SECURING
AN EXCHANGE 2000 OWA FRONTEND SERVER
WITH SECURITY TEMPLATES

Nelly Chien

GIAC Certified Windows Security Administrator (GCWN)
Practical Assignment
Version 3.1 (revised April 8, 2002)
Option 2 – Securing Windows 2000 With Security Templates

ABSTRACT

Microsoft Exchange 2000 server is a widely deployed enterprise messaging platform. Its Outlook Web Access (OWA) component provides web-based access to messaging data such as mail, calendaring and contacts. It is the purpose of this paper to select a publicly available security template, and to evaluate its effectiveness on an Exchange 2000 OWA server. The evaluation process will include application method, settings description, impact on functionality, and possible modification of the selected template. Other necessary security measures that are not configurable using a template file will also be discussed briefly.

TABLE OF CONTENTS

1 INTRODUCTION

Microsoft Corporation released its first enterprise messaging solution with Microsoft Exchange Server 4.0 in July of 1996. Since Exchange 4.0, Microsoft has offered increased functionality, robustness and security for its messaging product with Exchange version 5.0, Exchange version 5.5, and Exchange 2000. As of the writing of this paper, Exchange 2000 is the latest version of Exchange Server available. (Note that the next version, Exchange 2003, is scheduled for release in mid 2003.) According to a press release by Microsoft in January of 2002 [Ref: 13], Microsoft Exchange Server has a 43 percent install base of the messaging market, and that over a million Exchange 2000 licenses have been sold.

For many companies and corporations that have deployed Exchange 2000, deploying a web based solution that allows user HTTP / HTTPS access to the messaging environment offers many benefits. Exchange Outlook Web Access (OWA) allows users to check email virtually anywhere - on the road, at home and while vacationing. The only requirements for access are an Internet connection and a web browser. In a corporate environment, OWA can provide multi-platform (Macintoshes, UNIX, Linux, and Windows) access to the messaging system; it can also service the messaging needs of multiple users from a single desktop system (For example: on a manufacturing floor, or a public kiosk).

It is the purpose of this paper is to address the security concerns for deploying an Exchange 2000 Outlook Web Access Front End server. Specifically, this paper will attempt to identify publicly available security templates for Exchange 2000 OWA, to discuss the security settings of a selected set of templates, to detail the procedures for application of the templates, and to report on the effectiveness of the selected templates.

2 SYSTEM DESCRIPTION

To establish a common ground for discussion of the security issues relating to a Microsoft Exchange 2000 Outlook Web Access (OWA) Front End (FE) server, we will briefly describe the Active Directory architecture, the Exchange 2000 architecture, specific configuration settings, system requirements, and security requirements for our test Exchange 2000 OWA FE system.

2.1 General Architecture

An Exchange 2000 Outlook Web Access (OWA) server is a Windows 2000 server with Exchange 2000 installed. It is a member server in the Active Directory domain where the corporate Exchange Organization is installed, and a member of the corporate Exchange Organization. Web based access to information stored in the Exchange databases is provided through the Internet Information Server (IIS) 5.0 component of Windows 2000, the Exchange HTTP Internet Application Programming Interface (ISAPI), and the Exchange Web Storage System. The Web Distribution Authoring and Versioning (WebDAV) extension of HTTP is also employed to enhance performance and usability for Outlook Web Access clients.

An Exchange 2000 Front-End (FE) server is an Exchange 2000 server configured to proxy client requests to an appropriate Back-End Exchange 2000 server. User data is stored on the back-end server, and not on the front-end server. When a front-end server receives a user request, it queries the corporate Domain Name Server for location of directory servers, then it queries a Windows 2000 Active Directory server for the location of the requested data, authenticates the user, and returns the requested data to the user. Note that the option to configure an Exchange server as a front-end server is available only on Exchange 2000 Enterprise Edition.

An Exchange 2000 Outlook Web Access (OWA) Front-End (FE) server is an Exchange 2000 OWA server configured in Front End mode. This specific Exchange server proxies HTTP/HTTPS request for Exchange data, and provides Exchange users secured web based access to mail, calendaring, contacts, as well as to information stored in Exchange's Public Folder.

Our Exchange 2000 OWA Front-End server is physically located in the DMZ zone. It is situated behind the Internet firewall, and in front of the corporate Intranet firewall. The Internet firewall is configured to allow HTTPS access to the Exchange 2000 OWA FE server, and the Intranet firewall is configured to allow the Exchange 2000 OWA FE server to access all Back-End Exchange server, Active directory domain controllers, as well as the corporate Domain Name Service servers.

2.2 System Requirements

The functional requirements for our Exchange 2000 OWA FE server are as follows:

The Exchange 2000 OWA FE server must provide basic Exchange messaging functionalities such as the ability to send and receive email, to view calendar and contacts information, to schedule appointments, and to access Public Folder information. As these are built-in Exchange functionalities, no special configuration is necessary.

Exchange users must be able to access their mailboxes using implicit sign-on. Implicit sign-on allows a user to access his/her mailbox without specifying his/her mailbox alias explicitly within the URL request. To fulfill this access requirement, our Exchange 2000 OWA FE server needs to be in dual-authentication mode. Besides the benefit of implicit sign-on, as a front-end server in dual-authentication mode authenticates a user request before proxying it to a back-end server, dual-authentication also protects the back-end server from denial-of-service attacks. Dual-authentication support requires RPC communication between the front-end server and back-end domain controllers, and additional configuration on the Intranet firewall will be necessary.

The front-end OWA server is also required to allow direct HTTPS access to certain Exchange public folders. To fulfill this functional requirement, additional virtual directories need to be set up on both the front-end and the back-end Exchange servers.

Detailed information on implication and configuration of the above-required functionalities can be found at:

1. KC Lemson and M. Martin, "Using Microsoft Exchange 2000 Front-End Servers", Microsoft Exchange Server Series, October 2002.
2. Microsoft Knowledge Base Article Q224196 "Restricting Active Directory Replication Traffic to a Specific Port"

2.3 Security Requirements

The security requirements for our Exchange 2000 OWA FE server are as follows:

As Basic Authentication must be enabled on the front-end server for support of dual authentication, to achieve password security, Secure Sockets Layer (SSL) encryption must be used when client communicates with front-end server. In addition to enabling and configuring SSL, we will also redirect the default Exchange OWA URL (http://server.domain.com/exchange) to https://server.domain.com/exchange.

As our Exchange 2000 OWA FE server resides in an Internet-exposed perimeter network, no local Exchange data should reside on this server. To ensure that no Exchange messaging data reside locally, the default Exchange mailbox store and public folder store will be deleted on the front-end server.

Since no data will be stored locally on the server, and all Exchange back-end servers are protected by TrendMicro's ScanMail for Exchange v. 5.1, no virus protection software or backup software agent is required on the Exchange 2000 OWA FE server.

As Internet Information Server 5.0 is a key component of an Exchange OWA server, and its default installation state in notoriously unsecured, measures to harden IIS against possible attacks should include:

- Remove all unnecessary ISAPI extensions and filters
- Remove all sample applications, administrative scripts and help files
- Move website root directory from the system partition
- Tighten NTFS permissions on system utilities
- Remove support for Remote Data Service (RDS)
- Install URLScan.dll ISAPI filter
- Enable HTTP Protocol Logging

To further harden the Exchange 2000 OWA FE server against attackers, all unnecessary system services should be disabled on the system. The system should only run the minimal set of services required for its operation.

Also, security auditing needs to be enabled to provide alerts for potential security breach. In additional to failure access audits, success access audits should also be enabled for account management, policies and configuration updates.

To ensure that this server downloads and installs patches and hot-fixes approved by an administrator, it needs to be a member of the corporate "Software Update Services" (SUS) environment. Windows Update component on the Exchange 2000 OWA FE server must be able to connect to the corporate SUS server, and to download and install patches as configured by the SUS administrator.

Detailed information on implication and configuration on some of the above-required functionalities can be found at:

1. KC Lemson and M. Martin, "Using Microsoft Exchange 2000 Front-End Servers", Microsoft Exchange Server Series, October 2002.
2. Microsoft Knowledge Base Article Q279681 "How to Force SSL Encryption for an Outlook Web Access 2000 Client"
3. Microsoft Knowledge Base Article Q268822 "OWA How to Redirect http://<server_name>/exchange Users to Use https:// Prefix"
4. J. Fossen, "Securing Windows 5.5: Securing Internet Information Server", SANS Institute, 2002.
5. Microsoft Corporation, Software Update Services Deployment White Paper.

3 System Configuration

The following is a brief description of the hardware and software configuration of our Exchange 2000 OWA Front-End Server.

3.1 Hardware Configuration

- Dell PowerEdge 1550
- Dual Pentium III 1.0 GHz Processor
- 1 GB of RAM
- Two 4 GB SCSI disk – hardware mirrored
- Logical Drives:
  - C:\ - 2 GB (System Drive)
  - D:\ - 1 GB (Exchange 2000 binaries)
  - E:\ - 1 GB (Website Data)

3.2 Software Configuration

- Microsoft Windows 2000 Server (Member of corporate Active Directory domain)
- Microsoft Windows 2000 Server Service Pack 3
- Microsoft Exchange 2000 Enterprise Edition (Member of corporate Exchange Organization)
- Exchange 2000 Service Pack 3
- Hotfixes Installed:
  - Q323172
  - Q324096
  - Q324380
  - Q326830
  - Q326886
  - Q327696
  - Q329115
  - Q329834
  - Q328310
  - Q329170
  - Q810833

3.3 Exchange 2000 Configuration

- Set Exchange 2000 server in "Front-End" mode.
- Deleted default Mailbox store and Public store.
- Created additional Virtual HTTP servers to match those on Back-End servers.

3.4 Internet Information Server Configuration

- Installed SSL certificate for default OWA website. Configured website to require 128 bit SSL access.
- Redirected all HTTP request for default OWA website to HTTPS.
- Set access permission for all HTTP virtual directories to allow Basic Authentication.

Detailed information on Exchange 2000 configuration and Intranet firewall requirements can be found at:

1. KC Lemson and M. Martin, "Using Microsoft Exchange 2000 Front-End Servers", Microsoft Exchange Server Series, October 2002.

4 IDENTIFYING PUBLICLY AVAILABLE SECURITY TEMPLATES

To properly secure an Exchange 2000 Outlook Web Access Front End server, a search on security templates for Windows 2000 domain member server, Exchange 2000 server, and Internet Information Server 5.0 has been performed at the following organizations and agencies:

Center for Internet Security (CIS)
SANS Institute
National Security Agency (NSA)
Defense Information Systems Agency (DISA)
National Institute of Stands and Technology (NIST)
Microsoft Corporation

The following table lists some publicly available security templates from the above organizations that are relevant to the task at hand:

Templates	Description
CIS-Win2k-Level-1-v.1.1.inf	Center for Internet Security's Windows 2000 Level 1 security template. Developed by Microsoft Corporation for CIS. http://www.cisecurity.org/
W2k_server.inf	NSA's security template for Windows 2000 member or standalone servers. http://nsa1.www.conxion.com/win2k/download.htm
Hisecweb.inf	Microsoft's security template for a Windows 2000 web server http://download.microsoft.com/download/win2000srv/SCM/1.0/NT5/EN-US/hisecweb.exe
SecureInternetWebServer.inf	Windows 2000 Resource Kit Secure Internet Web Server template Available on Windows 2000 Resource Kit CDROM
Basicsv.inf	Microsoft's default server security template. Installed by default to %systemroot%\security\templates\
Baseline.inf	Microsoft's baseline template for Windows 2000 Application Server. Part of "Security Operations Guide for Windows 2000 Server" by Microsoft Corporation.
IIS Incremental.inf	An incremental security template for IIS 5.0 server, to be applied on top of baseline.inf. Part of "Security Operations Guide for Windows 2000 Server" by Microsoft Corporation.
OWA FrontEnd Incremental.inf	An incremental security template for Exchange 2000 OWA FrontEnd server, to be applied on top of baseline.inf. Part of "Security Operations Guide for Exchange 2000 Server" by Microsoft Corporation.

From the list of templates presented above, only "OWA FrontEnd Incremental.inf" is specifically tailored for an Exchange 2000 Outlook Web Access server in Front End mode. As Microsoft specifically develops this template for our target system, one would expect the combination of "baseline.inf" and "OWA FrontEnd Incremental.inf" templates to create a security configuration that best suit our needs. It is with this in mind that we select these two templates for deployment and evaluation here.

Application and settings of these two selected templates are discussed in "Security Operations Guide for Windows 2000 Server" [Ref: 17] and "Security Operations Guide for Exchange 2000 Server" [Ref: 16]. It is expected that the selected templates will significantly tighten security on the system by modifying user rights, tightening file system and Windows registry access, configuring audit policies, and disabling unnecessary services.

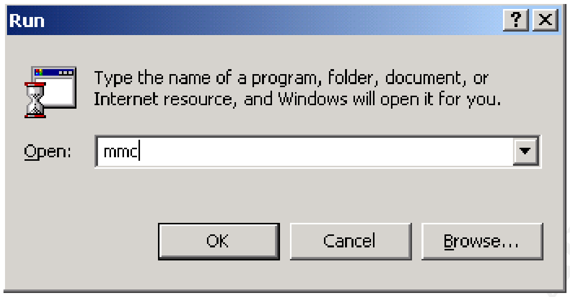
As our selected templates are developed specifically for our target system, we expect that OWA functionality would not be impaired by application of the templates. However, as participation in a Software Update Services environment is an additional requirement for our system, it is uncertain if the templates settings will impact that functionality.

5 Template Settings

Detailed settings in our selected templates can be viewed using the “Security Template” snap-in available in Microsoft Management Console (MMC). One should always view and understand all security settings within a template before applying it.

To view the settings of a specific security template, one starts by:

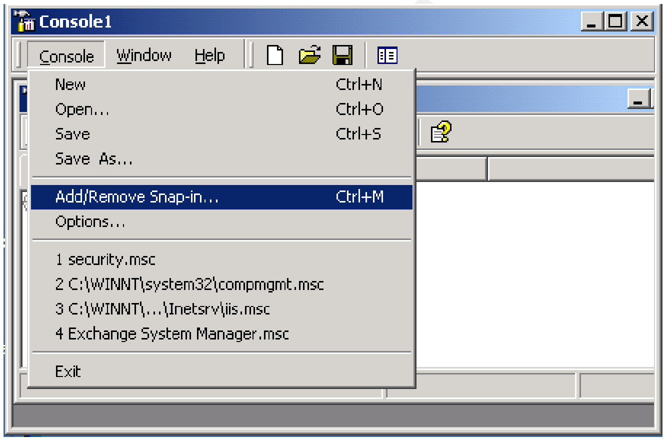
Bringing up a skeleton MMC console by clicking **Start**, select **Run**, and **Open** “mmc”



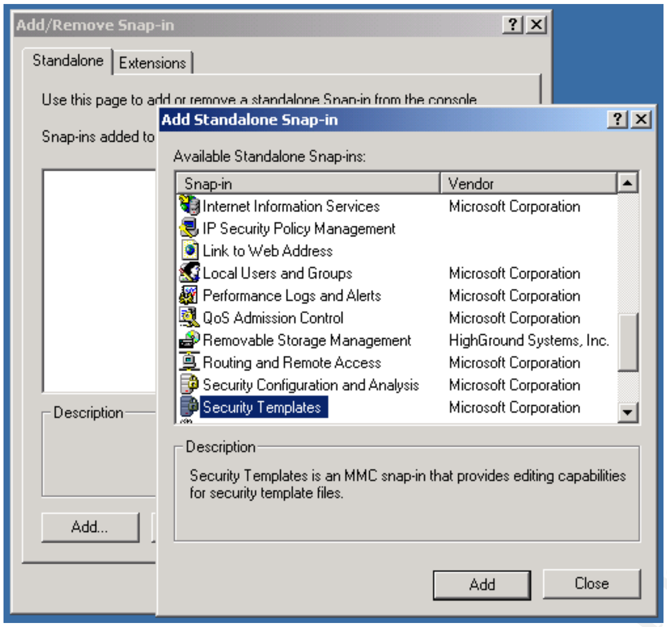
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

From the skeleton MMC console, select **Console** from the menu, and select **Add/Remove Snap-in.**


Console1
Console
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 security.msc
2 C:\WINNT\system32\compmgmt.msc
3 C:\WINNT\...\Inetsrv\iis.msc
4 Exchange System Manager.msc
Exit

Click **Add** in the Add/Remove Snap-in Window; Select “**Security Templates**” in the Add Standalone Snap-in windows; Click **Add**; Click **Close**; Click **OK**



Use this page to add or remove a standalone Snap-in from the console.

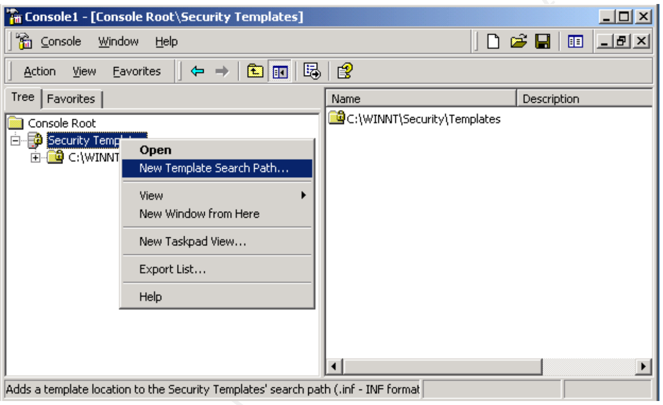
Available Standalone Snap-ins:

Snap-in	Vendor
Internet Information Services	Microsoft Corporation
IP Security Policy Management	
Link to Web Address	
Local Users and Groups	Microsoft Corporation
Performance Logs and Alerts	Microsoft Corporation
QoS Admission Control	Microsoft Corporation
Removable Storage Management	HighGround Systems, Inc.
Routing and Remote Access	Microsoft Corporation
Security Configuration and Analysis	Microsoft Corporation
Security Templates	Microsoft Corporation

Description

Security Templates is an MMC snap-in that provides editing capabilities for security template files.

From the MMC Console, right click on **Security Templates** and select **New Template Search Path**

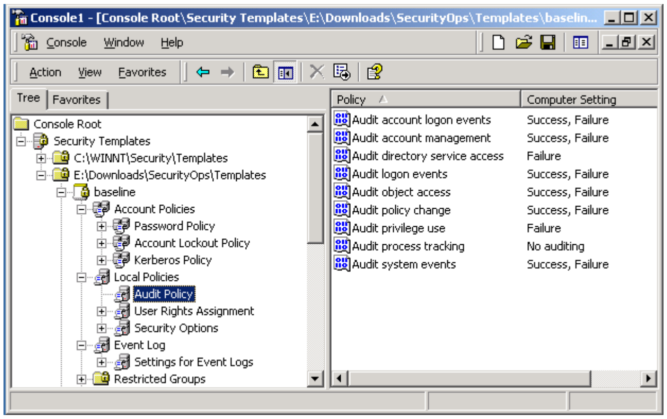


C:\WINNT\Security\Templates

Adds a template location to the Security Templates' search path (.inf - INF format

Browse to the path of the targeted security templates, and click **OK**.

The resulting MMC console will resemble the following:



Console1 - [Console Root\Security Templates\E:\Downloads\SecurityOps\Templates\baselin...

```
Console Root
  Security Templates
    C:\WINNT\Security\Templates
    E:\Downloads\SecurityOps\Templates
      baseline
        Account Policies
          Password Policy
          Account Lockout Policy
          Kerberos Policy
        Local Policies
          Audit Policy
          User Rights Assignment
          Security Options
        Event Log
          Settings for Event Logs
        Restricted Groups
```

Policy	Computer Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

Using the custom MMC console created above, we can explore the settings of our selected templates. Only explicitly defined settings will be discussed in this section.

5.1 Microsoft's baseline template for Windows 2000 Application Server: Baseline.inf

5.1.1 Account Policies:

No policy defined.

5.1.2 Audit Policies:

Audit policies define whether occurrence of certain event will be logged in the System's Security Log. Proper security logging alerts administrators of potential security breach, and provides valuable information for investigation of such breach. By default, security auditing is turned off on Windows 2000 Server systems.

Audit Policies in baseline.inf are defined as follows:

Account Logon Events – Audit Success and Failure
Audit events related to a user or a system logging on to the domain or system. When a user logs on with a domain account, "Account Logon" events are logged on the authenticating domain controller. On a member server, "Account Logon" events audit login attempts with an account in the local SAM database. For our Exchange 2000 OWA FE server, only two local user accounts (ISUR_<%systemname%> & IWAM_<%systemname%>) should generate Account Logon Events on the local system; all other audit entries in this category should be examined closely.

Account Management – Audit Success and Failure
Audit events related to changes in the local SAM database. Modification of accounts, groups, and group membership are recorded. As hackers might attempt to enable a

disabled account, change an account password, or cause an account to be locked-out during a brute-force password attack, it is important to enable auditing for this category.

Directory Service Access – Audit Failure Only
Audit events related to Active Directory containers' and objects' access. To configure auditing of objects, in addition to enabling auditing of Directory Service Access, all objects targeted for audit needs to have their System Access Control List (SACL) updated. In the SACL, auditing should be enabled for the Everyone group to capture all unauthorized access. Due to high amount of successful audits generated in normal operation, only failure events should be audited.

Logon Events – Audit Success and Failure
Audit events related to a domain user, a local user or a system accessing the server either locally or remotely. Events logged include use of incorrect password, and logon attempt by a disabled or expired account. Failure audits will alert administrators of unauthorized access. Successful audits will assist administrator in determining the method of breach should the system become compromised.

Object Access – Audit Success and Failure
Audit events related to access of local resources, including files, folders, printers & system registry keys. Similar to "Directory Service Access", the target object's SACL needs to be updated by enable auditing for the Everyone group. Failure audits will alert administrators of unauthorized access attempts.

Policy Change – Audit Success and Failure
Audit events related to changes in the system policies, including account policy, audit policy, user rights assignment, and security options. As hacker might attempt to modify the security policies on a system to cover its track, it is important to audit for both success and failure attempts.

Privilege Use – Audit Failure Only
Audit events related to exercising of user rights. As an event is logged each time a user attempts to exercise a right, a large number of events will be generated during normal operations. Typically, one only audits failure attempt for this category.

Process Checking – No Auditing
Audit events related to creation and termination of processes, as well as access of objects by a process. Due to large number of events generated, this type of auditing is usually enabled only during troubleshooting or debugging.

System Events – Audit Success and Failure
Audit events related to system changes, including system shutdown and restart, changing of system time, and clearing of event logs. As hackers might attempt to reboot a system to gain access, or to clear the security log to cover its tracks, it is important that we audit both success and failure System Events.

Detailed information on audit policies and typical event entries can be found at:

- J. Fossen's "Securing Windows 5.2 Windows 2000/XP: Group Policy and DNS" [Ref: 6]
- "Windows 2000 Group Policy Reference" section of Microsoft Windows 2000 Resource Kit [Ref: 15]
- Chapter 6 "Auditing and Intrusion Detection" of Security Operations Guide for Microsoft Windows 2000 Server [Ref:17]
- Chapter 4 "Secure Configuration" of SIAC's Windows 2000 Security Configuration Guide Version 1.0 [Ref: 19]

Note that discussions of audit policies here are based on, and sometimes quoted from, material available in the above list.

5.1.3 User Rights Assignment

No User Rights Assignment policy defined.

5.1.4 Security Options

Security Options Policies in baseline.inf are defined as follows:

Additional restrictions for anonymous connections
Default: None. Rely on default permissions
Template Setting: No access without explicit anonymous permissions (most restrictive)
Registry Key: MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,2
The default configuration for anonymous connections allows for null user sessions, through which hackers can connect to the system and enumerate users, shares, account policies and other sensitive information. Unless required by a backwards compatibility issue, one should always set the strictest restriction for anonymous connections.

Allow server operators to schedule tasks
Default: Not Defined
Template Setting: Disabled
Registry Key: MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl=4,0
Enabling this setting allow members of Server Operators group, in addition to Local Administrators, to submit jobs via the Scheduler Service. This setting should be disabled such that potential hackers have one less means for penetrating the system. In addition, the Scheduler service should be disabled on the system.

Allow system to be shut down without having to log on
Default: Disabled
Template Setting: Disabled
Registry Key: MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon=4,0
Enabling this option will give anyone the ability to shut down the system without first authenticating as a valid user. Unless a valid reason exists, this setting should be disabled on all systems.

Allowed to eject removable NTFS media
Default: Administrators
Template Setting: Administrators
Registry Key: MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,0
Only members of the Administrators group are given the rights to eject removable NTFS media.

Amount of idle time required before disconnecting session
Default: 15 minutes
Template Setting: 15 minutes
Registry Key: MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect=4,15
The proposed setting is the default settings on Windows 2000 server. Server Message Block (SMB) session will be disconnected after 15 minutes of inactivity. If client activity resumes, the SMB session will be automatically reconnected.

Audit the access of global system objects
Default: Disabled
Template Setting: Disabled
Registry Key: MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects=4,0
Enabling this policy will cause system objects to be created with updated System Access Control List (SACL), and access to these system objects will subsequently be logged. Due to the large amount of audit events generated when this setting is enabled, unless required by a stringent audit policy, it is typically not necessary to audit such events.

Audit use of Backup and Restore privilege
Default: Disabled
Template Setting: Disabled
Registry: MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,0
Rights to perform backup and restore operation is not one of the users rights logged in the “Privilege Use” Audit policy. To audit use of backup and restore privilege, we need to enable this setting as well as “Privilege Use” setting in Audit policy.

Automatically log off users when logon time expires
Default: Policy not available
Template Setting: Enabled
This setting is applicable only on a domain controller, and does not apply on a member server.

Automatically log off users when logon time expires (local)
Default: Enabled
Template Setting: Enabled
Registry Key: MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1
When enabled, this setting will forcibly disconnect any user connected beyond the allowed logon hours.

Clear virtual memory pagefile when system shuts down
Default: Disabled
Template Setting: Enabled
Registry Key: MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown=4,1
Enabling this setting will clear sensitive information stored in the pagefile when a system shuts down. If a hacker attempts to access the pagefile by rebooting the system to an alternate installation or operating system, sensitive information will not be available. Enabling this option will lengthen the shut down time of the system.

Digitally sign client communication (always) *Default: Disabled*
Digitally sign client communication (when possible) *Default: Enabled*
Digitally sign server communication (always) *Default: Disabled*
Digitally sign server communication (when possible) *Default: Enabled*
Template Settings: Enabled for all four policies
Registry Keys:
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
Digitally signing communication on a system prevents a hacker from hijacking a server session. Unless both the client and server are authenticated, communication will not take place. Enabling this setting offers more security but will impact performance by about 10% to 15%.

Disable CTRL+ALT+DEL requirement for logon
Default: Disabled
Template Setting: Disabled
Registry Key: MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
The CTRL+ALT+DEL requirement for user logon is a defense against spoofing of user login session. Unless a special requirement exists, this setting should not be enabled.

Do not display last user name in logon screen
Default: Disabled
Template Setting: Enabled
Registry Key: MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1
Enabling this policy causes the logon prompt in Windows 2000 to not display the account name last used to log on to the system. This enhances security, as a potential hacker will not easily gain knowledge of a valid username. To further enhance security, one should also rename well-known usernames such as administrator.

LAN Manager Authentication Level
Default: Send LM & NTLM responses
Template Setting: Send NTLMv2 response only\refuse LM & NTLM
Registry Key: MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,5
LM and NTLM are authentication protocols supported by Windows 2000 for backwards compatibility. These protocols are much less secure than NTLM v2, and are susceptible

to password cracking techniques. We should require the exclusive use of NTLM v2 authentication protocol whenever possible.

Number of previous logons to cache (in case domain controller is not available)
Default: 10 logons
Template Setting: 0 logons
Registry Key: MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0
Setting this policy to a non-zero number will allow a user to log on to the system using cached credential, in case a domain controller is not available. In situation when an administrator changes a domain account password or disables an account for security purposes, if this setting is non-zero, a malicious user could disconnect the system from the network and log in successfully using cached credentials.

Prevent system maintenance of computer account password
Default: Disabled
Template Setting: Disabled
Registry Key: MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4,0
By default, Windows 2000 system changes its computer account password every 7 days. Enabling this policy will disable this default behavior. Since the system account password is used to create a secure channel with the domain controller (when the corresponding policies are enabled), system maintenance of computer account password should not be prevented.

Prevent users from installing printer drivers
Default: Enabled
Template Setting: Enabled
Registry Key: MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers=4,1
Enabling this policy will deny the Users group rights to install printer on the system. As regular users have no need to install printer on an application server, this setting should be enabled.

Prompt user to change password before expiration
Default: 14 days
Template Setting: 14 days
Registry Key: MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,14
Prompting user to change password 14 days before expiration is the default local setting on a Windows 2000 server. Unless a valid requirement exists to modify the advance notification interval, the default setting is adequate.

Recovery Console: Allow automatic administrative logon
Recovery Console: Allow floppy copy and access to all drives and all folders
Default: Disabled
Template Settings: Disabled
Registry Key:
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=4,0

The Recovery Console is a Windows 2000 component used for troubleshooting a system that does not startup properly. This component can be preinstalled into the boot options, or can be run from a Windows 2000 CD. By default the Recovery Console will prompt for an administrator password before allowing interactive access to the system. Also, access to all data on the system is disabled by default. As changing these default behavior will create severe security vulnerabilities, these policies should be disabled.

Restrict CD-ROM access to locally logged-on user only
Restrict floppy access to locally logged-on user only
Default: Disabled for both policies
Template Settings: Enabled for both policies
Registry Key:

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1

Enabling these policies will restrict network access to CD-ROM and floppy drives. As it is not a requirement on most application server for remote users to access these drives, these policies should be enabled.

Secure channel: Digitally encrypt or sign secure channel data (always) *Default: Disabled*
Secure channel: Digitally encrypt secure channel data (when possible) *Default: Enabled*
Secure channel: Digitally sign secure channel data (when possible) *Default: Enabled*
Template Settings: Enabled for all three policies
Registry Key:

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1

The secure channel referenced in these policies is the NetLogon channel that a server established with a domain controller (DC) upon system startup. Traffic through this channel includes transfer of DC's public key, user's master key, and password changes. The system account's password is used to encrypt and sign packets through this channel if so configured.

Enabling the "Digitally encrypt or sign secure channel data (always)" policy will require that all traffic over the secure channel be either encrypted or signed. Note that even though secure channel is authenticated, and sensitive information is encrypted, the secure channel is not integrity checked and not all information is encrypted.

Enabling either the "Digitally encrypt or sign secure channel data (always)" or "Digitally encrypt secure channel data (when possible)" policy will automatically enables the "Digitally sign secure channel data (when possible)" policy.

The "Digitally encrypt or sign secure channel data (always)" policy should only be enabled if all of the domain controllers in all the trusted domains support signing and sealing. That is, all domain controllers and domain members need to be either Windows 2000/.Net or Windows NT 4.0 SP4 and later.

Secure channel: Require strong (Windows 2000 or later) session key
Default: Disabled
Template Setting: Enabled
Registry Key: MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,1
This policy is only supported in environment where all domain controllers and member servers are Windows 2000/.NET systems. Details on the key used and the encryption strength are currently not documented by Microsoft. However, Jason Fossen noted in "Security Windows 5.1 – Windows 2000/XP Active Directory" [Ref: 5] that "it is likely that the encryption is at least 128-bit RC4", and that "the key probably derived from the computer's own Kerberos master key."

Send unencrypted password to connect to third-party SMB servers
Default: Disabled
Template Setting: Disabled
Registry Key: MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,0
Enabling this policy will allow Server Message Block (SMB) redirector to send password in clear-text to non-Microsoft SMB servers that does not support password encryption. Unless absolutely required and relevant security measures have been put in place, this policy should be disabled.

Shut down system immediately if unable to log security audits
Default: Disabled
Template Setting: Enabled
Registry Key: MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1
In combination with a properly configured retention method for the security event log, and an archival mechanism for the security log, enabling this policy will ensure that all security events on a system is audited and archived. This policy should be enabled in environment where security auditing is a high priority.

Smart card removal behavior
Default: No Action
Template Setting: Lock Workstation
Registry Key: MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,1
This policy applies to environment where smart card is used for logon authentication. On removal of a smart card, the proposed setting will protect the user session by locking the workstation.

Strengthen default permissions of global system objects (e.g. Symbolic Links)
Default: Enabled
Template Setting: Enabled
Registry Key: MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
This setting affects the Discretionary Access Control List (DACL) of various system objects. Enabling this setting will strengthen the DACL such that non-administrator will have limited access to system objects. This policy is enabled locally by default on Windows 2000 Professional and Sever systems.

Unsigned driver installation behavior
Default: Not Defined
Template Setting: Do not allow installation
Registry Key: MACHINE\Software\Microsoft\Driver Signing\Policy=3,2
This setting applies to installation of system device drivers that are not certified by the Windows Hardware Quality Lab.

Unsigned non-driver installation behavior
Default: Not Defined
Template Setting: Warn but allow installation
Registry Key: MACHINE\Software\Microsoft\Non-Driver Signing\Policy=3,1
This setting applies to installation of non-device driver software, such as applications, that has not been certified.

Detailed information on security options can be found at:

- J. Fossen's "Securing Windows 5.2 Windows 2000/XP: Group Policy and DNS" [Ref: 6]
- "Windows 2000 Group Policy Reference" section of Microsoft Windows 2000 Resource Kit [Ref: 15]
- Chapter 4 "Securing Servers Based on Role" of Security Operations Guide for Microsoft Windows 2000 Server [Ref:17]
- Chapter 4 "Secure Configuration" of SIAC's Windows 2000 Security Configuration Guide Version 1.0 [Ref: 19]

Note that discussion of security options here are based on, and sometimes quoted from, material available in the above list.

5.1.5 Event Logs Settings

Maximum application log size
Maximum security log size
Maximum system log size
Default: 512 kilobytes
Template Settings: 10240 kilobytes
Maximum file size for all three event logs are set to 10,240 KB.

Restrict guest access to application log
Restrict guest access to security log
Restrict guest access to system log
Default: Disabled
Template Settings: Enabled
By default, anonymous access to information in event logs is allowed. Enabling these policies will allow only users who possess "Manage auditing and security log" rights to access the event logs.

Retain application log
Retain security log
Retain system log
Default: 7 Days
Template Settings: Not defined
This setting specifies the number of days event logs is retained. It is used when the retention method for event logs is set to “Overwrite events by days”.

Retention method for application log
Retention method for security log
Retention method for system log
Default: By Days
Template Settings: Manually
Setting the retention method to “Manually” requires that the event log file be manually cleared. When this setting is used in combination with the security options “Shut down system immediately if unable to log security audits”, it is crucial that a log archival and clearing procedure exists. The default settings for retention method is to overwrite events older that 7 days. One could also set the event logs to be overwritten as needed; however, this setting is the least secure as a hacker could overwrite the security log with large amount of meaningless data.

Shut down the computer when the security audit log is full
Default: Disabled
Template Setting: Enabled
In combination with a properly configured retention method for the security event log, and an archival mechanism for the security log, enabling this policy will ensure that all security events on a system is audited and archived. This policy should be enabled in environment where security auditing is a high priority. It is recommended in “Windows 2000 Security Configuration Guide” ” [Ref: 19] that one uses the Security Options “Shut down system immediately if unable to log security audits” to configure this setting.

5.1.6 Restricted Groups

Not Defined

5.1.7 System Services – Security Settings

The security template, baseline.inf, alters two attributes of a Windows 2000 service, the access control list (ACL) for the service in question and the service’s startup option. We will discuss ACL modifications in this subsection, and startup option in the next subsection.

As ACLs for a service determine who have the rights to read, write, delete, as well as start/stop/pause a service, regardless of the service’s startup type, it is important that these ACLs be configured properly. If a user has full control rights to a service disabled for security purposes, a hacker who succeeds in impersonating that user will be able to enable and start the service.

Using the Windows 2000 Resource Kit utility sc.exe, we examined the default security settings of Windows services by executing "sc.exe sdlist" against every installed service on our Exchange 2000 OWA FE system. The output of sc.exe is in Security Descriptor Definition Language (SDDL) format. Details on SDDL is available at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/security_descriptor_definition_language.asp.

The following is a table summarizing default ACLs on all services installed.

Services	Default Access Rights
Alerter Computer Browser DHCP Client Distributed File System Distributed Link Tracking Client Distributed Transaction Coordinator DNS Client Event Log License Logging Service Logical Disk Manager Messenger Net Logon Plug and Play Print Spooler Protected Storage Remote Registry Service Removable Storage RunAs Service Server Simple Mail Transport Protocol (SMTP) System Event Notification Task Scheduler TCP/IP NetBIOS Helper Service Workstation	○ Authenticated Users: Read ○ Power Users: Read and Start Service ○ Built-in Administrators: Full ○ Server Operators: Full ○ Local System: Read and Start/Stop/Pause
Application Management	○ Everyone: Read less "User Defined Control" ○ Built-in Administrators: Full ○ Power Users: Read less "User Defined Control" ○ Interactive Users: Read less "User Defined Control" & "Read Permissions". Start Service ○ Built-in Users: Read less "User Defined Control" & "Read Permissions". Start Service ○ Child objects inherit above rights.
ClipBook Network DDE Network DDE DSDM	○ Everyone: Read less "User Defined Control" ○ Built-in Administrators: Full ○ Power Users: Read less "User Defined Control" ○ Interactive Users: Read less "User Defined Control" & "Read Permissions". Start Service ○ Child objects inherit above rights. ○ Server Operators: Full
COM+ Event System	○ Local System: Read and Start/Stop/Pause ○ Built-in Administrators: Full ○ Authenticated Users: Read ○ Power Users: Read and Start/Stop/Pause ○ Everyone: Read and Start

Automatic Updates Background Intelligent Transfer Service Distributed Link Tracking Server Fax Service File Replication IIS Admin Service Indexing Service Internet Connection Sharing Intersite Messaging Logical Disk Manager Administrative Service Microsoft Exchange Event Microsoft Exchange IMAP4 Microsoft Exchange Information Store Microsoft Exchange Management Microsoft Exchange MTA Stacks Microsoft Exchange POP3 Microsoft Exchange Routing Engine Microsoft Exchange Site Replication Service Microsoft Exchange System Attendant Microsoft Search NetMeeting Remote Desktop Sharing Network Connections Network News Transport Protocol (NNTP) NT LM Security Support Provider Performance Logs and Alerts Remote Access Auto Connection Manager Remote Procedure Call (RPC) Locator Routing and Remote Access Smart Card Helper Telnet Terminal Services Uninterruptible Power Supply Windows Installer Windows Management Instrumentation World Wide Web Publishing Service	○ Local System: Read and Start/Stop/Pause ○ Built-in Administrators: Full ○ Authenticated Users: Read ○ Power Users: Read and Start/Stop/Pause
IPSEC Policy Agent	○ Authenticated Users: Read less "User Defined Control" ○ Power Users: Read and Start ○ Built-in Administrators: Full ○ Server Operators: Full ○ Local System: Read and Start/Stop/Pause
Kerberos Key Distribution Center Windows Management Instrumentation Driver Extensions	○ Everyone: Read less "User Defined Control" ○ Built-in Administrators: Full ○ Power Users: Read less "User Defined Control" & "Change Template" ○ Interactive Users: Read less "User Defined Control"& "Read Permissions". Start Service ○ Child objects inherit above rights.
QoS RSVP Remote Access Connection Manager	○ Authenticated Users: Read and Start ○ Power Users: Read and Start/Stop/Pause ○ Built-in Administrators: Full
Remote Procedure Call (RPC) Security Accounts Manager Telephony Windows Time	○ Everyone: Read less User Defined Control ○ Built-in Administrators: Full ○ Power Users: Read less "User Defined Control" ○ Interactive Users: Read less "User Defined Control"& "Read Permissions". Start Service ○ Built-in Users: Read less "User Defined Control"& "Read Permissions". Start Service ○ Child objects inherit above rights.
Smart Card	○ Creator Owner: Full ○ Built-in Administrators: Full ○ Everyone: Read less "User Defined Control". Start Service
Utility Manager	○ Authenticated Users: Read ○ Power Users: Read and Start/Stop/Pause ○ Built-in Administrators: Full ○ Server Operators: Full ○ Local System: Read and Start/Stop/Pause

Now that we have explored and documented the default ACLs on services installed, we will examine the ACLs settings for Windows services in our security template. Upon examination of the [Service General Setting] section in the security template file (baseline.inf), we find that every service referenced by the template has the following security descriptor string:

```
D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY) S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD).
```

Referencing Microsoft's documentation on Security Descriptor Definition Language (SDDL), we translate the above security descriptor string to be:

Windows Services	Template Configured ACLs
All Windows services referenced in baseline.inf	Access Rights o Interactive Users: Read o Built-in Administrators: Full o Local System: Full Auditing o Everyone: Audit on all failure access

Note that not all services installed on our Exchange 2000 OWA FE system are referenced in the baseline.inf template. Services not referenced are:

- Automatic Updates
- Background Intelligent Transfer Service
- Microsoft Exchange Event
- Microsoft Exchange IMAP4
- Microsoft Exchange Information Store
- Microsoft Exchange Management
- Microsoft Exchange MTA Stacks
- Microsoft Exchange POP3
- Microsoft Exchange Routing Engine
- Microsoft Exchange Site Replication Service
- Microsoft Exchange System Attendant
- Microsoft Search

5.1.8 System Services – Startup Type

As discussed previously, the security template, baseline.inf, alters two attributes of a Windows 2000 service. We have discussed the access control list (ACL) modification in the previous subsection; we will now discuss startup type modification in this subsection.

There are three service startup types: Automatic, Manual and Disabled. Services with Automatic startup will be loaded automatically when a system boots; services with a Manual startup will start when needed, either triggered by an application, a user action or when a service dependent on it starts; services with a Disabled startup type will not start unless its startup type is changed.

5.1.8.1 System Services Installed

The following table enumerates all services installed on our Exchange 2000 OWA FE server, their default startup type, and their default status. The last column shows the startup type modification by baseline.inf.

Service Name	Default Status	Default Startup Type	Baseline.inf Template Settings
Alerter	Started	Automatic	Disabled
Application Management		Disabled	Disabled
Automatic Updates	Started	Automatic	Not Defined
Background Intelligent Transfer Service		Manual	Not Defined
ClipBook		Manual	Disabled
COM+ Event System	Started	Manual	Manual
Computer Browser	Started	Automatic	Disabled
DHCP Client	Started	Automatic	Automatic
Distributed File System	Started	Automatic	Disabled
Distributed Link Tracking Client	Started	Automatic	Automatic
Distributed Link Tracking Server		Manual	Disabled
Distributed Transaction Coordinator	Started	Automatic	Disabled
DNS Client	Started	Automatic	Automatic
Event Log	Started	Automatic	Automatic
Fax Service		Manual	Disabled
File Replication		Manual	Disabled
IIS Admin Service	Started	Automatic	Disabled
Indexing Service		Manual	Disabled
Internet Connection Sharing		Manual	Disabled
Intersite Messaging		Disabled	Disabled
IPSEC Policy Agent	Started	Automatic	Disabled
Kerberos Key Distribution Center		Disabled	Disabled
License Logging Service	Started	Automatic	Disabled
Logical Disk Manager	Started	Automatic	Automatic
Logical Disk Manager Administrative Service		Manual	Manual
Messenger	Started	Automatic	Disabled
Microsoft Exchange Event		Manual	Not Defined
Microsoft Exchange IMAP4	Started	Automatic	Not Defined
Microsoft Exchange Information Store	Started	Automatic	Not Defined
Microsoft Exchange Management	Started	Automatic	Not Defined
Microsoft Exchange MTA Stacks		Automatic	Not Defined
Microsoft Exchange POP3	Started	Automatic	Not Defined
Microsoft Exchange Routing Engine	Started	Automatic	Not Defined
Microsoft Exchange Site Replication Service		Disabled	Not Defined
Microsoft Exchange System Attendant	Started	Automatic	Not Defined
Microsoft Search	Started	Automatic	Not Defined
Net Logon	Started	Automatic	Automatic
NetMeeting Remote Desktop Sharing		Manual	Disabled
Network Connections	Started	Manual	Manual
Network DDE		Manual	Disabled
Network DDE DSDM		Manual	Disabled
Network News Transport Protocol (NNTP)	Started	Automatic	Disabled
NT LM Security Support Provider	Started	Manual	Disabled
Performance Logs and Alerts		Manual	Manual
Plug and Play	Started	Automatic	Automatic
Print Spooler	Started	Automatic	Disabled
Protected Storage	Started	Automatic	Automatic
QoS RSVP		Manual	Disabled
Remote Access Auto Connection		Manual	Disabled

Manager			
Remote Access Connection Manager		Manual	Disabled
Remote Procedure Call (RPC)	Started	Automatic	Automatic
Remote Procedure Call (RPC) Locator	Started	Manual	Disabled
Remote Registry Service	Started	Automatic	Automatic
Removable Storage	Started	Automatic	Disabled
Routing and Remote Access		Disabled	Disabled
RunAs Service	Started	Automatic	Disabled
Security Accounts Manager	Started	Automatic	Automatic
Server	Started	Automatic	Automatic
Simple Mail Transport Protocol (SMTP)	Started	Automatic	Disabled
Smart Card		Manual	Disabled
Smart Card Helper		Manual	Disabled
System Event Notification	Started	Automatic	Automatic
Task Scheduler	Started	Automatic	Disabled
TCP/IP NetBIOS Helper Service	Started	Automatic	Automatic
Telephony	Started	Manual	Disabled
Telnet		Manual	Disabled
Terminal Services		Disabled	Disabled
Uninterruptible Power Supply		Manual	Disabled
Utility Manager		Manual	Disabled
Windows Installer		Manual	Disabled
Windows Management Instrumentation	Started	Automatic	Disabled
Windows Management Instrumentation Driver Extensions	Started	Manual	Manual
Windows Time	Started	Automatic	Automatic
Workstation	Started	Automatic	Automatic
World Wide Web Publishing Service	Started	Automatic	Disabled

To understand the template's settings, we need to understand the basic functionality and security impact of each individual service. What follows is a brief description of every service referenced in the baseline.inf template, some of its security concerns, as well as dependencies on the service. Description of services is based on, and sometimes quoted from, information available in Microsoft documentation "Glossary of Windows 2000 Services" [Ref: 11].

5.1.8.2 System Services installed but disabled by template

The following are services installed on our Exchange 2000 OWA FE server, and are disabled by the baseline.inf template.

Alerter
This service is used to send administrative alerts to users and remote computers. Unless an application on the system uses the NetAlertRaise or NetAlertRaiseEx APIs, such as Performance Log and Alerts, this service can be disabled.

Application Management
This service is used to manage application deployment (assign, publish & remove) of the software installation component of Active Directory IntelliMirror technology. Typically, as managed application deployment is targeted at end user workstation, this service can be disabled on application server.

ClipBook

Allows sharing of information between systems using Clipbook viewer. This service can be disabled.

Computer Browser

Allows a system to browse network resources in the browse list. With this service disabled, one must know the exact network path when locating resources on the network. This service also allows a system to become a master or backup browser when required. This service can be disabled, as browsing is typically not a requirement on application servers.

Distributed File System

This service integrates disparate file shares into a single logical namespace. Unless DFS is specifically required, this service can be disabled on most servers.

Distributed Link Tracking Server

This service tracks files movement within and between NTFS volumes in a domain. It enables DLT Client to track files referenced by shortcuts and OLE links after the files have been moved or renamed. Typically this service runs on a domain controller, and can be disabled on a member server.

Distributed Transaction Coordinator

This service coordinates transactions that are distributed across various network systems. It is a required service for distributed transactions configured through Component Service (COM+), Messaging Queue (MSMQ) and MS SQL services. Unless it is required by an application, this service can be disabled.

Fax Service

This service allows the system to send and receive faxes. Unless required by an application, this service can be disabled.

File Replication

This service maintains file synchronization among multiple servers. It is required on domain controllers for replication of SysVol, and on servers with fault-tolerant DFS volumes.

IIS Admin Service

This service is required on systems running any Internet Information Server components. “Microsoft Exchange IMAP4”, “Microsoft Exchange Information Store”, “Microsoft Exchange MTA Stacks”, “Microsoft Exchange POP3”, “Microsoft Exchange Routing Engine”, “Network News Transport Protocol”, “Simple Mail Transport Protocol”, and “World Wide Web Publishing Services” all depends on the “IIS Admin Service.”

Indexing Service

Provides fast access to local and remote files, as well as to web content by building an index for all textual content in files and documents. Unless required by an application, this service can be disabled.

Internet Connection Sharing

This service allows a system with direct Internet access to become an "Internet Gateway" by providing Network Address Translation (NAT), IP addressing (via DHCP) and name resolution (DNS) services to other local hosts. This service is typically used in home or small offices.

Intersite Messaging

This service allows sending and receiving of SMTP messages between Active Directory sites. It is used for Active Directory mail based replication between domain controllers.

IPSEC Policy Agent

This service manages IPSec policy, starts the Internet Key Exchange (IKE) and coordinates IPSec policy setting with the IPSec driver. This service is required on system using the IPSec protocol.

Kerberos Key Distribution Center

This service enables users to logon to an Active Directory domain using Kerberos as the authentication protocol. This service is required only on Active Directory domain controller.

License Logging Service

This service tracks client license usage for various Microsoft server products and updates the licensing database on the Site License server. If disabled, license-tracking information will not be available; however, this will not impact functionality of server products.

Messenger

This service is used to send and receive administrative alerts generated by administrators or by the Alerter service. Unless required by an application, this service can be disabled.

NetMeeting Remote Desktop Sharing

This service allows authorized user to remotely access the system's desktop using Microsoft NetMeeting. As remote desktop access provides a venue for attack, this service should be disabled.

Network DDE

This service allows programs on the same system or different systems to share data via Dynamic Data Exchange (DDE). The "ClipBook" service is dependent on "Network DDE". Unless required by an application, this service should be disabled.

Network DDE DSDM

This service manages Dynamic Data Exchange (DDE) conversation, and is used by the “Network DDE” service exclusively. The “Network DDE” service is dependent on “Network DDE DSDM” service. Unless required by an application, this service should be disabled.

Network News Transport Protocol

This service allows a system to be a Network News Transport Protocol (NNTP) server. It is a required component when installing Exchange 2000 server; however, this service can be disabled if the server is not used as a news server.

NT LM Security Support Provider

This service allows user to logon to the domain using NTLM authentication protocol. It also provides security to remote procedure call (RPC) programs that use transports other than named pipes. The “Microsoft Exchange System Attendant” and “Microsoft Search” services are dependent on “NT LM Security Support Provider”.

Print Spooler

This service manages local and remote print jobs. The “Fax Service” is dependent on “Print Spooler” service.

QoS RSVP

Provides network signaling and local traffic control setup functionality for QoS-aware programs. This service can be disabled if QoS-aware program is not used on the system.

Remote Access Auto Connection Manager

This service creates autodial connection (dial-up or VPN) when a user or application attempts to access a remote system or share unsuccessfully. This service can be disabled on most systems.

Remote Access Connection Manager

This service manages remote access connection. When a user accesses a remote location via the “Network and Dial-up Connections”; this service will creates, maintain and disconnects the remote connection. “Internet Connection Sharing” and “Remote Access Auto Connection Manager” are dependent on “Remote Access Connection Manager” service. If this service is disabled, connections through “Network and Dial-up Connections” will fail.

Remote Procedure Call (RPC) Locator

The service helps locate RPC servers and provides name services for RPC clients. The “Microsoft Exchange System Attendant” is dependent on “Remote Procedure Call Locator” service.

Removable Storage

This service manages removable storage medium, such as tapes, CDs, and tape libraries. It is primarily used by backup and remote storage applications. This service can be disabled if not specifically required by an application.

Routing and Remote Access

This service provides multi-protocol routing, as well as dial-up and VPN remote access services. If these functionalities are not in use, the service can be disabled.

RunAs Service

This service allows a user, who has logged on to the system with a set of credentials, to execute a program with alternate credentials.

Simple Mail Transport Protocol

This service provides email transport functionality. If such functionality is not required on the system, this service can be disabled.

Smart Card

This service provides smart card support on the systems. If smart card is not used, this service can be disabled.

Smart Card Helper

Provides support for legacy smart card readers attached to the computer. If this service is disabled, non Plug n Play smart card reader will not be supported.

Task Scheduler

This service allows a program or a batch file to run unattended at scheduled times. If job scheduling is a required functionality on the system, this service needs to be enabled. However, as this could also be a venue for hackers to execute malicious code on the system, the rights to submit schedule jobs needs to be tightened accordingly.

Telephony

This service provides Telephony API (TAPI) support, and allows programs to act as clients to telephony equipment. If this service is disabled, services and programs that require TAPI support, such as RAS and modem support, will not run. “Fax Service”, “Remote Access Auto Connection Manager”, and “Remote Access Connection Manager” services are dependent on “Telephony” service.

Telnet

Provides Telnet service to remote users. This service allows telnet client to logon and execute programs on the system via a telnet client or a command line interface. As this service could be a venue for attack, it should be disabled.

Terminal Services

Terminal Services allows users to logon and access a remote system via a remote desktop session. Users connected via Terminal Services have all the rights of a user that is logged on locally. As remote desktop access could be a venue for attack, this service should be disabled. However, if remote desktop access is required, one should at a minimum harden this service by changing its default listening port.

Uninterruptible Power Supply
This service manages communication with a connected UPS device. In the event of a power outage, a UPS device can initiate a system shutdown through this service. Enabling this service will minimize possible data loss related to a "hard" shutdown of the system.

Utility Manager
This service manages accessibility tools on a system, and is typically not required on servers.

Windows Installer
This service manages installation, update and removal of application according to instructions contained in the application's .MSI file. If disabled, application management through Windows Installer will fail.

Windows Management Instrumentation
This service provides system management data to various management applications. Access to management data, such as events generated by applications and services, are provided by WMI through various programming interfaces. If this service is disabled, many application and tools that requires WMI will fail, including some functionality within Microsoft's "Computer Management" tool. "Microsoft Exchange Management" service is dependent on "Windows Management Instrumentation" service.

World Wide Web Publishing Service
This service provides HTTP access to the system. This service is required on a web server.

5.1.8.3 Services Installed and left Enabled by Template

The following are services that are installed on our Exchange 2000 OWA FE system, and are enabled by the baseline.inf template. The baseline.inf template does not change the default startup type of these services.

COM+ Event System (Startup: Manual)
This service provides automatic distribution of events to subscribing Common Object Model (COM) components. The service "System Event Notification" is dependent on COM+ Event System service. If this service is disabled, applications and services that subscribe to COM events will fail.

DHCP Client (Startup: Automatic)
This service allows a system to contact a DHCP server and obtain IP configurations. This service can be disabled on systems with statically configured IP settings.

Distributed Link Tracking Client (Startup: Automatic)
The Distributed Link Tracking (DLT) client service ensures that shortcuts and Object Link Embedding (OLE) objects continue to work after the original files have been moved or renamed.
If this service is disabled, a user on the local system would not be able to track links on remote servers, and remote links to local objects would also not be tracked.

DNS Client (Startup: Automatic)
DNS client service queries DNS server for IP name resolution. It is a critical component for system participating in an IP based network. If this service is disabled, the system will not be able to locate domain controllers and other devices using DNS names.

Event Log (Startup: Automatic)
This service records events generated by services and programs in log files viewable using Event Viewer. Information logged includes status and error messages generated by system services and applications, as well as security auditing information. The “File Replication” and “Microsoft Exchange System Attendant” services depend on the “Event Log” service.

Logical Disk Manager (Startup: Automatic)
This service monitors Plug and Play events for disk drives and passes volume and disk information to the “Logical Disk Manager Administrative Service.” If this service is disabled, Disk Management snap-in will not displayed updated disk information when a drive is removed or added to the system. This service is also required for dynamic drives.

Logical Disk Manager Administrative Service (Startup: Manual)
This service performs disk management requests including disk initialization, disk partitioning, volume formatting, recovery of fault tolerant volume, and changes to pagefile. This service starts when required, and stops when the requested task is completed.

Net Logon (Startup: Automatic)
Net Logon service, on a member server, maintains a secure channel with a domain controller for authentication of domain accounts. It is a required service for servers participating in a Windows domain environment.

Network Connections (Startup: Manual)
This service manages objects in the Network and Dial-Up Connections folder. If this service is disabled, one will not be able to create new network connections, connect via dial-up connections, configure existing connections, obtain status information, and use Internet Connection Sharing. However, there is no loss in network connectivity if the service is disabled after the appropriate network settings are configured.

Performance Logs and Alerts (Startup: Manual)
This service is used to collect performance data on local or remote systems, as well as generate alerts when a predefined threshold is reached. Performance logging and alerts are configured through the “Performance Logs and Alerts” snap-in.

Plug and Play (Startup: Automatic)
This service enables a system to recognize and adapt to hardware changes with minimum user intervention. Microsoft documents that “stopping or disabling this service will result in system instability”. The “Fax Service”, “SmartCard” and “Telephony” services are dependent on “Plug and Play” service.

Protected Storage (Startup: Automatic)
This service provides protected storage for sensitive data, and it prevents unauthorized access to that data. If this service is disabled, information protected, such as private keys, will not be available to users or services. The “IIS Admin Service” is dependent on “Protected Storage” service.

Remote Procedure Call (RPC) (Startup: Automatic)
This service provides endpoint mapper and other miscellaneous RPC services. Numerous services are dependent on “Remote Procedure Call (RPC)” service, including “IIS Admin Service” and “Microsoft Exchange System Attendant”. If this service is disabled, the system will not boot.

Remote Registry Service (Startup: Automatic)
This service provides remote access to the system’s registry. It is required for remote administrator to access registry information. This service is also required for some applications, such as the HFNetChk utility.

Security Accounts Manager (Startup: Automatic)
This service signals other services that the Windows 2000 “Security Accounts Manager” subsystem is ready to accept request. If disabled, services that require access to the local SAM will fail. The “Distributed Transaction Coordinator” and “Intersite Messaging” services are dependent on “Security Accounts Manager” service.

Server (Startup: Automatic)
This service provides RPC and named pipe support, and it allows sharing of local resources such as files and printers. “Computer Browser”, “Distributed File System”, and “Microsoft Exchange System Attendant” are services dependent on “Server” service. Some administration tools might also require the Server service. Note that as the Server service shares file over the SMB protocol, and web server share files over HTTP, this service is not a required component on a “pure” web server.

System Event Notification (Startup: Automatic)
This service tracks system events such as Windows logon and power events, and notifies COM+ EventSystem subscriber of these events. COM+ EventSystem also

notifies “System Event Notification” of some events. “Background Intelligent Transfer Service” is dependent on “System Event Notification” service.

TCP/IP NetBIOS Helper Service (Startup: Automatic)
This service enables support for NetBIOS over TCP/IP (NETBT) and NetBIOS name resolution. If this service is disabled, NetBT's clients, such as Netlogon, might stop responding.

Windows Management Instrumentation Driver Extensions (Startup: Manual)
This service tracks drivers that have registered WMI information to publish. If the service is turned off, clients cannot access the WMI information published by drivers. “Background Intelligent Transfer Service” is dependent on “WMI Driver Extensions” service.

Windows Time (Startup: Automatic)
This service is responsible for time synchronization. As Kerberos authentication is dependent on time synchronization, it is important that time is synchronized in an active directory domain environment. In a domain environment, time is synchronized with a domain controller. In a workgroup environment, time can be synchronized with a pre-configured external time source.

Workstation (Startup: Automatic)
This service provides network connections and communication. If this service is disabled, connections cannot be made to remote systems using Microsoft network. “Workstation” is a required service for servers participating in a domain environment. Many services are dependent on the “Workstation” service, including “Alerter”, “Background Intelligent Transfer Service”, “Computer Browser”, “Distributed File System”, “Messenger”, “Microsoft Exchange System Attendant”, “Net Logon”, and “Remote Procedure Call (RPC) Locator”.

Note that the following services are referenced in the baseline.inf template, but are not installed on our Exchange 2000 OWA FE server. We will list them for reference purpose, but will not discuss them in details.

- Boot Information Negotiation Layer Service (BINLSVC)
- Certificate Services (CertSvc)
- Cluster Service (ClusSvc)
- DHCP Server
- DNS Server
- Single Instance Storage Groveler (A component of Remote Installation Service)
- Internet Authentication Service (IAS)
- Site Server ILS Service (LDAPSVCX)
- TCP/IP Print Server (LPDSVC)
- File Server for Macintosh (MacFile)
- Print Server for Macintosh (MacPrint)
- FTP Publishing Service (MSFTPSVC)
- Message Queuing (MSMQ)

- On-Line Presentation Broadcast (NSLService)
- Windows Media Monitor Service (Nsmonitor)
- Windows Media Program Service (nsprogram)
- Windows Media Station Service (nsstation)
- Windows Media Unicast Service (Nsunicast)
- Gateway Service for Netware (WCWorkstation)
- SAP Agent (NwSapAgent)
- Remote_Storage_Engine
- Remote_Storage_File_System_Agent
- Remote_Storage_Subsystem
- Remote_Storage_User_Link
- Simple TCP/IP Services (SimpTcp)
- SNMP Service
- SNMP Trap Service (SNMPTRAP)
- Terminal Services Licensing (TermServLicensing)
- Trivial FTP Daemon (TFTPD)
- Windows Internet Name Service (WINS)

5.1.9 Registry

The security template, baseline.inf, alters two attributes of a Windows 2000 registry key, the access control list (ACL) for the key in question and specific registry key value. While ACLs modification can be viewed via the Security Templates snap-in, as shown on page 7, modification of registry value can be viewed only in the section titled "Registry Values" in baseline.inf.

5.1.9.1 Permission Modification

As the Windows registry stores many configurations and parameters of system services and applications, it is important that access to this data be limited. Permissions on registry key are set to prevent unauthorized viewing, modification, and deletion of registry's keys and values. If not properly configured, a hacker might be able to delete a registry key and render the system inoperable.

Even though registry key permissions settings can be viewed from the Security Templates snap-in, we can also evaluate the settings by direct examination of the "Registry Keys" section in baseline.inf. The "Registry Keys" section defines permission settings on registry key using Security Descriptor Definition Language (SDDL). Details information on Security Descriptor Definition Language (SDDL) can be found at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/security_descriptor_definition_language.asp.

The following table summarizes permission settings on registry keys in baseline.inf.

Registry Key	Baseline.inf Permissions Modification
"MACHINE\Software\Classes" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" "MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout" "MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts" "MACHINE\SYSTEM\CurrentControlSet\Control\Computername" "MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex" "MACHINE\SYSTEM\CurrentControlSet\Control\ProductOptions" "MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers" "MACHINE\SYSTEM\CurrentControlSet\Services\EventLog" "MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip"	○ Allow inheritable permissions from parent to propagate to this object. ○ Everyone: Read Propagate to all subkeys
"MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider" "MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy" "MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer" "MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009" "MACHINE\SYSTEM\Clone" "MACHINE\SYSTEM\ControlSet001" "MACHINE\SYSTEM\ControlSet002" "MACHINE\SYSTEM\ControlSet003" "MACHINE\SYSTEM\ControlSet004" "MACHINE\SYSTEM\ControlSet005" "MACHINE\SYSTEM\ControlSet006" "MACHINE\SYSTEM\ControlSet007" "MACHINE\SYSTEM\ControlSet008" "MACHINE\SYSTEM\ControlSet009" "MACHINE\SYSTEM\ControlSet010" "MACHINE\SYSTEM\CurrentControlSet\Enum" "MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles" "USERS\.DEFAULT\SOFTWARE\Microsoft\Protected Storage System Provider"	○ Allow inheritable permissions from parent to propagate to this object.
"MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg"	○ Disallows inheritable permissions from parent to propagate to this object. ○ Builtin-Administrators: Full control. Propagate to all subkeys. ○ Backup Operators: Read.
"MACHINE\SOFTWARE\Microsoft\NetDDE" "USERS\.DEFAULT\Software\Microsoft\NetDDE" "MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Security"	○ Disallows inheritable permissions from parent to propagate to this object. ○ Builtin-Administrators: Full control. Propagate to all subkeys. ○ Local System: Full Control. Propagate to all subkeys. ○ Creator Owner: Full Control. Propagate to all subkeys.

"MACHINE\Software" "MACHINE\SOFTWARE\Microsoft\Secure" "MACHINE\SOFTWARE\Microsoft\SystemCertificates" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AEDebug" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Classes" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontMapper" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SecEdit" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows" "MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" "MACHINE\System" "USERS\.DEFAULT"	○ Disallows inheritable permissions from parent to propagate to this object. ○ Builtin-Users: Read. Propagate to all subkeys. ○ Power Users: Read. Propagate to all subkeys ○ Builtin-Administrators: Full control. Propagate to all subkeys. ○ Local System: Full Control. Propagate to all subkeys. ○ Creator Owner: Full Control. Propagate to all subkeys.
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AsrCommands"	○ Disallows inheritable permissions from parent to propagate to this object. ○ Builtin-Users Read. Propagate to all subkeys. ○ Power Users: Read. Propagate to all subkeys ○ Builtin-Administrators: Full control. Propagate to all subkeys. ○ Local System: Full Control. Propagate to all subkeys. ○ Creator Owner: Full Control. Propagate to all subkeys. ○ Backup Operators: Read, Set Value, Create Subkey, and Delete. Propagate to all subkeys
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib"	○ Disallows inheritable permissions from parent to propagate to this object. ○ Interactive-Users: Read. Propagate to all subkeys. ○ Builtin-Administrators: Full control. Propagate to all subkeys. ○ Local System: Full Control. Propagate to all subkeys. ○ Creator Owner: Full Control. Propagate to all subkeys.

To evaluate how the template permission settings above differs from default settings, we imported the baseline.inf file into the "Security Configuration and Analysis" snap-in, and analyzed the default installation of our Windows 2000 OWA FE server against this template. We found that many of the registry permission settings in baseline.inf are actually default configurations. Only four exceptions are noted, and they are given below:

MACHINE\Software	
Default Permissions ○ Bulitin-Users: Read ○ Power Users: Read, Set Value, Create Subkey, and Delete permissions. ○ Administrator: Full Control ○ Creator Owner: Full Control ○ Terminal Server User: Read, Set Value, Create Subkey, and Delete permissions. ○ System: Full Control ○ Disallows inheritable permissions from parent to propagate to this object. ○ Permissions above propagate to all subkeys	Template Modification ○ Builtin-Users: Read. ○ Power Users: Read. ○ Builtin-Administrators: Full control. ○ Local System: Full Control ○ Creator Owner: Full Control. ○ Disallows inheritable permissions from parent to propagate to this object. ○ Permissions above propagate to all subkeys
MACHINE\Software\Classes	
Default Permissions ○ Built-in Users: Read ○ Power Users: Read, Set Value, Create Subkey, and Delete permissions. ○ Builtin-Administrators: Full Control ○ Creator Owner: Full Control ○ Terminal Server User: Read, Set Value, Create Subkey, and Delete permissions. ○ Everyone: Read ○ System: Full Control ○ Disallows inheritable permissions from parent to propagate to this object. ○ Permissions above propagate to all subkeys	Template Modification ○ Everyone: Read ○ Disallows inheritable permissions from parent to propagate to this object. ○ Permissions above propagate to all subkeys
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AsrCommands	
Default Permissions ○ Builtin-Users: Read ○ Power Users: Read ○ Builtin-Administrators: Full Control ○ Creator Owner: Full Control. ○ System: Full Control ○ Disallows inheritable permissions from parent to propagate to this object. ○ Permissions above propagate to all subkeys	Template Modification ○ Builtin-Users: Read. ○ Power Users: Read. ○ Builtin-Administrators: Full control. ○ Local System: Full Control. ○ Creator Owner: Full Control. ○ Backup Operators: Read, Set Value, Create Subkey, and Delete permissions. ○ Disallows inheritable permissions from parent to propagate to this object. ○ Permissions above propagate to all subkeys
MACHINE\System\CurrentControlSet\Control\Print\Printers	
Default Permissions ○ Everyone: Read ○ Builtin-Users: Read ○ Power Users: Read, Set Value, Create Subkey, and Delete permissions. ○ Builtin-Administrators: Full Control ○ Creator Owner: Full Control ○ Terminal Server User: Read, Set Value, Create Subkey, and Delete permissions. ○ System: Full Control ○ Allow inheritable permissions from parent to propagate to this object. ○ Permissions above propagate to all subkeys	Template Modification ○ Allow Everyone (WD) Read access. ○ Allow inheritable permissions from parent to propagate to this object. ○ Permission propagates to all subkeys

Comparing the default permissions with the template modification listed above, we found that baseline.inf tightens access permissions for all four registry keys. Access for the group “Terminal Server User” is removed, and access for the group “Power Users” is tightened. One exception is that the template grants additional access rights to “MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AsrCommands” for the group “Backup Operators.”

Even though many of the settings specified in the template are configured by default, it is still important to have them explicitly specified in the template file. If the security template is applied to the system via a Group Policy Object (GPO) linked to an Organization Unit (OU) where the system resides, any local setting that deviates from the template setting will be corrected when the GPO’s settings are refreshed locally.

The analysis result from “Security Configurations and Analysis” snap-in also shows some other default registry key’s permissions as being different from the baseline.inf template settings. These non-compliant keys are marked with a red “x” in the analysis output. Two examples of supposed non-compliance are Machine\Software\Policies and Machine\System\CurrentControlSet\Services. These non-compliant keys are somewhat mysterious as permissions were not defined for them in baseline.inf, and I have failed to locate any documentation on this subject.

5.1.9.2 Registry Values Modification

Most of the entries in the [Registry Values] section of baseline.inf relate to policy settings in “Security Options”. However there are a few entries whose modification is not viewable from the “Security Templates” snap-in. We will discuss those entries in this sub-section.

MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255
Setting this registry value to 255 will disable autorun on all drive types.
See Q198771 “How to Lock Down Windows NT and Internet Explorer 4.01 Desktop” for details.

MACHINE\System\CurrentControlSet\Control\LSA\MSV1_0\NtlmMinServerSec=4,536870912
Setting this registry value to 536870912 in decimal or 0x20000000 in Hex will causes connection to fail for applications using NTLMSSP, if message confidentiality is in use but 128-bit encryption is not negotiated. Note that 128-bit encryption is not supported on Windows NT system.
See Q147706 “How to Disable LM Authentication on Windows NT” & Q239869 “How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT” for details.

MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation=4,1
Setting this registry value to 1 will disable automatic short file name (8.3 name) creation.
See Q210638 “How to disable Automatic Short File Name Generation” for details.

MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog=4,20000
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog=4,20

```
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta=4,10
```

Adf.sys handles connection attempts to Windows Socket application, such as FTP servers and HTTP servers. The above four registry entries harden adf.sys against malicious SYN attacks. For detail descriptions of the above registry key and its security consequences, see Q142641 "Internet Server Unavailable Because of Malicious SYN Attacks" for details.

```
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxPortsExhausted=4,5
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions=4,3
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions=4,2
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=4,2
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=4,300000
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,2
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableSecurityFilters=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand=4,1
```

All of the above parameters hardens Microsoft TCP/IP stack against Denial of Service Attacks. For detail descriptions of the above registry key and its security consequences, see Q315669 "How To: Harden the TCP/IP Stack Against Denial of Service Attacks in Windows 2000", J. Fossen "Securing Windows 5.5: Securing Internet Information Server" [Ref: 7], and Q238643 "Microsoft Windows 2000 TCP/IP Implementation Details."

5.1.10 File System

To properly secure a system, access to local files and directories needs to be configured appropriately. While most administrators will configure NTFS permissions to control access to data files, restricting access to system binaries and utilities are often overlooked. The "File Security" section of baseline.inf template tightens NTFS permissions on system boot files, system root directory, program files directory, as well as system command files.

The following table summarizes files and directories permission settings in the template baseline.inf. Unless specified explicitly, all permissions enumerated are set to propagate to all subfolders and files.

Files and Directories	Baseline.inf Permission Modification
%SystemRoot% %SystemDirectory%	Disallow inheritable permission to propagate from parent. Builtin-Users: Read and Execute Builtin-Administrators : Full System: Full Creator Owner: Full Everyone: Read and Execute
%SystemDrive%\ %SystemDrive%\autoexec.bat	Disallow inheritable permission to propagate from parent. Child objects inherit permissions from this object Builtin-Administrators: Full Authenticated Users : Read and Execute System: Full

%SystemDrive%\boot.ini %SystemDrive%\ntdetect.com	Disallow inheritable permission to propagate from parent. Child objects inherit permissions from this object Builtin-Administrators: Full System: Full
%SystemDrive%\config.sys	Disallow inheritable permission to propagate from parent. Authenticated Users : Read and Execute Builtin-Administrators : Full System: Full
%SystemDrive%\ntldr %SystemDrive%\io.sys	Disallow inheritable permission to propagate from parent. Builtin-Administrators : Full System: Full
%SystemDrive%\Inetpub	Disallow inheritable permission to propagate from parent. Child objects inherit permissions from this object Builtin-Administrators: Full Everyone: Read and Execute System: Full
%SystemRoot%\repair %SystemRoot%\Temp %SystemRoot%\security %SystemRoot%\system32\config %SystemRoot%\system32\logfiles %SystemRoot%\system32\dllcache %SystemRoot%\system32\ias	Disallow inheritable permission to propagate from parent. Builtin-Administrators : Full System: Full Creator Owner: Full
%ProgramFiles% %SystemRoot%\addins %SystemRoot%\Connection Wizard %SystemRoot%\Driver Cache %SystemRoot%\java %SystemRoot%\msagent %SystemRoot%\speech %SystemRoot%\twain_32 %SystemRoot%\Web %SystemRoot%\system32\dhcp %SystemRoot%\system32\drivers %SystemRoot%\system32\CatRoot %SystemRoot%\system32\mui %SystemRoot%\system32\ShellExt %SystemRoot%\system32\wbem %SystemRoot%\system32\wbem\mof	Disallow inheritable permission to propagate from parent. Builtin-Users: Read and Execute Builtin-Administrators : Full System: Full Creator Owner: Full
%SystemRoot%\explorer.exe	Allow inheritable permission to propagate from parent. Everyone: Read and Execute

%SystemRoot%\System32\ append.exe, at.exe, attrib.exe, cacls.exe, cmd.exe, command.com, cscript.exe, debug.exe, exe2bin.exe, finger.exe, ftp.exe, hostname.exe, mmc.exe, mountvol.exe, nbtstat.exe, net.exe, net1.exe, netsh.exe, netstat.exe, nslookup.exe, ntsd.exe, pathping.exe, ping.exe, rcp.exe, , regedt32.exe, regini.exe, regsvr32.exe, rexec.exe, route.exe, rsh.exe, runas.exe, runonce.exe, secedit.exe, share.exe, telnet.exe, termsrv.exe, tlntadmn.exe, tlntsess.exe, tlntsvr.exe, tftp.exe, tracert.exe, tsadmin.exe, tscon.exe, tskill.exe, tsprof.exe, tsshutdn.exe, wscript.exe, xcopy.exe, arp.exe, change.exe, chglogon.exe, chgport.exe, chgusr.exe, chkdsk.exe, chkntfs.exe, cipher.exe, cluster.exe, compact.exe, convert.exe, dfscmd.exe, doskey.exe, edlin.exe, expand.exe, fc.exe, find.exe, findstr.exe, forcedos.exe, iisreset.exe, ipconfig.exe, ipxroute.exe, label.exe, logoff.exe, lpq.exe, lpr.exe, makecab.exe, mem.exe, msg.exe, ntbackup.exe, print.exe, query.exe, rasdial.exe, recover.exe, register.exe, replace.exe, reset.exe, routemon.exe, router.exe, setpwd.exe, shadow.exe, snmp.exe, snmptrap.exe, subst.exe, tsdiscon.exe, chcp.com, diskcomp.com, diskcopy.com, format.com, mode.com, more.com, tree.com, usrmgr.exe %SystemRoot%\regedit.exe	Disallow inheritable permission to propagate from parent. Child objects inherit permissions from this object Builtin-Administrators: Full
%SystemDrive%\Documents and Settings %SystemRoot%\CSC %SystemRoot%\debug %SystemRoot%\Offline Pages %SystemRoot%\Profiles %SystemRoot%\Registration %SystemRoot%\system32\appmgmt %SystemRoot%\system32\DTCLog %SystemRoot%\system32\GroupPolicy %SystemRoot%\system32\NTMSData %SystemRoot%\system32\ReinstallBackups %SystemRoot%\system32\repl %SystemRoot%\system32\repl\import %SystemRoot%\system32\repl\export %SystemRoot%\system32\Setup %SystemRoot%\system32\spool\printers %SystemRoot%\Tasks	Do not allow permissions on this file or folder to be replaced. This setting is to ensure that permissions will be overwritten inadvertently by the template.

Instead of attempting to enumerate the default permissions on all the files and folders referenced in baseline.inf, we will concentrate our discussion on how permissions on some key files and folders are modified. To view the default permissions, one can either go to the security tab of the file or folder properties, or use the Windows 2000 Resource Kit utility showacls.exe.

One of the most important ACLs modifications in baseline.inf is on the %systemdrive% directory. By default, the group Everyone has full control to the system root drive (typically C:\), and this permissions is configured to propagate to all subfolders and files. Baseline.inf tightens the access rights on the system drive from allowing everyone “Full Control” to “Read and Execute” only. As this change will propagate to all subfolders and files that inherit from parent, it will substantially reduce the risk of hackers tempering with files on the root drive, and will also impede their ability to create malicious files.

Another important ACLs modification is on the %systemroot%\Inetpub directory. By default, Everyone has Full Control on this directory. As the Inetpub\wwwroot is the default home directory on an IIS server, allowing everyone to have full access is a severe and unacceptable security risk. Baseline.inf tightens the ACLs to allow Everyone "Read and Execute" access only. Note that to better secure the system, as discussed by Fossen [Ref: 7] and Scambray & McClure [Ref: 18], the inetpub directory should be relocated from the system drive.

Baseline.inf also tightens ACLs on system utilities and command files within the %SystemRoot%\System 32 directory to only allow Administrators access to these utilities. By default, everyone has read and execute rights on the most, if not all, of these utilities. They include powerful and potentially dangerous tools such as cmd.exe, tftp.exe, regedit.exe, and rsh.exe. Access to these tools will greatly facilitate hackers in comprising a system. On a typical application server, only Adminstrators should have the need to run these tools.

5.2 Microsoft's incremental template for Exchange 2000 OWA FrontEnd server: OWA FrontEnd Incremental.inf

The template "OWA FrontEnd Incremental.inf" provided by Microsoft is to be applied on top of the baseline.inf template discussed above. This template specifically modifies system services startup type, system services security and file security for an Exchange 2000 OWA FrontEnd server.

5.2.1 System Services – Security Settings

The following is the list of services referenced in "OWA FrontEnd Incremental.inf":

- IIS Admin Service
- IPSEC Policy Agent
- Microsoft Exchange Event
- Microsoft Exchange IMAP4
- Microsoft Exchange Information Store
- Microsoft Exchange Management
- Microsoft Exchange MTA Stacks
- Microsoft Exchange POP3
- Microsoft Exchange Routing Engine
- Microsoft Exchange Site Replication Service
- Microsoft Exchange System Attendant
- Microsoft Search
- Remote Procedure Call (RPC) Locator
- World Wide Web Publishing Service

Similar to security settings for system services in the baseline.inf template, security on all of the above services is set to:

- Administrators: Full Control
- Interactive Users: Read

- System: Full Control
- Audit all failure access: Everyone

Compared to the default security settings for these services, as listed in table in subsection 5.1.7, the template settings here tightens access rights for the "Power Users" group and configures auditing parameters.

5.2.2 System Services – Startup Type

The following table enumerates services referenced in the template "OWA FrontEnd Incremental.inf", their default startup type, and their default status. The last column shows the startup type modification by the template.

Service Name	Default Status	Default Startup Type	OWA FrontEnd Incremental.inf Template Settings
IIS Admin Service	Started	Automatic	Automatic
IPSEC Policy Agent	Started	Automatic	Automatic
Microsoft Exchange Event		Manual	Disabled
Microsoft Exchange IMAP4	Started	Automatic	Disabled
Microsoft Exchange Information Store	Started	Automatic	Disabled
Microsoft Exchange Management	Started	Automatic	Disabled
Microsoft Exchange MTA Stacks		Automatic	Disabled
Microsoft Exchange POP3	Started	Automatic	Disabled
Microsoft Exchange Routing Engine	Started	Automatic	Automatic
Microsoft Exchange Site Replication Service		Disabled	Disabled
Microsoft Exchange System Attendant	Started	Automatic	Disabled
Microsoft Search	Started	Automatic	Disabled
Remote Procedure Call (RPC) Locator	Started	Manual	Automatic
World Wide Web Publishing Service	Started	Automatic	Automatic

5.2.2.1 Services Disabled by Template

Microsoft Exchange Event

The Exchange Event service in Exchange 2000 exists for backwards compatibility with server-side scripting of Exchange 5.5. It is not a required service on a front end OWA server.

Microsoft Exchange IMAP4

The Exchange IMAP4 service allows IMAP4 clients to connect and retrieve email. It is not a required service on a front end OWA server.

Microsoft Exchange Information Store

The Exchange Information Store service supports data storage (mailboxes and public folders data) on the server. Since a front end OWA server queries backend server for data, this service can be disabled during regular operations. However, as noted in "Using Microsoft Exchange 2000 Front-End Servers" [Ref: 9], the "Information Store" service needs to be running when an administrator makes configuration changes through “Internet Services Manager”. Also, “Microsoft Exchange Event” service is dependent on “Microsoft Exchange Information Store” service.

Microsoft Exchange Management
The Exchange Management service is introduced with Exchange 2000 service pack 2. This service allows configuration of directory access through the Exchange System Manager interface, and is a crucial component for message tracking. As a front-end OWA server is typically not involved in message routing within an Exchange organization, this service can be safely disabled.

Microsoft Exchange MTA Stacks
The MTA Stacks service supports message routing to foreign messaging system using X.400 and gateway connectors. It is not a required service on a front end OWA server.

Microsoft Exchange POP3
The Exchange POP3 service allows POP3 clients to connect and retrieve email. It is not a required service on a front end OWA server.

Microsoft Exchange Site Replication Service
The Exchange Site Replication Service supports replication of site and configuration information in a mixed Exchange 5.5 and Exchange 2000 environment. It is not a required service on a front end OWA server.

Microsoft Exchange System Attendant
The Exchange System Attendant service is responsible for various Exchange maintenance tasks. As all of these maintenance tasks are not applicable on a front-end OWA server, this service can be disabled. However, note that this service needs to be running when making configuration changes to the server. “Microsoft Exchange MTA Stacks” and “Microsoft Exchange Information Store” services depend on “Microsoft Exchange System Attendant” service.

Microsoft Search
The Microsoft Search service supports full-text indexing on an Exchange server. As no local data storage exists on a front-end OWA server, this service can be disabled.

5.2.2.2 Services Enabled by Template

IIS Admin Service
The IIS Admin Service allows for administration of the Internet Information Services. This service must be enabled on a web server.

IPSEC Policy Agent
The IPSEC Policy Agent is required for implementing IPSec security policy on the server. It is recommended that IPSec policy be set up for communication between a front-end OWA server and backend Exchange 2000 servers / Windows 2000 domain controllers. If IPSec policy is not implemented, this service can be disabled.

Microsoft Exchange Routing Engine

The Microsoft Exchange Routing Engine provides Exchange routing capability, and is a crucial component of Exchange 2000. This service must be running on all Exchange 2000 servers.

Remote Procedure Call (RPC) Locator

The RPC Locator service helps RPC clients locate RPC servers for name services support. It is a required service for communicating with Windows 2000 domain controllers. The “Microsoft Exchange System Attendant” service is dependent on the “Remote Procedure Call Locator” Service.

World Wide Web Publishing Service

The WWW Publishing Service is the core service for a web server, it must be enabled on a front-end OWA sever.

5.2.3 File System

“OWA FrontEnd Incremental.inf” template modifies NTFS permissions for the following folders:

Folder Name	Default Settings	OWA FrontEnd Incremental.inf Template Settings
%SystemDrive%\inetpub\mailroot %SystemDrive%\inetpub\nntpfile	Inherit from parent object. Everyone: Full Control	Disallow inheritable permission to propagate from parent. Builtin-Administrators: Full Control System: Full Control
%SystemDrive%\inetpub\nntpfile\root	Inherit from parent object. Everyone: Full Control	Disallow inheritable permission to propagate from parent. Everyone : Full Control
%SystemDrive%\Inetpub	Inherit from parent object. Everyone: Full Control	Disallow inheritable permission to propagate from parent. Child objects inherit permissions from this object Builtin-Administrators: Full Control Everyone: Read and Execute System: Full Control

Recall that baseline.inf tighten access for the directory %systemroot%\inetpub to only allows “Everyone” “Read and Execute” access. “OWA FrontEnd Incremental.inf” here further tightens the NTFS permissions on the subfolders %systemroot%\inetpub\mailroot and %systemroot\inetpub\nntpfile to only allows full access by “Built-in Administrators” and “System”. Also, for functionality of NNTP, “OWA FrontEnd Incremental.inf” relaxes the ACLs on %systemroot%\nntpfile\root to allow Everyone full access.

6 Template Application and Maintenance

6.1 Application Methods

To apply settings in a security template on a system, the template needs to be imported to a Group Policy Object (GPO) processed by the target system. A member server of an Active Directory domain processes GPOs that are linked to the Local system, the Active Directory Site, the Active Directory Domain, and the Organizational Unit where the system resides. GPOs linked to a site or a domain are typically reserved for configuring all systems (servers and clients) within a domain and site boundary, and are generally not used to configure application servers.

Security templates are typically applied to application servers by two methods: one is direct modification of the system's Local Group Policy Object (GPO) using the "Security Configuration and Analysis" snap-in; the other is application through a Group Policy Object (GPO) linked to an Organizational Unit (OU) where the target system resides. For member servers of an Active Directory domain, where management of systems via an Organizational Unit structure is possible, it is preferred that security settings be applied through an OU level Group Policy Object.

The first reason for applying security template settings via GPO at an OU level relates to the order of GPOs processing on a system. If multiple GPOs are assigned for a system, the system processes them in the following order:

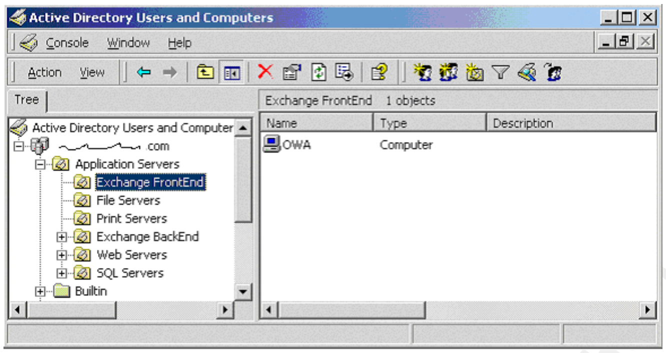
- Local GPO
- Site GPO
- Domain GPO
- Parent Organizational Unit GPO
- Child Organizational Unit GPO

If conflicting settings exist in the GPOs being processed, settings in the GPO processed later override settings in earlier processed GPOs. This default behavior can be modified if the "No Override" option is set for the earlier GPO, and if the "Block Policy Inheritance" option is not set for the later processed GPO. Since the Local GPO is processed first, and it cannot be set to "Block Policy Inheritance", it is the policy with the least influence. To ensure that security template settings would be not override inadvertently by a later processed GPO, it is recommended that settings be enforced through a GPO linked to an Organization Unit.

Applying security template settings through GPO on an OU level also eases administration overhead. Multiple servers requiring identical security settings can be easily configured through OU membership. Members added to an OU will automatically processed the GPO linked to that OU, eliminating the need of configuring Local GPO individually. Also, Organizational Unit level GPOs are refreshed automatically on the targeted system every 90 minutes by default, this ensure that any unintended changes on local security settings will be overwritten by the pre-configured settings.

6.2 Application Procedure

Following the recommendation in Microsoft's "Security Operations for Microsoft Windows 2000 Server" [Ref: 17], we will create a top level Organizational Unit named "Application Servers" in the Active Directory domain for management of all application servers. A GPO named "Baseline Settings", created by importing the baseline.inf template, will be linked to the "Application Servers" OU. Within the "Application Servers" OU, we will create a child OU named "Exchange FrontEnd". A GPO named "FrontEnd OWA Settings", created by importing the "OWA FrontEnd Incremental.inf" template, will be linked to the "Exchange FrontEnd" OU. All Exchange Front-End OWA servers will be members of the "Exchange FrontEnd" OU.



Name	Type	Description
OWA	Computer	

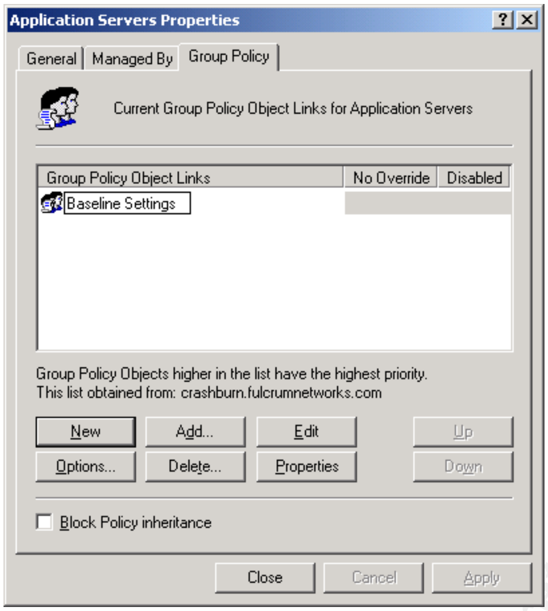
Step-by-Step procedure to achieve the above is as follow:

1. To create the "Application Servers" Organizational Unit
   - Run "Active Directory Users and Computers"
   - Right Click on the domain name; Select New – Organizational Unit
   - Enter "Application Servers" in the name box; Click OK

2. To create the "Exchange FrontEnd" child Organizational Unit
   - Right Click on OU "Application Servers"; Select New – Organization Unit
   - Enter "Exchange FrontEnd" in the name box; Click OK

3. To create and configure the "Baseline Settings" GPO in "Application Servers" OU
   - Right Click on "Application Servers" OU; Select Properties
   - Go to the "Group Policy" tab; Select New

- Input “Baseline Settings” as the policy name.


Application Servers Properties

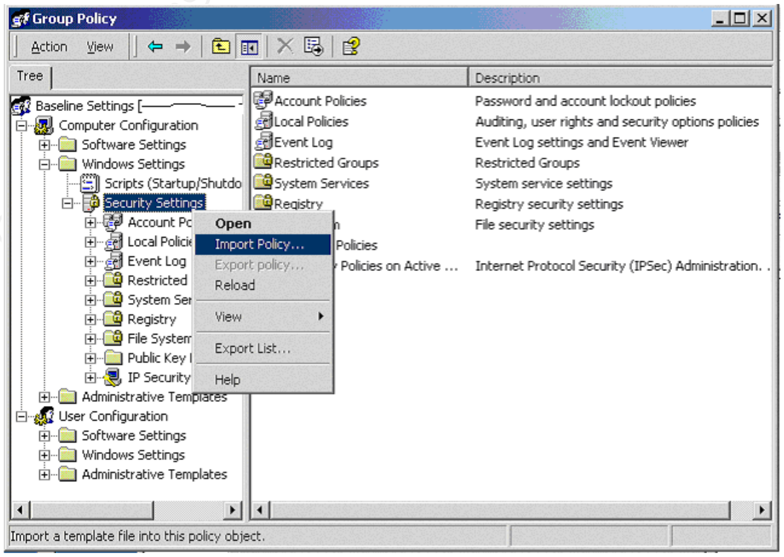
Current Group Policy Object Links for Application Servers

Group Policy Object Links	No Override	Disabled
Baseline Settings		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: crashburn.fulcrumnetworks.com

- Highlight “Baseline Settings” in the above windows
- Click Properties to open the “Baseline Settings Properties” window
- Select “Disable User Configuration settings” in the General tab; Click Yes; Click OK.

4. To import security template “baseline.inf” into “Baseline Settings” GPO
   - Highlight “Baseline Settings” in the above “Application Servers Properties” window
   - Click Edit to bring up the “Group Policy” snap-in.
   - Browse to the “Security Settings” node under “Computer Configuration”
   - Right Click on the “Security Settings” node; Select “Import Policy…”


Group Policy

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options policies
Event Log	Event Log settings and Event Viewer
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
...n	File security settings
Policies	
Policies on Active ...	Internet Protocol Security (IPSec) Administration. .

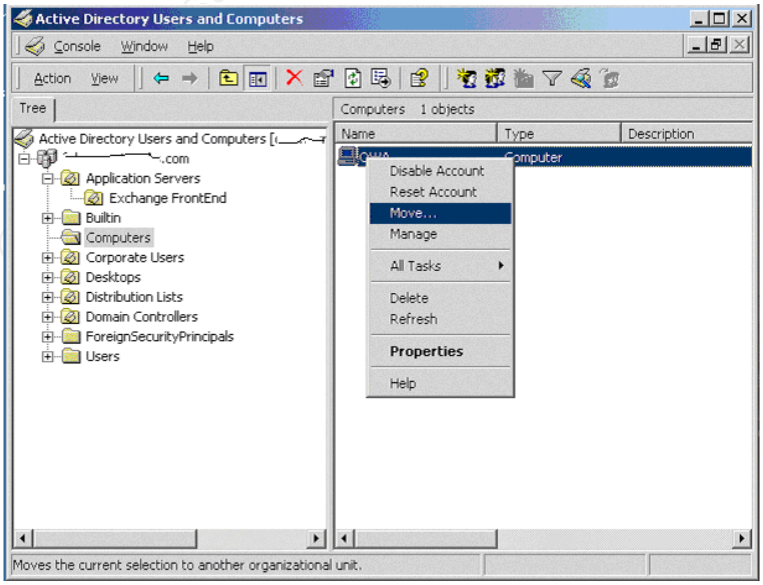
Import a template file into this policy object.

- Browse to location of “baseline.inf” file; Click OK
- Close “Group Policy” snap-in
- Close “Application Servers Properties” window.

5. To create and configure the “FrontEnd OWA Settings” GPO in “Exchange FrontEnd” OU
    - From “Active Directory Users and Computers”
    - Right Click on “Exchange FrontEnd” OU; Select Properties
    - Go to the “Group Policy” tab; Select New
    - Input “FrontEnd OWA Settings” as the policy name.
    - Highlight “FrontEnd OWA Settings”
    - Click Properties to open the “FrontEnd OWA Settings Properties” window
    - Select “Disable User Configuration settings” in the General tab; Click Yes; Click OK.

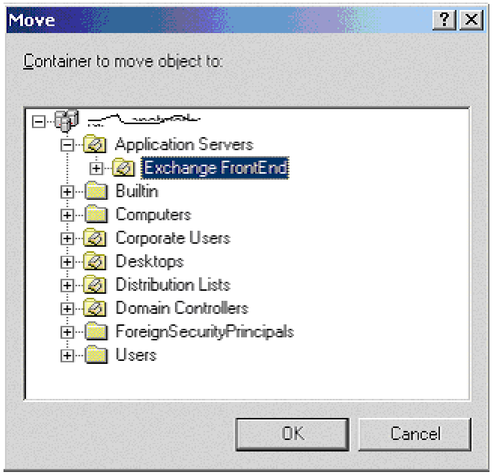
6. To import security template “OWA FrontEnd Incremental.inf” into “FrontEnd OWA Settings” GPO
    - Highlight GPO “FrontEnd OWA Settings” in the “Exchange FrontEnd Properties” window
    - Click Edit to bring up the “Group Policy” snap-in.
    - Browse to the “Security Settings” node under “Computer Configuration”
    - Right Click on the “Security Settings” node; Select “Import Policy…”
    - Browse to location of “OWA FrontEnd Incremental.inf” file; Click OK
    - Close “Group Policy” snap-in
    - Close “Exchange FrontEnd Properties” window.

7. To move an Exchange FrontEnd OWA server into the “Exchange FrontEnd” OU
    - From “Active Directory Users and Computer”
    - Locate the target Exchange OWA server in the Computer container
    - Right Click the server name; Select Move



Moves the current selection to another organizational unit.

- Browse to the “Exchange FrontEnd” OU; Click OK



- Close “Active Directory Users and Computers”

Note that the Exchange FrontEnd OWA server needs to be fully configured and tested before moving it to the destined OU. Some security template settings limit the ability to configure certain aspects of the system, such as setting up SSL certificates for website.

8. Restart the target server for all of the security configurations to take effect.

6.3 Modification and Maintenance of Security Templates

As settings in our security templates are applied through GPOs linked to the OU where our Exchange 2000 FrontEnd Server resides, modification and maintenance of the templates are greatly simplified.

6.3.1 Template Modification

Security templates can be modified either directly by opening the <template>.inf file with a text editor (such as notepad.exe), or through a mmc snap-in (such as Security Templates or Group Policy Editor).

Modifying security template files using a text-editor can be perform by individuals who are familiar with the template format. In general, it will be more intuitive to modify the template using a graphical MMC snap-in. However, there are certain settings in the template, such as registry value edits, that are not exposed through any MMC snap-in. In such instance, direct file modification using a text-editor is the only option.

Security template file can be modified using the “Security Template” snap-in. Viewing of template settings using this tool is discussed in Section 5 “Template Settings” of this paper. From the same interface used for viewing the templates, one could also modify/add/remove any security settings displayed. To save the modifications, one need to right click on the template name and select save. The corresponding template file will then be updated.

Both modification methods described above generate a modified <template.inf> file. In order to push the updated settings to a target system, one needs to update the corresponding Group Policy Object with the updated template file. The procedure for updating a GPO is similar to that outlined in Step 4 'To import security template "baseline.inf" into "Baseline Settings" GPO' in Subsection 6.2" Application Procedure", where one would supply the updated template file when prompted.

Once the updated security template file is imported into an appropriate GPO, all systems within the OU where the GPO is linked will be automatically updated. By default, GPOs are refreshed on target systems every 90 minutes. No administrator intervention is necessary to propagate the settings to individual systems. If, however, an administrator wants to accelerate this process, he/she could use the built-in windows utility "secedit.exe". By executing

secedit /refreshpolicy machine_policy /enforce

on the target system, the local system will immediately download the updated GPO and refresh its security policy.

Note that security settings can also be modified directly using Group Policy Editor on a GPO object that is linked to an OU. The following are the steps involved:

- From "Active Directory Users and Computers", browse to the target OU
- Right Click on the OU, and select Properties
- Go to the Group Policy Tab, select the GPO to be modified, click Edit.
- From the new window for Group Policy Editor, browse to Security Settings node
- Make desired modification.

However, as it is currently not possible to export modified security settings from this interface into a <template>.inf file for backup purposes, this method is not recommended.

6.3.2 Maintenance Tasks

As security template settings are assigned to systems using GPO on an OU level, maintenance of this process equates to maintenance of Group Policy Object replication and application within the domain.

Group Policy Objects are stored on the Sysvol shares on all domain controllers within an Active Directory domain. Distributed File System service running on domain controllers is responsible for keeping this replicated object in synchronization. Group Policy Objects configuration is stored within the Active Directory database, and is replicated among domain controllers as part of the Active Directory database. Proper configuration of the Active Directory architecture is a prerequisite for ensuing GPO replication and assignment. As Active Directory configuration is a topic beyond the scope of this paper, we will not discuss it in details.

Assuming that we have a properly deployed Active Directory architecture, GPO replication and assignment should be a relatively maintenance free process. The following are some tools useful in supporting and troubleshooting GPO replication and assignment:

Event Viewer – Application Log
Administrators should review the application log on a regular basis. Events with the source "SceCli" are related to security policy settings on the local system. Under normal operation, event ID 1704 with description "Security policy in the Group policy objects are applied successfully" should be logged occasionally.

GPResult.exe
A built-in Windows utility, GPResult.exe is a command line tool that displays detailed information on Group Policy application on the local system. Some information of interest includes when GPO was applied last, from which domain controller was the GPOs obtained, and from which GPO did the system received various settings.

GPOTool.exe
A Windows 2000 Resource Kit utility, GPOTool is a command line tool that verifies consistency of GPO replication. GPOTool will display detailed version information if GPOs are not synchronized among domain controllers, or if a GPO object in Sysvol does not correspond to the GPO configuration stored in Active Directory.

Security Configuration and Analysis
This Windows MMC snap-in allows administrators to analyze current local security settings against a predefined database. An example on using this tool is illustrated in Step 4 of Subsection 7.1 "Verification Procedure" of this paper.

SecEdit.exe
A built-in Windows utility, secedit.exe is a command line tool for analyzing, configuring, refreshing and exporting security settings. The most common usage is probably "secedit /refreshpolicy machine_policy /enforce", which instructs the local system to immediately download the latest GPOs and apply the security settings.

To further secure and protect our security configurations, we should also perform the following:

- Ensure that Active Directory database and "System State" are being backed up regularly.
- Backup all security templates imported by Group Policy Objects. These files will serve as documentation for security configurations, and can also be used to recreate the GPO in a disaster recovery situation.

- Set appropriate permissions on Group Policy Objects and Organizational Units; ensure that only authorized administrators have rights to create/delete/modify Group Policy Objects.
- Verify that auditing on GPO objects is enabled. Success and failure auditing should be enabled on all write/create/delete events. This will provide tracking information as to when and by whom GPO is being edited.
- Note and record revision numbers for GPO. The revision number should stay constant unless the GPO has been edited. This information is available on the General tab of GPO Properties.

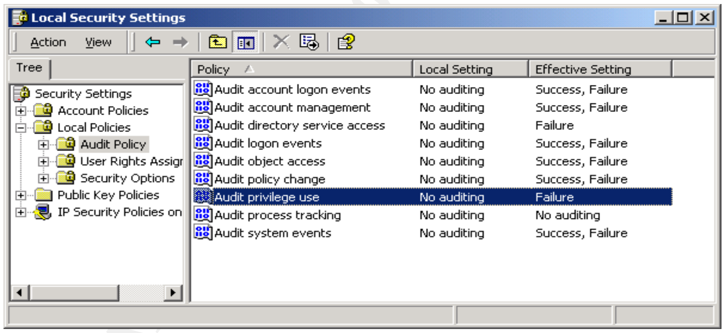
7 Verification and Testing of Template Settings

7.1 Verification Procedure

To verify that template settings are properly applied on the target system, the following was performed.

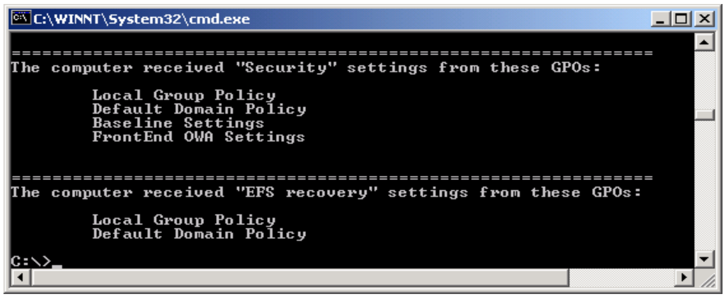
1. Ran "Event Viewer"
   Verified that Event ID 1704 "Security policy in the Group Policy objects are applied successfully" is logged on the system's application log.

2. Ran "Local Security Policy" snap-in from "Administrative Tools"
   Verified that settings specified in the security templates are reflected in "Effective Setting"



Policy	Local Setting	Effective Setting
Audit account logon events	No auditing	Success, Failure
Audit account management	No auditing	Success, Failure
Audit directory service access	No auditing	Failure
Audit logon events	No auditing	Success, Failure
Audit object access	No auditing	Success, Failure
Audit policy change	No auditing	Success, Failure
Audit privilege use	No auditing	Failure
Audit process tracking	No auditing	No auditing
Audit system events	No auditing	Success, Failure

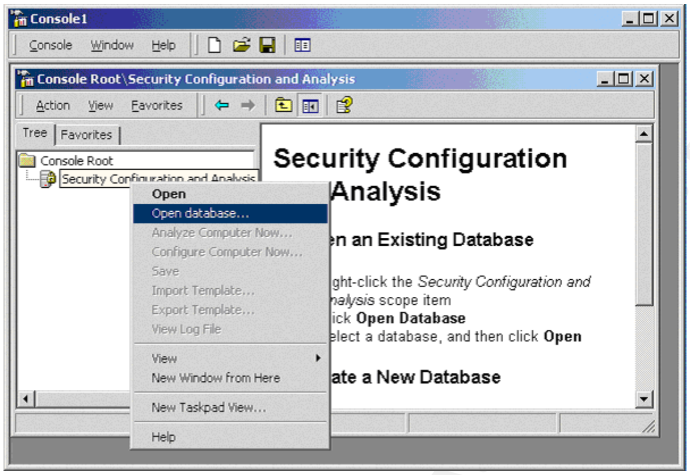
3. Ran the Windows Resource Kit utility "gpresult.exe"
   The output of gpresult showed all the GPOs processed by the local system.



```
===============================================================
The computer received "Security" settings from these GPOs:

        Local Group Policy
        Default Domain Policy
        Baseline Settings
        FrontEnd OWA Settings

===============================================================
The computer received "EFS recovery" settings from these GPOs:

        Local Group Policy
        Default Domain Policy

C:\>_
```

4. Ran “Security Configuration and Analysis” snap-in and obtained detailed settings information. Detailed procedure is as follows:

   a) Follow the procedure in Section 5 “Template Settings” to create a custom MMC console. Select the snap-in “Security Configuration and Analysis” instead of “Security Templates” as directed in Section 5.
   b) Right click on **Security Configuration and Analysis**; Select Open database



Security Configuration Analysis

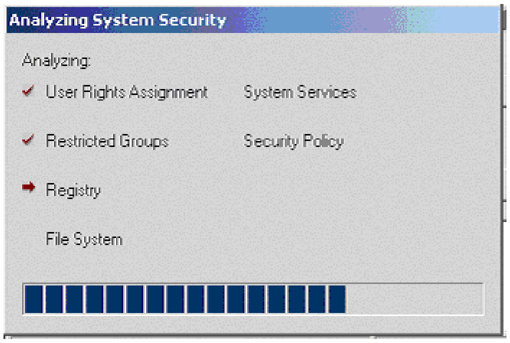
n an Existing Database

ght-click the *Security Configuration and nalysis* scope item
ick **Open Database**
elect a database, and then click **Open**

ate a New Database

   c) Type “owa.sdb” in the file name box: Click Open. Note that the name used is not relevant.
   d) From the “Import Template” window, browse to the location of the template “baseline.inf”; Click Open
   e) Right click again on Security Configuration and Analysis; Select “Import Template …”
   f) From the “Import Template” window, browse to the location of the template “OWA FrontEnd Incremental.inf”; Ensure that the checkbox for “Clear this database before importing” is NOT checked; Click Open.
   g) Analyze the local system settings against the templates setting by right clicking on Security Configuration and Analysis, and select “Analyze Computer Now …”
   h) Click OK to the default error log path.

i) The following is displayed during the analysis process

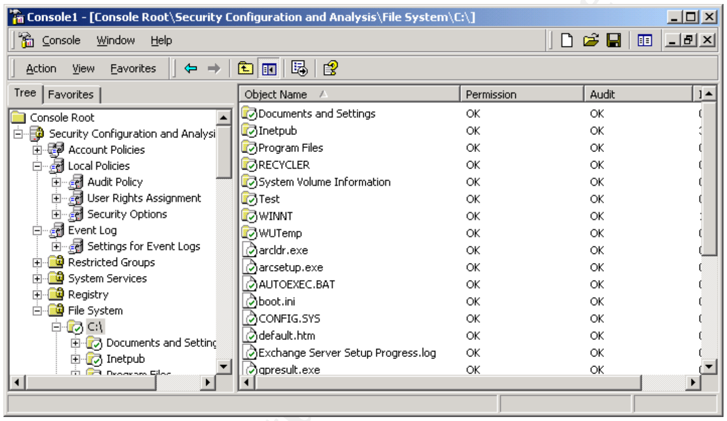


Analyzing System Security

Analyzing:

- ✓ User Rights Assignment — System Services
- ✓ Restricted Groups — Security Policy
- ➡ Registry
- File System

j) After the analysis is complete, browse to various nodes on the left pane to verify successful application of template settings. A green checkmark next to an object name signifies that the local setting is consistent with the template settings on that object; and a red cross signifies that the local setting differs from the template settings.



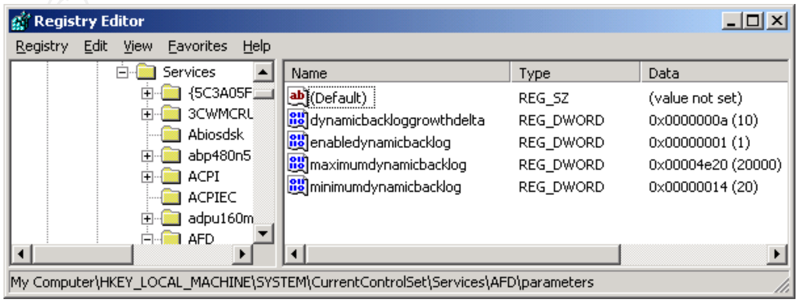
Console1 - [Console Root\Security Configuration and Analysis\File System\C:\]

Object Name	Permission	Audit
Documents and Settings	OK	OK
Inetpub	OK	OK
Program Files	OK	OK
RECYCLER	OK	OK
System Volume Information	OK	OK
Test	OK	OK
WINNT	OK	OK
WUTemp	OK	OK
arcldr.exe	OK	OK
arcsetup.exe	OK	OK
AUTOEXEC.BAT	OK	OK
boot.ini	OK	OK
CONFIG.SYS	OK	OK
default.htm	OK	OK
Exchange Server Setup Progress.log	OK	OK
gpresult.exe	OK	OK

k) Exit the Console; Save Console for future use.

5. Ran registry editor (regedit.exe)

   Verified that registry values modifications imposed in baseline.inf are updated on the local system. Note that the "Security Configuration and Analysis" tool does not reveal these modifications.



Registry Editor

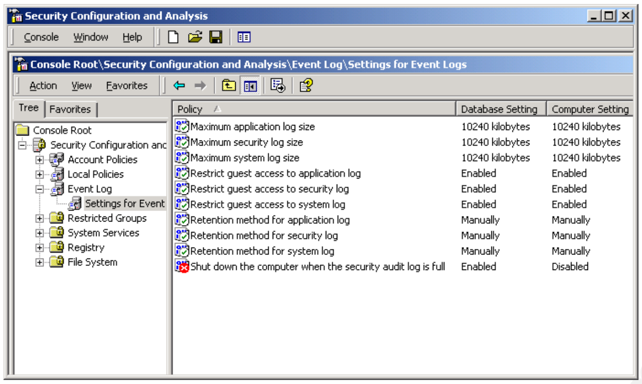
Name	Type	Data
(Default)	REG_SZ	(value not set)
dynamicbackloggrowthdelta	REG_DWORD	0x0000000a (10)
enabledynamicbacklog	REG_DWORD	0x00000001 (1)
maximumdynamicbacklog	REG_DWORD	0x00004e20 (20000)
minimumdynamicbacklog	REG_DWORD	0x00000014 (20)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\parameters

7.2 Issues with Templates Application

During verification of security templates application by methods enumerated above, we noticed that the Security Configuration and Analysis tool reported two areas of discrepancies between local system settings and desired template settings.

The first discrepancy is located in Security Settings | Event Log | Settings for Event Logs. The “Enabled” setting for “Shut down the computer when the security audit log is full” is not set.

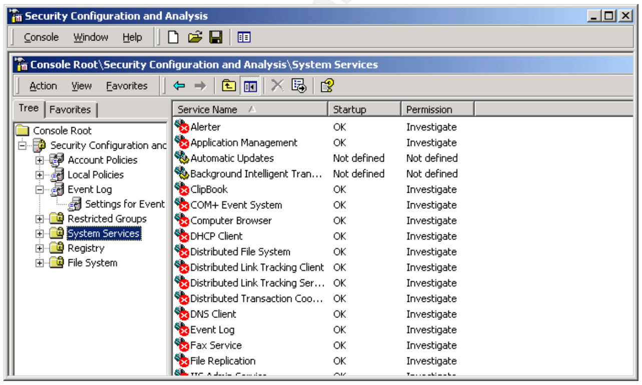


Console Root\Security Configuration and Analysis\Event Log\Settings for Event Logs

Policy	Database Setting	Computer Setting
Maximum application log size	10240 kilobytes	10240 kilobytes
Maximum security log size	10240 kilobytes	10240 kilobytes
Maximum system log size	10240 kilobytes	10240 kilobytes
Restrict guest access to application log	Enabled	Enabled
Restrict guest access to security log	Enabled	Enabled
Restrict guest access to system log	Enabled	Enabled
Retention method for application log	Manually	Manually
Retention method for security log	Manually	Manually
Retention method for system log	Manually	Manually
Shut down the computer when the security audit log is full	Enabled	Disabled

This setting exists in the template baseline.inf, and can be viewed via the Security Templates snap-in. However, upon review of the “Baseline Settings” GPO, this one particular setting has not been imported. Repeated attempts to import this setting into the GPO also failed. The reason for failure is currently unknown, and we failed to locate a Microsoft article that documents this apparent bug. After manually updating this setting in “Baseline Settings” GPO using Group Policy Editor, we verified that this security setting did get propagated and configured on the target system.

The second discrepancy is that permissions on all configured system services are reported as mismatched.



Console Root\Security Configuration and Analysis\System Services

Service Name	Startup	Permission
Alerter	OK	Investigate
Application Management	OK	Investigate
Automatic Updates	Not defined	Not defined
Background Intelligent Tran…	Not defined	Not defined
ClipBook	OK	Investigate
COM+ Event System	OK	Investigate
Computer Browser	OK	Investigate
DHCP Client	OK	Investigate
Distributed File System	OK	Investigate
Distributed Link Tracking Client	OK	Investigate
Distributed Link Tracking Ser…	OK	Investigate
Distributed Transaction Coo…	OK	Investigate
DNS Client	OK	Investigate
Event Log	OK	Investigate
Fax Service	OK	Investigate
File Replication	OK	Investigate

Viewing the details on each service revealed that while access permissions is configured according to our template settings; the auditing setting seems to be missing. Upon testing of system service access (see next subsection for details), we confirmed that auditing is indeed configured appropriately on the target system.

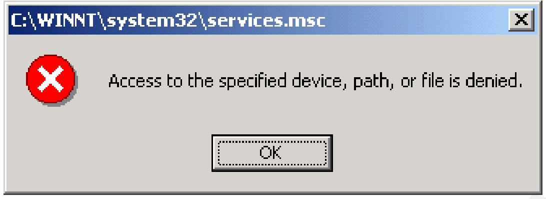
7.3 Testing of Template Settings

To confirm that security settings in our templates did get configured properly on the target system, we will perform the following tests.

7.3.1 Access to System Services

A user without administrative rights will attempt to access services on the target system, and change their startup settings. If security settings are configured as expected, the user will succeed in reading the service status, fail in the attempt to change the service start-up type, and a failure event will be logged in security log. Detailed procedure and findings are as follows:

A regular user logged on to the target system, and attempted to access the "Services" snap-in. Access to snap-in is denied. This denial is a result of tightened NTFS permissions of the mmc.exe utility.

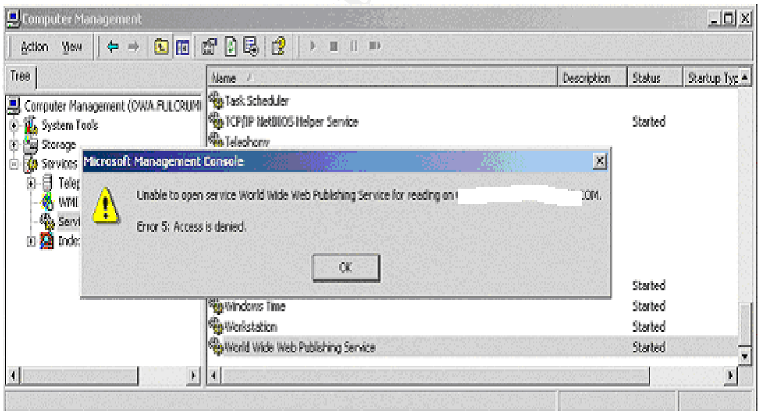


C:\WINNT\system32\services.msc

Access to the specified device, path, or file is denied.

The user then logged on to another system in the same domain, ran Computer Management snap-in, and connected to the target system. User was able to browse to the services node, and to display the lists of system services on the target system.

User then attempted to change the start-up option by opening the "World Wide Web Publishing Services". Access to the service's properties window was denied.



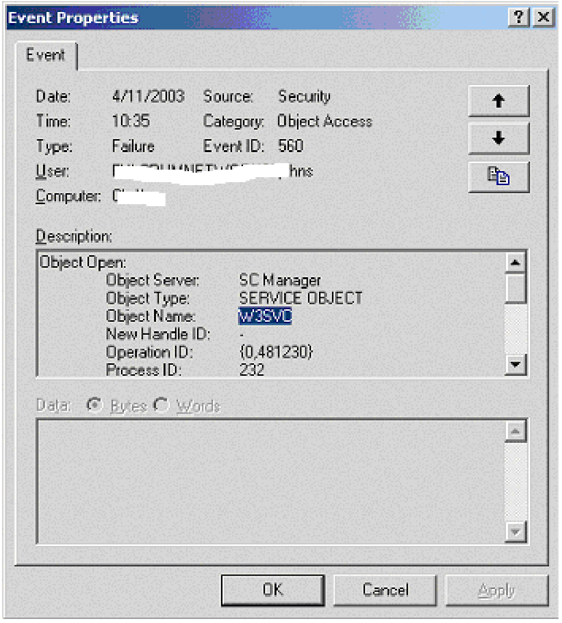
Name	Description	Status	Startup Typ
Task Scheduler			
TCP/IP NetBIOS Helper Service		Started	
Telephony			
		Started	
Windows Time		Started	
Workstation		Started	
World Wide Web Publishing Service		Started	

Microsoft Management Console

Unable to open service World Wide Web Publishing Service for reading on [redacted] COM.

Error 5: Access is denied.

A review of the security log shows that this failure access attempt was audited.

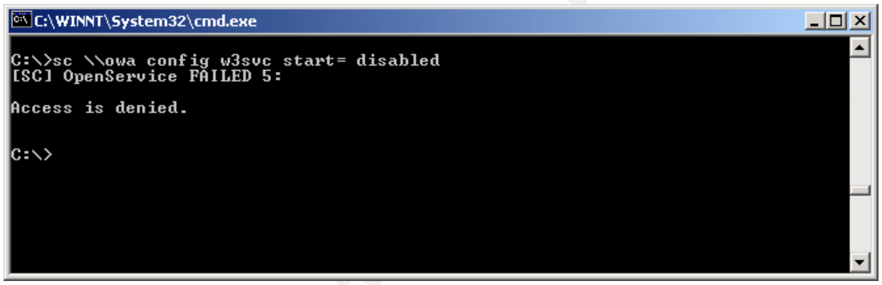


Date: 4/11/2003 Source: Security
Time: 10:35 Category: Object Access
Type: Failure Event ID: 560
User: [redacted] hns
Computer: [redacted]

Description:

```
Object Open:
        Object Server:      SC Manager
        Object Type:        SERVICE OBJECT
        Object Name:        W3SVC
        New Handle ID:      -
        Operation ID:       {0,481230}
        Process ID:         232
```

User then attempted to change the start-up type by using the Resource Kit utility “sc.exe”, and was denied access.



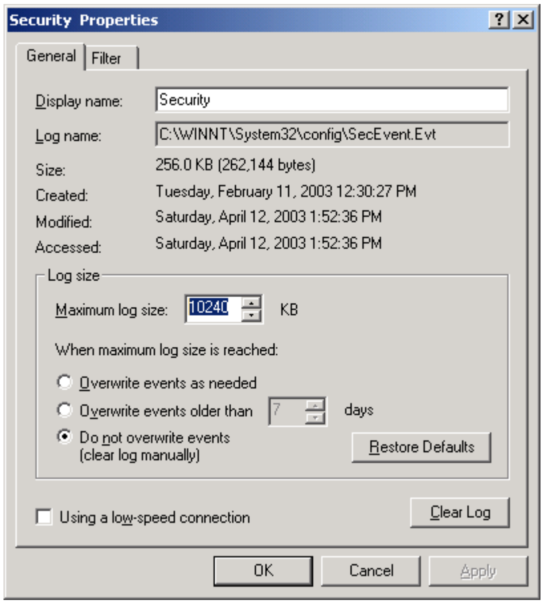
```
C:\>sc \\owa config w3svc start= disabled
[SC] OpenService FAILED 5:

Access is denied.


C:\>
```

The above procedure demonstrates that Access Control List (ACL) on system services is configured per our template settings. An Interactive User with no administrative rights can only view limited information on system services, and is denied access on configuration attempts. Also, failure access attempts are being audited.

The same procedure was also performed as an administrator and all configuration attempts were successful.

7.3.2 Security Log Settings

Reviewing properties of security log in Event Viewer showed that log settings are configured according to the template baseline.inf. The maximum log size was set to 10,240 KB, and the option to clear log manually is enabled.



Security Properties

General | Filter

Display name: Security

Log name: C:\WINNT\System32\config\SecEvent.Evt

Size: 256.0 KB (262,144 bytes)

Created: Tuesday, February 11, 2003 12:30:27 PM

Modified: Saturday, April 12, 2003 1:52:36 PM

Accessed: Saturday, April 12, 2003 1:52:36 PM

Log size

Maximum log size: 10240 KB

When maximum log size is reached:

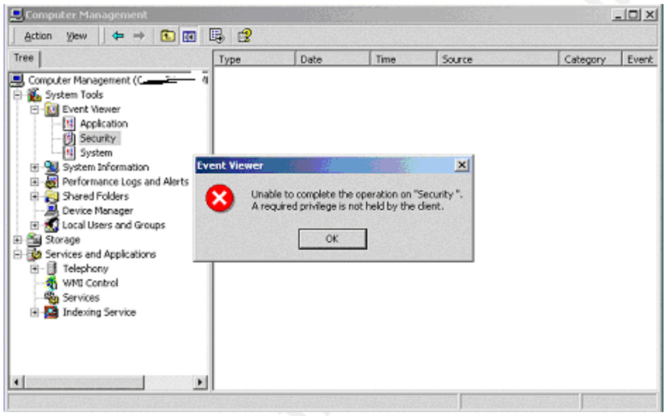
○ Overwrite events as needed

○ Overwrite events older than 7 days

● Do not overwrite events (clear log manually)

□ Using a low-speed connection

A user without administrative rights attempted to view details of the security logs, and was denied access. This behavior is consistent with the enabled setting on “Restrict guest access to security log”.



Computer Management

Computer Management (C[redacted]

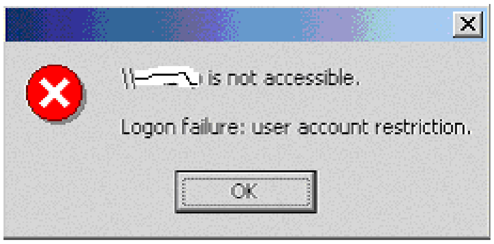
Event Viewer

Unable to complete the operation on "Security ". A required privilege is not held by the client.

We also verified the Event Log setting of “Shut down the computer when the security audit log is full” by performing the following:

- From Event Viewer on the target system, obtained properties of the security log, and noted the current logfile size.
- Opened “Baseline Settings” GPO with Group Policy Editor, and temporarily changed the Maximum log size setting for security log to be slightly over the noted current log size.
- Forced GPO download and refresh on the target system by running “secedit /refreshpolicy machine_policy /enforce”. Rebooted the target system for changes to take effect.
- Manually generated security audits to fill up the security log on the target system.

Shortly after the security log file size reached the maximum allowable size, the target system rebooted automatically. After the system rebooted, a regular user attempted to logon locally to the target system and was denied access. The target system displayed a prompt "*Your account is configured to prevent you from using this computer. Please try another computer*." Attempt to access the target system remotely also failed. The error message displayed was:



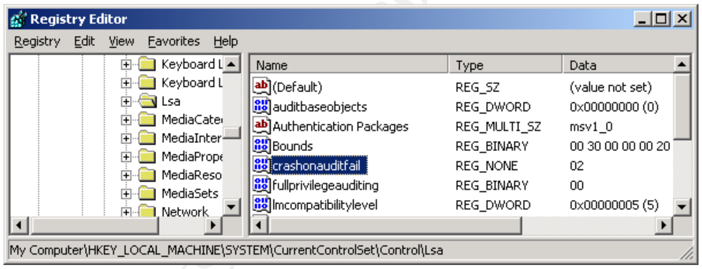
\\[redacted] is not accessible.

Logon failure: user account restriction.

Access to Exchange Outlook Web Access page on the target system also failed with error "HTTP 404: File Not Found". It is noted in Microsoft Knowledge Base article Q160783 "Error: Users cannot log on to a workstation" that if a system is rebooted from a failure to log auditing events, only administrators will have access to the target system.

After successfully logged on to the target system as a user with administrative rights, the following were performed to re-enable general access to the system:

- ○ Manually cleared the security log
- ○ Reset the registry key MACHINE\System\CurrentControlSet\Lsa\crashonauditfail from "02" to "01"



Name	Type	Data
(Default)	REG_SZ	(value not set)
auditbaseobjects	REG_DWORD	0x00000000 (0)
Authentication Packages	REG_MULTI_SZ	msv1_0
Bounds	REG_BINARY	00 30 00 00 00 20
crashonauditfail	REG_NONE	02
fullprivilegeauditing	REG_BINARY	00
lmcompatibilitylevel	REG_DWORD	0x00000005 (5)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

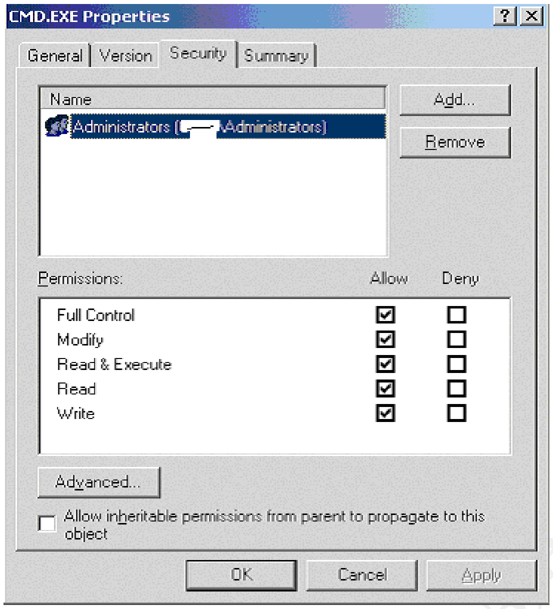
- ○ Rebooted the system.

As demonstrated by the above procedure, the Event Log setting "Shut down the computer when the security audit log is full" does work as expected. However, even though the system behaved as expected, one should note that no meaningful event log message was logged for this process. One would expect that, at a minimum, an event would be logged for the security log being full. The only logged message for this process was that the prior system shutdown was unexpected.

7.3.3 System utility access

The last verification for template settings will be users' access to various system utilities. The security template, baseline.inf, tightens NTFS permissions on many system utilities such only users with administrator rights can execute them.

Logged on as an administrator, the NTFS permissions on the system utility cmd.exe is noted as follows:

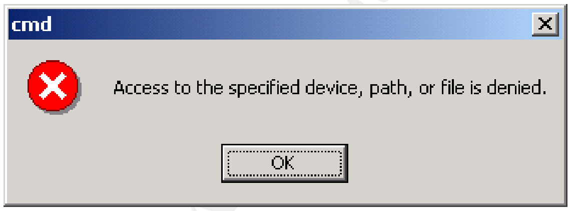


Name: Administrators ([redacted]\Administrators)

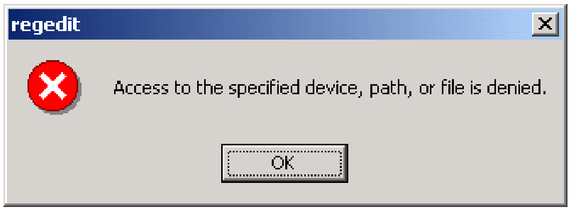
Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
Read	☑	□
Write	☑	□

□ Allow inheritable permissions from parent to propagate to this object

Logged on as a user without administrative rights, we attempted to execute system utilities, such as cmd.exe and regedit.exe, and were denied access. The error received were:



Access to the specified device, path, or file is denied.



Access to the specified device, path, or file is denied.

As demonstrated by the above procedure, file access security settings as configured by the template does work as expected.

8 Testing System Functionality

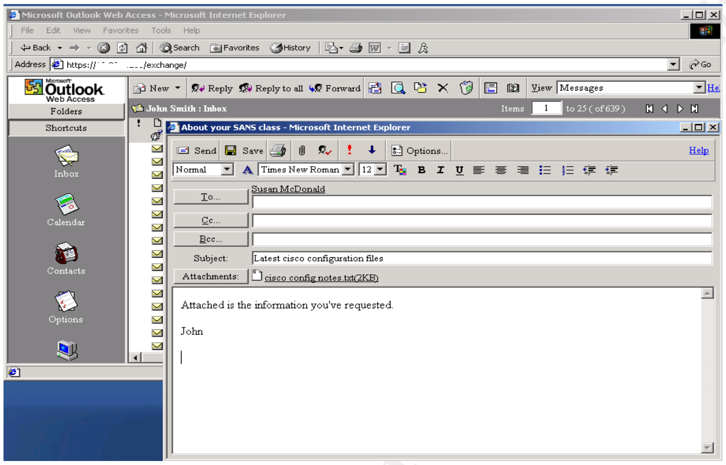
The sole purpose of our Exchange 2000 Front End OWA server is to provide users HTTPS access to the corporate Exchange 2000 messaging environment. We will verify that after application of the templates, users are still able to send/receive email, view contact information, schedule appointments, and access public folder information.

We will also test an administrator's ability to manage the system by attempting to apply Windows and Exchange service packs, to create a new virtual directory for custom public folder access, and to apply an Exchange 2000 Post SP3 rollout up patch. Lastly, we will verify that Windows Update on the target server is able to connect to the corporate Software Update Server to download and install approved Windows patches and hotfiixes.

8.1 Exchange User Access

From a remote workstation, we were able to logon to a non-administrator mailbox on the Exchange 2000 OWA FE server, and successfully performed the following:

The user was able to read, send and receive email.


Microsoft Outlook Web Access - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Go
Outlook Web Access
Folders
Shortcuts
Inbox
Calendar
Contacts
Options
New Reply Reply to all Forward
View
Send Save Options... Help
To...
Cc...
Bcc...

Address: https:// /exchange/

View: Messages

John Smith : Inbox — Items 1 to 25 (of 639)

About your SANS class - Microsoft Internet Explorer

Normal — Times New Roman — 12

To: Susan McDonald

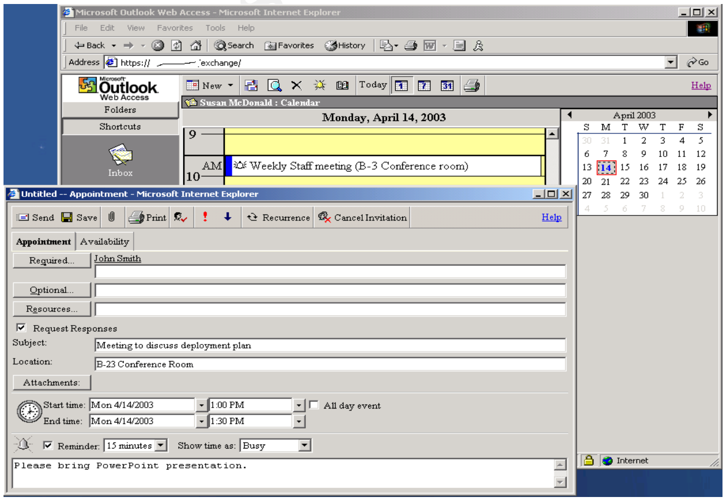
Subject: Latest cisco configuration files

Attachments: cisco config notes.txt(2KB)

Attached is the information you've requested.

John

The user was able to view calendar information, resolve another user's name using Exchange's global address list, and schedule a meeting request. We also verified that the intended recipient received the meeting request.


Microsoft Outlook Web Access - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Go
Outlook Web Access
Folders
Shortcuts
Inbox
New Today Help
Untitled -- Appointment - Microsoft Internet Explorer
Send Save Print Recurrence Cancel Invitation Help
Appointment Availability
Required...
Optional...
Resources...
Attachments:
Internet

Address: https:// 'exchange/

Susan McDonald : Calendar

Monday, April 14, 2003

9 AM 10 — Weekly Staff meeting (B-3 Conference room)

April 2003

S	M	T	W	T	F	S
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

Required: John Smith

☑ Request Responses

Subject: Meeting to discuss deployment plan

Location: B-23 Conference Room

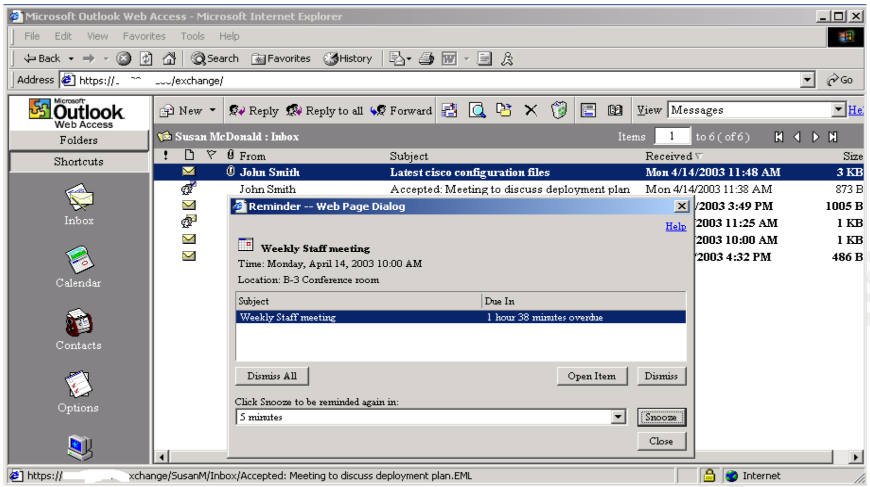
Start time: Mon 4/14/2003 1:00 PM ☐ All day event

End time: Mon 4/14/2003 1:30 PM

☑ Reminder: 15 minutes Show time as: Busy

```
Please bring PowerPoint presentation.
```

Reminders for scheduled appointments also functioned as expected.


Microsoft Outlook Web Access - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address https://. ~~ ..../exchange/
Go
Microsoft Outlook Web Access
Folders
Shortcuts
Inbox
Calendar
Contacts
Options
New Reply Reply to all Forward
View Messages
He
Items 1 to 6 (of 6)
Help

Susan McDonald : Inbox

From	Subject	Received	Size
John Smith	Latest cisco configuration files	Mon 4/14/2003 11:48 AM	3 KB
John Smith	Accepted: Meeting to discuss deployment plan	Mon 4/14/2003 11:38 AM	873 B
		/2003 3:49 PM	1005 B
		2003 11:25 AM	1 KB
		2003 10:00 AM	1 KB
		/2003 4:32 PM	486 B

Reminder -- Web Page Dialog

Weekly Staff meeting
Time: Monday, April 14, 2003 10:00 AM
Location: B-3 Conference room

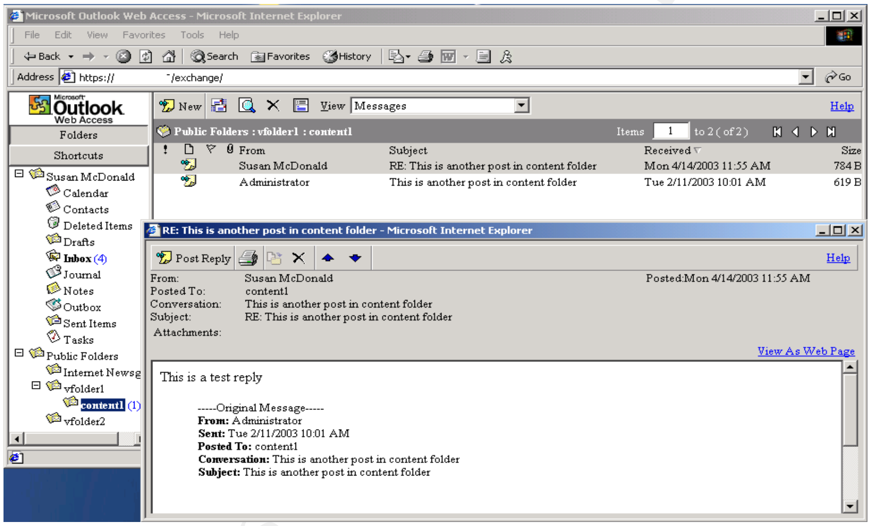
Subject	Due In
Weekly Staff meeting	1 hour 38 minutes overdue

Dismiss All Open Item Dismiss

Click Snooze to be reminded again in:
5 minutes Snooze
Close

https:// xchange/SusanM/Inbox/Accepted: Meeting to discuss deployment plan.EML Internet

Lastly, the user was able to view Exchange public folder information.



Public Folders : vfolder1 : content1

From	Subject	Received	Size
Susan McDonald	RE: This is another post in content folder	Mon 4/14/2003 11:55 AM	784 B
Administrator	This is another post in content folder	Tue 2/11/2003 10:01 AM	619 B

RE: This is another post in content folder - Microsoft Internet Explorer

From: Susan McDonald Posted:Mon 4/14/2003 11:55 AM
Posted To: content1
Conversation: This is another post in content folder
Subject: RE: This is another post in content folder
Attachments:

This is a test reply

-----Original Message-----
From: Administrator
Sent: Tue 2/11/2003 10:01 AM
Posted To: content1
Conversation: This is another post in content folder
Subject: This is another post in content folder

In summary, the template application did not affect the usability of Exchange Outlook Web Access.

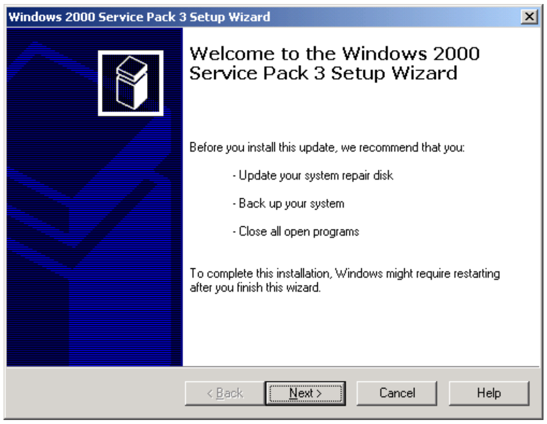
8.2 Administrator Access – Management Tasks

While logged on as an administrator on the Exchange 2000 OWA FE server, we attempted to perform the following:

8.2.1 Reinstall Windows 2000 Service Pack 3

Windows 2000 Service Pack 3 is reapplied on the system to test whether an administrator is able to install service pack after the security templates settings are configured. Ideally, one would install a new service pack to test this functionally. However, as service pack 3 is the latest SP at the time of writing of this paper, and SP3 is already installed on the target system, testing will be performed by reinstallation of the service pack.

Re-installation of Windows service pack 3 was successful.

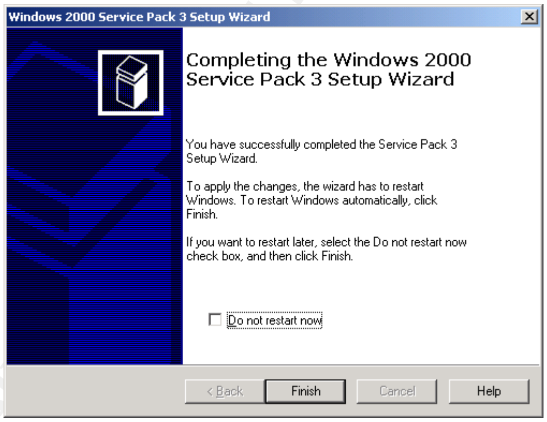


Welcome to the Windows 2000 Service Pack 3 Setup Wizard

Before you install this update, we recommend that you:

- Update your system repair disk
- Back up your system
- Close all open programs

To complete this installation, Windows might require restarting after you finish this wizard.



Completing the Windows 2000 Service Pack 3 Setup Wizard

You have successfully completed the Service Pack 3 Setup Wizard.

To apply the changes, the wizard has to restart Windows. To restart Windows automatically, click Finish.

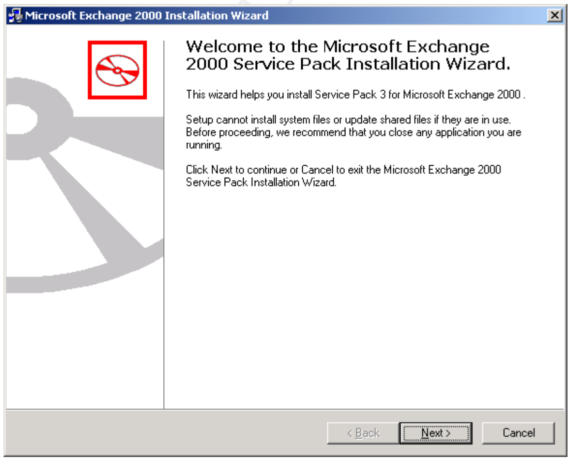
If you want to restart later, select the Do not restart now check box, and then click Finish.

□ Do not restart now

8.2.2 Reinstall Exchange 2000 Service Pack 3

We will reinstall Exchange 2000 service pack 3 on the target systems to test an administrator's ability to install Exchange service pack after the security templates settings are configured.

Exchange SP3 installation started without problems.



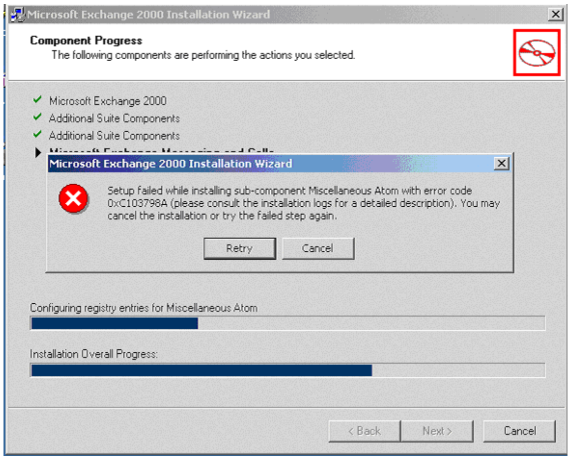
Welcome to the Microsoft Exchange 2000 Service Pack Installation Wizard.

This wizard helps you install Service Pack 3 for Microsoft Exchange 2000 .

Setup cannot install system files or update shared files if they are in use. Before proceeding, we recommend that you close any application you are running.

Click Next to continue or Cancel to exit the Microsoft Exchange 2000 Service Pack Installation Wizard.

However, during the installation process, the following error message was displayed.



Microsoft Exchange 2000 Installation Wizard

Component Progress
The following components are performing the actions you selected.

- ✓ Microsoft Exchange 2000
- ✓ Additional Suite Components
- ✓ Additional Suite Components

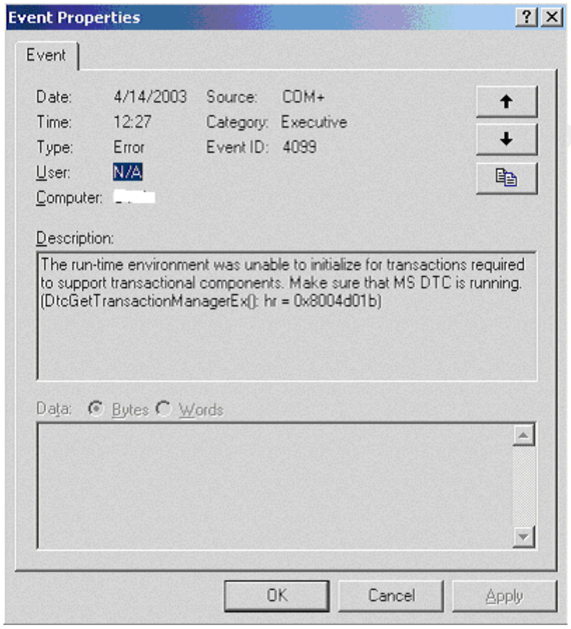
Microsoft Exchange 2000 Installation Wizard

Setup failed while installing sub-component Miscellaneous Atom with error code 0xC103798A (please consult the installation logs for a detailed description). You may cancel the installation or try the failed step again.

Configuring registry entries for Miscellaneous Atom

Installation Overall Progress:

Upon review of Event Logs, we found two related error events. One complained about MSDTC (Distributed Transaction Coordinator) service being disabled, and the other complained about WinMgmt (Windows Management Instrumentation) service being disabled.



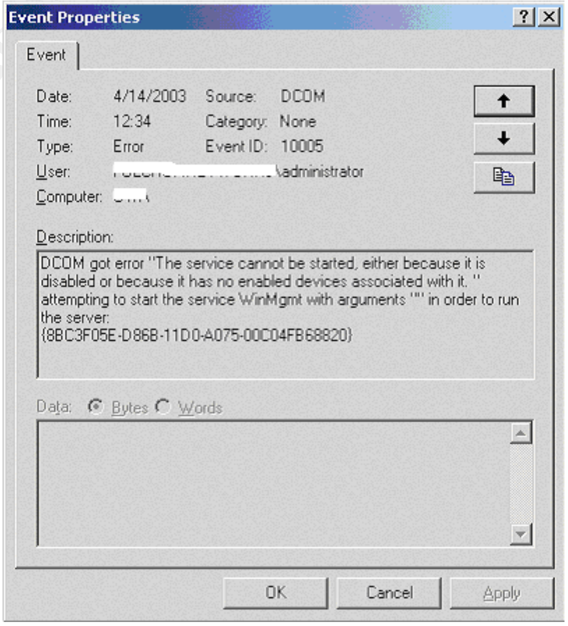
Event Properties

Event

Date: 4/14/2003 Source: COM+
Time: 12:27 Category: Executive
Type: Error Event ID: 4099
User: N/A
Computer: [redacted]

Description:
The run-time environment was unable to initialize for transactions required to support transactional components. Make sure that MS DTC is running. (DtcGetTransactionManagerEx(): hr = 0x8004d01b)

Data: ● Bytes ○ Words



Event Properties

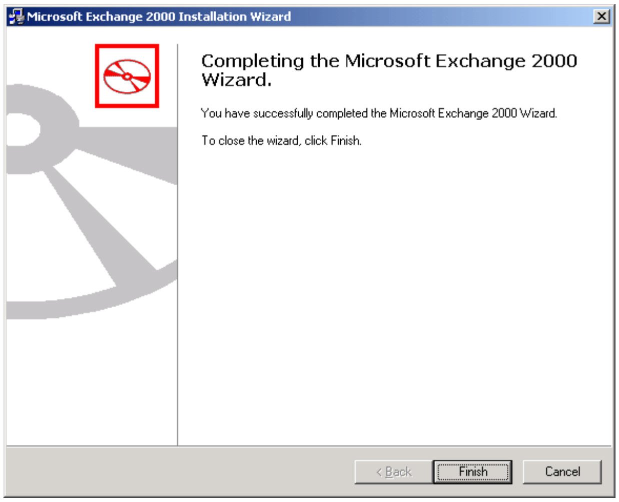
Event

Date: 4/14/2003 Source: DCOM
Time: 12:34 Category: None
Type: Error Event ID: 10005
User: [redacted]\administrator
Computer: [redacted]

Description:
DCOM got error "The service cannot be started, either because it is disabled or because it has no enabled devices associated with it. " attempting to start the service WinMgmt with arguments "" in order to run the server:
{8BC3F05E-D86B-11D0-A075-00C04FB68820}

Data: ● Bytes ○ Words

After manually enabling the MSDTC and WinMgmt services, Exchange SP3 installation completed without errors.



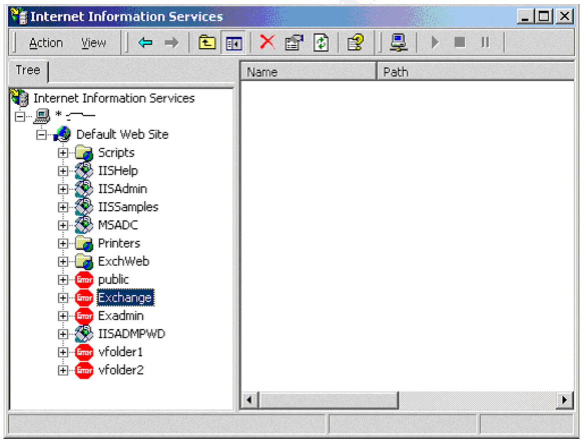
Completing the Microsoft Exchange 2000 Wizard.

You have successfully completed the Microsoft Exchange 2000 Wizard.

To close the wizard, click Finish.

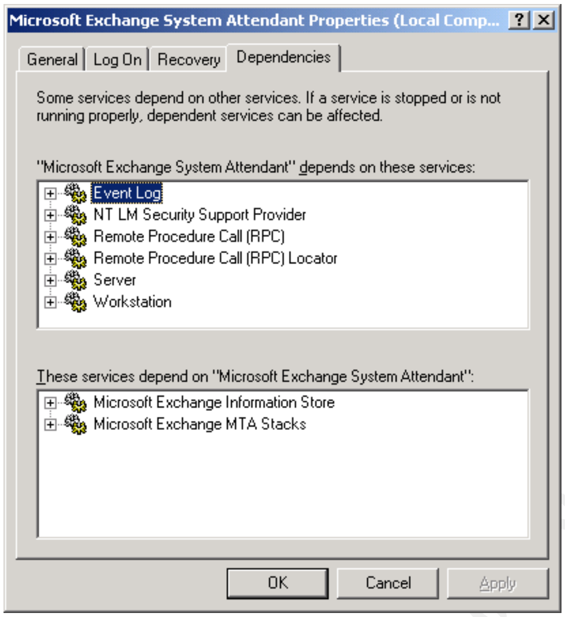
8.2.3 Create new Exchange 2000 virtual folder

We tested creation of a new virtual directory "newinfo" by first creating the virtual directory on an Exchange 2000 backend server, and then on the Exchange 2000 Front-End OWA server. However, after the customary wait time for Exchange 2000 to complete this setup process, the new virtual directory was not accessible via Outlook Web Access. Upon inspection of IIS configuration via IIS Manager, we found that the new virtual folder information was not propagated to the IIS metabase. Note that the virtual folder "newinfo" is not being displayed in IIS manager. (The red errors next to virtual directories on an OWA front-end server are expected, and do not impact OWA functionality)



Most IIS related configurations on an Exchange 2000 server needs to be performed using Exchange System Manager. Once configured, this information is stored in the Active Directory database, and the Metabase Update service is responsible for replicating these changes to the IIS metabase. Metabase Update service is hosted by the Exchange System Attendant service. Since our security templates disabled the "Exchange System Attendant" on our Exchange 2000 Front-End OWA server, the IIS metabase was not updated of the new virtual directory.

To complete the creation of the new virtual directory, we need to temporarily start the "Exchange System Attendant" service. Note that all dependency services of System Attendant also need to be started, including "NT LM Security Support Provider" service.


Microsoft Exchange System Attendant Properties (Local Comp...
General
Log On
Recovery
Dependencies

Some services depend on other services. If a service is stopped or is not running properly, dependent services can be affected.

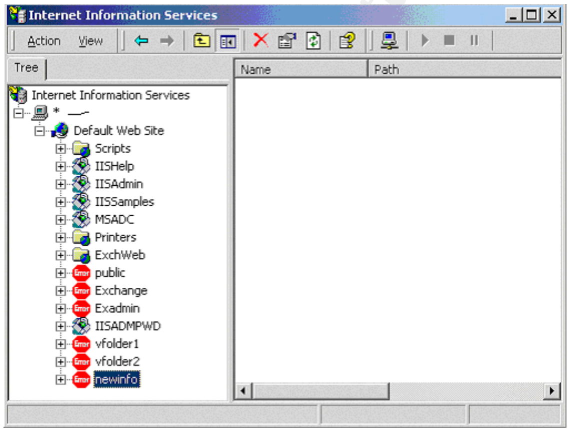
"Microsoft Exchange System Attendant" depends on these services:

- Event Log
- NT LM Security Support Provider
- Remote Procedure Call (RPC)
- Remote Procedure Call (RPC) Locator
- Server
- Workstation

These services depend on "Microsoft Exchange System Attendant":

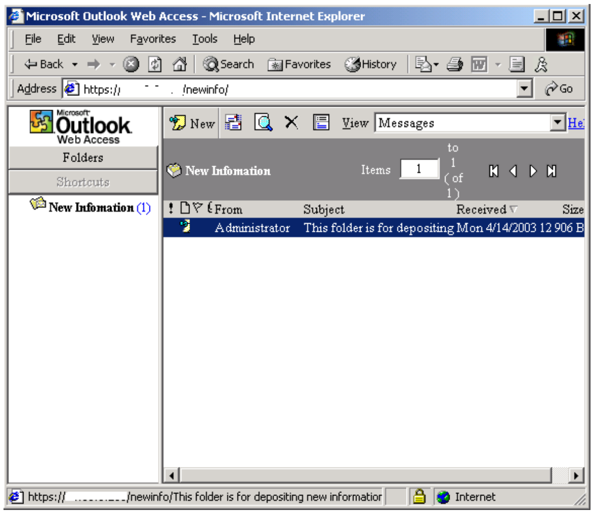
- Microsoft Exchange Information Store
- Microsoft Exchange MTA Stacks

Shortly after the Exchange System Attendant service was started, IIS manager displayed the new virtual directory "newinfo",



```
Internet Information Services
  * 
    Default Web Site
      Scripts
      IISHelp
      IISAdmin
      IISSamples
      MSADC
      Printers
      ExchWeb
      public
      Exchange
      Exadmin
      IISADMPWD
      vfolder1
      vfolder2
      newinfo
```

and Outlook Web Access users were able to access the new virtual directory using https:\\<server.domain.com>\newinfo.



Microsoft Outlook Web Access - Microsoft Internet Explorer

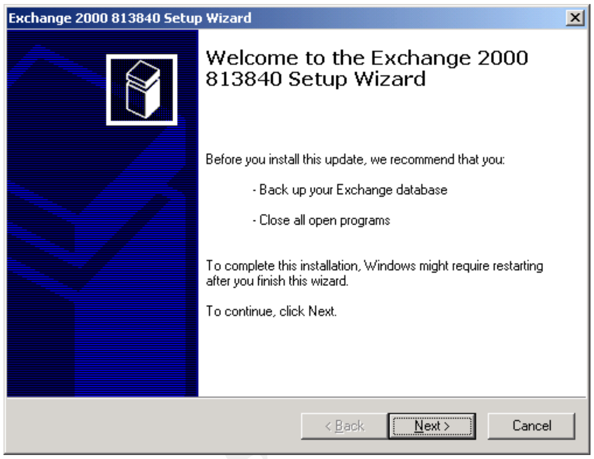
File Edit View Favorites Tools Help
Back Search Favorites History
Address https:// /newinfo/ Go
Microsoft Outlook Web Access
Folders
Shortcuts
New Infomation (1)
New View Messages
New Infomation
Items 1 to 1 (of 1)
! From Subject Received Size

Administrator This folder is for depositing Mon 4/14/2003 12 906 B

https:// /newinfo/This folder is for depositing new informatior Internet

8.2.4 Applying Exchange Post SP3 Rollup Patch 6396.1

The last manual administrative task we will test is installation of an Exchange 2000 patch. Specifically we will install the Post SP3 Rollup patch 6396.1. Installation of this patch was successful.



Exchange 2000 813840 Setup Wizard

Welcome to the Exchange 2000 813840 Setup Wizard

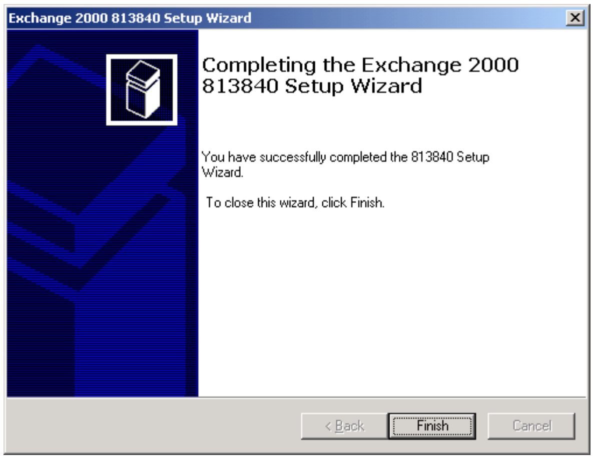
Before you install this update, we recommend that you:

- Back up your Exchange database

- Close all open programs

To complete this installation, Windows might require restarting after you finish this wizard.

To continue, click Next.



Exchange 2000 813840 Setup Wizard

Completing the Exchange 2000 813840 Setup Wizard

You have successfully completed the 813840 Setup Wizard.

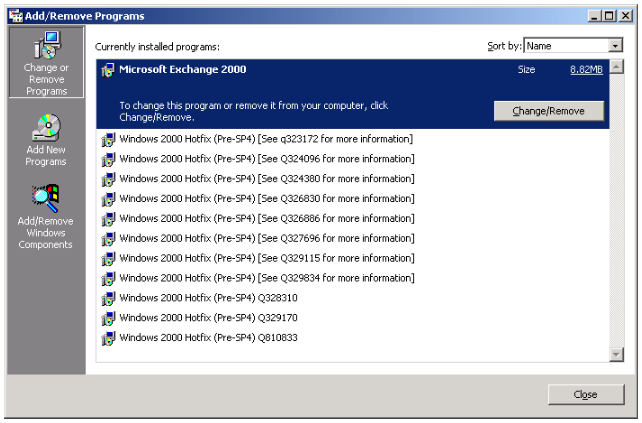
To close this wizard, click Finish.

In summary, the security template application did affect manageability of the target system. However, as management tasks can be performed after temporarily relaxing security measures, and as these tasks do not occur frequently, the reduced manageability is acceptable.

8.3 SUS functionality

To test Windows Update functionality on the target server in an SUS environment, we performed the following:

Note existing patches on the target system



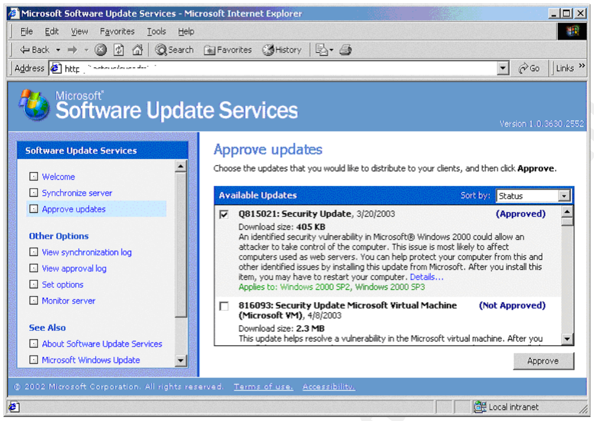
Currently installed programs: Sort by: Name

Microsoft Exchange 2000 Size 8.82MB

To change this program or remove it from your computer, click Change/Remove. Change/Remove

- Windows 2000 Hotfix (Pre-SP4) [See q323172 for more information]
- Windows 2000 Hotfix (Pre-SP4) [See Q324096 for more information]
- Windows 2000 Hotfix (Pre-SP4) [See Q324380 for more information]
- Windows 2000 Hotfix (Pre-SP4) [See Q326830 for more information]
- Windows 2000 Hotfix (Pre-SP4) [See Q326886 for more information]
- Windows 2000 Hotfix (Pre-SP4) [See Q327696 for more information]
- Windows 2000 Hotfix (Pre-SP4) [See Q329115 for more information]
- Windows 2000 Hotfix (Pre-SP4) [See Q329834 for more information]
- Windows 2000 Hotfix (Pre-SP4) Q328310
- Windows 2000 Hotfix (Pre-SP4) Q329170
- Windows 2000 Hotfix (Pre-SP4) Q810833

On the SUS server, approved a hotfix that has not been installed on the target system. Specifically Q815021.



Microsoft Software Update Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address Go Links
Microsoft Software Update Services
Version 1.0.3630.2552
Software Update Services
Welcome
Synchronize server
Approve updates
Other Options
View synchronization log
View approval log
Set options
Monitor server
See Also
About Software Update Services
Microsoft Windows Update
© 2002 Microsoft Corporation. All rights reserved. Terms of use. Accessibility.
Local intranet

Approve updates

Choose the updates that you would like to distribute to your clients, and then click **Approve**.

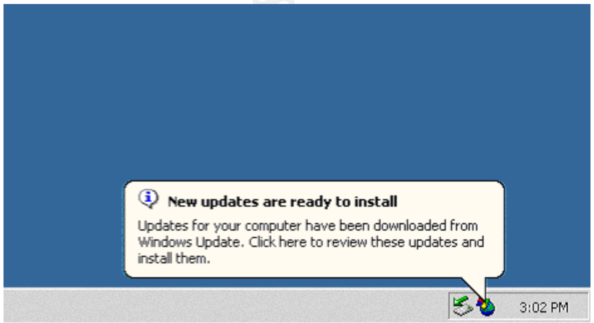
Available Updates Sort by: Status

☑ **Q815021: Security Update**, 3/20/2003 **(Approved)**
Download size: **405 KB**
An identified security vulnerability in Microsoft® Windows 2000 could allow an attacker to take control of the computer. This issue is most likely to affect computers used as web servers. You can help protect your computer from this and other identified issues by installing this update from Microsoft. After you install this item, you may have to restart your computer. Details...
Applies to: Windows 2000 SP2, Windows 2000 SP3

□ **816093: Security Update Microsoft Virtual Machine (Microsoft VM)**, 4/8/2003 **(Not Approved)**
Download size: **2.3 MB**
This update helps resolve a vulnerability in the Microsoft virtual machine. After you

Approve

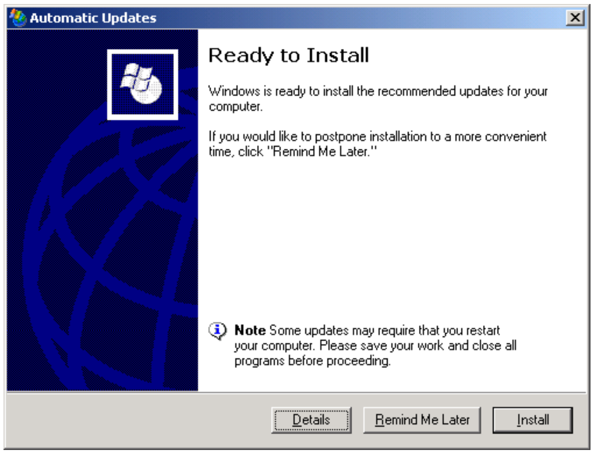
Logged on to the target system as administrator, and waited for Windows Update notification.



New updates are ready to install

Updates for your computer have been downloaded from Windows Update. Click here to review these updates and install them.

Manually ran Automatic Updates



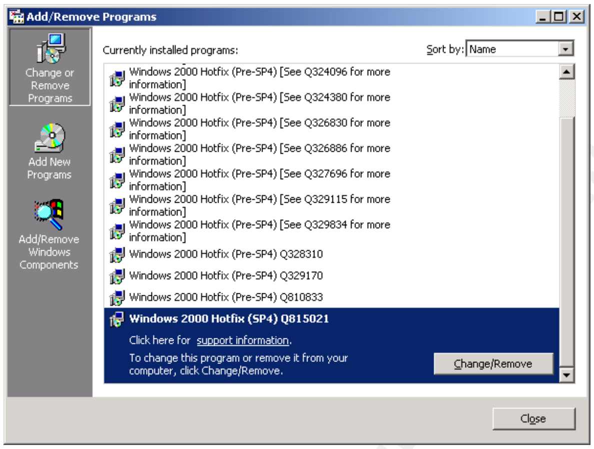
Ready to Install

Windows is ready to install the recommended updates for your computer.

If you would like to postpone installation to a more convenient time, click "Remind Me Later."

Note Some updates may require that you restart your computer. Please save your work and close all programs before proceeding.

Verified that hotfix Q815021 was installed on the target server.



Currently installed programs:

Sort by: Name

Windows 2000 Hotfix (Pre-SP4) [See Q324096 for more information]
Windows 2000 Hotfix (Pre-SP4) [See Q324380 for more information]
Windows 2000 Hotfix (Pre-SP4) [See Q326830 for more information]
Windows 2000 Hotfix (Pre-SP4) [See Q326886 for more information]
Windows 2000 Hotfix (Pre-SP4) [See Q327696 for more information]
Windows 2000 Hotfix (Pre-SP4) [See Q329115 for more information]
Windows 2000 Hotfix (Pre-SP4) [See Q329834 for more information]
Windows 2000 Hotfix (Pre-SP4) Q328310
Windows 2000 Hotfix (Pre-SP4) Q329170
Windows 2000 Hotfix (Pre-SP4) Q810833
Windows 2000 Hotfix (SP4) Q815021

Click here for support information.

To change this program or remove it from your computer, click Change/Remove.

In summary, the template security settings do not impact "Software Update Services" functionally on the target system.

9 Templates Modification

Based on testing of template settings and system functionality above, the two security templates, baseline.inf and "OWA FrontEnd Incremental.inf", did harden our Exchange 2000 FrontEnd OWA server without seriously impacting functionality. The templates' settings did have an adverse impact on manageability of the target system; however, executing certain manual tasks prior to performing the affected management tasks can circumvent the adverse impact. Thus, it is not necessary to relax existing settings in the templates (one exception to this is noted in subsection 9.7 "System Services").

Upon review of all settings available in a security template, we found that some additional modifications can be made to further harden the target system. As settings in the baseline template (baseline.inf) will be applied to other servers in the "Application Servers" OU, and modified settings might not be applicable to other servers, these modifications will be made on the incremental template for Exchange 2000 OWA FrontEnd server (FrontEnd OWA Incremental.inf).

9.1 Account Policies

While Active Directory domain accounts are subjected to the Domain account policies defined in a GPO applied at the domain level, local accounts on a member server are not affected by the domain security settings. Since local accounts can exist and might have rights to local resources, it is important that they be subjected to a set of account policies.

We will configure the account policies settings in "FrontEnd OWA Incremental.inf", including Password Policy and Account Lockout Policy, such that they mirror settings in Account Policies for the domain.

9.2 Audit Policies

Audit Policies defined by the template are sufficient and do not require modification.

9.3 User Rights Assignment

User Rights Assignment policy defined by the template are sufficient and do not require modification.

9.4 Security Options

The following policies can be modified to further tighten security on the target system.

Rename administrator account
Rename guest account
Both the administrator account and the guest account should be renamed from their defaults. This will present one extra obstacle for hackers when they try to comprise the system.

9.5 Event Logs Settings

Event logs settings defined by the template are sufficient and do not require modification.

9.6 Restricted Groups

As member of the local Administrators and Power Users group have extended rights on the local system, we should set up a policy to restrict their memberships.

The local Administrator group should contain only the global group "Domain Admins" and the local administrator account. The "Power Users" group should not contain any members.

9.7 System Services

There are three areas of modification for system services configurations in our security templates. The first is to include in the templates all services that are installed on the target system and are not previously referenced; The second relates to enabling a disabled service for system functionality; The third is to disable additional services that are not required for system functionality.

9.7.1 New Services

The following are services installed on our target system, but have not been referenced by our templates:

Automatic Updates
This service enables download and installation of critical Windows updates. It is a crucial component for system participating in the Microsoft "Software Update Services" (SUS) environment. This service should be configured to start "Automatically".

Background Intelligent Transfer Service
This services transfer file in the background using idle network bandwidth, and is required on system participating in the Microsoft "Software Update Services" (SUS) environment. This service should be configured to start "Manually".

Besides defining the startup type for the above services, we also need to configure their security settings. Similar to security settings on all services defined in the template, these two services should have the following ACLs:

- Administrators: Full Control
- Interactive Users: Read
- System: Full Control
- Audit all failure access: Everyone

9.7.2 Services to be Enabled

The following service is disabled by the template but is actually required on our target system.

License Logging Service
According to Lemson & Martin [Ref: 9], the license logging service needs to be running on an Exchange 2000 Front-end OWA server, as IIS will not accept more than 10 simultaneous SSL connections otherwise. We need to modify the template setting to re-enable this service.

9.7.3 Services to be Disabled

The following are services enabled by the template, but are actually not required on our target server. Description of these services can be found in Section 5.1.8.3 "Services Installed and left Enabled by Template"

DHCP Client
As our Exchange 2000 Front-End OWA server is configured with static IP settings. This service can be disabled.

Distributed Link Tracking Client
Link tracking functionality is not required on an Exchange 2000 Front-End OWA server.

Network Connections
Once network settings are configured, this service can be disabled. If re-configuration of network settings is required, administrator can temporarily enable and start this service.

Remote Registry Service
This service is not required on our target server.

Server Service
This service is not required on our target server during normal operation. It might be required to perform some system maintenance tasks, and can be enabled manually when needed.

9.8 Registry

The biggest deficiency on the selected template configurations for registry settings is on auditing. While most registry key is configured to inherit auditing settings from parent above, auditing is not configured at the root of HKEY_Local_Machine. To allow auditing on registry edits and failure access, we should modify our template to:

Enable audit on all failure access at the root of HKEY_Local_Machine.

Enable audit on successful writes and delete at the root of HKEY_Local_Machine.

9.9 File System

While the NTFS permissions settings in our security templates sufficiently tighten access to the system partition, they do not configure NTFS permissions for other partitions. As our target server contains three separate logical partitions, C:\ for the system partition, D:\ for the application partition, and E:\ for the webroot partition, we should modify the template to properly secure these additional logical drives. The default NTFS permissions on additional logical drive are to grant full control access to Everyone.

Both the application drive D:\ and the webroot drive E:\ should be configured with the following access rights:

Administrators: Full Control
System: Full Control
Users: Read and Execute.

Also, even though the "FrontEnd OWA Incremental.inf" template tightens NTFS permissions on %SystemDrive%\inetpub\nntpfile to only allow full control by Administrators and the local system account; the template then relaxes NTFS permission on the sub directory %SystemDrive%\inetpub\nntpfile\root to allow Everyone full control. This is done to allow for NNTP functionality. As NNTP is not a required functionality on our target server, this relaxation of NTFS permissions is not necessary.

10 Other Security Measures

The two security templates, "Baseline.inf" and "OWA FrontEnd Incremental.inf", discussed in this paper harden an Exchange FrontEnd OWA server significantly by imposing many configuration changes. However, these templates alone are not sufficient in protecting the target server. Some additional security measures are discussed in Microsoft's "Security Operations Guide For Exchange 2000" [Ref: 16] and Microsoft's "Security Operations Guide For Microsoft Windows 2000 Server" [Ref: 17].

To further secure an Exchange 2000 Front-End OWA server, we need to implement the following.

10.1 Tighten "Default Domain Policy" GPO

By default, the "Default Domain Policy" GPO in every Active Directory domain dictates configurations of domain-wide account policy. Tightening security settings in this GPO is necessary to protect member servers in the domain. If domain accounts with administrative rights on a member server have a weak password policy, it can be easily compromised. Once compromised, hackers will be able to use that account to obtain full access on a member server. For further information on tightening the "Default Domain

Policy" GPO and other domain wide settings, refer to Chapter 5 "Securing the Domain Infrastructure" in Microsoft's documentation "Secure Windows 2000 Server".

10.2 Tighten Internet Information Server

As Internet Information Server (IIS) is a crucial component on an Exchange 2000 Front-End OWA server, and its default configuration is notoriously insecure, it is vital that we properly harden this component. Many checklists on tightening IIS exist, including National Security Agency's "Guide to the Secure Configuration and Administrator of Microsoft Internet Information Services 5.0"; Microsoft's "Security Internet Information Services 5 Checklist, and SANS Institute's checklists for securing IIS [Ref: 7].

Microsoft has released the IIS Lockdown wizard with the URLScan tool to help administrators harden an IIS server. The IIS Lockdown wizard removes potentially dangerous and unnecessary functionality of an IIS server; and the URLScan tool configures the IIS server to block potentially dangerous command in an URL request. Information on this tool and download location can be found at Microsoft's webpage "IIS Lockdown Tool". Microsoft's knowledge base article Q325864 "How to: Install and User the IIS Lockdown wizard", and Q326444 "How To: Configure the URLScan Tool", also provides detailed information on installation and configurations. However, as the default configuration of this tool will break some Exchange OWA functionality, it is important to consult Microsoft's knowledge base article Q309677 "Known Issues and Fine Tuning when you use the IIS Lockdown wizard in an Exchange 2000 environment" before running this tool on an Exchange 2000 OWA server.

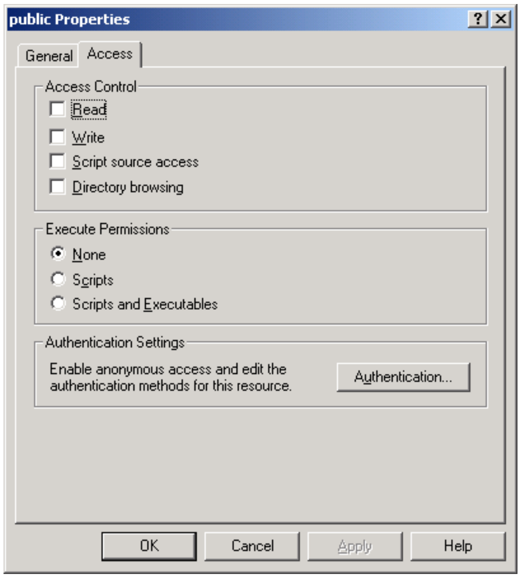
Even though the IIS Lockdown wizard addresses many security concerns of IIS, further tightening of IIS on Exchange 2000 OWA server can be achieved by performing additional tasks listed in SANS Institute's checklists for securing IIS [Ref: 7]. such as:

- Moving the OWA website root directory to a partition that contains no operating system or application files.
- Remove Remote Data Service (RDS) support
- Delete all administrative scripts from the \Inetpub\AdminScritps folder
- Disable NETBIOS, File and Print Sharing, and Client for Microsoft Networks from the Internet facing network adapter card.

10.3 WebDAV Consideration

Web Distributed Access and Development (WebDAV) is an extension of HTTP 1.1 used on an Exchange 2000 OWA server to enhance performance and usability for Outlook Web Access clients. It is a crucial component of OWA and cannot be disabled. However, as WebDAV can potentially allow users to create and modify files on remote IIS server, its presence does pose additional security risks.

As all Exchange related IIS virtual directories on an Exchange FrontEnd OWA server points to data securely located on a backend server, the risk exposed by WebDAV is minimized. Access to Exchange data are secured by ACLs set on mailboxes and public folders, and not by access permissions set on HTTP virtual directory. In fact, examination of a default Exchange HTTP virtual directory shows that no access is granted on the virtual directory level.



Access Control
□ Read
□ Write
□ Script source access
□ Directory browsing

Execute Permissions
● None
○ Scripts
○ Scripts and Executables

Authentication Settings
Enable anonymous access and edit the authentication methods for this resource.

To secure our Exchange 2000 FrontEnd OWA server against possible WebDAV related exploits, we need to ensure that only Exchange HTTP directories exist on the system. If non-Exchange HTTP virtual directory ever needs to be present, we need to ensure that it is properly secured.

10.4 Firewall configuration

To secure our Exchange 2000 FrontEnd OWA server in a DMZ zone, proper firewall configurations is required. The following tables list the required access on the Internet firewall and Intranet firewall. Details information on firewall requirements can be found in Lemson and Martin "Using Microsoft Exchange 2000 Front-End Servers" [Ref: 9].

Internet Firewall: Allow access to Exchange FrontEnd OWA server from:

Source	Service	Protocol/Port
Any	HTTPS	TCP/443

Intranet Firewall: Allow access from Exchange FrontEnd OWA server to:

Destination	Service	Portocol/Port
Backend Exchange Servers	HTTP	TCP/80
Backend Exchange Servers	Link State Algorithm Routing	TCP/691
Active Directory Domain Controllers	LDAP to Directory	TCP/389 UDP/389
Active Directory Domain Controllers	LDAP to Global Catalog	TCP/3268
Active Directory Domain Controllers	Kerberos Authentication	TCP/88 UDP/88
Active Directory Domain Controllers	Remote Procedure Call	TCP/1600 *
Internal Domain Name Servers	DNS Lookup	TCP/53 UDP/53

* Note that RPC traffic with Active Directory domain controllers has been configured to use a specified port (Ex: TCP/1600) per Microsoft Knowledge Base article Q224196 "Restricting Active Directory Replication Traffic to a Specific Port."

10.5 Deploy IP Security

As HTTP traffic between Exchange FrontEnd OWA server and Exchange backend servers cannot be encrypted using SSL, we should consider deploying IP security (IPSec) to secure communication with backend servers. Refer to Microsoft's product documentation for configuration and deployment of IPSec.

10.6 Management Tasks

To ensure that a system stays secure, it is important that the following management tasks are performed regularly:

- Review, test, and deploy service packs, hotfixes and security patches.
- Auditing and intrusion detection.
- Management of event logs, including clearing and backing up of security logs.

Optionally, one can deploy products specifically designed to automate and facilitate these tasks.

As a thorough discussion of all the above tasks is out of the scope of this paper, we have only presented them in brief. Detailed information on configurations and impact of these tasks can be found in the references cited above.

11 Conclusion

For the purpose of securing an Exchange 2000 Front-End Outlook Web Access server using security templates, this paper documents the process of template selection, description, application, testing, evaluation and modification. Additional security measures not configurable via a template file were also discussed.

The templates selected were Microsoft's "Baseline Template for Windows 2000 Application Server (baseline.inf), and Microsoft's "Incremental Template for Exchange 2000 OWA FrontEnd Server (OWA Frontend Incremental.inf)". These templates were selected as they were the only publicly available templates that most closely matched the target system to be secured.

The selected set of templates hardens our target server by tightening audit policies, configuring security options and event logs settings, disabling unnecessary system services, setting permissions on system services, and restricting access to system files and registry keys. Most of the settings imposed by the selected set of templates are thoroughly discussed in this paper.

Upon application and testing of the selected templates, we found that they harden the target system without seriously impacting functionality. All required user functionalities work after template application. While some management tasks failed after template application, these failures can be circumvented by temporarily relaxing some security measures prior to performing the management tasks.

Even though the selected security templates did harden our target server, they were not sufficient to thoroughly secure the system. Having a hardened domain security policy, running the Microsoft IIS Lockdown wizard, deploying IPSec policy, and proper firewall configurations are some of the additional security measures required.

In conclusion, for an Exchange 2000 Front-End OWA server deployed in a properly configured Windows 2000 domain and Exchange 2000 environment, implementing the selected security template settings with the additional security measures should sufficiently secure the target system.

12 References

1. J. Ayala, Windows 2000 Server Services, Part 2: Tools and Tips for management fundamental components of the Windows architecture, Windows & .NET Magazine, November 2001.
2. M. Burnett, Securing Microsoft Services, SecurityFocus, May 2002.
3. T. Dodds, W. Kerby, M. Howard, Data Security and Data Availability for End Systems", Microsoft Solution Frameworks, 2000.
4. B. English, Securing Exchange 2000 Server E-mail, SANS Info Sec Reading Room, March 2002.
5. J. Fossen, "Securing Windows 5.1 Windows 2000/XP: Active Directory", SANS Institute, 2002.
6. J. Fossen, "Securing Windows 5.2 Windows 2000/XP: Group Policy and DNS", SANS Institute, 2002
7. J. Fossen, "Securing Windows 5.5: Securing Internet Information Server", SANS Institute, 2002.
8. J. Haney, Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset, National Security Agency, July 2002.
9. KC Lemson and M. Martin, "Using Microsoft Exchange 2000 Front-End Servers", Microsoft Exchange Server Series, October 2002.
10. J. McBee, OWA 2000 Security and Scalability, Exchange and Outlook Administrator, January 2002.
11. Microsoft Corporation, Glossary of Windows 2000 Services, July 2001.
12. Microsoft Corporation, Microsoft Exchange 2000 Server Resource Kit, Microsoft Press, 2000.
13. Microsoft Corporation, Microsoft Exchange Server Winning the Enterprise with 100 Million Seats Sold, Jan 2002.
14. Microsoft Corporation, Microsoft Outlook Web Access in Microsoft Exchange 2000 Server, Exchange Core Documentation, Exchange User Education, May 2002.
15. Microsoft Corporation, Microsoft Windows 2000 Resource Kit, Microsoft Press, 2000.
16. Microsoft Corporation, Security Operations Guide for Exchange 2000, Microsoft Press, July 2002.
17. Microsoft Corporation, Security Operations Guide for Microsoft Windows 2000 Server, Microsoft Press. February 2003.
18. J. Scambray and S. McClure, "Hacking Exposed Windows 2000: Network Security Secrets & Solutions", Osborne/McGraw-Hill, 2001.

19. Science Applications International Corporation, Windows 2000 Security Configuration Guide Version 1.0, Microsoft Corporation, October 2002.

20. W. Walker, Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0, National Security Agency, March 2002.