from Creating Top-level Folders in Exchange", (v3.0) (10/9/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;256131&Product=exch2k (1/19/2004)

[24] Glenn, Walter & Chellis, James, "MCSE Exchange 2000 Server Administration", Alameda CA-USA, Sybex 2001, p190-195. ISBN 0-7821-2898-X

Combinations of these permissions define 9 possible roles.

- Owner – has ALL permissions above.
- Publishing Editor – has All, except for folder ownership and folder contact.
- Editor – has All, except for folder ownership, create subfolder, and folder contact.
- Publishing Author – same as Publishing Editor but can only modify their own objects.
- Author – Same as Editor but can only modify their own objects.
- Noneediting Author – Can create objects, delete their own objects, read object and folder is visible.
- Contributor – Create objects and folder visible.
- Reviewer – Read items and folder visible.
- None – Folder visible.

For higher security hidden folder hierarchy and special security through distribution lists should be considered. For such folders a root folder should be created with an ambiguous name, example: "Folder_Number_9". Then make it visible to the qualified users only[25]. Additional subfolders should be created with the right permissions and content. Again, these folders should become visible for qualified users only. This layer of abstraction can facilitate truly security for public folders. Permissions on these subfolders can be done with distribution lists – for Author, Noneditting Author, Contributor, Reviewer, and none roles. Each distribution list can assign specific roles to the subfolders. The owner of these distribution lists, of course, would be the data owner or business manager whose responsibility is to ensure that only proper users are added to these distribution lists. Any change that requires a role with higher permission, the Exchange administrators should be contacted. This would of course require a member of the EA or EPEA group to fulfill the request. No other group or user would have ownership of these folders except the EA and EPEA groups.

## Antivirus for Exchange Server

The greatest pitfall for Exchange is the high volume of viruses and worms directed at this platform. This vector of attacks has made virus detection and removal a high priority for any exchange administrator. The best one can do is to minimize potential damage of an outbreak and to create multiple levels of defense.

### The Gateway

The outside connection to the Internet is your fist opportunity to stop potential attacks. Setup a gateway server running different OS and mail system. A multitude of products are available for this purpose - ranging from Liniux server to

[25] Glenn, Walter & Chellis, James, "MCSE Exchange 2000 Server Administration", Alameda CA-USA, Sybex 2001, p194-195. ISBN 0-7821-2898-X

black box solutions. This bastion server should have software installed to scrub email attachments by type. A list of attachment types can included exe, com, scr, and many others. The goal is to make a list that can be acceptable by your company and its associates. In addition the software should be configurable for blocking specific filenames since many worms have hard-coded attachments names in them. You should also have a good network of people who can observe and read antivirus vendors web sites and news groups to learn about new alerts of potential attacks. This will give your organization an opportunity to be proactive in screening out viruses and worms. Then the server should check for viruses in the remaining attachments, scrub for spam and then send the mail to the first internal Exchange 2000 gateway mail server.

This internal gateway Exchange 2000 server should also check for viruses with a product that is manufactured by a different company then the one used on the bastion server. This mix of vendors is important - not all companies see virus releases in the wild the same way. Some create new definition files (dat file) for every variant out there as soon as possible, while others wait for the next update cycle to occur before releasing the dat file to the public.

Even with this nice gateway solution a virus or worm can still get into your mail system. It only takes one person moving an infected file on a floppy or USB mini drive or on a home made music CD or even the company laptop that shares home and work offices.

**Internal Servers**
The goal with internal servers is to protect each one with both an OS and an Exchange aware antivirus (AV). For purposes of quick updating and ease of centralized control, an enterprise solution with central internal update point should be considered. This would require all servers to run the same AV product and have them all point to one internal server for updated dat files. Most of these enterprise solutions also have an update console which can alert you of dat file version installed on each server and which one are reporting virus findings. Most can even page your support team. The main point in this part of the AV solution is to be able to manage updates quickly and be notified of a virus issue.

**Workstation Anti-Virus (AV)**
Another level of in depth AV protection, each and every workstation in your organization should have an OS AV installed. Also, if Outlook is installed an AV that can scan emails should be available. These workstations should be configures to check for updates everyday.

To resolve the issue of employee's home computer becoming a source of infection, consider start an employee compensation program for home AV software. Looking at a risk/cost analysis - it is better for the company to reimburse employees $30.00 for an AV solution then to risk losing much more with a virus outbreak. In addition some AV vendors allow for employees to install

company licensed software on home computers. This is sometimes written into companies purchased license agreements. This is a factor that should be considered when pricing enterprise AV solutions.

**Disaster Recovery**
This is your last level of defense – restoring the system to pre-infected state.

Are your servers backed up fully every week and differentially or incrementally backed-up every day? This is when you want the reassurance that you are backing up and that you have tested your backups. More information about backups is available in the section *Server Drive Configuration & Backups.*

**Configuration Issue for AV installed on Exchange 2000 Server**
There are two levels of Antivirus (AV) protection that you would like to have installed on each Exchange server. First and for most, an OS level AV that can scan both memory and files for viruses. For this to cooperate with an Exchange the following files types and folders should be excluded from scanning[26]:

- The Exchange M drive
- Exchange Log files and database files – Exchsrvr\Mdbdata
- Exchange MTA files – Exchsrvr\Mtadata
- Additional log files - Exchsrvr\server_name.log
- Virtual server folder – Exchsrvr\Mailroot
- Working folder used for file conversion – Exchsrvr\MDBData
- Site Replication Service (SRS) – Exchsrvr\Srsdata folder
- IIS system files %SystemRoot%\System32\Inetsrv folder
- In addition whenever you use the offline maintenance utilities such as Eseutil.exe they should be used in a temp folder where the AV is not actively engaged.

Also the following four file extension types should be excluded from memory resident file scanner: edb, stm, chk and log[27].

Secondly, an Exchange 2000 aware AV that can scan mail in the Information Store and remove infected files before they become a problem. There are many types of scanners that support this process. They are MAPI scanners, VAPI/AVAPI & VSAPI scanners, and finally ESE-bases scanners. MAPI scanners do not work well on live email system and are unable to scan an infected email before a user opens the message[28]. There are other drawbacks that should make MAPI our least likely AV scanner type. The next is the VAPI,

[26] Microsoft Corp, "XADM: Exchange and Avtivirus Software" (v7.1) (12/12/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k (1/19/2004)
[27] Microsoft Corp, "XADM: Exchange and Avtivirus Software" (v7.1) (12/12/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k (1/19/2004)
[28] Microsoft Corp, "XADM: Exchange and Avtivirus Software" (v7.1) (12/12/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k (1/19/2004)

AVAPI, and VSAPI scanners. They all do a great job in scanning and removing viruses and are supported by Microsoft telephone tech support. The best version of this variety is the newly supported VAPI 2.0 version, which can be used on Exchange 2000 with SP1. This version of VAPI can proactively scan attachments and remove issues before a user even opens the attachment. VAPI 2.0 is even better then waiting for user's action to initiate the scanning process, which is the default for VAPI 1.0. Finally, ESE base scanners which add a layer of code in between the IS and other parts of Exchange 2000. So that all information going into or out of the IS is scanned. This scanner type is not supported by Microsoft. In reviewing the various scanner types, VAPI 2.0 has the best features and support.

## Network Consideration for an Exchange

A domain controller which is also functioning as a global catalog server should be on each physical network or geographical site. This will allow for easy AD queries and quick response times.

For Exchange to properly communicate, the servers - in a single routing group - are required to have a good connection between them. For all practical experience this means a single network segment. Although Microsoft touts the added feature to allow communications on multiple routing groups between servers on a single administrative group, this added feature does not enhance security nor is it available if the exchange environment is running in mixed mode. A potential security issue arises with these server communications with each other, since these communications are unencrypted. This potential wire ease dropping can be eliminated in two ways.

**IP Security (IPSec)**
IPSec can be enabled on each exchange server. This is a function of the Windows 2000 OS and can be administrated through AD and IPSec policies[29]. This will allow for servers to encrypt all data transferred between them. This is a powerful added security feature for the Widows 2000 environment and can add security not just for Exchange but for all other applications services as well. There is one major drawback that has been identified with this solution. Routing protocols RIP, RIP version2, and Open Shortest Path First (OSPF) cannot be used with IP Security (IPSec) or IP-to-IP tunnels[30]. To resolve this shortcoming you can use routing protocols such as Layer 2 tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP).

[29] Robichaux, Paul & Chellis, James, "MCSE Windows 2000 Network Infrastructure Administration", Alameda CA-USA, Sybex, 2001. Chapter 11: "Managing IP Security" p 495-546 ISBN 0-7821-2949-8
[30] Microsoft Corp, "IPSec and IP-to-IP tunnels do not work with routing Protocols such as RIP and OSPF", (v2.0),(11/13/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;227523&Product=win2000 (Jan/19/2004)

**Key Management Server (KMS)**
The use of Key Management Server requires a certificate of authority server (CA) to be established somewhere within the enterprise. In addition, three certificate templates are required to be installed on the CA server before KMS can be installed.

- Enrollment Agent
- Exchange User
- Exchange Signature Only

During the install a KMS password is generated, this password will be needed each time the service is stated. The password can be copied in two ways. You can manually copy it on a piece of paper or copied it to two floppy disks. The first disk is the original; the second is a backup copy. The server running KMS will need this disk or the password typed in each and every time it's booted or the service is restarted. The service by default does not start automatically, you can configure this if one of the floppies is available in the A drive. The password can be reset if there is a change in your employment team. From a security stand point it is obvious that neither of these methods are optimal.

Once KMS allows Exchange 2000 users to encrypt email and digitally sign email, your enterprise is truly secure, if everyone uses these features in every email sent. This can be configured within each Outlook client to sign and encrypt all email.

Any email that can be sniffed on the line will be encrypted and illegible. This is by far the best way to safeguard Microsoft Exchange 2000 email system. The release notes found on the CD (\realeasenotes.html) give a great overview of how to implement KMS and CA authority in your enterprise.

The only draw back to this very nice solution is the extra availability of exchange administrators. If the KMS server goes down, someone will have to be available to start it up with the correct password. This in conjunction with the extra servers required to implement the solution. These essentially why so few of these systems are used worldwide.

## Some final thoughts: Passwords and C.I.A Security

The most basic of all security principles – passwords should be complex and lengthy – to insure integrality[31]. A ten or more characters combining Arabic numbers and special characters for any account with administrative privileges should meet security requirements.

[31] Ullirch, J., "Windows XP: Surviving the First Day", (v1.1) (11/23/2003) http://www.sans.org/rr/papers/index.php?id=1298 p2(1/20/2004)

Some features described in this document such as AV console and KMS have a single shared ID and may result in some CIA issues, but changing the passwords often and whenever a team changes occurs should alleviate this issue.

The basic principles of confidentiality, integrity, and availability [32] can best be seen when examining a mail system. Each definition lends itself to an aspect of email security, to enhance each:

Confidentiality – Encrypted every part of your Exchange 2000 email system, all network traffic until it exits your system via the gateway to the internet.

Integrity – Keep close control over ACL with in your email systems, especially on public folders.

Availability - Be sure to keep your IS relatively small so that a restore of the database takes only a few hour with your backup system. Keep additional warm spare computer available on each site for quick turn around of hardware issues.

## Conclusion

This document is a beginning for Exchange 2000 security infrastructure. And, it aligned some aspects of security and CIA that can now be handled. Here is the summary:

- With proper groups you can now control access to Exchange administrative functions. Given detailed level of permissions to perform functions within an Exchange 2000 environment.
- Proper file/share permissions to harden mail servers.
- Full and proper backups – full with incremental and/or differential.
- Proper uses of AV scan system.
- In depth virus protection.
- IPSec or KMS features to fully secure your email system

Generally speaking, the underling issue for all true security issues lies with cost. Is worth the cost of securing the system versus the potential financial loss derived from malicious attacks or security laps? This risk analysis needs to be performed for any your organization that is interest in safeguarding its valuable resources.

[32] Krutz, Ronald & Vines, Russell, "The CISSP Prep Guide – gold edition", Indianapolis, Indiana-USA, Wiley Publishing Inc 2003, p3 ISBN 0-471-26802-x

## References


1. Microsoft Corp, "Microsoft Exchange Server Winning the Enterprise with 100 Million Seats sold" (Jan 23, 2002) http://www.microsoft.com/presspass/press/2002/jan02/01-23MarketLeaderPR.asp (Jan 20, 2004)
2. Pitsenbarger, Trent, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000" (v1.2) (10/13/2003) http://nsa2.www.conxion.com/ Download Zipped Archive for Windows 2000 Guides and open W2k21.pdf p5-7 (11/10/2003)
3. Pitsenbarger, Trent, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000" (v1.2) (10/13/2003) http://nsa2.www.conxion.com/ Download Zipped Archive for Windows 2000 Guides and open W2k21.pdf p5-7 (11/10/2003)
4. Microsoft Corp, "Minimum permissions Necessary to Perform Exchange-Related Tasks", (v8.0) (10/9/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;316792&Product=exch2k (1/17/2004)
5. Glenn, Walter & Chellis, James, "MCSE Exchange 2000 Server Administration", Alameda CA-USA, Sybex 2001, p591-592.ISBN 0-7821-2898-X
6. Glenn, Walter & Chellis, James, "MCSE Exchange 2000 Server Administration", Alameda CA-USA, Sybex 2001, p594-596. ISBN 0-7821-2898-X
7. Glenn, Walter & Chellis, James, "MCSE Exchange 2000 Server Administration", Alameda CA-USA, Sybex 2001, p592-593. ISBN 0-7821-2898-X
8. Microsoft Corporation, "XADM: How to Set Up Exchange 2000" (8/14/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;262068&Product=exch2k (1/20/2004)
9. Pitsenbarger, Trent, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000" (v1.2) (10/13/2003) http://nsa2.www.conxion.com/ Download Zipped Archive for Windows 2000 Guides and open W2k21.pdf p6 (11/10/2003)
10. Microsoft Corp, "XADM: How to Enable Message Tracking in Exchange 2000 Server" (v1.1) (6/17/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;246856&Product=exch2k (1/19/2003)
11. Microsoft Corp, "XADM: Tracking log and Queue Viewer Allows Access to Message Subject" (v1.1) (6/17/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;246867&Product=exch2k (1/19/2004)
12. Microsoft Corp, "How to change the share permissions on the Message Tracking share in Exchange 5.5 and in Exchange 2000" (v1.0) (8/25/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;825222&Product=exch2k (1/19/2004)

13. Microsoft Corp, “Set Size Limits for Messages”, (v6.0) (12/18/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;322679&Product=exch2k (1/18/2004)
14. Microsoft Corp, “XADM: Security Tab Not available on All Objects in System Manager”, (v1.2) (7/8/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;259221&Product=exch2k (1/18/2004)
15. Glenn, Walter & Chellis, James, “MCSE Exchange 2000 Server Administration”, Alameda CA-USA, Sybex 2001, p624-627. ISBN 0-7821-2898-X
16. Glenn, Walter & Chellis, James, “MCSE Exchange 2000 Server Administration”, Alameda CA-USA, Sybex 2001, p624-627. ISBN 0-7821-2898-X
17. Microsoft Corp, “How to: Help Secure Post Office Protocol Client Access in Exchange 2000”, (v2.0) (6/25/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;319273&Product=exch2k (1/19/04)
18. Glenn, Walter & Chellis, James, “MCSE Exchange 2000 Server Administration”, Alameda CA-USA, Sybex 2001, p624-627. ISBN 0-7821-2898-X
19. Microsoft Corp, “How to: Secure Internet Message Access Protocol Client Access in Exchange 2000” (v1.3) (6/5/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;319278&Product=exch2k (1/24/2004)
20. Glenn, Walter & Chellis, James, “MCSE Exchange 2000 Server Administration”, Alameda CA-USA, Sybex 2001, p663. ISBN 0-7821-2898-X
21. Pitsenbarger, Trent, “Guide to the Secure Configuration and Administration of Microsoft Exchange 2000” (v1.2) (10/13/2003) http://nsa2.www.conxion.com/ Download Zipped Archive for Windows 2000 Guides and open W2k21.pdf p13 this included the picture of Microsoft Exchange Server (11/10/2003)
22. Pitsenbarger, Trent, “Guide to the Secure Configuration and Administration of Microsoft Exchange 2000” (v1.2) (10/13/2003) http://nsa2.www.conxion.com/ Download Zipped Archive for Windows 2000 Guides and open W2k21.pdf p13 this included the picture of Microsoft Exchange Server (11/10/2003)
23. Microsoft Corp, “Restricting Users from Creating Top-level Folders in Exchange”, (v3.0) (10/9/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;256131&Product=exch2k (1/19/2004)
24. Glenn, Walter & Chellis, James, “MCSE Exchange 2000 Server Administration”, Alameda CA-USA, Sybex 2001, p190-195. ISBN 0-7821-2898-X

25. Glenn, Walter & Chellis, James, “MCSE Exchange 2000 Server Administration”, Alameda CA-USA, Sybex 2001, p194-195. ISBN 0-7821-2898-X
26. Microsoft Corp, “XADM: Exchange and Avtivirus Software” (v7.1) (12/12/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k (1/19/2004)
27. Microsoft Corp, “XADM: Exchange and Avtivirus Software” (v7.1) (12/12/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k (1/19/2004)
28. Microsoft Corp, “XADM: Exchange and Avtivirus Software” (v7.1) (12/12/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k (1/19/2004)
29. Robichaux, Paul & Chellis, James, “MCSE Windows 2000 Network Infrastructure Administration”, Alameda CA-USA, Sybex, 2001. Chapter 11: “Managing IP Security” p 495-546 ISBN 0-7821-2949-8
30. Microsoft Corp, “IPSec and IP-to-IP tunnels do not work with routing Protocols such as RIP and OSPF”, (v2.0),(11/13/2003) http://support.microsoft.com/default.aspx?scid=kb;en-us;227523&Product=win2000 (Jan/19/2004)
31. Ullirch, J., “Windows XP: Surviving the First Day”, (v1.1) (11/23/2003) http://www.sans.org/rr/papers/index.php?id=1298 p2 (1/20/2004)
32. Krutz, Ronald & Vines, Russell, “The CISSP Prep Guide – gold edition”, Indianapolis, Indiana-USA, Wiley Publishing Inc 2003, p3 ISBN 0-471-26802-x

# Appendix A

This section is a direct copy from Microsoft Knowledge base article Q316792 "Minimum permissions Necessary to Perform Exchange-Related Tasks"
http://support.microsoft.com/default.aspx?scid=kb;en-s;316792&Product=exch2k

## Part 1:

**autoReplyMessage**
**adminDisplayName**
**displayName**
**dLMemDefault**
**homeMDB**
**homeMTA**
**legacyExchangeDN**
**mail**
**mailNickname**
**mAPIRecipient**
**mDBUseDefaults**
**msExchADCGlobalNames**
**msExchControllingZone**
**msExchFBURL**
**msExchHideFromAddressLists**
**msExchHomeServerName**
**msExchMailboxGuid**
**msExchMailboxSecurityDescriptor**
**msExchPoliciesExcluded**
**msExchPoliciesIncluded**
**msExchResourceGUID**
**msExchUserAccountControl**
**proxyAddresses**
**quotaNotificationStyle**
**quotaNotificationSchedule**
**showInAddressBook**
**targetAddress**
**textEncodedORAddress**

## Part 2:

**adminDisplayName**
**altRecipient**
**authOrig**
**autoReplyMessage**
**deletedItemFlags**
**delivContLength**
**deliverAndRedirect**
**displayNamePrintable**
**dLMemDefault**
**dLMemRejectPerms**
**dLMemSubmitPerms**
**extensionAttribute1**
**extensionAttribute2**
**extensionAttribute3**
**extensionAttribute4**
**extensionAttribute5**

**extensionAttribute6**
**extensionAttribute7**
**extensionAttribute8**
**extensionAttribute9**
**extensionAttribute10**
**extensionAttribute11**
**extensionAttribute12**
**extensionAttribute13**
**extensionAttribute14**
**extensionAttribute15**
**folderPathname**
**garbageCollPeriod**
**hideDLMembership**
**homeMDB**
**homeMTA**
**internetEncoding**
**legacyExchangeDN**
**mail**
**mailNickname**
**mAPIRecipient**
**mDBOverHardQuotaLimit**
**mDBOverQuotaLimit**
**mDBUseDefaults**
**mDBStorageQuota**
**msExchADCGlobalNames**
**msExchControllingZone**
**msExchExpansionServerName**
**msExchFBURL**
**msExchHideFromAddressLists**
**msExchHomeServerName**
**msExchMailboxGuid**
**msExchMailboxSecurityDescriptor**
**msExchPoliciesIncluded**
**msExchPoliciesExcluded**
**msExchRecipLimit**
**msExchResourceGUID**
**oOFReplyToOriginator**
**protocolSettings**
**proxyAddresses**
**publicDelegates**
**quotaNotificationSchedule**
**quotaNotificationStyle**
**reportToOriginator**
**reportToOwner**
**securityProtocol**
**showInAddressBook**
**submissionContLength**
**targetAddress**
**textEncodedORAddress**
**unauthOrig**

## Part 3:

**homeMDB**
**homeMTA**
**msExchHomeServerName**
**targetAddress**

Last Updated: July 25th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS Boston 2017 | Boston, MA | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| Community SANS Omaha SEC401* | Omaha, NE | Aug 14, 2017 - Aug 19, 2017 | Community SANS |
| SANS New York City 2017 | New York City, NY | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS Salt Lake City 2017 | Salt Lake City, UT | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS Virginia Beach 2017 | Virginia Beach, VA | Aug 21, 2017 - Sep 01, 2017 | Live Event |
| SANS Adelaide 2017 | Adelaide, Australia | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style | Virginia Beach, VA | Aug 21, 2017 - Aug 26, 2017 | vLive |
| SANS Chicago 2017 | Chicago, IL | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| Community SANS Pasadena SEC401 @ NASA | Pasadena, CA | Aug 23, 2017 - Aug 30, 2017 | Community SANS |
| Mentor Session - SEC401 | Minneapolis, MN | Aug 29, 2017 - Oct 10, 2017 | Mentor |
| SANS San Francisco Fall 2017 | San Francisco, CA | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| SANS Tampa - Clearwater 2017 | Clearwater, FL | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| Mentor Session - SEC401 | Edmonton, AB | Sep 06, 2017 - Oct 18, 2017 | Mentor |
| SANS Network Security 2017 | Las Vegas, NV | Sep 10, 2017 - Sep 17, 2017 | Live Event |
| Community SANS Albany SEC401 | Albany, NY | Sep 11, 2017 - Sep 16, 2017 | Community SANS |
| Mentor Session - SEC401 | Ventura, CA | Sep 11, 2017 - Oct 12, 2017 | Mentor |
| Community SANS Columbia SEC401 | Columbia, MD | Sep 18, 2017 - Sep 23, 2017 | Community SANS |
| Community SANS Dallas SEC401 | Dallas, TX | Sep 18, 2017 - Sep 23, 2017 | Community SANS |
| Community SANS Boise SEC401 | Boise, ID | Sep 25, 2017 - Sep 30, 2017 | Community SANS |
| Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style | Baltimore, MD | Sep 25, 2017 - Sep 30, 2017 | vLive |
| Community SANS New York SEC401 | New York, NY | Sep 25, 2017 - Sep 30, 2017 | Community SANS |
| Rocky Mountain Fall 2017 | Denver, CO | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS London September 2017 | London, United Kingdom | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS Baltimore Fall 2017 | Baltimore, MD | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS Copenhagen 2017 | Copenhagen, Denmark | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Community SANS Sacramento SEC401 | Sacramento, CA | Oct 02, 2017 - Oct 07, 2017 | Community SANS |
| SANS DFIR Prague 2017 | Prague, Czech Republic | Oct 02, 2017 - Oct 08, 2017 | Live Event |
| Community SANS Charleston SEC401 | Charleston, SC | Oct 02, 2017 - Oct 07, 2017 | Community SANS |
| Mentor Session - SEC401 | Arlington, VA | Oct 04, 2017 - Nov 15, 2017 | Mentor |
| Community SANS Indianapolis SEC401 | Indianapolis, IN | Oct 09, 2017 - Oct 14, 2017 | Community SANS |