Exam Manual

LearnSmart

Microsoft Server 2003 Network Security Admin (70-299)

Microsoft Certified Systems Administrator (MCSA)

This LearnSmart exam manual is designed to steer you towards success when you take the Server 2003 Network Security Admin exam (70-299). By studying this exam manual, you will become familiar with a variety of exam-related content, including:

- Security Policies
- Patch Management Infrastructure
- Security for Network Communications
- Authentication, Authorization and PKI
- And more!

Give yourself the competitive edge necessary to further your career as an IT professional and purchase this exam manual today!

Server 2003 Network Security Admin (70-299) LearnSmart Exam Manual

Product ID: 2183
Production Date: July 18, 2011
Total Questions: 16

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Volume, Corporate, and Educational Sales

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

1-800-418-6789
solutions@learnsmartsystems.com

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Table of Contents

Abstract

This Exam Manual will help you prepare for Microsoft Exam 70-299, Implementing and Administering Security in a Microsoft Windows Server 2003 Network. Exam topics include four domains. The exam assesses your ability to implement, manage, maintain, and troubleshoot security issues in a Windows Server 2003 environment. Topics covered include security policy configuration and management, patch deployment, IPSec deployment, management, and troubleshooting, wireless network security, and Certificate Services deployment, configuration, managing, and troubleshooting.

What to Know

Before you take this exam, you should know first off that it is going to be quite difficult. Expect to spend a great deal of time in rigorous study and familiarizing yourself with advanced security concepts. In particular, you should strive to be intimately familiar with:

- Security templates and policies
- Server security based on server roles
- Patch deployment, management, and troubleshooting
- Internet Protocol Security (IPSec) deployment and troubleshooting
- IPSec policy configuration and management
- Wireless network security
- Secure Sockets Layer (SSL) certificate management
- Remote access security
- Authentication, authorization, and group structure
- Installation, configuration, and management of Certificate Services

This exam is 35 questions in length, and you will have 155 minutes to complete it. It covers questions on implementing, managing, and troubleshooting security on computers running Windows Server 2003.

While preparing for the exam, you should work with the tools and techniques covered on the exam. In particular, you should set up a network of computers running Windows Server 2003 and Windows XP Professional, and install and configure tools such as Microsoft Baseline Security Analyzer (MBSA), security templates, security policies, Internet Protocol Security (IPSec), SSL, remote access security, authentication and authorization, and Certificate Services. You can obtain a 180-day evaluation version of Windows Server 2003 from Microsoft. You can also use virtual computer software, such as Microsoft Virtual PC, to set up multiple virtual computers on a single physical machine. Evaluation versions of virtual computer software are available from several sources, such as Microsoft and VMware.

With over 2 hours reserved for the exam, you will have plenty of time to complete the test. Don't rush it. The exam allows you to mark questions you are unsure of and return to them later. Use this feature. On the first pass, work through the exam and answer all the questions that you are sure of, taking time to mark questions you need to come back to; on the second pass, spend time on the questions you marked that presented more of a challenge. Even if you are unsure of the correct answer, determine the ones you know are incorrect. This will help you narrow your options and give you a better chance at passing the exam.

Implementing, Managing, and Troubleshooting Security Policies

You can configure security policies as part of Group Policy in Windows Server 2003. Microsoft includes the objectives in this section to ensure that security administrators are able to plan, configure, implement, and troubleshoot security policies on servers that perform various roles on the network. For an overview of security policy deployment, see the *Microsoft Windows Server 2003 Deployment Kit*, "Deploying Security Policy" chapter as well as links cited therein.

Another valuable reference for many topics discussed in this exam manual is the excellent *Five Key Lessons to Securing Your Active Directory* e-book by Roberta Bragg. The e-book is a valuable companion to this exam manual for anyone wanting to pass the 70-299 exam.

Planning Security Templates

Windows Server 2003 provides a series of predefined security templates, which you can use as-is or modify according to the security requirements of your network. The following predefined security templates are found by default in the %systemroot%\security\templates folder:

Template	Usage
Compatws.inf	Modifies the default file and registry permissions for the Users group so that members of the Users group can run most applications that have not been certified by the Windows Logo program.
DC security.inf	Created when a server is promoted to a domain controller and provides default security settings for domain controllers.
Hisecdc.inf	Provides a very high level of security to domain controllers. You should note that this template may reduce the functionality of the servers to which it is applied.
Hisecws.inf	Provides a very high level of security to member servers and client computers. You should note that this template may reduce the functionality of the servers or workstations to which it is applied.
Notssid.inf	Removes Terminal Server security identifiers (SIDs) from the file system and registry when Terminal Services is not being run.
Rootsec.inf	Defines the permissions for the root of the system drive (%systemdrive%).
Securedc.inf	Provides enhanced security settings for domain controllers that are less likely to affect system compatibility than those in the highly secure templates.
Securews.inf	Provides enhanced security settings for member servers and client computers that are less likely to affect system compatibility than those in the highly secure templates.
Setup security.inf	Created during installation of a server or client computer, this template provides default security settings that are specific for each computer and vary according to whether the installation was an upgrade or a new installation.

Security Template Components

You can define the following security components by using security templates:

- *Account Policies* – Includes settings that define the length, complexity, and usage of passwords, conditions for account lockouts, and Kerberos policy definitions.
- *Local Policies* – Specifies the types of actions to be audited, user rights that are assigned to various security groups, and a large range of security options that define specific actions, such as access to network shares and devices, logon conditions, and so on.
- *Event Log* – Defines the properties of the Windows system, security, and application logs that are viewed in Event Viewer.
- *Restricted Groups* – Enables you to restrict the membership in default security groups, such as the Administrators group.
- *System Services* – Enables you to specify the startup type of various services on the network.
- *Registry* – Defines permissions applied to various registry keys.
- *File System* – Defines permissions applied to folders and files.

Planning Security Templates According to Computer Role

Servers performing different roles require different security settings. Web servers running Internet Information Services (IIS) or e-mail servers running Microsoft Exchange Server 2000 or 2003 that are exposed to the Internet have different security requirements from internal servers, such as domain controllers or file servers. The following are several suggestions to follow in planning templates:

- Use the File System node to apply permissions to Web-based folders on IIS servers or to folders on SQL servers referenced by Web-based applications accessed from the Internet.
- For additional suggestions on configuring security templates on Web servers, see Securing Your Web Server.
- To ensure that settings applied to Internet-facing servers do not change, use Task Scheduler together with a script to run **secedit /analyze** against the custom security template on a regular basis.
- Microsoft's Windows Server 2003 Security Guide provides sample security templates for domain controllers, file servers, Internet Authentication Service (IAS) servers, IIS servers, infrastructure servers, and several other roles. These templates include legacy client (low security), enterprise client (medium security), and high security levels.

Keep in mind that you can duplicate a default template and use the duplicate to configure the appropriate settings for servers playing a defined role. We discuss configuring security templates next.

Configuring Security Templates

- To configure security templates, create a Microsoft Management Console (MMC) snap-in. Click **Start** > **Run**, type **mmc**, and then press **Enter**. From the **File** menu, select **Add/Remove Snap-in**. Click **Add**, select **Security Templates**, click **Add**, and then click **Close**. Click **OK**.
- As shown in *Figure 1*, the console you created enables you to create new templates and modify existing ones to meet the security needs of your network.

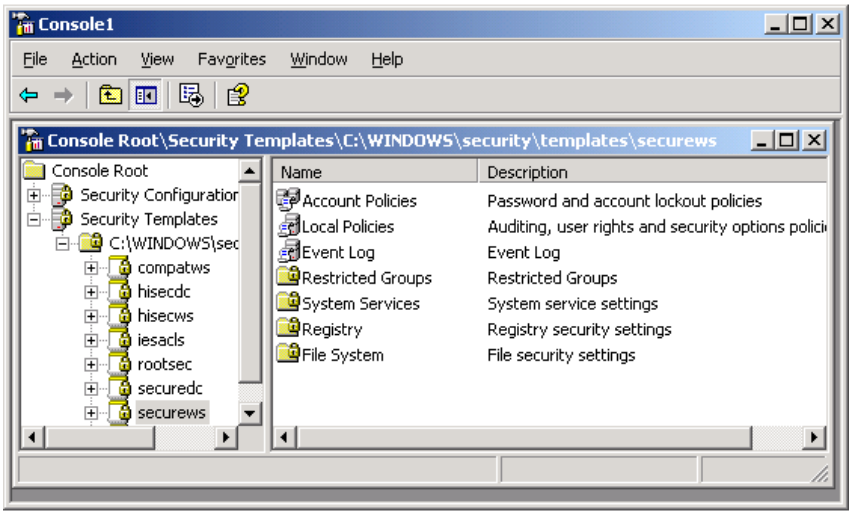


Figure 1 – You Can Configure Security Templates from the Security Templates Snap-in

- Because security templates are text-based files, you can edit them using Notepad if you desire. However, this method is not recommended.
- You should create a duplicate template before editing it because this enables you to return to the original template should problems arise later. Right-click the desired template in the console tree and select **Save As**. Type a name for the duplicate template and click **Save**.
- Do not edit the Setup Security.inf template because this action removes the option of reapplying default security settings.

We have outlined the components of security templates that are available for configuration. Now we take a look at these components and the most common settings that you can configure.

Registry and File System Permissions

The Registry and File System nodes enable you to configure access permissions on discretionary access control lists (DACLs) and audit settings on system access control lists (SACLs) for registry keys, and for files and folders, respectively. Refer to Using Security Templates in the Microsoft Windows XP Professional Resource Kit Documentation for more information.

To configure registry permissions, right-click **Registry** and select **Add Key**. Browse to the registry key for which you want to set permissions and click **OK**. You can configure the appropriate permissions from the Database Security dialog box that opens. To configure file system permissions, right-click **File System** and select **Add File**. Browse to the folder for which you want to set permissions and click **OK**. In either case, the Add Object dialog box presents you with the following options:

- *Propagate Inheritable Permissions to all Subfolders and Files* – Inherited permissions on child objects are adjusted according to permissions you have defined here. Explicit access control entries (ACEs) on child objects are not modified.
- *Replace Existing Permissions on all Subfolders and Files with Inheritable Permissions* – Overrides explicitly defined ACEs on child objects.
- *Do Not Allow Permissions on this File or Folder to be Replaced* – Prevents permissions being set for a folder or key from being inherited by lower objects.

Account Policies

From this location you can specify password policies, account lockout policies, and Kerberos policies for domain computers. Keep in mind that a Group Policy object (GPO) containing account policies must be applied at the domain level for the policies to be effective. However, account policies can be specified at the organizational unit (OU) level for use with a machine local user account only.

The following password policies are available (recommended settings achieve adequate security in most situations; some cases may require different settings):

- *Enforce password history* – Prevents users from reusing passwords until the specified number of passwords has been used. It is recommended that you set this to at least 24.
- *Maximum password age* – Defines the maximum number of days after which a user must change his/her password. It is recommended that you set this to 30 to 60 days.
- *Minimum password age* – Defines the minimum number of days before a user can change a new password. It is recommended that you set this to a nonzero number so that a user cannot cycle through a series of passwords.
- *Minimum password length* – Defines the minimum number of characters in an acceptable password. It is recommended that you set this to at least 8.
- *Password must meet complexity requirements* – Requires that a password contain at least three of the four character types: uppercase letters, lowercase letters, numerals, and special characters. It is recommended that you enable this setting.
- *Store passwords using reversible encryption* – Provides reduced security because passwords are stored in a form that is essentially plain text. It is recommended that you disable this setting.

Account lockout policies specify the criteria for locking a user out after entering a number of incorrect passwords. The following account lockout policies are available:

- *Account lockout duration* – Specifies the number of minutes before a locked out account is unlocked. It is recommended that you set to 0 to specify an unlimited duration (an administrator must unlock the account).
- *Account lockout threshold* – Specifies the number of incorrect passwords that can be entered before the account is locked out. It is recommended that you set to a small number, such as 5.
- *Reset account lockout counter after* – Specifies the number of minutes after which the account lockout counter is reset to 0. It is recommended that you set to at least 30 minutes.

Kerberos policy settings govern authentication requirements, such as ticket lifetimes and computer clock synchronization tolerance. In most cases, you should not need to modify these from their defaults. In particular, you should not increase the clock synchronization tolerance because this action could invite replay attacks.

Policy (*.pol) Files

Policy files are files with the .pol extension that are used to specify system policy on pre-Windows 2000 computers. You need to use System Policy Editor to create the **Ntconfig.pol** file for use with Windows NT 4.0 computers and the **Config.pol** file for use with Windows 9x computers.

Audit Policies

Found under Local Policies, audit policies define the types of events that will be audited and logged into a computer's security log, which you can view from Event Viewer. You can configure auditing of successful or failed attempts at performing the following actions:

- *Account logon events* – Attempts at logging onto a computer using a domain user account.
- *Account management* – Creation, modification, or deletion of user or group accounts, or changes in account properties, including passwords.
- *Directory service access* – Access of an Active Directory object that contains its own SACL.
- *Logon events* – Attempts at logging onto a computer using a local user account.
- *Object access* – Access of a file, folder, or printer that is configured for auditing.
- *Policy change* – Changes to user rights assignment, audit policies, or trust policies.
- *Privilege use* – A user exercising a user right.
- *Process tracking* – Actions taken by an application, such as program activation, process exit, handle duplication, or indirect object access.
- *System events* – Users shutting down or restarting a computer, or events that affect a computer's system or security log.

User Rights Assignment

Found under Local Policies, user rights define a series of actions that a user can take on a computer system. They include logon rights, which govern how a user can log on (for example, locally, across the network, or through Terminal Services), and privileges, which govern the system tasks a user is able to perform (for example, backing up files and directories, adding workstations to a domain, or changing the system time). Policies defined in this subnode allow you to define which users or groups are permitted to perform these actions. For more information, check out User Rights Assignment in Microsoft TechNet.

Security Options

Also found under Local Policies, security options define a series of policy options that can be used to enhance security throughout your enterprise. Policies include options that govern access to devices, such as floppy drives and CD-ROM drives, digital encryption or signing of data, driver installation behavior, and so on. *Figure 2* shows a subset of the options available from this node. For descriptions of the available options, refer to Security Options.

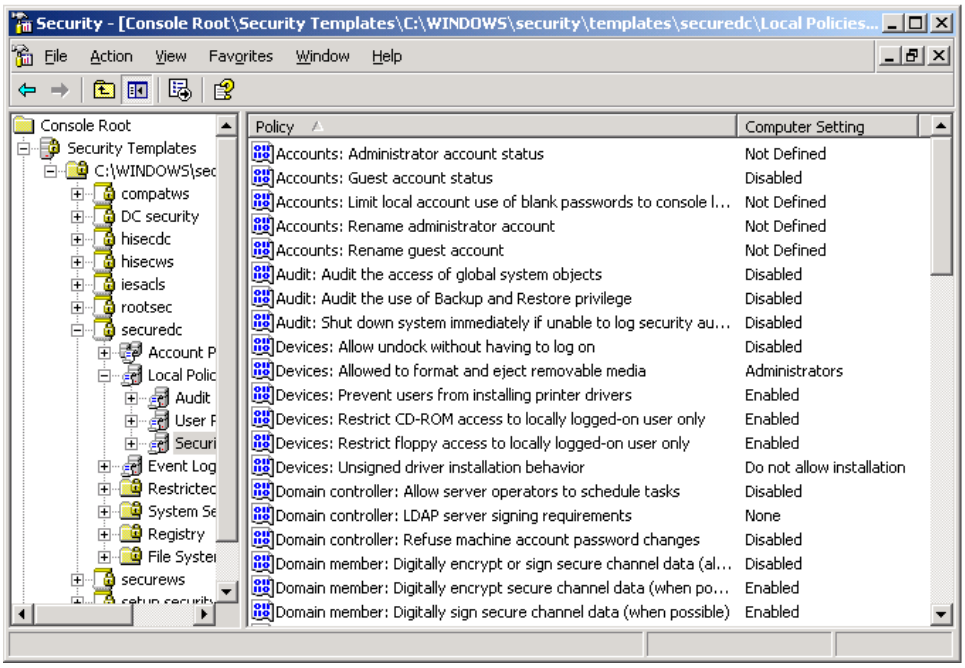


Figure 2 - The Security Options Subnode Provides a Large Number of Security Settings

System Services

The System Services subnode enables you to define which system services will start and their access permissions. You can configure each service with one of the following startup modes:

- *Automatic* – Service automatically starts when the computer is started.
- *Manual* – Service does not automatically start but can be started manually.
- *Disabled* – Service cannot be started.

Restricted Groups

The Restricted Groups subnode enables you to control the membership of security groups defined on the local computer (local groups) or in the domain (universal, global, or domain local groups). You can define the following group properties:

- *Members* – Defines who belongs or does not belong to the restricted group.
- *Member of* – Specifies which other groups to which the restricted group belongs.

For more information on restricted groups, refer to Restricted Groups.

Event Logs

The Event Logs subnode enables you to control attributes of the logs displayed by the Event Viewer application: the system, security, and application logs. For each of these logs, you can define the following properties:

- *Maximum log size* – The maximum size of the log, in 64KB increments.
- *Prevent local guest group from accessing* – Determines if guests are prevented from accessing the log. This setting is valid only for Windows 2000 and Windows XP computers.
- *Retain* – Specifies the number of days information contained in the log will be retained.
- *Retention method* – Enables you to define a retention method for each log, as one of: **Overwrite events by days**, **Overwrite events as needed**, or **Do not overwrite events (clear log manually)**. If you must retain all events, select the **Do not overwrite events** option. You should then archive events and clear the log manually on a periodic basis, or else new events will not be recorded.

For more information on event log policies, refer to Settings for Event Logs.

Deploying Security Templates

Microsoft provides the Security Configuration and Analysis snap-in and the Secedit command-line tool for comparing local computer security settings against security templates and applying template settings to the local computer. You can also use Group Policy to apply template settings to all computers in a site, domain, or OU. For general design recommendations in security template deployment, refer to Design Recommendations for Using Predefined Security Templates.

Using Security Configuration and Analysis

To use Security Configuration and Analysis, you need to add this snap-in to a blank console, as described for security templates. It is a good practice to add both of these templates to the same console, as previously shown in *Figure 1*. Then proceed as follows:

1. Create a database containing the template settings to be used. Right-click **Security Configuration and Analysis** and select **Open Database**. Type a name for the new database and click **Open**. From the Import Template dialog box, select the required security template and then click **Open**.
2. To compare your computer's security settings to those contained in the template you have specified, right-click **Security Configuration and Analysis** and select **Analyze Computer Now**. Click **OK** to accept the log file path provided or browse to another location if desired.
3. To view the results of your analysis, expand the Security Configuration and Analysis node in the console tree and select the desired subnode. The results of the analysis will appear in the details pane.
    - Security settings that differ from those defined in the template are displayed with a red "X" icon and the database and computer settings are displayed.
    - Security settings that agree with those defined in the template are displayed with a green check mark icon.
    - A question mark icon appears if the entry is not found in the database and was not analyzed.
    - An exclamation point icon appears if the entry is found in the database but not on the local computer.
    - No icon appears in cases where the database setting was not defined or not analyzed.
4. To apply the template security settings to the computer, right-click **Security Configuration and Analysis** and select **Configure Computer Now**. Specify or browse to the location of an error log file, and then click **OK**. A Configuring Computer Security dialog box tracks the progress of configuration. When this process is completed, repeat the analysis to view its results.

Using the Secedit Command

You can use the **secedit** command to analyze and configure system security from the command line. By using this command, you can script the application of security settings or schedule this task to be run at predetermined times with the Task Scheduler. The basic syntax is as follows:

secedit {/analyze | /configure} /db *filename*.sdb [/cfg *filename*] [/overwrite] [/log *filename*] [/quiet]

Where:

- **/analyze** performs an analysis of existing settings and **/configure** configures security settings against the specified database.
- **/db** specifies the name of the database to be used.
- **/cfg** specifies a security template to be imported into the database.
- **/overwrite** empties the database prior to importing a new security template.

- **/quiet** specifies that the analysis or configuration occurs without displaying additional comments.

Secedit also performs several additional tasks. For further information, consult Secedit.

Using Group Policy to Deploy Security Templates

Group Policy enables you to apply consistent security settings across all computers in a site, domain, or OU. To apply settings contained in a security template to Group Policy, open the Group Policy Object Editor focused on a GPO linked to the desired Active Directory container. Expand the **Computer Configuration\Windows Settings** node, right-click **Security Settings**, and select **Import Policy**. From the **Import Policy From** dialog box (*Figure 3*), select the appropriate security template and click **Open**. If you need to clear the database of any previously imported templates, select the **Clear this database before importing** check box. You may need to do this if the database contained settings imported previously from a different template.

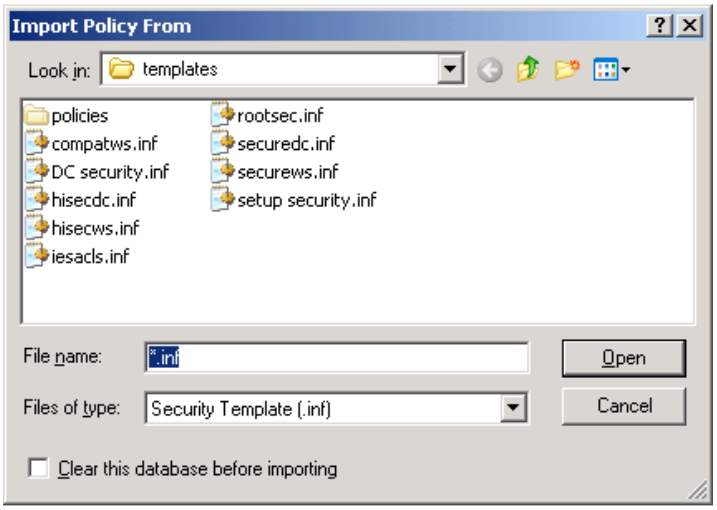


Figure 3 – Apply Settings in a Security Template to a GPO by Using the Import Policy From Dialog Box

For more information on using Group Policy to deploy security templates, check out How To Apply Group Policy and Security Templates with Windows Server 2003. For information on using the Group Policy Management Console (GPMC) for deploying security templates, refer to How Group Policy Management Console Works.

Troubleshooting Security Template Problems

Security Configuration and Analysis and Secedit

The log files created by Secedit and by Security Configuration and Analysis provide information that is useful should problems arise when using these tools. You may also encounter one of the following errors when using these tools:

- *Access is denied. Import failed* – You are using a non-administrative account. Use the RunAs command or log on with an administrative account.
- *Error 1208: An extended error has occurred* – You are attempting to open a read-only database. Change the permissions on the database in use or create a new database.

Group Policy

Errors encountered in applying security templates by means of Group Policy can be varied and difficult to troubleshoot. You should check the Event Viewer logs because errors are frequently logged in the system, application, or File Replication service (FRS) logs when policies fail to apply as expected.

You may encounter errors with event IDs 1000 or 1001 that repeat at 5- to 7-minute intervals (*Figure 4*). These errors indicate missing or incorrect information in the %systemroot%\sysvol\domain\Policies Group Policy structure. Replication may also be failing. You should check the status of Group Policy and FRS replication using **Replmon** or **Repadmin**, and force replication if necessary. You may need to restore this directory structure from backup.

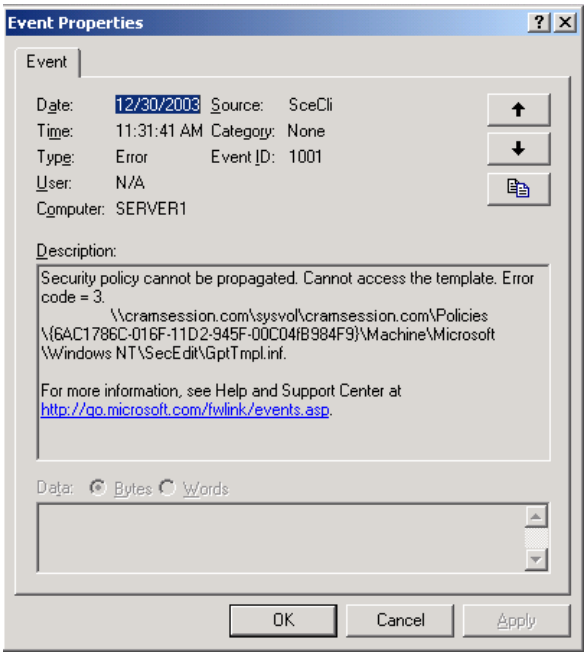


Figure 4 – Problems Accessing Group Policy Templates Result in Event ID 1000 or 1001 Errors

Errors with event IDs 1030 and 1058 that repeat approximately every 6 minutes indicate that one or more subfolders in SYSVOL may be missing or corrupted. You may need to restore SYSVOL from backup or obtain this folder from another domain controller. You may need to reset user rights in the default domain GPO.

Errors with event IDs 1000, 1202, 412, and 454 received on a member or stand-alone server may indicate a corrupted local Group Policy database.

Troubleshooting Security Templates in a Mixed Operating System Environment

Windows 2000

When you apply security templates in an environment containing computers running operating systems older than Windows XP or Windows Server 2003, various problems can occur. In Windows 2000 environments, problems are generally minor, but you may encounter one of the following issues:

- Importing a Windows 2000-based security template to a Windows Server 2003 domain controller (or vice versa) may cause unpredictable results. Always use the correct version of the security templates.
- If you are using the Hisecws.inf or Securews.inf security templates on client computers, communication failures with Windows NT 4.0 or Windows 2000 servers may occur if the clocks differ by more than 30 minutes.

Windows NT 4.0

In environments containing computers running Windows NT 4.0, several issues may occur. Most importantly, communication problems can occur when the Hisec*.inf security templates are in use:

- Domain controllers running Windows NT 4.0 cannot authenticate user logons unless they run Service Pack 4 or higher.
- Client computers are unable to communicate with computers running Windows NT 4.0 unless they run Service Pack 4 or higher or with Windows 98 computers. They cannot communicate with computers running only LAN Manager if they are configured with either the Hisec*.inf or Secure*.inf security templates because these templates configure the LAN Manager authentication level policy to refuse LM authentication.
- When Hisecdc.inf is applied to domain controllers, no domain controllers in any trusted or trusting domain can run operating systems older than Windows 2000.

Refer to Selecting Predefined Security Templates for additional information on communication problems that may occur when computers running older operating systems are present.

You should also remember that Group Policy cannot be used to apply security templates to computers running Windows NT 4.0 or Windows 9x. You should use scripts with command-line tools, such as Secedit.exe, to apply security templates to these computers.

Troubleshooting Security Policy Inheritance

When you use Group Policy to apply security templates, you can apply the templates to the local GPO, or to a GPO linked to any of several Active Directory containers. Remember that Group Policy settings are applied in the sequence local, site, domain, OU, and child OU, and that settings applied later in this sequence overwrite those applied earlier. In addition, you can use Block Policy inheritance and No Override to modify the sequence of GPO application. However, Microsoft recommends that you use these options sparingly because they can cause policy inheritance problems that can be difficult to troubleshoot. For more information, see Policy inheritance.

Troubleshooting the application of security templates in a complex Active Directory structure can be a challenging task. New to Windows Server 2003 is Resultant Set of Policy (RSoP), which queries Windows XP Professional and Windows Server 2003 computers for the sequence in which policies have been applied. You can use RSoP in either of the following modes:

- *Planning mode* – Performs a "what if" analysis of the effects of proposed policy changes on a specified computer/user combination.
- *Logging mode* – Obtains information on the sequence of existing GPO application for a specified computer/user combination. This mode is most useful in troubleshooting the application of security policies.

You can perform a logging mode query by using any of the following three methods:

- Click **Start** > **Run**, type **rsop.msc**, and press **Enter**. This performs a logging mode query on the current user/computer combination.
- Create a custom console containing the RSoP snap-in. From this console, you can start the Resultant Set of Policy Wizard and enter the required parameters.
- From Active Directory Users and Computers, right-click the required user and select **All Tasks** > **Resultant Set of Policy (Logging)**. The Resultant Set of Policy Wizard starts and asks for the required user.

You can run the Resultant Set of Policy Wizard from the RSoP console as follows:

1. In the console tree, right-click **Resultant Set of Policy** and select **Generate RSoP Data**. Then click **Next**.
2. Select the appropriate mode. When troubleshooting security policy application, this will be logging mode.
3. Select the computer and user for which you want to display policy results, and click **Next** after each selection.
4. Click **Finish** when the completion page appears. The RSoP console reappears with the analysis information displayed.
5. To view the results, expand the listings in the console tree. For example, to display computer security settings, expand **Computer Configuration\Windows Settings\Security Settings**, and select the appropriate branch.
6. To view policy precedence, right-click the required policy and select **Properties**, and then select the **Precedence** tab.
7. Is shown in *Figure 5*, this tab displays the names of the GPOs applied and their settings. The policy that appears at the top of the list is the one whose settings prevail over those displayed lower in the list.

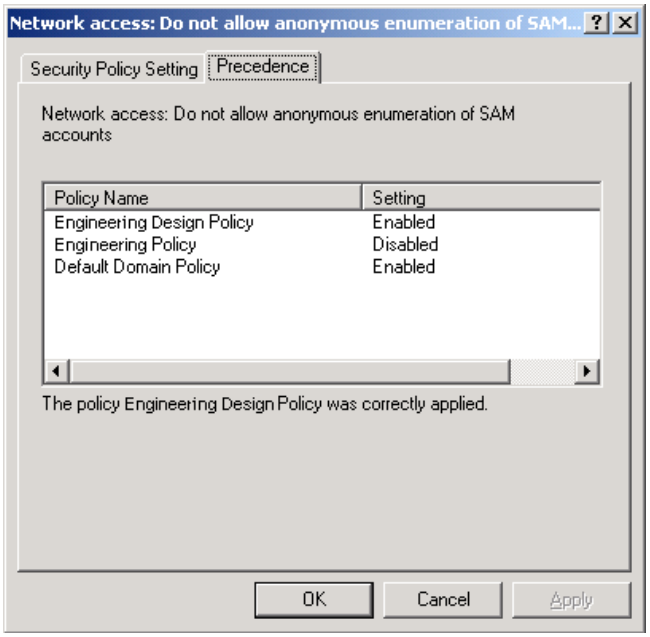


Figure 5 – Displaying the List of GPOs Configured for a Specified Policy

8. To display the list of all GPOs that have applied, right-click either **Computer Configuration** or **User Configuration** and select **Properties**. The resulting dialog box provides the following information:
    - *General tab* – Provides the list of GPOs applied.
    - Error Information tab – Provides information on any GPO components that failed to apply properly (*Figure 6*). You can use this information to troubleshoot policy application problems.

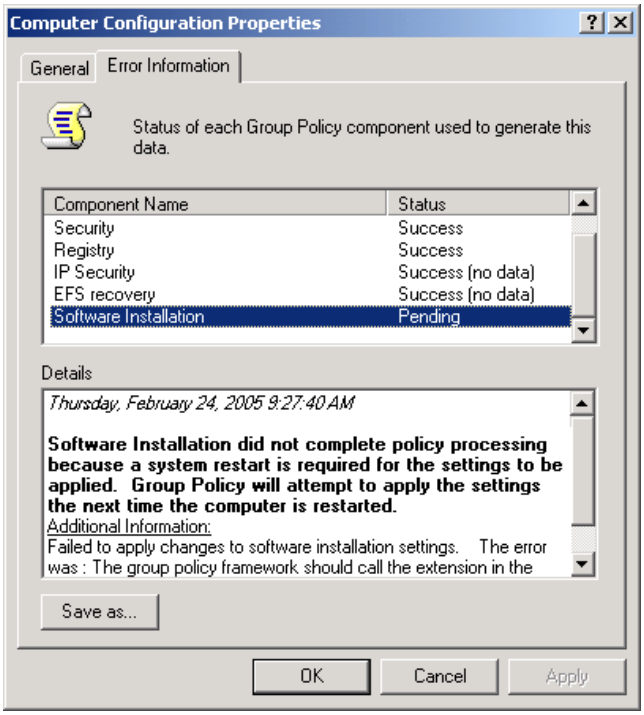


Figure 6 – The Error Information Tab Offers Information about GPO Processing Problems

You can also use the **gpresult** command to obtain RSoP logging mode information from the command line. This command is useful for scripting GPO troubleshooting. However, it does not provide policy precedence data.

Troubleshooting Removal of Security Template Settings

Group Policy is replicated along with other components of Active Directory. By default, Active Directory is replicated between domain controllers within the same site at 5-minute intervals. Replication to other sites occurs at 180-minute intervals unless otherwise configured. You may need to use **Replmon** or **Repadmin** to force Active Directory replication sooner.

If settings have not been removed, you may need to force Group Policy reapplication. To do so, type **gpupdate /force** at the command prompt.

If settings do not appear to be removed at a client computer that is subject to the GPO, have the user log off and log back on. This reapplies all Group Policy settings, and should correct the problem.

Configuring Additional Security Based on Computer Roles

Server security requirements depend upon the role(s) played by each server in the enterprise. We have briefly mentioned the use of customized templates for securing servers according to computer roles. The Windows Server Security Guide includes recommendations for hardening servers according to server role, and provides chapters for member servers, domain controllers, infrastructure servers, file servers, print servers, IIS servers, IAS servers, certificate services servers, and bastion hosts.

- *SQL Server 2000* – You should use Windows Authentication mode and assign a strong password to the system administrator (sa) account. You should limit the privilege level of SQL Server services, and ensure that ports to the SQL server are not open at the firewall. In addition, you should audit connections to the SQL server.
- *Exchange server* – The Exchange Server 2003 Security Hardening Guide provides security tips and customized security templates to assist you in securing servers running Exchange Server 2003. This companion to the Windows Server Security Guide provides tips on specific situations, such as protecting against spam, denial of service (DoS) attacks, address spoofing, and virus attacks, as well as organizing the structure of Active Directory in support of security templates used by Exchange Server. It includes a series of security templates that you can deploy by means of Group Policy.
- *Domain controller* – You should configure security measures directed at domain controllers by using the Default Domain Controllers policy GPO, which is linked to the Domain Controllers OU by default. Consult the Windows Server Security Guide for recommendations and security templates designed to protect domain controllers in each of three security environments. This guide includes recommendations concerning audit policy, user rights assignments, event log settings, and services that should be configured for automatic startup, and Domain Name System (DNS) recommendations.
- *IAS server* – This server acts as a Remote Access Dial-In User Service (RADIUS) server for authenticating users connecting to Routing and Remote Access (RRAS) servers. You should ensure that the IAS service is enabled and that service accounts are not configured to run under the security context of a domain account. You should also rename the Administrator account and ensure that the Guest account remains disabled. Links accessed from Securing IAS provide additional tips.
- *IIS server* – Unlike previous versions of IIS, IIS 6.0 on Windows Server 2003 is installed in a locked-down state in which most features, such as Active Server Pages, Server Side Includes, WebDAV publishing, and Front Page Server Extensions, are not enabled. You should enable only those features that are required by your particular installation. You should also ensure that well-known accounts and service accounts (particularly the IUSR_*servername* account used for anonymous access) are properly secured, and that appropriate permissions are specified for all Web content.
- *Desktop client computers* – You should configure security levels according to the type of use, such as Internet or e-mail access. In particular, watch out for user-supplied communication methods, such as wireless access points and modems. Microsoft Baseline Security Analyzer (covered later in this exam manual) may be of use here.
- *Portable client computers* – Additional security methods beyond those used for desktop computers are dictated by the possibility of theft and wireless remote network access. Use the Encrypting File System (EFS) to secure sensitive files and folders and consider the use of a specialized security template for these computers.
- *Kiosks* – Because these computers provide public access to anyone, you should lock them down as tightly as possible. Use Group Policy loopback processing to ensure that computer-based settings override user-based settings. Configure them with a user account that has only the bare minimum of privileges and permissions assigned to it.

Planning Network Zones for Computer Roles

Internet Explorer provides the following four network zones, which are assigned to one of four default Internet security levels:

- *Restricted Sites* – Designed for sites that may provide questionable content, this zone is assigned the High security level.
- *Internet* – The default zone for sites that are not assigned to other zones, this zone is assigned the Medium security level.
- *Local Intranet* – Designed for sites located on the local intranet, this zone is assigned the Medium-low security level.
- *Trusted Sites* – Designed for sites that can be trusted to never cause harm, this zone is assigned the Low security level.

Microsoft provides the Internet Explorer Enhanced Security Configuration, which raises the security level of the Trusted Sites zone to the Medium security level and that of the Internet zone to the High security level. It also modifies several security settings found on the Advanced tab of the Internet Properties dialog box. You can add the Internet Explorer Enhanced Security Configuration from the Add/Remove Windows Components application of the Control Panel Add or Remove Programs applet in Windows Server 2003.

You can apply enhanced security zone configuration using Group Policy by navigating to the **User Configuration\Windows Settings\Internet Explorer Maintenance\Security** node. Right-click **Security Zones and Content Ratings** and select **Properties**. This displays the dialog box shown in *Figure 7*, from which you can specify the Internet Explorer enhanced security configuration by selecting the **Import the current security zones and privacy settings** option. Click **Modify Settings** to customize the settings provided, if necessary. Doing so opens the Internet Properties dialog box, from which you can modify settings on the Security or Privacy tabs as required for your network. You can also modify content ratings of sites permitted for display by selecting the **Import the current content ratings settings** option. For more information, see Security and Privacy Settings.

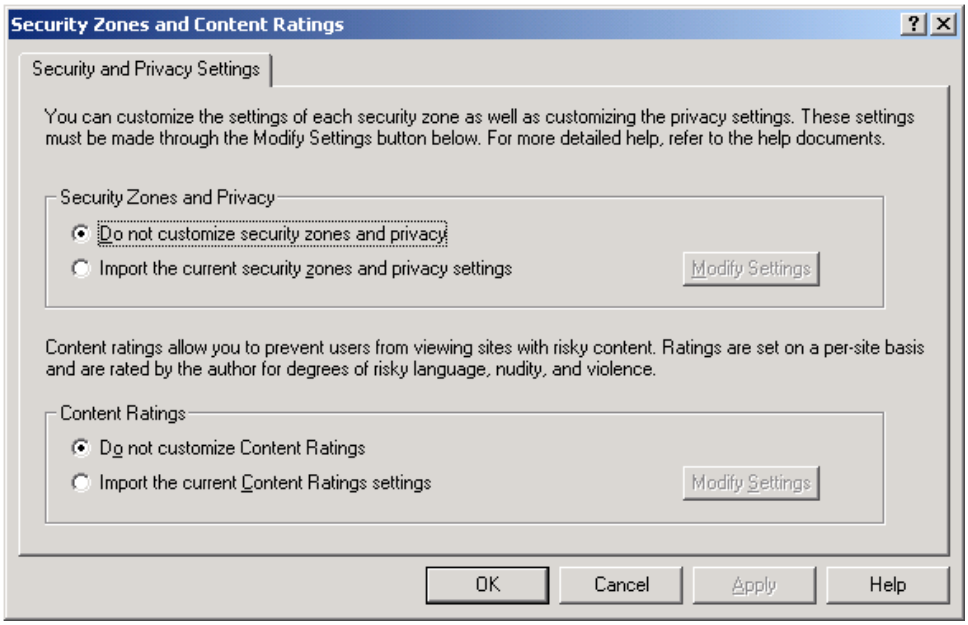


Figure 7 – The Security Zones and Content Ratings Dialog Box Enables You to Configure Group Policy for Security Zones and Content Ratings

Planning and Configuring Software Restriction Policies

Software restriction policies enable you to specify the types of software that are allowed to run on your network. By doing so, you can allow only those applications that are required by users in the performance of their jobs, and restrict other programs, such as games. This is helpful in preventing programs from sources, such as e-mail attachments, from running.

You can configure software restriction policies from the Windows Settings\Software Restriction Policies node of either the Computer Configuration or User Configuration branch of the Group Policy Object Editor. Either location enables you to specify any of the following policy rules:

- *Certificate rule* – Identifies software according to signing certificate, which can be used to specify the source of trusted software.
- *Hash rule* – Uses a hashing algorithm to compare the hash of a specified program to that of a program that a user attempts to run, to determine whether the application or file should run.
- *Internet zone rule* – Available only for Windows Installer packages, this specifies the Internet Explorer zone of programs that can be executed.
- *Path rule* – Identifies allowable software according to its local or Uniform Naming Convention (UNC) file path.

For each of these rules, you can configure programs to be Unrestricted (allowed to run) or Disallowed (forbidden).

Planning Security for Infrastructure Services

Infrastructure services include DNS, the Dynamic Host Configuration Protocol (DHCP), and Windows Internet Name Service (WINS). The Windows Server 2003 Security Guide includes recommendations for securing these services. You should use Group Policy to apply security settings and Internet Protocol Security (IPSec) filters designed to control network traffic to and from these servers. We discuss IPSec later in this exam manual.

The following are several best practices that you should observe:

- Make sure that you have configured auditing and logging. We discuss these in the next section. On the DHCP server, you should access the **DHCP** snap-in, right-click the **DHCP** server in the console tree, and select **Properties**. Then select **Enable DHCP audit logging** from the **General** tab of the server's **Properties** dialog box. By default, the DNS server logs its events to the DNS server log, which you can view from Event Viewer or the DNS snap-in. Finally, make a habit of reviewing the logs regularly.
- Make sure that the DHCP and WINS services are running and that the DHCP servers are authorized in Active Directory. They cannot service clients unless you have performed these tasks.
- Protect the DHCP servers from DoS attacks. An attacker could request all available IP addresses and prevent the server from serving legitimate clients. Also follow the recommended 80/20 rule for splitting DHCP scopes between two servers.
- As with other server roles, you should rename the Administrator account and assign it a complex password. You should also ensure that the Guest account remains disabled.
- Configure DNS servers with Active Directory-integrated zones and ensure that the servers are configured to allow only secure dynamic updates. Limit zone transfers on internal DNS servers to other internal DNS servers only.
- Ensure that the DNS cache is secured against cache pollution. See Chapter 6 of Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I for additional recommendations on securing DNS servers.

Planning and Configuring Auditing and Logging

Log files and audit traces are important components of server security baselines. They serve to identify abnormal behavior that may indicate intrusion attempts on your network. We have already discussed audit policies, which you can implement by means of Group Policy. Keep in mind that different computer roles may require different levels of auditing.

Windows Events

Windows Server 2003 records various Windows events in the event logs that you can view from Event Viewer. These include the system, security, and application logs on all servers, plus additional logs (DNS server, directory service, and File Replication service) that appear on domain controllers and other servers configured with the appropriate roles. You should make a habit of checking the event logs on a regular basis, and set up a scheme for archiving logs. Changes in behavior as indicated in the logs may indicate intrusion attempts.

Unauthorized access of your servers may also result in abnormal server performance levels. You can use System Monitor to configure alerts and have these logged to the Application log.

Internet Information Services (IIS)
IIS logs enable you to obtain information about visitors to your Web sites and problematic issues, including attempts at unauthorized access. By default, logging in the W3C Extended Log File Format is enabled in IIS 6.0. You can control logging properties, such as log schedules, and extended logging properties from the Logging Properties dialog box. As with other log types, you should make a habit of archiving old logs so that you can compare them with logs that may indicate intrusion.

Firewall Log Files
Firewall logs contain information about network traffic passing through the firewall, and in particular its packet filters. Internet Security and Acceleration (ISA) Server 2004 enables you to log data related to the Firewall, Web Proxy, and Simple Mail Transfer Protocol (SMTP) Message Screener services. You can specify the types of actions to be logged and the types of databases to be used, such as SQL or Microsoft Data Engine (MSDE).

Types of events that may indicate intrusion attempts include the following:

- *Blocked access attempts* – Frequent appearances suggest intrusion attempts.
- *Repeated traffic to particular ports* – Suggests a DoS or distributed denial of service (DDoS) attack.
- *Suspicious signatures* – Suggests the presence of worms, viruses, or other malicious software (malware).

Netlogon Log Files
The Netlogon service in Windows Server 2003 maintains a secure communication channel between client computers and domain controllers for user authentication. It creates a debugging file called Netlogon.log, which is located in the %systemroot%\ debug folder. This file records many types of logon problems, including logon attempts with unknown user names, disabled or expired accounts, logons outside allowed hours, locked out accounts, and so on. A large number of these attempts may indicate attempts at brute force password cracking or DoS attacks. See Account Passwords and Policies for more information.

Remote Access Service (RAS) Log Files
RRAS servers in Windows Server 2003 log activities to the following locations:

- *The system log in Event Viewer* – Logs a large number of system and logon-related activities.
- *Log files located at %systemroot%\System32\LogFiles* – When the RRAS server is configured to use Windows authentication and accounting, these files record information related to authentication request, accounting requests, and periodic status. You need to configure these actions from the RRAS snap-in for them to take effect. Select **Remote Access Logging** in the console tree. Right-click **Local File** in the details pane, select **Properties**, and then select the actions you want to record. Information in these logs assists you in troubleshooting failed access attempts by legitimate users as well as incursion attempts by unauthorized users. See Logging for more information.
- *IAS log files* – Located on the IAS server, these log files record the same information as the RRAS log files described previously when RRAS servers are configured to use RADIUS authentication.

Analyzing Security Configuration

After you have configured security baselines and configurations for your servers and client computers, you can analyze their security configuration as required. You can use Microsoft Baseline Security Analyzer or Security Configuration and Analysis for this purpose.

Microsoft Baseline Security Analyzer (MBSA)
MBSA scans Windows-based computers for security vulnerabilities. It checks computers running Windows 2000, XP, and Server 2003 for critical updates and patches, and determines the need for further system hardening. If you go to Microsoft's website and download MBSA as a Microsoft Windows Installer (.msi) package file, double-click the downloaded file and follow the instructions provided to install this application. As shown in *Figure 8*, MBSA provides several options for the type of vulnerabilities it scans for.

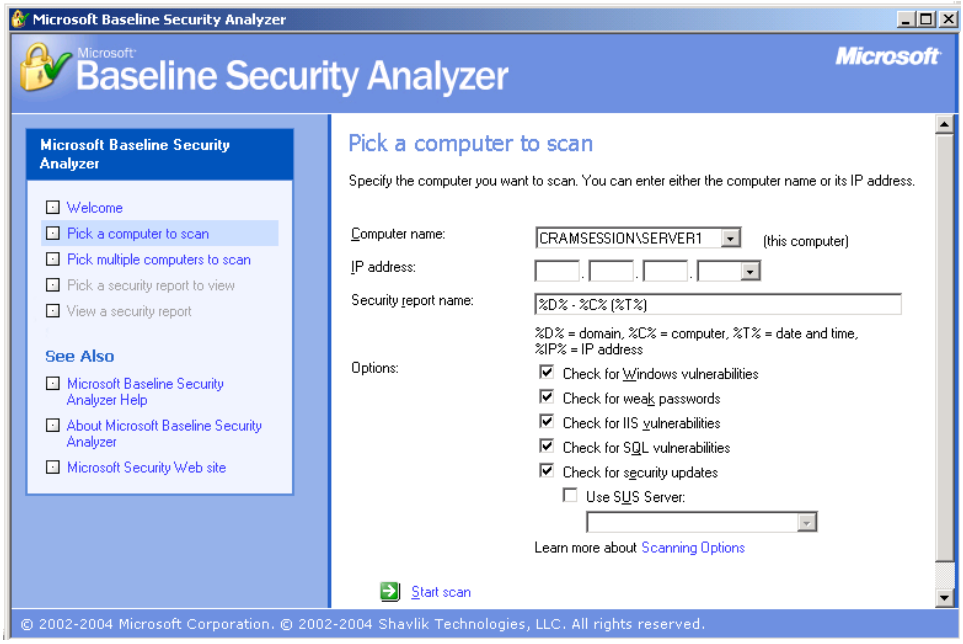


Figure 8 – MBSA Scans One or More Computers for Multiple Security Vulnerabilities

You can also run MBSA from the command line (Mbsacli.exe). This enables you to include MBSA in scripts and schedule the scripts to be run at multiple times.

We discuss the uses of MBSA in greater detail later in this Exam Manual.

Security Configuration and Analysis
Earlier in this exam manual, we mentioned the use of Security Configuration and Analysis for analyzing and configuring security templates. This tool is also useful in scanning computers for their security configuration. After opening the database containing the required template, right-click **Security Configuration and Analysis** and select **Analyze Computer Now**.

If you want to add the existing settings to your database, double-click each setting in the details pane, ensure that **Define this policy in the database** is selected, specify the appropriate setting, and then click **OK**. When you are finished, right-click **Security Configuration and Analysis** and select **Save**. If you want to create a new template from the results, right-click **Security Configuration and Analysis**, and select **Export Template**. Then provide a name for the new template and click **Save**.

Implementing, Managing, and Troubleshooting Patch Management Infrastructure

Keeping applications and operating systems properly updated is a full-time job of many network and security administrators. As vulnerabilities are discovered, Microsoft and other software manufacturers distribute updates that are designed to mitigate these vulnerabilities.

- A **patch** (also called a security update) is an update that addresses one or a small number of vulnerabilities or configuration problems.
- Microsoft considers a **hotfix** to be a single, cumulative package that addresses a specific problem that has been identified by a company through Microsoft Product Support Services. Hotfixes are generally released in a more timely fashion than patches or service packs.
- A **service pack** is a cumulative series of hotfixes, security updates, and other updates. It also might include new functionality (such as the Security Center incorporated into Windows XP Service Pack 2 (SP2) and Windows Server 2003 SP1).

For additional information on current security updates and security information in general, be sure to consult Trustworthy Computing: Security.

Planning the Deployment of Service Packs and Hotfixes

While some companies apply every patch and hotfix that comes along, others tend to follow a "wait and see" attitude. Worms such as SQL Slammer that appeared in the summer of 2003 can exploit weaknesses for which patches exist, and the fact that this worm played so much havoc is indicative of the need to deploy the appropriate patches in a timely manner. On the other hand, some patches have been known to break software functionality, so indiscriminate patch application is not without its problems as well. Microsoft recommends the following four-phase approach to patch management:

- *Assess* – Check out what your production network contains, how it might be impacted by security vulnerabilities, and the corresponding need for security updates.
- *Identify* – Recognize new updates as they are released and determine their need and relevance to your operating environment.
- *Evaluate and plan* – Determine the need for deploying each update and test it in an environment that simulates your production network.
- *Deploy* – Roll out the update to the operating environment and ensure that deployment is successful.

Microsoft has standardized on a monthly schedule for releasing patches on the second Tuesday of every month, with an advance notification of the updates to be released on the previous Thursday. Occasionally, they will release an especially critical update at a different time. For more information on the update release schedule, refer to Revamping the Security Bulletin Release Process.

Microsoft also provides a catalog of all available updates at the Windows Update Catalog Web site. You can use Internet Explorer to search this site to obtain required updates for downloading and installing across networks. It is especially valuable for updating computers on networks that do not normally have access to the Internet.

Evaluating the Applicability of Service Packs and Hotfixes

Microsoft's TechNet Security Center provides information on the most recent security updates. Updated during each monthly patch release, this site provides links to security bulletins and Knowledge Base articles that provide detailed information on each update, including the problems each one repairs. Links to security news and other products and technologies are also included. In addition, you can sign up for email notification of security updates from the Microsoft Security Notification Service.

Microsoft rates vulnerabilities fixed by its patches and updates with the following levels that assist you in determining the importance of released updates:

- *Critical* – An attacker could release a worm that is propagated on the Internet without further user action.
- *Important* – The vulnerability could compromise the confidentiality, integrity, or availability of data or other network resources.
- *Moderate* – Exploitation is mitigated by factors including the difficulty of exploitation, default configuration, or auditing.
- *Low* – The vulnerability offers minimal impact or is extremely difficult to exploit.

It is important to keep a record of the types of computers on your network and the software that they run, so that you can evaluate the need for deploying a particular update, as well as potential problems that might arise. Maintain an up-to-date inventory of computers, their operating systems, and installed software. Microsoft's Systems Management Server (SMS) facilitates the management of computers, networks, applications, and patches, and helps you to keep abreast of the challenges faced in deploying the appropriate updates. You can also use Microsoft Software Update Service (SUS) for managing updates. We discuss SUS later in this document.

Testing the Compatibility of Service Packs and Hotfixes for Existing Applications

- Before you implement patches, hotfixes, and service packs on your production network, you should test them on computers that are representative of those on which they will eventually be installed.
- Newsgroups and forums that discuss Windows updates are also useful because problems associated with them are often reported in these locations.
- You can use SUS to automatically download available updates to a server, from which they can be tested, approved, and rolled out to production computers.

- Refer to Software Update Services for additional information about SUS and its successor, Windows Update Services (WUS), which is expected to be available before the end of 2005. SUS is available for download.
- SMS provides enterprise-level management of patches and updates, including those for third-party software products that are not supported by SUS. While SMS does provide this level of support, you should be aware that this is a high-cost alternative most suitable for larger enterprises.

The following are several recommendations that you should follow when testing updates:

- Set up a test lab that contains servers and client computers representative of computers throughout your network. It should contain computers running all operating systems used on the network; for example, Windows 2000 Professional and Windows XP Professional. This lab should contain a server on which you have installed SUS.
- Configure an Automatic Updates policy that points the lab computers to the SUS server for obtaining updates. We discuss this policy later in this exam manual.
- Review the updates before installing them, and make a note of which updates you have installed.
- Have users that are familiar with the important applications work with them on the test computers and report any problems that might arise. These should include all the principal functions performed in a typical business day.
- If problems arise, remove the updates using the Control Panel Add or Remove Programs applet. Continue the testing until you are satisfied that the updates function properly and can be approved for the production environment.
- Virtualization software such as Microsoft Virtual PC or Virtual Server is useful for test labs because it reduces the hardware requirements and allows for faster setup and rebuild time.

For more information on the patch testing and deployment process using SUS, refer to Patch Managment Using Microsoft Software Update Services.

Planning Patch Deployment Environments for Both the Pilot and Production Phases

- Although testing patches in a lab environment catches the major problems that could affect productivity, it cannot catch all problems that can result from poorly designed patches
- In a pilot deployment, you deploy patches to a segment of your production network (for example, one department or a small group of knowledgeable users) and watch for problems before deploying them to the entire network.
- You can use SUS together with a group policy that is linked to the OU in which the pilot group resides to perform such a deployment.
- You can also use a secondary SUS server to select and approve only a subset of available patches for testing purposes.

The following are several results you should watch for during the pilot deployment:

- Computers should restart properly after each update has been installed.
- All line of business and other critical applications should perform properly and without slow-down after the updates have been installed.
- Each update should have an uninstall feature that permits its removal without affecting other updates or applications.

Always notify the affected users and ensure the cooperation of management before beginning the pilot deployment. You need to be ready for users reporting problems; should such problems occur, you may need to remove the update from the SUS server and uninstall it from the affected clients. After completion of the pilot deployment phase, review the results to identify any changes or modifications necessary to roll out the updates to the entire network.

Planning the Batch Deployment of Multiple Hotfixes

Many hotfixes and other updates require a reboot to complete installation. Deployment of multiple hotfixes can become tedious and time-consuming should a large number of reboots be required. To this end, Microsoft developed a command-line tool called **Qchain.exe** that installs multiple hotfixes without the need for rebooting until after the last hotfix is installed. This tool works for all updates that use **Hotfix.exe** or **Update.exe** as the updating mechanism.

- For updates that were created after December 2002, you can create scripts that run the **Update.exe** installer program for each update, and then restart the computer after installing the last update.
- Run **update.exe** with the **/z** and any other needed switches, followed by **qchain.exe**. Then restart the computer.
- All the latest updates, including Windows Server 2003 updates, have Qchain functionality built into them. When you use Automatic Updates with SUS or Windows Update, these updates are automatically chained without administrator intervention.

Update.exe supports the following switches:

- **/f** – Closes other programs at shutdown
- **/n** – Does not back up files for hotfix removal
- **/z** – Does not restart the computer after hotfix installation
- **/q** – Installs hotfixes in quiet mode without user interaction
- **/m** – Uses unattended setup mode in Windows 2000
- **/u** – Uses unattended setup mode in Windows XP
- **/l** – Lists hotfixes that have been installed
- **/o** – Overwrites original equipment manufacturer (OEM) files without prompt

Planning a Rollback Strategy

Even when thoroughly tested in a lab and pilot environments, patches sometimes break existing applications or cause other problems. Consequently, it is important that you have a patch rollback strategy in place before you begin patch deployment. To this end, Microsoft has included rollback capability in all patches that are installed by using **Update.exe** or Windows Installer .msi files. SMS 2003 integrates with SUS 2.0 and WUS to provide rollback capabilities.
Several methods of patch rollback are possible:

- Add or Remove Programs in Control Panel contains references to most updates and enables you to manually remove them. However, you need to visit each affected computer to perform the removal.
- System Restore can restore a Windows XP Professional computer to a point in time before the update was installed. However, this method works only on Windows XP computers and also requires that you visit each affected computer. Note that System Restore automatically creates a restore point when you use Windows Update or Automatic Updates to install patches or other updates.
- If you have used a GPO to deploy patches that were installed using Windows Installer packages, you can remove the patch by removing the installation package from the GPO. Select the Immediately Uninstall the Software from Users and Computers option when removing the package.
- You may be able to write a script that uninstalls patches that were installed using Windows Installer packages.
- You can remove the affected patches from the approved list in SUS or WUS to prevent their reapplication.
- If you have integrated (slipstreamed) updates with the Windows installation media, you must reinstall the operating system from media without the updates in order to remove them.

Using MBSA to Assess the Current Status of Service Packs and Hotfixes

As mentioned earlier in this exam manual, MBSA scans computers running Windows NT 4.0/2000/XP/Server 2003 and determines the need for additional critical updates and system hardening.

You can scan a range of computers or even an entire domain from an installation of MBSA on a computer running Windows 2000 or later. You can even scan computers on a remote network across a firewall or a filtering router, provided that you have opened TCP ports 139 and 445, and UDP ports 137 and 138.

MBSA checks a large range of Windows security configurations, as well as Internet Explorer and Outlook security zone settings, and Microsoft Office macro settings and Windows Media Player. The following are the major Windows, IIS, and SQL vulnerabilities that MBSA scans for:

- *Windows vulnerabilities* – Missing security updates and service packs, weak or blank passwords, use of autologon, enabling of the Guest account, membership of the local Administrator account, unnecessary services running, and whether auditing is enabled. File shares present are also reported, along with their permissions.

- *IIS vulnerabilities* – Whether the IIS Lockdown tool 2.1 has been run, enabling of IIS logging, the presence of IIS sample applications, use of IIS on a domain controller, installation of the IIS Admin virtual folder, and enabling of parent paths. Installation of scripts and Microsoft Advanced Data Connector (MSADC) virtual directories are also reported.
- *SQL vulnerabilities* – Strength of password on the systems administrator (sa) account, the sysadmin role including the Administrators group membership, the number of role holders, and SQL service accounts as members of the local Administrators group. Missing SQL security updates, the SQL Server authentication mode type, use of SQL Server on a domain controller, installation folder access permissions, and weak or blank passwords are also checked.

Perform the following procedure to scan the computers on your network:

1. On the Welcome page, select **Scan more than one computer**.
2. Enter the domain name or the IP address range of the computers to be scanned. If you want to use a SUS server to check for security updates, enter the name or IP address in the list box provided. Then click **Start scan**.
3. When scanning has completed, click **Pick a security report to view**.
4. As shown in *Figure 9*, the report that appears displays vulnerabilities that MBSA has found.

Figure 9 – The MBSA Report Provides Information on a Computer's Security Vulnerabilities

Each entry in the report is flagged with an icon representing the vulnerability status:

- *Green check mark* – Critical or non-critical check has passed
- *Blue "i"* – Information item or check not performed
- *Yellow "X"* – Non-critical check has failed
- *Red "X"* – Critical check has failed

You can obtain additional information by selecting the links provided beneath each scan result. In particular, the Result Details link provides additional information such as the user names whose passwords do not pass the security tests as well as suggestions for correcting the various problems.

Microsoft provides a file called **Mssecure.xml** to ensure that MBSA is kept up to date. When you run MBSA, it checks for an updated version of this file and downloads it by means of a digitally signed, compressed file named **Mssecure.cab**. If necessary, you can download the file manually and copy it to the Program Files\Microsoft Baseline Security Analyzer folder.

For answers to frequently asked questions on MBSA, check out Microsoft Baseline Security Analyzer (MBSA) 1.2.1 Q&A.

Using the MBSA Command-Line Tool to Assess Current Patch Levels with Scripted Solutions

- **Mbsacli.exe** is an update of the older Microsoft Network Security Hotfix Checker (**Hfnetchk.exe**) application.
- You can script the scanning of a series of computers and use Task Scheduler to enable automatic, periodic scanning.
- You can control its actions by specifying switches that perform actions such as specifying the computers to be scanned, the items to be checked (IIS, SQL, password strength, the presence of security updates), reports produced, and so on.
- You can also use the **/hf** switch to run in HFNetChk mode, which provides backwards compatibility and some additional functionality such as the use of XML data sources and scanning of computers named in a text file.

For a complete description of the available swithces, type **mbsacli /?** at the command prompt.

Deploying Service Packs and Hotfixes

Methods available for deploying patches, service packs, hotfixes, and other updates to new and existing computers on your network include the following:

- Manual installation of updates by using Windows Update.
- Use of SUS in conjunction with Group Policy or SMS to deploy updates to existing computers.
- Use of slipstreaming, custom scripts, and implementation using Remote Installation Services (RIS) to include updates directly into new operating system installations.

Use of Windows Update to Manually Install Updates

- Windows Update connects to the Microsoft Windows Update Web site to manually download and install updates on a stand-alone Windows 2000/XP/Server 2003 computer.
- On a Windows XP or Windows Server 2003 computer, click **Start > All Programs > Windows Update**. From the main Windows Update page, click the **Scan for updates** link and wait while Windows Update scans your computer. When it presents the list of available updates, click the link provided to review the updates. Click **Remove** to remove any you do not want to install, and then click **Install** to install the updates.

Use of SUS to Deploy Updates to Existing Computers

You can install SUS on a computer running Windows 2000 Server or Windows Server 2003. This server also needs to have IIS installed, and you should have at least 6GB of free space for storing the updates for deployment to computers on the network.
SUS provides the following advantages:

- You can approve individual updates on every SUS server. Doing so enables you to test and deploy updates on a scheduled basis.
- You can configure client computers to obtain their updates from the SUS server. This also includes computers that are not connected to the Internet.
- You can set up a parent-child SUS server architecture that supports up to 15,000 clients per SUS server. You can copy updates from a primary SUS server to secondary SUS servers without the need for the secondary servers to be connected to the Internet.

SUS is available as a free download from Microsoft. When the download is completed, perform the following steps to install SUS:

1. Double-click the executable file. When the setup wizard starts, click **Next**.
2. Accept the licensing terms and click **Next**.
3. Click **Typical** to install SUS with default settings or **Custom** to customize the SUS installation.
4. Note the URL displayed on the Ready to Install page that client computers will use to access the SUS server, and then click **Install**.
5. When the completion page appears, note the URL displayed that you can use to configure SUS, and then click **Finish**.
6. Internet Explorer opens this URL and displays a welcome page. Click the links provided to learn more about SUS.
7. To download updates from the Microsoft Windows Update Web site, click **Synchronize Server > Synchronize Now**. A Catalog Download Progress bar displays the progress of the download. You can also set up a schedule for downloading updates by clicking **Synchronization Schedule**. A dialog box opens from which you can configure daily or weekly synchronization, and specify the time and the number of retries to attempt should the synchronization fail.
8. To approve updates for distribution to client computers, click **Approve Updates**. On the Approve Updates page, select the updates to be approved, and then click **Approve**.

For more information on using SUS to obtain and deploy updates, refer to Software Update Services, Part 1.

Use of Group Policy to Enable Automatic Updates

- Group Policy enables you to ensure that all affected client computers receive updates from the SUS server on a timely basis.
- In a GPO linked to the appropriate Active Directory container, open the Group Policy Object Editor and navigate to the **Computer Configuration\Administrative Templates\Windows Components\Windows Update** node.
- Right-click the **Configure Automatic Updates** policy in the right pane and choose **Properties** to open the dialog box shown in *Figure 10*.

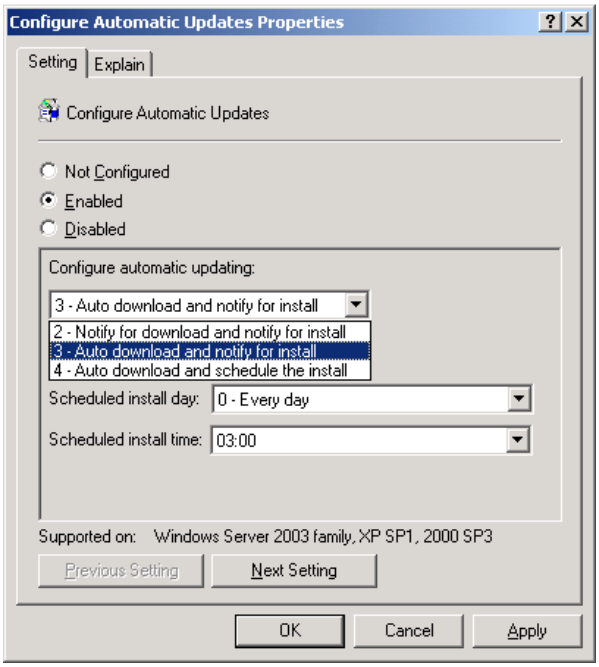


Figure 10 – Group Policy Provides You with Three Options for Configuring Client Computers for Automatic Updates

- Enable this policy and choose from the following options in the Configure Automatic Updating drop-down list box:
  - *2 – Notify for download and notify for install* – Displays an icon in the notification area when updates are available for download. The user needs to click this icon to select the specific updates for download. The user is notified again when the updates have been downloaded, and needs to click this icon a second time to install them.
  - *3 – Auto download and notify for install* – Automatically downloads the updates and displays an icon in the notification area when updates are available. The user needs to click this icon to install them. This is the default setting.

- *4 – Auto download and schedule the install* – Automatically downloads and installs the updates on the day and time that you configure in the list boxes provided. If any of the updates require a restart, the computer is restarted automatically.

- Point your client computers to the SUS server for obtaining their updates. To do so, enable the **Specify intranet Microsoft update service location** policy, found in the same node of the Group Policy Object Editor. As shown in *Figure 11*, type the URL displayed when you installed SUS in the text boxes provided.

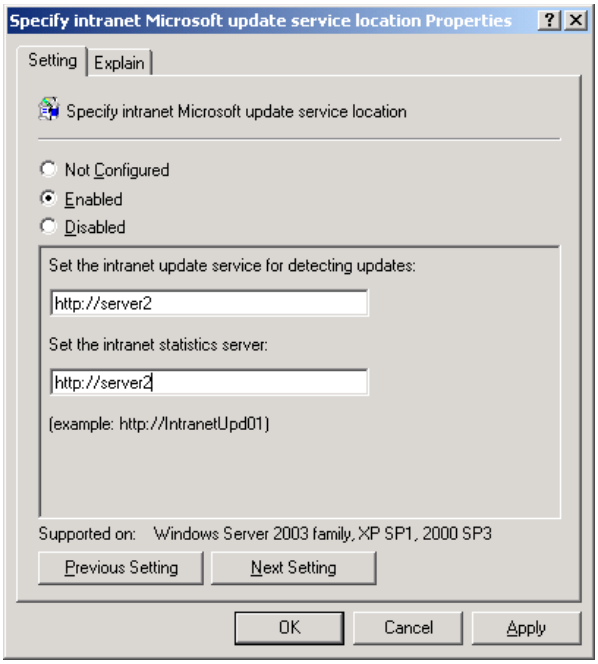


Figure 11 – Using Group Policy to Direct Client Computers to Your SUS Server

Group Policy also enables you to configure the following additional policy settings:

- *Reschedule Automatic Updates scheduled installations* – Enables you to specify the number of minutes after startup that Automatic Updates waits before performing a scheduled installation that was missed because the client computer was not running or connected to the network.

- *No auto-restart for scheduled Automatic Updates installations* – Prevents an automatic restart of a computer, and requires that the user manually restart the computer after updates have been installed. The user should perform this restart when required so that Automatic Updates can detect future updates properly.

Use of SMS to Deploy Updates

SMS 2003 contains a Software Update Management feature that enables you to deploy, audit, and track updates on an enterprise basis. Using this feature, you can manage updates to other software applications such as Microsoft Office, as well as Windows updates. It includes the following tools:

- *Software update inventory tools* – Scan all computers on the network and provide an inventory of all software updates that have been installed. Help to identify those computers that require updates.
- *Software Updates Installation Agent* – Determines which updates are required by network computers and ensures that only the required updates are installed.
- *Distribute Software Updates Wizard* – Assists you in evaluating available updates, obtaining additional information about these updates, and selecting the updates to be deployed. You can also perform additional tasks such as prioritizing updates, specifying installation parameters, and performing additional customizations. It also downloads the updates, distributes them to distribution points, and creates distribution programs and advertisements.

For more information about using SMS to deploy updates, refer to Management Architecture Guide: Version 2.0, Chapter 6 - Administration Tools, Systems Management Server.

Deployment of Updates on New Servers and Client Computers

It is possible to save a tremendous amount of time by deploying updates to the operating system on new computers at the same time you first install the operating system. You can accomplish this task by means of slipstreaming, the use of custom scripts, or the use of RIS.

Slipstreaming of Service Pack Files

The concept of slipstreaming refers to the inclusion of service pack files (for example, Windows Server 2003 SP1 or Windows XP SP2) directly within the installation media. Perform the following steps to create a slipstreamed installation:

1. Create a shared folder on a server and copy the I386 folder from the operating system installation CD-ROM to this folder.
2. Copy the service pack installation files to the same partition.
3. Open a command prompt, navigate to this partition, and extract the service pack files (for example, type **xpsp2 –x** to extract Windows XP SP2 files).
4. Specify a folder to which these files are to be extracted.
5. From the command prompt, navigate to a subfolder named **i386\update**.
6. Type **update /integrate:x:** (where *x*: is the partition on which the installation files are located).
7. Click **OK** when informed that the integrated installation is completed.

You can now perform a slipstreamed installation by pointing computers to this shared folder or by burning these files to a CD-ROM.

Use of Scripts and RIS

- You can use **Update.exe**, which we have already described, to script the installation of updates on new computers that are being installed by means of an unattended installation file such as Winnt.sif.
    - Simply include the **Update.exe** or **Hotfix.exe** command(s) with the appropriate parameters in the [GuiRunOnce] section of the unattended installation file. These commands install updates in sequence.
    - Use the **/u** and **/z** switches described earlier to install these updates in unattended mode and prevent the computer from restarting after each update (if the computer were to restart, subsequent updates would not be installed).
- You can use custom scripts and RIS to ensure that new computers are installed with the latest service packs, hotfixes, and updates included.
    - The use of RIS involves preparing a standard operating system installation together with the required applications, and then using **Riprep.exe** to image this installation to the RIS server.
    - Simply update the source computer with the latest service packs, hotfixes, and patches before performing the imaging.
    - Retain the source computer and add additional updates as they are released, and then re-image the computer before using RIS to install additional new computers.

Implementing, Managing, and Troubleshooting Security for Network Communications

Hackers and crackers are employing tactics such as packet sniffing, spoofing, DoS, man-in-the-middle, and other types of attacks against networks to disrupt communications and steal important data. This section provides a thorough grounding of IPSec. It also introduces wireless network security, Secure Sockets Layer (SSL), and remote access security.

Planning IPSec Deployment

Deciding Which IPSec Mode to Use

You can choose from transport mode or tunnel mode according to the type of network traffic you need to secure:

- *Transport mode* – Secures traffic between two computers on the same network, for example, server to server or client to server.
- *Tunnel mode* – Secures traffic between two different networks, as defined by tunnel end points, which are normally routers or other devices connecting the networks.

Planning Authentication Methods for IPSec

IPSec in Windows Server 2003 supports three authentication methods:

- *Kerberos* – As used for domain authentication in Windows 2000/XP/Server 2003 Active Directory, Kerberos V5 is the default IPSec authentication method, and should be used in all situations for authentication within the same domain or a trusted domain.
- *Certificates* – You can use a public key certificate in situations involving Internet access, communications with external business partners, or other communications involving computers that do not use Kerberos V5.
- *Preshared keys* – This method uses a case-sensitive alphanumeric character string that is known to both client and server. It is simple to use because it does not require Kerberos or the presence of a PKI; however, the character string is stored in plain text and could be captured by an attacker. You should use this method only if neither of the other methods is suitable.

For several examples of when you would use each of these authentication methods, refer to Selecting IPSec Authentication Methods.

Testing the Functionality of Existing Applications and Services

The application of any type of security methodology poses the possibility of breaking functionality or at the very least, reduction of performance. You need to be aware of the effect of IPSec on your network operations, both in terms of time and effort required to configure and maintain IPSec as well as its effect on network functionality. The following are several factors you should take into consideration when planning the use of IPSec on your network (see Weighing IPSec Tradeoffs for more information):

- *Slower creation of connections* – IPSec needs to negotiate every network connection and authenticate its end points. This can take one to three seconds on the average.
- *Reduced computational performance* – Actions such as processing, filtering, encrypting, and decrypting of network packets all take processor cycles to accomplish. In addition, increased packet size resulting from the headers added by IPSec places additional load on networks and processors.
- *Impact upon network processing technologies* – Security headers added to packets may impact tools such as routers, firewalls, load-balancing devices, network address translation (NAT) devices, stateful filtering controls, and intrusion detection systems (IDS). You may need to enhance such technologies so that they are able to interact with IPSec-secured traffic, for example by use of NAT Transversal (NAT-T). We discuss NAT-T later in this exam manual.
- *Loss of clustering connectivity* – Many technologies used for clustering and load balancing use the same IP address for more than one node. Windows Server 2003 IPSec contains extensions that accommodate this situation; however, current Windows 2000 and XP implementations do not support these extensions and may cause loss of connectivity when nodes are added or removed.
- *IPSec may impact communications with domain controllers* – IPSec can block Kerberos-related authentication traffic and cause communications to fail.

As with security updates it is useful to employ a test lab to test the impact of IPSec policies on your applications and services before deploying the policies to the production network.

Configuring IPSec Policies to Secure Communications between Networks and Hosts

Group Policy enables you to configure IP Security policies at any level including local policies. You can create your own IPSec policy to meet special network needs, use a default IPSec policy (*Figure 12*), or modify a policy according to your network requirements:

- *Secure Server (Require Security)* – Requires that all connections be secured with IPSec. Any device (such as a pre-Windows 2000 computer) that cannot use IPSec is unable to communicate with a computer on which this policy is specified. Unsecured ICMP traffic, such as ping, is supported.
- *Server (Request Security)* – All connections with computers that can use IPSec are secured, but this rule enables unsecured communications with devices that are unable to use IPSec. You can combine this policy with the Client (Respond Only) policy to secure all communications involving IPSec-aware computers.
- *Client (Respond Only)* – Contains only a single rule that secures communications with other computers when secured communication is requested.

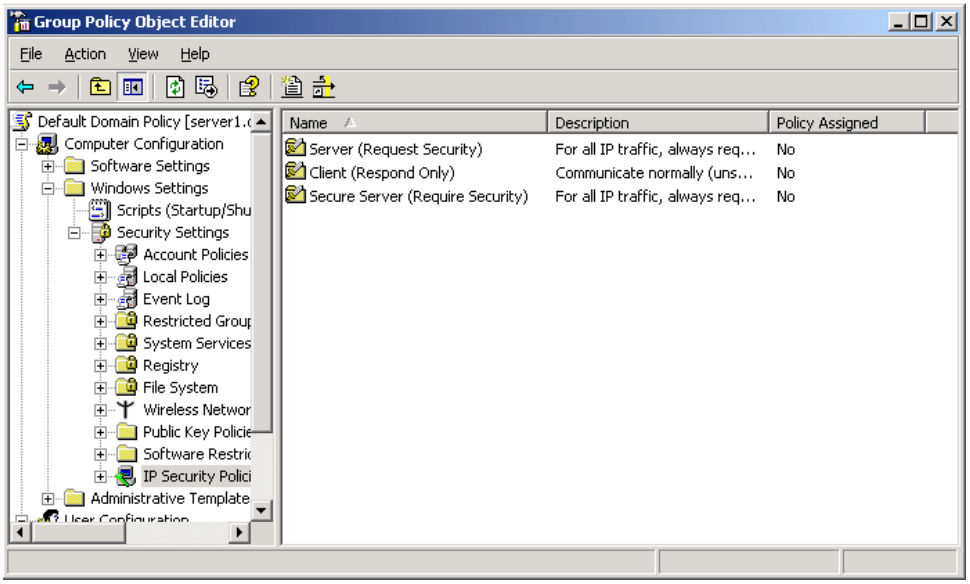


Figure 12 – Group Policy Provides Three Default IPSec Security Policies

IPSec Policy Rules

Every IPSec policy contains one or more policy rules. These rules govern all actions permitted by the security policy, and contain the following components:

- *Filter list* – Defines one or more filters that identify the type of traffic governed by the rule according to protocols, ports, and IP address ranges
- *Filter action* – Defines the type of action (**Permit**, **Block**, or **Require Security**) for packets matching the filter list
- *Authentication methods* – Define the methods (Kerberos, certificates, or preshared keys) used by the rule
- *Tunnel endpoint* – Specifies the use of tunnel mode and the IP address of the tunnel endpoint
- *Connection type* – Specifies whether the rule applies to dial-up connections, LAN connections, or both

To modify IPSec policy rules, double-click the desired policy in the Group Policy Object Editor (*Figure 12*). This displays the Rules tab of the Properties dialog box for that policy, with a summary of the rule properties. Select the rule to be modified and click **Edit** to access the Edit Rule Properties dialog box. You can also create a new rule by clicking **New** and specifying the properties in the New Rule Properties dialog box.

Configuring IPSec Authentication

The Authentication Methods tab of the New Rule Properties or Edit Rule Properties dialog box enables you to configure authentication methods used by the IPSec rule. From this dialog box, you can perform any of the following tasks:

- *Add an authentication method* - Click **Add** and select the desired authentication method from the New Authentication Method Properties dialog box (see *Figure 13*). If configuring certificate-based authentication, click **Browse** to browse for the required CA. If configuring preshared key authentication, type the required character string. Then click **OK**.
- *Change the existing authentication method* - Click **Edit** to open the Edit Authentication Method Properties dialog box, which provides the same choices as shown in *Figure 13*.
- *Change the order of preference* - Select an authentication method and click **Move up** or **Move down** as required. IPSec attempts to use the first authentication method specified and, if necessary, tries additional methods in sequence.
- *Remove an authentication method* - Select it and click **Remove**.

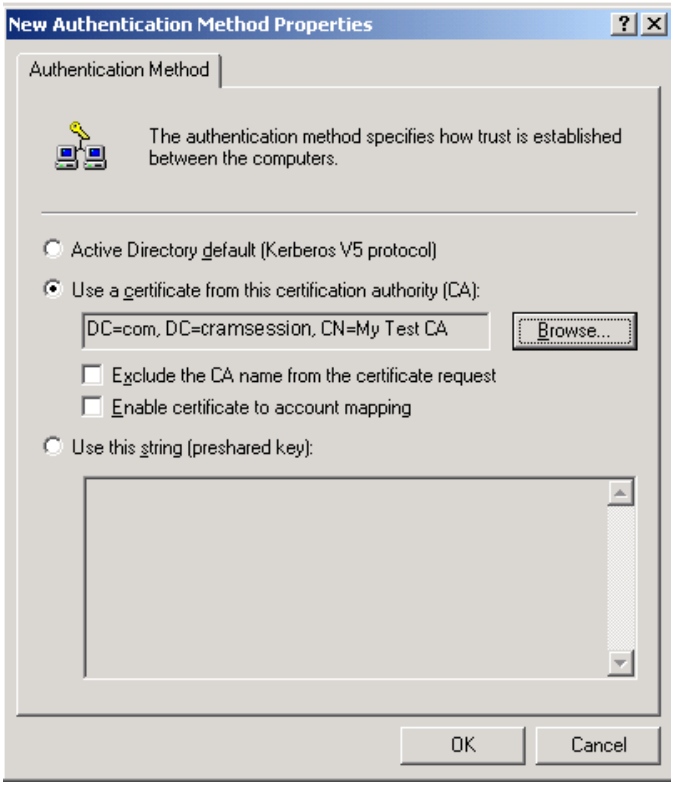


Figure 13 – The New Authentication Method Properties Dialog Box Enables You to Configure IPSec Authentication Methods

For more information on configuring authentication methods, refer to Define IPSec authentication methods.

Configuring Encryption Levels

IPSec uses a hashing algorithm to ensure message integrity, either Secure Hash Algorithm 1 (SHA1) or Message Digest 5 (MD5), and a symmetric encryption algorithm, either Data Encryption Standard (DES) or Triple Data Encryption Standard (3DES).

Perform the following procedure to configure encryption methods:

1. From the General tab of the security policy's Properties dialog box, click **Settings**, and then click **Methods**.
2. On the Key Exchange Security Methods dialog box (see *Figure 14*), perform one of the following actions:
    - To add a security method, click **Add**. Specify the required integrity algorithm (MD5 or SHA1), encryption algorithm (DES or 3DES), and Diffie-Hellman group (low, medium, or high), and then click **OK**.
    - To edit an existing method, click **Edit** and specify the same choices.

- To remove a method, select it and click **Remove**.
- Use the **Move up** or **Move down** buttons to change the preference order.

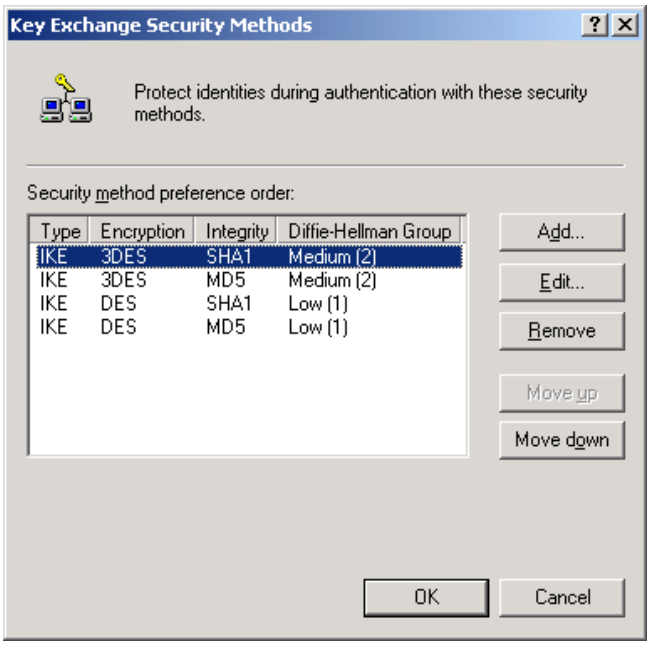


Figure 14 – The Key Exchange Security Methods Dialog Box Enables You to Edit Encryption and Integrity Algorithms and Diffie-Hellman Groups

Key Management

Keys are the codes used with the encryption and integrity algorithms used by IPSec. Secure communication is accomplished by two computers having access to the same key without sending the key across the network. IPSec uses Diffie-Hellman keying material of lengths of 768, 1024, or 2048 bits, known as Low (1), Medium (2), or High (3), respectively. The longer the keys, the greater the protection but the more processing power required. You can specify key lengths in the Key Exchange Security Methods dialog box already discussed and shown in *Figure 14*.

It is necessary to generate new keys at defined intervals to reduce the chance of compromise. You should be aware of the following parameters:

- *Key lifetimes* – Determine when a new key is created. You can specify either a length of time in seconds or number of kilobytes (KB) after which a new key is generated. To specify key lifetimes, access the Security Methods tab of the Edit Rule Properties dialog box for the IPSec rule in use. Select a security method and click **Edit**. In the Edit Security Method dialog box, select **Custom** and click **Settings**. In the Custom Security Method Settings dialog box (see *Figure 15*), specify values for kilobytes and/or time.

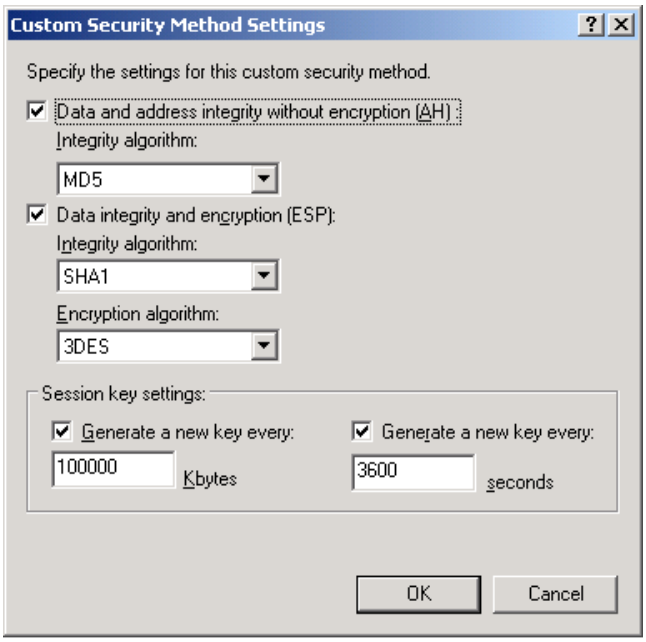


Figure 15 – The Custom Security Method Settings Dialog Box Enables You to Specify AH and ESP Algorithms, as Well as Key Lifetime Settings

- *Perfect forward secrecy (PFS)* – Determines how a new key is created and ensures that compromise of one key enables access to only the portion of data protected by this key. Two types of PFS are available:
  - *Master key PFS* – Requires re-authentication for each key regeneration
  - *Session key PFS* – Uses a new Diffie-Hellman exchange to generate a new master key without the need for re-authentication. Although this is the most secure method of rekeying, it can impact negatively on server performance.

For more information on key lifetimes and PFS, refer to Key management and protection.

Configuring IPSec Protocols

- *Authentication Header (AH)* – Enables authentication, integrity, and anti-replay, but does not encrypt data. It encapsulates each packet with an AH header, and then signs the packet to ensure integrity and authentication. It accomplishes these actions by using the MD5 or SHA1 hashing algorithms already mentioned.
- *Encapsulating Security Payload (ESP)* – Provides all actions accomplished by AH, and in addition provides for data confidentiality by encrypting the contents of each packet. It encapsulates each packet with ESP header and trailer, and then encapsulates with a new IP tunnel header that contains the IP addresses of the tunnel endpoints. It uses the same integrity algorithms as AH, and uses the DES or 3DES encryption algorithms in addition.

- You can specify the use of either AH or ESP for either transport mode or tunnel mode. In ESP transport mode, the data in the IP payload is encrypted and signed only. To configure the mode used by an IPSec rule, access the Tunnel Setting tab of the rule's Edit Rule Properties dialog box. To specify transport mode, select **This rule does not specify an IPSec tunnel**. To specify tunnel mode, select **The tunnel endpoint is specified by this IP address**, and type the IP address in the box provided.
- To specify IPSec protocols and encryption methods, access the Custom Security Method Settings dialog box referred to for configuring key lifetimes and previously shown in *Figure 15*. This dialog box enables you to select AH, ESP, or both, and enables you to choose the desired algorithms.

Configuring IPSec Filters and Filter Actions

- The IP Filter List tab of a policy rule's Edit Rule Properties dialog box enables you to configure the properties of filter lists and their associated actions. By default, rules contain filter lists for all ICMP traffic and all IP traffic.
- To create a new filter list, click **Add**. In the IP Filter List dialog box, click **Add** and follow the instructions provided by the IP Filter Wizard. You will need to specify the following properties:
    - *Mirrored* – Creates a second filter with the exact opposite source and destination addresses.
    - *Source address* – Specify source address options according to My IP Address, or specific IP addresses, subnets, or DNS name. You can also specify according to DHCP, DNS, or WINS servers.
    - *Destination address* – Specify the same destination address options as described for source address options.
    - *IP protocol type* – Specify the IP protocol type or choose **Any** for all IP protocols. For TCP and UDP, you can specify the source and destination ports used by the filter, or choose **Any Port**.
- To edit a new or existing filter list, click **Edit**. The IP Filter List dialog box opens for the selected filter list, and enables you to configure the same properties listed here for a new filter list.
- To select and edit filter actions select the **Filter Action** tab. Click **Add** to specify your own filter action, or select from one of the following actions:
    - *Permit* – Permits the passage of unsecured IP packets.
    - *Request Security (Optional)* – Requests clients to establish secured communications, but will communicate with untrusted clients in an unsecured manner.
    - *Require Security* – Requires clients to establish secured communications, and will not communicate with untrusted clients.
- On the Filter Action tab, you can also edit an action by selecting it and clicking **Edit**. This enables you to select AH and ESP integrity and confidentiality algorithms, key lifetimes, PFS, and other options.

Deploying and Managing IPSec Policies

Use of Local Policy Objects or Group Policy Objects

- You can configure IPSec policies at any of the local, site, domain, OU, or child OU levels. Policies are applied in this sequence, with policies applied later in the sequence overriding conflicting policies specified earlier in the sequence.
- To use a local policy, click **Start > All Programs > Administrative Tools > Local Security Policy**. The IP Security Policies on Local Computer node enables you to configure all the options we have discussed in this exam manual on a local policy.
- To use a site-based policy, open Active Directory Sites and Services. Right-click the desired site and choose **Properties**. From the Group Policy tab, click **Edit** to edit an existing GPO or **New** to create a new GPO. Navigate to the **Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Active Directory** node.
- To use a domain-based or OU-based policy, open Active Directory Users and Computers, right-click the desired domain or OU, and choose **Properties**. Proceed as described for site-based policies.

Use of Commands and Scripts

- You can use **Ipsecpol.exe** to configure local or remote IPSec policies on Windows 2000 computers. This tool is available for download from Microsoft. It does not work on Windows XP or Windows Server 2003 computers, you instead use **netsh**.
- The **netsh ipsec** command enables you to manage IPSec on computers running Windows Server 2003. It is useful for scripting IPSec configuration across multiple servers.
- The **netsh ipsec static** command enables you to create new IPSec policies without affecting active policies. You can perform the same types of policy configuration actions from the command line as we discussed for GUI-based actions, and script these actions for applying to multiple servers. To obtain information on available subcommands, type **netsh ipsec static /?**.
- The **netsh ipsec dynamic** command enables you to display the active IPSec condition and modify the configuration of active IPSec policies in real time. To obtain information on available subcommands, type **netsh ipsec dynamic /?**.

Deploying IPSec Certificates

Recall that you can use Kerberos, certificates, or preshared keys for IPSec authentication purposes. Certificate-based authentication is most useful when you need to use IPSec for communication between different Active Directory forests when no trust relationship exists, such as with partner companies, customers, or suppliers. You should also use certificate-based authentication when communicating with non-IPSec-aware computers such as UNIX, Linux, or pre-Windows 2000 computers.

Computers that use IPSec need to have a Computer certificate and an IPSec certificate installed in order to communicate. You can obtain the required certificates from a Windows 2000 or Windows Server 2003-based certification authority (CA). You can configure a policy in a GPO linked to the appropriate Active Directory container that requests and installs the appropriate certificates:

1. Navigate to the **Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Automatic Certificate Request** node.
2. Right-click this node and choose **New > Automatic Certificate Request**. The Automatic Certificate Request Setup Wizard starts. Click **Next**.
3. From the Certificate Template screen, select the IPSec template, as shown in *Figure 16*. Click **Next** and then click **Finish**.
4. Repeat these steps and select the **Computer** template. You should see the Computer and IPSec certificate requests displayed in the details pane. The next time computers affected by this GPO restart, they will automatically receive these certificates.

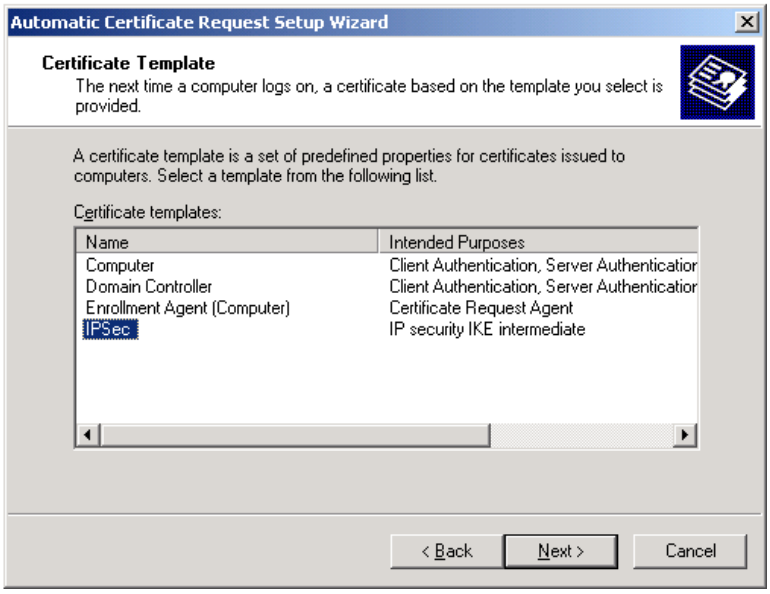


Figure 16 – Configuring Automatic IPSec Certificate Requests

When you receive an IPSec certificate, you need to place it in the Trusted Root Certification Authorities certificate store on each computer that requires certificate-based IPSec communication.

Troubleshooting IPSec

Microsoft has provided several monitoring and logging tools that assist you in monitoring and troubleshooting problems with IPSec. For an overview of several troubleshooting techniques, refer to IPSec troubleshooting tools. For causes of and solutions to several common IPSec problems, refer to IPSec Troubleshooting.

Using IP Security Monitor to Monitor IPSec Policies

Windows XP Professional and Windows Server 2003 provide the IP Security Monitor snap-in, which is useful in diagnosing several problems including the failure to apply a security policy, problems with key lifetimes or expired security associations, or delays in establishing communications between servers.

To use IP Security Monitor, add the snap-in to a blank MMC console. As shown in *Figure 17*, the console thus created can monitor IPSec activities on the local computer. To monitor additional computers, right-click **IP Security Monitor** in the console tree and choose **Add computer**.

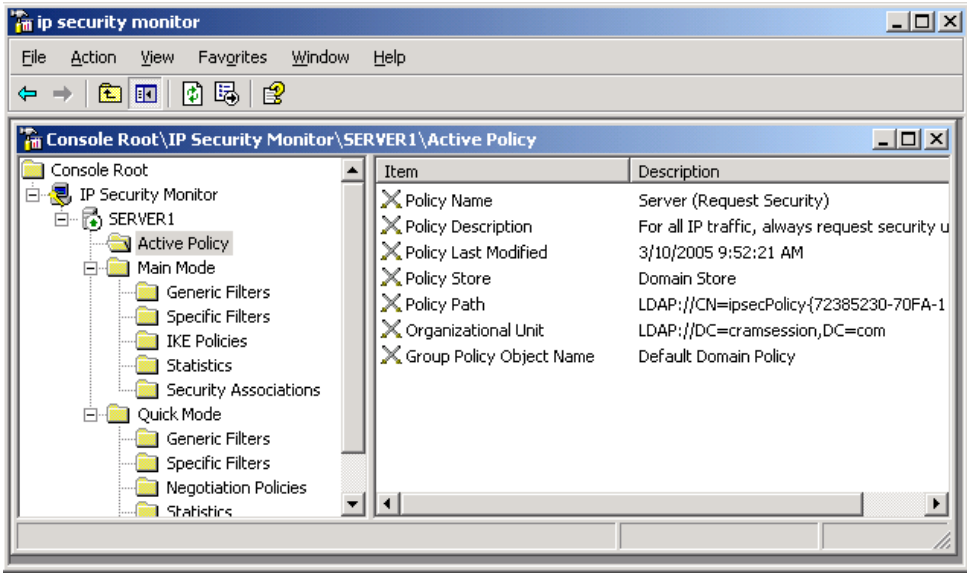


Figure 17 – The IP Security Monitor Snap-in Can Obtain a Considerable Amount of Information Related to IPSec Activities

The IP Security Monitor snap-in can obtain the following information:

- Active IPSec policy details, including the policy name and description, the date and time of last policy modification, the policy store (local or domain), the Lightweight Directory Access Protocol (LDAP) path to the Active Directory-based IPSec policy in use, the LDAP organizational unit (or domain for a domain-based policy), and the name of the GPO in which the policy is configured.
- Main and quick mode statistics, including the following:

- Generic and specific filters applied by the active policy including direction and end-points, Internet Key Exchange (IKE) policy, and authentication methods. Double-click a generic filter to obtain additional information.
- Main mode details about IKE policies. Double-click a policy to view information about encryption, integrity, and Diffie-Hellman algorithms and key lifetimes.
- Statistics, including detailed information about data sent and received, errors encountered, and so on.
- Security associations, including information about the combinations of keys, protocols, and parameters that define the active policy's security rules.

Configuring IPSec Logging

- By configuring auditing for logon and policy change events, you can record information about failed main mode or quick mode negotiations in the Event Viewer Security log.
- You can configure more detailed IKE logging by enabling the IKE tracing log. To do so, open a command prompt and type **netsh ipsec dynamic set config ikelogging 1**. This creates the Oakley log, which is located at %systemroot%\Debug\Oakley.log and provides information about IPSec implementation and problems. For more information, see Enabling detailed tracing for Internet Key Exchange (IKE) negotiations.
- You can enable logging of IPSec driver per-packet drop events in the Event Viewer System log. To do so, open a command prompt and type **netsh ipsec dynamic set config ipsecdiagnostics 7**, and then restart the computer. For more information, consult Viewing IPSec-related events in Event Viewer.
- To modify the interval at which IPSec driver packet events are logged (which is 60 seconds by default), type **netsh ipsec dynamic set config ipseclogginterval <*time*>**, where <*time*> is the desired logging interval in seconds.
- The System and Application logs record several events that may be helpful in troubleshooting IPSec problems. Refer to IPSec: Security Audit Log for more information.
- When configuring IPSec logging, ensure that the system log has plenty of space (at least 10MB), and that you archive and clear the logs frequently.

Troubleshooting IPSec Across Networks

You need to be aware of several factors that can prevent IPSec communications across networks from succeeding, or that can result in unsecured communications taking place.

Network Address Translation (NAT)

- Problems can occur when you use implementations of NAT prior to Windows Server 2003 together with IPSec because NAT modifies the IP headers, causing IPSec to believe that they have been tampered with.
- Windows Server 2003 includes NAT-Transversal (NAT-T), which enables IPSec-secured traffic to pass through a NAT device properly.

- Early in 2005, Microsoft released an update that enhances L2TP/IPSec functionality to allow IPSec-secured traffic through NAT on Windows 2000 and Windows XP.

Port Filters and Protocol Filters
Improper configuration of IPSec filters on protocols, ports, or IP addresses may cause communications to fail or be unsecured. Windows Server 2003 provides several tools that assist you in determining the cause of these problems:

- RSoP in logging mode enables you to determine IPSec policy assignments. Simply navigate to the IP Security Policies subnode in the RSoP snap-in. Information displayed includes settings such as filter rules, filter actions, tunnel endpoints, authentication methods, and so on.
- You can use the IP Security Monitor snap-in to view the generic and specific filters that are in effect. You can search for all matches to a filter of a given type. To locate a filter, see To find a matching filter.
- Ensure that the correct filter has been selected from the IP Filter List tab of the Edit Rule Properties dialog box for the IP security rule in effect. Also ensure that the source and destination ports and addresses are properly specified; in particular, ensure that they have not been reversed.

Firewalls and Routers
If you are using Internet Security and Acceleration Server (ISA) 2000 or 2004 as a firewall and network address translator, you can configure IPSec for securing traffic between the internal computers and the ISA server. The following are some suggestions for troubleshooting communications failures:

- Use the Oakley logs to obtain information on the IPSec security association negotiation procedure.
- Use Network Monitor to gather details on the network traffic being sent during authentication and data transfer.
- Ensure that the firewall allows the forwarding of L2TP/IPSec traffic. In particular, you need to ensure that protocol ID 51 is allowed for AH traffic, and protocol ID 50 for ESP traffic. In addition, UDP port 500 must be open for inbound and outbound IKE traffic.

Troubleshooting IPSec Certificates

Recall that certificate-based authentication is useful for IPSec communication to untrusted domains and communications involving pre-Windows 2000 computers. The following are several IPSec certificate troubleshooting hints:

- Enterprise trust policies govern the use of external certificates for validating IPSec authentication. These policies, which are specified in an appropriate GPO, include certificate trust lists that establish your company's trust of external CAs.
- Use RSoP in logging mode to confirm the proper application of a GPO that includes an enterprise trust policy.
- As we mention later in this exam manual, applications such as IPSec use the certificate revocation list (CRL) to check certificate validity. By default, IPSec fails certificate validation only if the certificate is explicitly mentioned in the CRL. It ignores other problems such as a missing CRL. To ensure that it always checks for a valid CRL, open a command prompt and type **netsh ipsec dynamic set config strongcrlcheck value=2**.

- For more information on configuring enterprise trust policies and use of strong CRL checking related to IPSec, refer to Troubleshooting Certificate Status and Revocation.

Planning and Implementing Security for Wireless Networks

Wireless networks are becoming more important as they provide enhanced mobility and ease of connection for users who need to access networks and the Internet from diverse locations. Current wireless networks operate under the specifications of the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards, under which the following three sets of specifications are defined:

- *802.11b* – Uses a frequency of 2.4GHz to transmit data at a maximum bandwidth of 11Mbps. This is the original 802.11 standard.
- *802.11a* – Uses a frequency of 5.0GHz to transmit data at up to 54Mbps.
- *802.11g* – Provides backward compatibility with 802.11b by using a frequency of 2.4GHz to transmit data at up to 54Mbps.

The following two types of wireless networks are available and supported:

- *Ad hoc* – Refers to a direct wireless connection between two computers equipped with wireless network interface cards (NICs).
- *Infrastructure* – Refers to a wireless network containing an access point connected to a regular LAN.

Planning the Authentication Methods for a Wireless Network

Windows Server 2003 supports the following wireless authentication methods:

- *Open system authentication* – Any wireless device can connect to an access point, provided that they know the correct service set identifier (SSID) and wired equivalent privacy (WEP) key. You should use an additional authentication mechanism, such as 802.1x, in conjunction with this method to provide proper security.
- *Shared key authentication* – A wireless device can connect to the network by providing an alphanumeric character string known as a shared key or shared secret. This method is vulnerable to interception of the key by an intruder.
- *802.1x authentication* – Uses Extensible Authentication Protocol (EAP) to authenticate to a server such as a Remote Authentication Dial-In User Service (RADIUS) server. This provides a secure authentication method; however, it is vulnerable to man-in-the-middle attacks. To improve security, you should use this method together with a version of EAP that provides mutual authentication. The following versions of EAP are suitable for this purpose (see Understanding 802.1x authentication for wireless networks for more information):
    - *EAP-TLS* – Uses EAP in conjunction with Transport Layer Security (TLS) to provide certificate-based mutual authentication and encrypted key determination from the client to the authenticating server.
    - *EAP-MS-CHAP v.2* – Provides password-based user or computer authentication, in which both the server and client must know the password for authentication to be successful.

  - *EAP-PEAP* – Protected EAP (PEAP) provides a dedicated encryption channel, dynamic keying material generated from TLS, fast reconnection when roaming between access points, and server authentication that can protect against the use of unauthorized wireless access points.

Planning the Encryption Methods for a Wireless Network

When a user has been authenticated to a wireless network, she can send and receive data on the network as though she were wired directly to the network. At the same time, an intruder could intercept these transmissions without anyone on the network being aware of such an intrusion. Microsoft provides several methods of encrypting traffic being sent across a wireless network (WLAN):

- Wired Equivalent Privacy (WEP) – This is a basic form of encryption that uses a shared secret key and symmetrical encryption algorithm. The strongest available form of WEP uses 128-bit encryption. Despite this encryption strength, WEP is vulnerable to attack because attackers could compromise the shared secret as the RC4 encryption algorithm possesses a weakness that enables attackers to crack keys.
- 802.1x – Not to be confused with 802.11x, this is a port-based form of network access control that uses one of the EAP authentication protocols mentioned previously for authenticating the user and encrypting both the authentication and data transmission components. It provides stronger authentication and encryption levels than WEP. Use of 802.1x requires that the following components are present:
  - *Supplicant* – The 802.1x client that needs access to the network
  - *Authenticator* – The wireless access point to which the client connects
  - *Authentication server* – A RADIUS server such as Microsoft IAS that authenticates the client

Planning Wireless Access Policies

Group Policy in Windows Server 2003 enables you to control access to your wireless network by configuring a wireless access policy. In a GPO linked to the appropriate Active Directory container, navigate to the Computer Configuration\Windows Settings\Security Settings\Wireless Network (IEEE 802.11) Policies node. From here you can use the Wireless Network Policy Wizard to create a wireless policy. You can configure the following properties for your policy (see *Figure 18*):

- *Check for policy changes every* – Defines the interval at which clients check for policy changes. By default, this is 180 minutes.
- *Networks to access* – You can choose between Ad hoc or Infrastructure networks, or you can choose Any available network (access point preferred).
- *Use Windows to configure wireless network settings for clients* – Enables Windows clients to automatically configure their own wireless settings.
- *Automatically connect to non-preferred networks* – Enables clients to access networks not specified in the Preferred Networks tab. For maximum security, you should not select this option.
- *Preferred Networks tab* – Enables you to define the available networks to which wireless clients are allowed to connect. You can specify network properties and encryption types that will be used.

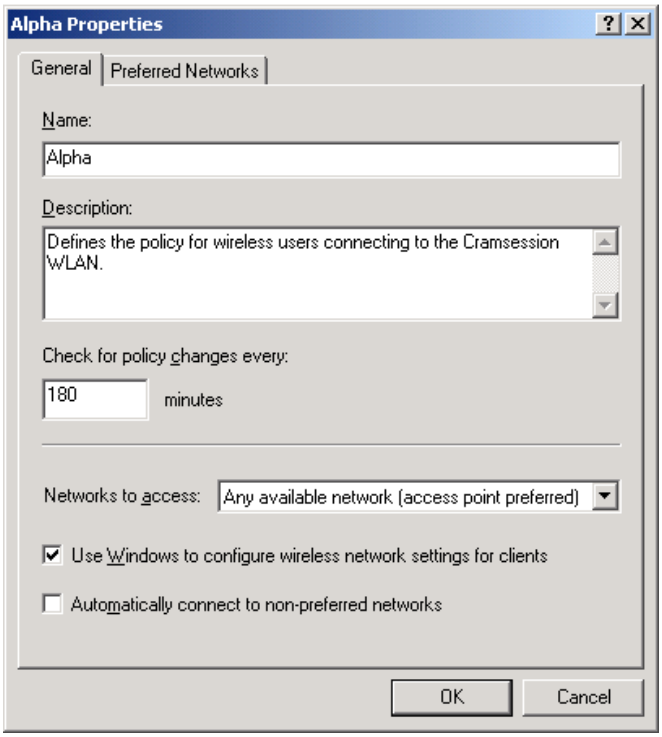


Figure 18 – The General Tab of a Wireless Access Policy Enables You to Configure the Conditions a Client Must Meet to Access Your Wireless Network

Configuring Wireless Encryption

When you have configured a wireless network policy in Group Policy, you can configure the use of WEP or IEEE 802.1x encryption in the policy. On the Preferred Networks tab of the wireless policy's Properties dialog box, click **Add** to create a new policy or **Edit** to edit an existing policy. You can then configure the following:

- Name and description for identifying the wireless network
- *WEP settings*, as follows:
    - *Data encryption (WEP enabled)* – Enables the use of WEP encryption.
    - *Network authentication (Shared mode)* – Enables shared-key authentication. If not selected, open system authentication is used.
    - *This key is provided automatically* – Automatically provides network keys to authenticated clients.
    - *This is a computer-to-computer (ad hoc) network; wireless access points are not used* – When selected, ad hoc networking is the only type of wireless networking used.

- *IEEE 802.1x tab* – Enables you to use IEEE 802.1x authentication and encryption, and provides the following settings (see *Figure 19*):
  - *EAPOL-Start message* - Determines whether Extensible Authentication Protocol over LAN (EAPOL) messages are transmitted, how they are sent, and time parameters for sending EAPOL messages.
  - *EAP type* – Specify **Smart Card or Protected EAP (PEAP)**, and click **Settings** to specify the settings with either EAP type.
  - *Authenticate as guest when user or computer information is unavailable* – Enables client computers to attempt authentication to the network when information is not available. You should leave this setting cleared.
  - *Authenticate as computer when computer information is available* – Enables client computers to attempt authentication to the network if a user is not logged on. You can select the computer authentication option to be used: **With user authentication**, **With user re-authentication**, or **Computer only**.

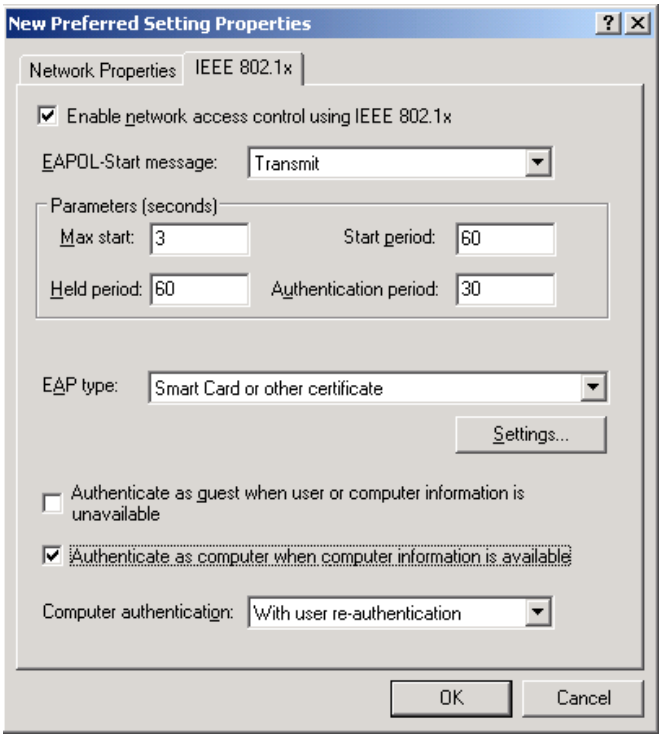


Figure 19 – The IEEE 802.1x Tab Provides Options for Configuring 802.1x Authentication and Encryption

Installing and Configuring Client Computer Wireless Support

Wireless network configuration depends on the operating system installed on the client computer. Computers running Windows XP or Windows Server 2003 support Wireless Zero Configuration, which enables these computers to automatically connect to available wireless networks. You need to manually configure computers running Windows 2000 for wireless networking.

Wireless Zero Configuration
A computer that is enabled for Wireless Zero Configuration scans for any available wireless access points and automatically configures the appropriate settings for access points that are found. It enables ad hoc networking if it does not find a wireless access point.

If you need to modify Wireless Zero Configuration settings, access the Wireless Networks tab of the connection's Properties dialog box in the Network Connections folder. From this tab you can configure the following:

- Available and preferred networks and their properties
- New wireless networks including the network name (SSID), WEP settings, and ad hoc or infrastructure modes
- The order with which the computer will attempt to make automatic connections

Manual Configuration of 802.1x Authentication
You can enable and configure the use of 802.1x authentication from the Authentication tab of the connection's Properties dialog box. The following are several available properties that you can configure:

- Use of a smart card or registry-based certificate for authentication
- Use of a smart card that has a different name from the user name of the logged-on user
- Use of IEEE 802.1x together with PEAP and MS-CHAP v2
- Validation of a server certificate including the domain to which the server belongs and its trusted root certification authority
- The previously described **Authenticate as guest when user or computer information is unavailable** and **Authenticate as computer when computer information is available** options

Deploying, Managing, and Configuring SSL Certificates

Secure Sockets Layer (SSL) is the protocol used for creating encrypted connections between Web servers and client browsers across the Internet for purposes such as the secure exchange of confidential information such as credit card data. It uses the HTTPS protocol and TCP port 443. Benefits of SSL include mutual authentication (the server and client each verify each other's identity), and the integrity and privacy of communications (ensures that no unauthorized user can read or modify the data).
The digital certificate used by SSL contains a pair of keys:

- The public key is freely available to anyone and can be used to encrypt information being sent to the server from a user's browser. The server sends a copy of this key to the user when she connects to a SSL-secured Web page.

- The private key is kept confidential at the server and is used to decrypt information sent from the browser.

Obtaining and Installing SSL Certificates

The Directory Security tab of a Web server's Properties dialog box enables you to obtain, install, and configure SSL certificates. You can obtain a SSL certificate from an external CA such as VeriSign or Thawte, or from an internal, self-signed CA. You use an external CA for all purposes that involve communication with external users such as operation of an e-commerce site, although it is possible to use a self-issued CA for internal communications such as on an intranet Web site. We discuss internal CAs later in this exam manual.

Perform the following steps to obtain a SSL certificate:

1. On the Directory Security tab of the Web site's Properties dialog box, click **Server Certificate**. The Web Server Certificate Wizard starts.
2. Click **Next**, select **Create a New Certificate**, and then click **Next** again.
3. To obtain an external certificate, select **Prepare the request now, but send it later**. To obtain a self-signed certificate, select **Send the request immediately to an online certification authority**.
4. Type a name for the certificate, and select a bit length.
5. Provide the information requested, including company, department, server name, geographical information, and SSL port.
6. If obtaining an external certificate, provide a file name for the certificate request. If obtaining a self-signed certificate, verify the name of the local CA.
7. Click **Finish** to complete the wizard. If obtaining an external certificate, you can now send the certificate request file to the CA. If obtaining a self-signed certificate, it is automatically installed on your server.
8. If you are obtaining an external certificate, run the Web Server Certificate Wizard again after you receive the certificate. It will ask for the media containing the certificate and then install it.

When you have successfully installed a SSL certificate, you can perform the following tasks:

- *View the certificate* – Click **View certificate** to see information about the certificate. The General tab informs you of the purpose, issuing, and validity of the certificate and its private key.
- *Configure secure communications properties* – Click **Edit** to display the Secure Communications dialog box shown in *Figure 20*. From this dialog box you can select **Require secure channel (SSL)** to specify that only encrypted communications can take place with this server. You can also configure the following properties:
    - *Require 128-bit encryption* – Both the server and client must utilize this encryption level.
    - *Client certificates* – You can choose to ignore, accept, or require client certificates. If you choose the latter, users without a valid client certificate will be denied access.
    - *Enable client certificate mapping* – Enables you to configure one-to-one or many-to-one mapping of certificates to Windows user accounts.
    - *Enable certificate trust list* – This is a predefined list of CAs from which certificates can be accepted.

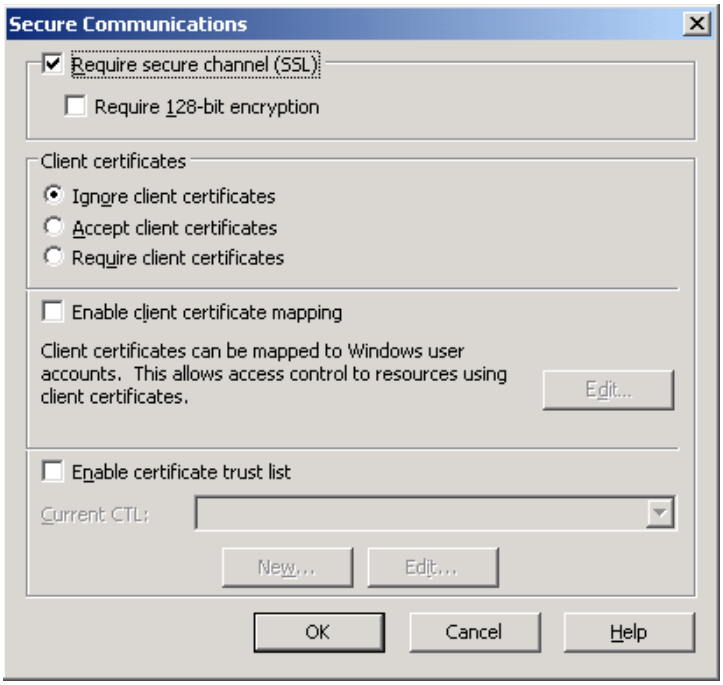


Figure 20 – The Secure Communications Dialog Box Enables You to Configure SSL Properties

Renewing Certificates

- Certificates have an expiry date, which you can view on the General tab or the Details tab after clicking **View certificate**.
- To renew a SSL certificate, access the Directory Security tab of the Web site's Properties dialog box and click **Server certificate**. The Web Server Certificate Wizard provides a choice for renewing certificates.

Configuring SSL to Secure Communications Channels

- You can use SSL as an alternative to IPSec for securing communications between Web servers and SQL servers. Use the Certificate Request Web pages to request a server authentication certificate for the SQL server. After receiving and installing the certificate, you can use the Certificates snap-in to verify that the certificate has been installed in the Personal certificate store. From the Certificates snap-in, you can also start the Certificate Request Wizard from the Personal certificate store (right-click this store and choose **All Tasks > Request New Certificate**. Then choose the **Computer** certificate type.) After you have done this, you can either force all clients to use SSL or allow them to choose whether to use SSL.

- Active Directory in Windows 2000 or Windows Server 2003 provides for the use of SSL over LDAP for securing communications with domain controllers. You can enable this by installing an enterprise CA on a domain controller. When you do this all domain controllers in the forest automatically enroll for and install the required certificates. You can also configure a policy in a GPO linked to the Domain Controllers OU that enables domain controllers to automatically receive certificates from an enterprise CA.
- You can use SSL to secure communications between e-mail servers and client computers. Exchange Server 2000 and 2003 use TLS for securing communications, and you can configure security for Simple Mail Transport Protocol (SMTP), Internet Mail Access Protocol 4 (IMAP4), Post Office Protocol 3 (POP3), and Outlook Web Access (OWA).
- You can use SSL to secure communications with SUS servers.

Configuring Security for Remote Access Users

Configuring Authentication for Secure Remote Access

Routing and Remote Access (RRAS) in Windows Server 2003 supports a series of authentication protocols for securely transmitting credentials of users making remote access connections.

- *Password Authentication Protocol (PAP)* - Sends credentials in clear text to the RRAS server. This method is not secure and should be used only if no other protocol is suitable.
- *Challenge Handshake Authentication Protocol (CHAP)* - Sends a challenge message to the client that is encrypted with MD5. The client can decrypt this message only if it knows the proper password. It then uses a hash algorithm to compare hashes with the client and server to complete authentication. However, CHAP uses a reversibly encrypted password, which is vulnerable to cracking. You can use CHAP to authenticate non-Microsoft client computers.
- *Microsoft CHAP (MS-CHAP) versions 1 and 2* - Use the same mechanism as CHAP but do not use the reversibly encrypted password. This allows MS-CHAP to be used with Microsoft Point-to-Point Encryption (MPPE) and Point-to-Point Tunneling Protocol (PPTP). Only Microsoft client computers support MS-CHAP.
- *Extensible Authentication Protocol (EAP)* - Uses authentication mechanisms of arbitrary lengths for validating a Point-to-Point Protocol (PPP) connection. Two types of EAP are available:
    - EAP-MD5 uses a challenge-response mechanism similar to that of CHAP, but sends the challenges and responses as EAP messages. It uses the MD5 algorithm for encrypting user names and passwords.
    - EAP-TLS uses certificate-based authentication to provide the strongest method of authentication, data encryption, and key exchange. It is the only protocol that supports smart card authentication.
- The process of multifactor authentication refers to the use of more than one authentication method at the same time. For example, smart card authentication is a form of multifactor authentication because it uses two items: the smart card (something you have) and its associated PIN (something you know). Other forms of authentication that can be used as a component of multifactor authentication include various types of biometric authentication (something you are) such as fingerprints or retinal scans.

Configuring and Troubleshooting VPN Protocols

A virtual private network (VPN) creates a secure tunneled connection from a remote client computer to a RRAS server across an insecure medium such as the Internet to. It can use either of the following two protocols:

- *Point-to-Point Tunneling Protocol (PPTP)* – Encapsulates data across an IP-based network without header compression or tunnel authentication. Using built-in MPPE encryption, PPTP can be used by all Windows clients.
- *Layer Two Tunneling Protocol (L2TP)* – Encapsulates data across IP, frame relay, X.25, or Asynchronous Transport Mode (ATM) networks. L2TP uses header compression and tunnel authentication, and does not provide encryption by itself (it works with IPSec encryption). It can be used by Windows 2000 and later clients only.

You can configure a Windows Server 2003 computer to act as a VPN server from the Routing and Remote Access snap-in. Right-click the server and select **Configure and Enable Routing and Remote Access**. The Routing and Remote Access Server Setup Wizard starts, which guides you through the process.
You should be aware of the following considerations when configuring and troubleshooting VPNs:

- *Internet service providers (ISPs)* – Use of an ISP simplifies the creation of a connection to the Internet. At the same time, however, the ISP becomes a component of your VPN connection, and configuration problems at the ISP end can create problems with your VPN. You should inform the ISP of your intent to operate a VPN across their setup.
- *Client operating systems* – As stated previously, any Windows client computer can use PPTP to access the VPN, but only Windows 2000/XP/Server 2003 computers can use L2TP/IPSec without additional configuration. Microsoft provides the L2TP/IPSec VPN client, which enables computers running Windows 98/Me/NT 4.0 to access a VPN using L2TP/IPSec.
- *Network address translation devices* - NAT enables you to use a private IP address range on your internal network. It translates public IP addresses used for Internet connection to the private addresses used internally. However, problems can occur with certain combinations of tunneling protocols and server operating systems:
    - *PPTP* – Using its built-in MPPE encryption, PPTP can interoperate properly with NAT servers running any Windows server operating system.
    - *L2TP* – When used with IPSec encryption, Microsoft VPN servers prior to Windows Server 2003 think that packets crossing the NAT device have been improperly modified; therefore these packets are dropped. Windows Server 2003 uses NAT-T, which enables VPN packets to pass through the NAT device.
- *Routing and Remote Access servers* – Support depends on the version of Windows running on the server. While Windows Server 2003 supports all PPTP and L2TP functionality, Windows 2000 Server supports all functions except NAT-T. Windows NT 4.0 Server supports PPTP but not L2TP.
- *Firewall servers* – These protect your network by filtering traffic attempting to access it, generally by the ports specified on the packets. You should ensure that the proper ports are open so that VPN traffic can reach your network, as follows:
    - PPTP traffic requires TCP port 1723. It also uses IP protocol ID 47 Generic Routing Encapsulation (GRE) for creating the VPN.

- L2TP traffic requires UDP port 1701. IPSec negotiation traffic using IKE requires UDP port 500. In addition, AH traffic requires IP protocol ID 50 and ESP traffic requires IP protocol ID 51.

Managing Client Configuration for Remote Access Security

Remote Access Policy

With RRAS in Windows Server 2003 you can configure one or more policies in the RRAS snap-in, and a user attempting to access the network remotely is evaluated according to the conditions of each policy in sequence. Remote access policies consist of three components: conditions, permissions, and profile:

- *Conditions* – As shown in *Figure 21*, conditions represent the attributes that a user's account must meet to satisfy the policy. Click **Add** to view the available attributes and their description. If a user does not meet the conditions of the policy, the next policy in effect (as displayed in the RRAS snap-in) is evaluated until a user meets the policy conditions. If a user does not meet the conditions of any available policy, he is denied access (implicit denial).

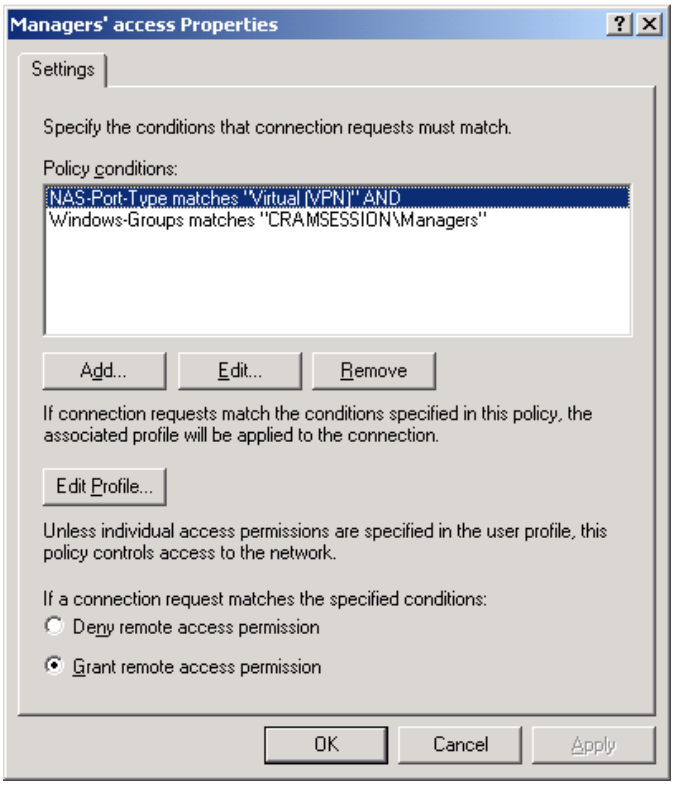


Figure 21 – The Conditions Specified in a Remote Access Policy's Properties Dialog Box Determine Whether a User Is Granted Remote Access to the Network

- *Permission* – The user account's Properties dialog box in Active Directory Users and Computers or Local Users and Groups contains a Dial-in tab that specifies his remote access permission. Available settings are:
    - *Allow access* – Allows access after the user has met the policy conditions
    - *Deny access* – Always denies the user remote access.
    - *Control access through Remote Access Policy* – Available only when the domain functional level is set to Windows 2000 native or higher, this option causes the user's remote access privileges to be evaluated against the policy profile before he is granted access.
- *Profile* – Each remote access policy can contain a further series of conditions that must be met before access is granted if a user's access permission is set to **Control access through Remote Access Policy**. Each profile contains the following components:
    - *Dial-in Constraints* – Contains dial-in conditions such as session and idle time limits, phone number restrictions, and media restrictions
    - *IP* – Contains IP address, input filter, and output filter restrictions
    - *Multilink* – Enables multilink (use of more than one phone line to increase available bandwidth)
    - *Authentication* – Specifies available authentication methods
    - *Encryption* – Specifies MPPE encryption strengths (40, 56, or 128-bit)
    - *Advanced* – Enables you to choose from a large number of additional attributes

Connection Manager Administration Kit (CMAK)

CMAK is a connection management utility that is included with Windows Server 2003. You can use CMAK to perform such tasks as distributing service profiles to remote clients, sending update information such as phone book lists for dialing to ISPs or branch offices to remote clients, and updating information to large numbers of remote clients. The following are some of the more important features that you can configure using CMAK:

- Phone book information, such as access numbers, used for VPN connection
- Dial-up networking entries including TCP/IP configuration information and basic and advanced security settings
- Routing table updates that define specific routes for network traffic accessing the VPN server
- Automatic configuration of Internet Explorer settings for a proxy server
- Custom actions such as programs that run automatically before, during, or after connection to the VPN
- Logon and phone book bitmaps and icons displayed to the user when connecting
- Notification area shortcut menu commands
- Help files and support information available to users
- License agreements and additional files used by the service profile

Planning, Configuring, and Troubleshooting Authentication, Authorization, and PKI

A *public key infrastructure* (PKI) is a system of certificates and CAs designed to verify the authenticity of entities including users, computers, and entire companies accessing resources or doing business across networks including the Internet.

Planning and Configuring Authentication

Ensuring proper authentication is in place is critical to the security of your network. For an introduction to the various types of authentication and tips on hardening user logons locally, wirelessly, by means of remote access, and at Web servers, refer to Learning Guide: Authentication.

Planning, Configuring, and Troubleshooting Trust Relationships

- You can establish a trust relationship to enable access to resources in one domain by users from a second domain. In a one-way trust relationship, the trusting domain makes its resources available for users in the trusted domain. A two-way trust relationship is simply the sum of two one-way trusts in opposite directions.
- By default, all domains in an Active Directory forest trust each other with a two-way transitive trust relationship. In other words, each domain makes its resources available to all other domains in the forest, and vice versa.
- No default trust relationships exist between domains in different forests. Active Directory enables you to create the following types of trust relationships between domains in different forests:
    - External trusts are individual one-way trust relationships set up between specific domains in two separate forests. External trusts can also involve Windows NT 4.0 domains and Kerberos realms (in the latter case, these trusts are known as realm trusts).
    - Forest trusts involve complete trust relationships between all domains in the forests involved, thereby enabling complete resource sharing throughout these forests. You can create forest trusts only between forests that are operating at the Windows Server 2003 forest functional level.
- A shortcut trust is an additional trust relationship between child domains within a forest. Such a trust provides a shortened authentication path for a user in one domain accessing a resource in another domain.
- You use the Active Directory Domains and Trusts console to manage trusts in Windows Server 2003. The Trusts tab of a domain's Properties dialog box (see *Figure 22*) provides information on all existing trust relationships and allows you to configure properties of these trust relationships.
- Click **New Trust** to access the **New Trust Wizard**, which helps you create all available types of trust relationships.
- After you have created a trust, the trust's Properties dialog box enables you to perform actions such as validating the trust relationship, changing its authentication scope (domain-wide or selective), and configure name suffix routing in forest trust relationships.

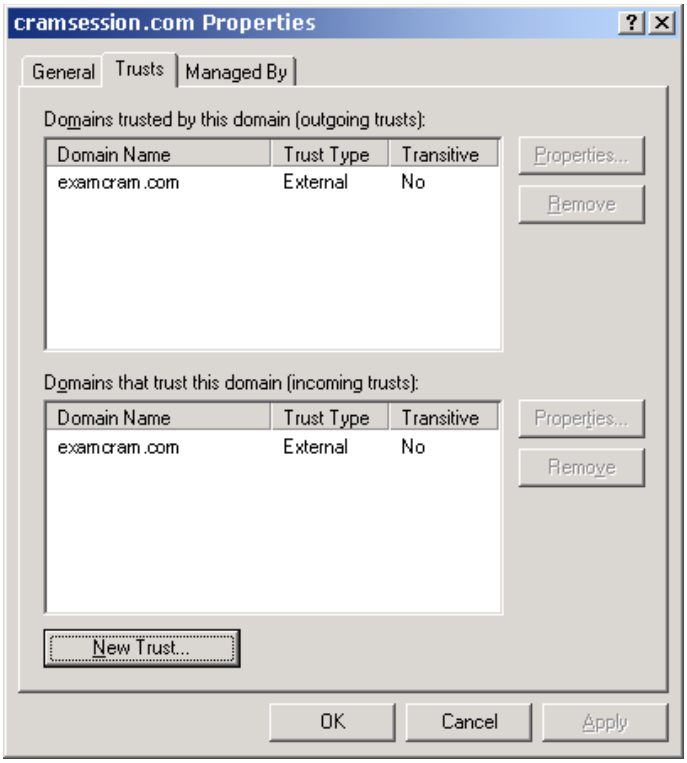


Figure 22 – You can Manage Trusts from the Trusts Tab of a Domain's Properties Dialog Box

Planning and Configuring Authentication Protocols

- By default, Active Directory in Windows 2000 and Windows Server 2003 uses the Kerberos V5 authentication protocol, which can be used with passwords or smart cards for logon. This protocol provides for mutual authentication, which verifies the identity of the server to which the user logs on, as well as the user herself.
- Active Directory also enables the LAN Manager (LM), NT LAN Manager (NTLM), and NTLMv2 protocols for authentications involving pre-Windows 2000 computers. This includes users on Windows 2000/XP Professional computers authenticating to a Windows NT 4.0 domain controller or users on Windows 9x or NT 4.0 Workstation computers authenticating to Windows 2000 or Windows Server 2003 domain controllers. Computers running Windows NT 4.0 SP4 and later can use NTLMv2, while earlier computers use the original version of NTLM. Windows 9x computers use LM for authentication.
- Group Policy provides the Network security: LAN Manager Authentication Level policy (see *Figure 23*), which defines the acceptable types of LM and NTLM responses. This policy is found in the Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options node.

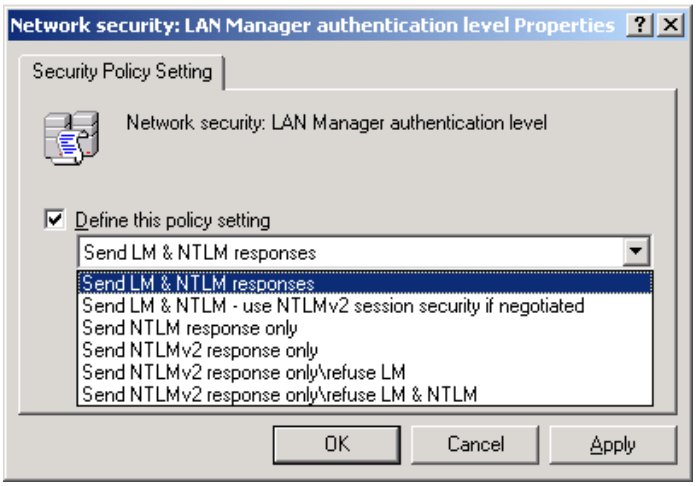


Figure 23 – The LAN Manager Authentication Level Policy Provides Six Levels of NTLM Authentication that Are Accepted for Logon to Active Directory

- Group Policy also provides the Do Not Store LAN Manager Hash Value on Next Password Change policy, which prevents the storage of the relatively weak LM hash value. You should enable this policy except when this hash value is needed for authenticating Windows 9x computers.

Planning and Configuring Multifactor Authentication

The traditional method of user name and password can be cracked using sniffing tools and password cracking programs. The concept of multifactor authentication attempts to reduce the risk of unauthorized users gaining access to the network. It refers to the use of more than one type of authentication together. The following types of authentication factors can be combined:

- *Something you have* – For example, a smart card or token
- *Something you know* – For example, the personal identification number (PIN) associated with the smart card
- *Something you are* – For example, retinal or fingerprint scans

The combination of smart cards and their associated PINs is the most common type of multifactor authentication currently in use. Planning smart card deployment involves selecting and obtaining smart card hardware, setting up a Microsoft PKI, and enrolling users for smart card certificates. Certificate Services provides the Smartcard Logon and Smartcard User certificate templates for this purpose. For more details, see Smart Card Deployment Planning Considerations.

Active Directory allows you to require that users employ smart cards for logon. In Active Directory Users and Computers, select the required users, right-click, and select Properties. In the Properties On Multiple Objects dialog box, select the Smart card is required for interactive logon option, as shown in *Figure 24*.

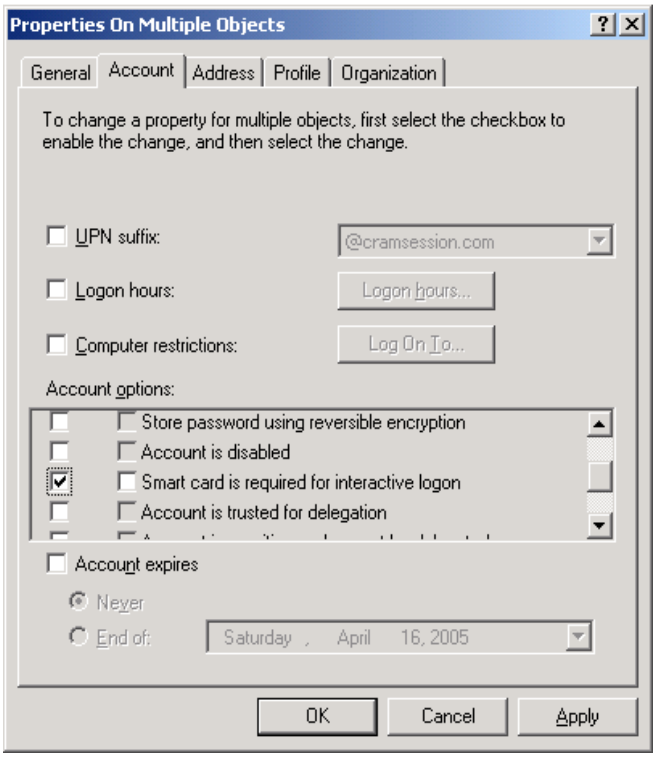


Figure 24 – Requiring Multiple Users to Use Smart Cards for Logon

Planning and Configuring Authentication for Web Users

Users can be authenticated to Web sites hosted on IIS by any of several available authentication methods. You can configure Web authentication in IIS by accessing the Directory Security tab of the Web site's Properties dialog box and clicking **Edit** in the **Authentication and Access Control** section of this tab. This opens the **Authentication Methods** dialog box shown in *Figure 25*, which enables the use of the following authentication methods:

- *Anonymous access* – Used by anyone that accesses a Web site without supplying a user name or password, this method uses a default local user account on the IIS server for access.
- *Basic* – Users log on to the Web site using a user name and password stored in the local user accounts database. This method is not secure because it passes the user name and password in clear text.
- *Digest* – Users log on to the Web site using a user name and password stored in Active Directory. This method protects the password by sending a hash value. The IIS server must be a domain member with access to a domain controller containing the Active Directory database.
- *Integrated Windows* – Uses NTLM or Kerberos to authenticate users to a domain account in Active Directory. When NTLM is used, passwords are sent by means of a hash value; when Kerberos is used, the Kerberos session ticket is passed.

- *.NET Passport* – Uses the .NET Framework to provide a single sign-on experience for authentication to e-commerce and other Web sites. Usernames and passwords are not stored on the IIS or Active Directory servers, but are hosted by a .NET central authentication server. However, it is possible to map passport names to accounts in Active Directory.

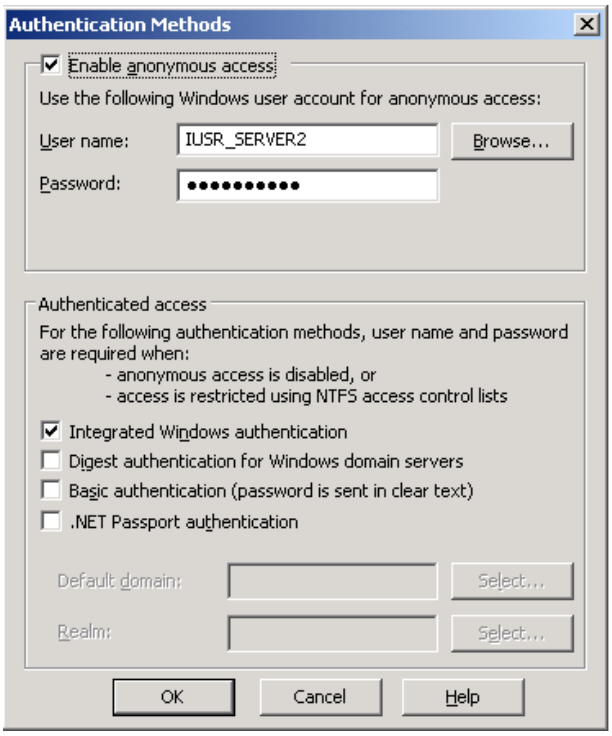


Figure 25 – The Authentication Methods Dialog Box in IIS Provides Several Authentication Choices

Planning and Configuring Delegated Authentication

Delegated authentication refers to the act of enabling a trusted network service to assume the identity of the user in order to connect to a second network service on the request of the user. An example is a situation in which a Web service needs to access a database server on behalf of a user. Delegated authentication requires that the Kerberos V5 authentication protocol be in use.
You can enable delegated authentication for users or computers from Active Directory Users and Computers, as follows:

- To enable delegated authentication for a computer, access the General tab of the computer's Properties dialog box and select the **Trust this computer for delegation** check box. You are warned that this is a security-sensitive operation. Click **OK** to accept this warning. A situation requiring this is the use of EFS to secure files redirected to a remote server, in which case the remote server needs to be trusted for delegation.

- To enable delegated authentication for a user, access the **Account** tab of the user's Properties dialog box. In the Account Options section, select the **Account is trusted for delegation** check box.

Planning Group Structure

Windows Server 2003, like previous Windows versions, includes the concept of groups to enable you to collect users with similar resource needs together, and thereby simplify the task of controlling access to resources such as files, folders, printers, and so on.

Deciding Which Types of Groups to Use

Active Directory in Windows Server 2003 provides the following two group types:

- *Security* – These groups have a security identifier (SID) associated with them, which enables them to be used for all security contexts such as assigning user rights or permissions to resources in Active Directory. You can also use security groups in non-security contexts such as email distribution.
- *Distribution* – These groups are designed for purposes such as email distribution lists, which do not require the assignment of security permissions. They do not have a SID associated with them, and cannot be assigned permissions.

Planning Security Group Scope

Active Directory in Windows Server 2003 provides the following three group scopes:

- *Universal* – These groups exist across multiple domains within a single forest. They can contain users or groups from anywhere in the forest, and can be assigned permissions to objects in any domain in the forest. They are available only if the domain functional level is set to Windows 2000 native or higher.
- *Global* – These groups exist within a domain and can contain users and groups from the domain in which they are created. You can assign permissions to resources in any domain in the forest.
- *Domain local* – These groups exist within a domain and can contain users and groups from any domain in the forest, and can be assigned permissions to objects within the domain in which they are created only.

Planning Nested Group Structure

The practice of nesting groups refers to adding groups as members of other groups. This enables you to simplify the granting of permissions by reducing the number of times you need to assign permissions. The extent of group nesting depends on the functional level at which the domain is operating. The Windows 2000 mixed domain functional level, which allows Windows NT 4.0 backup domain controllers to be present, allows only the extent of group nesting available with Windows NT: you can add global groups to domain local groups only.

When operating at the Windows 2000 native or Windows Server 2003 domain functional levels, enhanced group nesting is available. Table 1 describes the extent of group nesting possible.

Property	**Universal**	**Global**	**Domain Local**
Users that can be a member of the group	Users from any domain	Only users that belong to the domain in which the group resides	Users from any domain
Groups that can be nested into this group	Universal and global groups from any domain	Only global groups from the same domain	Universal and global groups from any domain, and domain local groups from the same domain
Groups into which this group can be nested	Universal groups and domain local groups in any domain	Universal and domain local groups from any domain, and global groups from the same domain	Only domain local groups from the same domain
Allowed resource access	Resources in any domain in the forest	Resources in any domain in the forest	Resources in the domain in which it exists

Table 1 - Group Nesting

Best practices recommend that you minimize the extent of group nesting within your enterprise. More specifically, you should follow the AGDLP rule, which states:

- Place accounts (A) into global groups (G).
- Add global groups to domain local groups (DL).
- Assign permissions (P) to domain local groups.

In a multiple domain forest, this rule is modified to AGUDLP, in which you add global groups to universal groups (U), and then add universal groups to domain local groups for permissions assignment. In particular, you should ensure that the membership of universal groups does not change frequently. You can accomplish this by never adding users directly to universal groups, but following the recommendation of adding global groups to universal groups instead. Each time the membership of a universal group changes, this change must be replicated to all global catalog servers in the forest, resulting in considerable bandwidth utilization in all but the smallest forests.

Planning and Configuring Authorization

Once a user has been authenticated and his group membership determined, he needs to have access to the resources he requires to perform his job tasks. This is the subject of authorization. Also involved is the assignment of user rights and the need for using digital signatures for verifying his ownership of data he transmits across the network.

Configuring Access Control Lists

Access control lists (ACLs) determine the objects a user is entitled to access, and the types of activities she is entitled to perform on these objects. Every object in Active Directory includes a security descriptor, which includes two types of ACLs that track the object's security information:

- *Discretionary access control lists (DACLs)* – Identify the users and groups that are granted or denied permission to an object. Each DACL contains a series of access control entries (ACEs) that specify the type of user access that is granted or denied.
- *System access control lists (SACLs)* – Identify users and groups that you can audit for successful or failed access to an object. We discussed auditing earlier in this CramSession.

You can configure ACLs from the Security tab of any object's Properties dialog box, also known as the ACL Editor (see *Figure 26*).

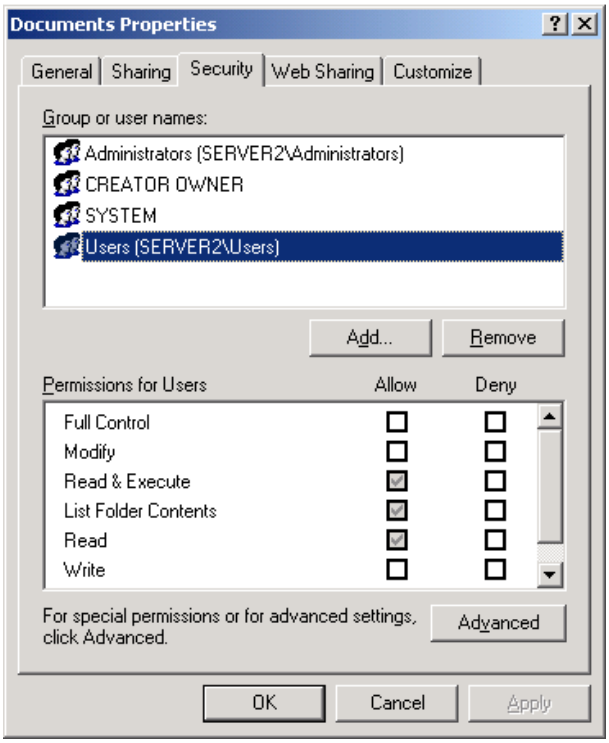


Figure 26 – The Security Tab of an Object's Properties Dialog Box Enables You to Configure its ACL

For information on configuring ACLs, refer to links accessed from Access Control in Active Directory. Keep in mind the following facts:

- The permission granted to a user is the cumulative total of all permissions she receives according to the groups to which she belongs. For example, a user who is member of the Sales and Managers groups receives the Full Control permission on a resource to which the Sales group has received the Read permission and the Managers group has the Full Control permission.
- Explicitly denied permissions (selected in the Deny column) override all allowed permissions. If the user in the previous point has an ACE that specifies Full Control in the Deny column, she receives no access to that object. You should be cautions when assigning specific denials because such denials can cause issues especially with permissions inheritance. Only use denials when absolutely necessary.
- Permissions are inherited from the root of a hierarchy (such as a disk partition) to objects beneath. Inherited permissions are shown by shaded check marks in the ACL editor. You can disable this inheritance from the Advanced Security Settings dialog box, accessible by clicking the **Advanced** button in *Figure 26*.
- Default containers, OUs, and many other Active Directory objects also have ACLs associated with them. To view and edit these ACLs, access the **View** menu in Active Directory Users and Computers and choose **Advanced Features**. The Properties dialog box for most objects contains a Security tab. However, Microsoft recommends that you not change the default permissions on these objects.
- You can use Group Policy and security templates to configure ACLs on a large range of Active Directory objects. We discussed configuring file and registry permissions earlier in this exam manual. For information on the types of actions you can perform, consult Securing Active Directory and links contained therein.
- Use **Xcacls.exe** to view and modify permissions from the command line.

Planning and Troubleshooting the Assignment of User Rights

User rights define what various users and members of groups can and cannot do on the network. The two classes of rights are Privileges and Logon Rights. Refer to User Rights Assignment for a description of all available user rights in Windows Server 2003.

Group Policy enables you to view and modify which groups are assigned various user rights. In the Group Policy Object Editor, access the **Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment** branch, as shown in *Figure 27*. Double-click the required user right, and in its Properties dialog box, select **Define these policy settings**. Add the required users or groups. As discussed earlier in this exam manual, you can also define user rights assignments in security templates, and use these templates to configure Group Policy.

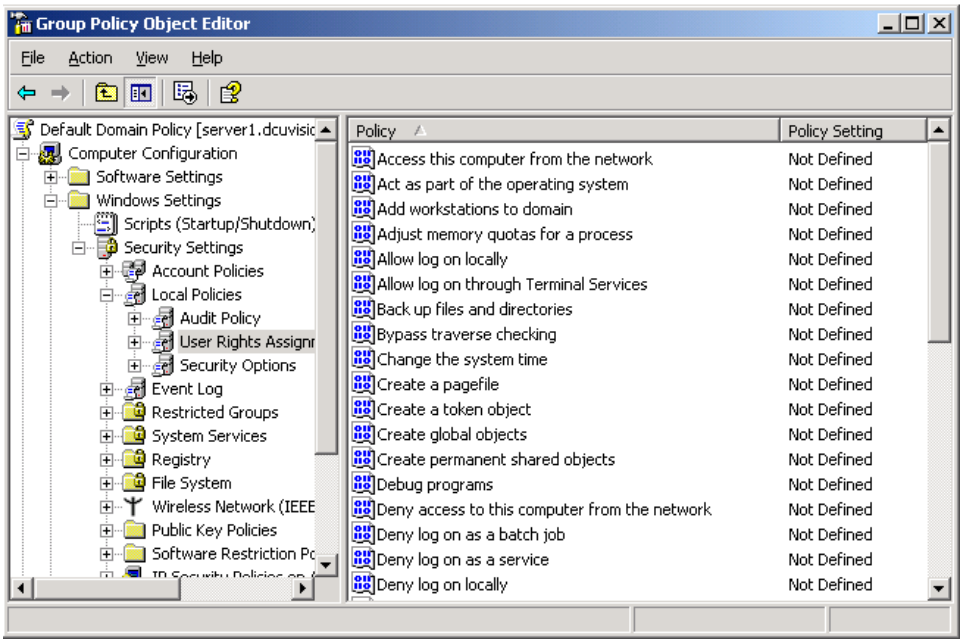


Figure 27 – The User Rights Assignment Branch of the Group Policy Object Editor Enables You to Assign User Rights

Planning Requirements for Digital Signatures

A digital signature is used to address the authentication, integrity, and non-repudiation of the document with which it is associated. In other words, it guarantees that the individual who claims to have sent the document actually sent it, and that it was not modified in transit. In addition, the sender cannot deny later that he actually sent it. Likewise, the digital signature ensures that the data was not sent by an imposter. On the other hand, a digital signature does not address confidentiality because it does not encrypt the message. For additional information on how a digital signature works, refer to Understanding Message Security.

Certificate Services in Windows Server 2003 provides several certificate templates that you can use for digital signature purposes, such as the User, Computer, and Administrator template. Issuing a certificate based on one of these templates enables the user to digitally sign documents.

Several policies available from the Security Options subnode of the Group Policy Object Editor govern the need for digitally signing data on the network:

- *Domain member: Digitally encrypt or sign secure channel data (always)* – Signing or encryption of secure channel traffic is required or the channel will not be established.
- *Domain member: Digitally sign secure channel data (when possible)* – Negotiates signing of secure channel traffic but allows communications if signing is not established.
- *Microsoft network client: Digitally sign communications (if server agrees)* – Requests server message block (SMB) packet signing of network traffic.

- *Microsoft network server: Digitally sign communications (if client agrees)* – The server negotiates SMB packet signing when requested by the client.
- Another two policies similar to the above two policies that state (always) require SMB packet signing and disables communication if signing cannot be negotiated.

Installing, Managing, and Configuring Certificate Services

A public key infrastructure (PKI) is a system of delivering digital certificates that verify the authenticity of an entity (individual, group, organization, etc.). For an overview of the services offered by a PKI, refer to Core PKI Services: Authentication, Integrity, and Confidentiality.

For a comprehensive overview of planning and implementing Certificate Services and PKI in Windows Server 2003, refer to Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure.

Installing and Configuring Certification Authorities

Although you could install Certificate Services on a single Windows Server 2003 computer to create a PKI, it is customary to create a hierarchy of CA servers. You can have either of the following two hierarchies:

- *Two-tier CA hierarchy* – Consists of a root CA that issues certificates to one or more subordinate CAs, which then issue certificates to users or computers requiring them.
- *Three-tier CA hierarchy* – Consists of a root CA that issues certificates to intermediate CAs. These CAs, which are configured as subordinate CAs, issue certificates to issuing CAs, which are subordinate to the intermediate CAs. The issuing CAs issue certificates to the users or computers.

Within each of these hierarchies, it is possible to have two types of CAs:

- *Enterprise CAs* – These are integrated with Active Directory and store their data in the Active Directory database, thereby taking advantage of Active Directory replication and fault tolerance. You need to have Active Directory running on the server on which you install an enterprise CA.
- *Stand-alone CAs* – These are not integrated with Active Directory and store their data locally. One common purpose of a stand-alone CA is to act as a root CA in a hierarchy and be taken offline except when needed to issue certificates to lower-level CA servers. Doing so reduces the chance of compromising the root CA's certificate, which would compromise the validity of all certificates issued by the CA and require their reissue.

Installing Root CAs
The root CA is always the first CA created when you set up a CA hierarchy. You should first install IIS so that the CA can issue certificates from its Certificate Enrollment Web pages. After you have done this, you can install the root CA from the Windows Components Wizard in Control Panel Add or Remove Programs. Perform the following tasks:

1. From the Windows Components Wizard, select **Certificate Services**, and accept the warning that the computer name and domain membership cannot be changed.
2. Select the type of CA required (see *Figure 28*).

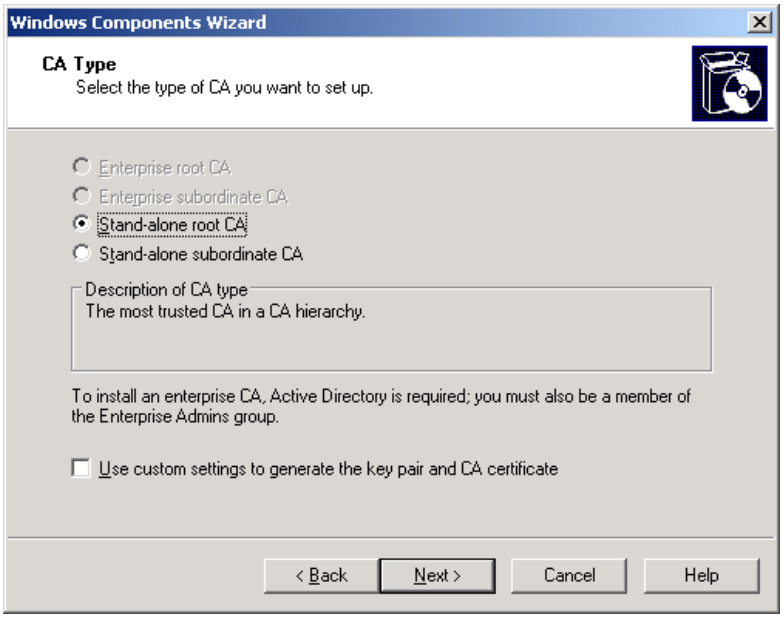


Figure 28 – The CA Type Page Provides a Choice of the Type of CA to be Set Up

3. Enter the required information on the CA Identifying Information page.
4. Accept or provide alternate locations for the certificate database, database log, and shared folder.
5. Click **Yes** to temporarily stop IIS, and insert the Windows Server 2003 CD-ROM.
6. Accept the requirement for enabling Active Server Pages (ASPs).
7. Click **Finish** when the completion page appears.

Installing Intermediate and Issuing CAs

Installing a subordinate CA is similar to that of a root CA; merely select the appropriate option from *Figure 28*. The wizard asks you to provide the name of the parent CA that will issue the certificate to the subordinate CA. In the case of an issuing CA in a three-tier hierarchy, this is the online intermediate CA. Alternately, you can save this request to a file on a floppy disk that you can submit to an offline root CA or a commercial CA.

Configuring Certificate Templates

All certificates issued by a Windows Server CA are based on certificate templates, which contain the rules and settings required for a certificate of a given type. Certificate Services in Windows 2003 supports two types of certificate templates:

- *Version 1 templates* – Initially provided by Windows 2000 Certificate Services, these templates are read-only and can be used on computers running Windows 2000 and later.
- *Version 2 templates* – New to Windows Server 2003, these templates support certificate autoenrollment and can be used on computers running Windows XP and Windows Server 2003 only. They are supported on CAs running Windows Server 2003 Enterprise or Datacenter editions only.

The Certificate Templates snap-in (**Certtmpl.msc**) enables you to perform all template configuration activities. You can duplicate existing templates and configure a large range of properties on existing and duplicated templates. To duplicate a template, right-click it and choose **Duplicate Template**. To configure the properties of any template, right-click it and choose **Properties**. Both actions open the template's Properties dialog box (*Figure 29*), which enables you to configure the following properties:

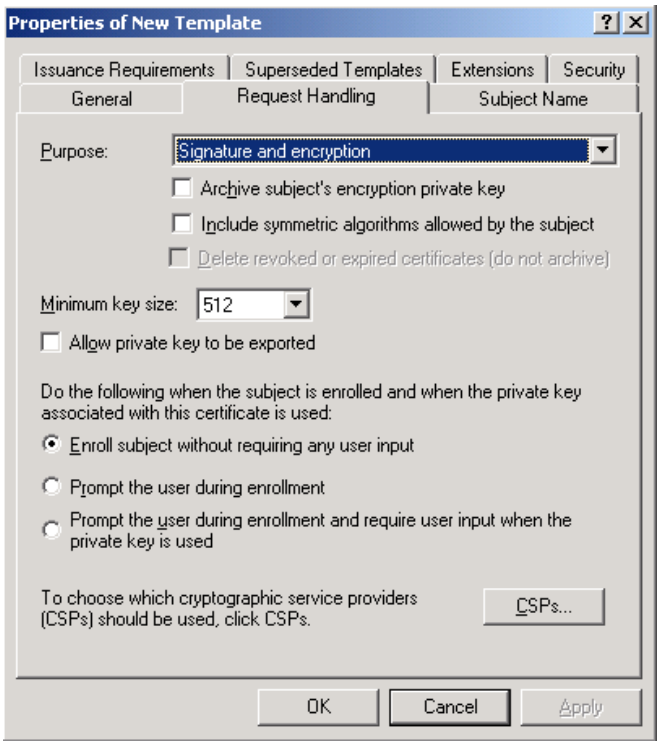


Figure 29 – You can Configure a Large Range of Certificate Properties from a Certificate Template's Properties Dialog Box

- *General tab* – Specifies validity and renewal periods, and publish certificates in Active Directory.
- *Request Handling tab* – Specifies certificate purposes, key size, export of private key, and extent of user input required during certificate enrollment. You can also choose which cryptographic service providers (CSPs) are used in certificate requests.
- *Subject Name tab* – Specifies the format of and the information to be included in the subject name.
- *Issuance Requirements tab* – Specifies requirements such as certificate manager approval and the number of authorized signatures required for certificate issuing.
- *Superseded Templates tab* – Enables you to specify one or more obsolete templates that this template supersedes.

- *Extensions tab* – Specifies the extensions included in the template and enables you to modify these extensions or add application policies that define how the certificate can be used.
- *Security tab* – Enables you to configure permissions for the template. You should note in particular that users that need to autoenroll for certificates need the Read, Enroll, and Autoenroll permissions.

Configuring, Managing, and Troubleshooting Certificate Revocation Lists

It may be necessary to revoke a certificate before its expiry date for a variety of reasons such as compromise of a certificate or resignation of an employee to which the certificate has been issued. When a certificate is revoked, it is published in a certificate revocation list (CRL), which informs services or applications that the certificate is no longer valid.

The following types of CRLs are available in Windows Server 2003:

- *Full* – Provide details about all certificates that have been revoked.
- *Delta* – Provide details about certificates that have been revoked since the previous full CRL was published. A delta CRL is shorter in length and can be published at more frequent intervals than a full CRL without use of excessive network bandwidth and processing power.

Information on all revoked certificates is displayed in the details pane of the Certification Authority snap-in when you select the **Revoked Certificates** node. To configure and manage CRLs, right-click this node and choose **Properties**. The **Revoked Certificate Properties** dialog box opens, which enables you to configure the publication intervals of full and delta CRLs. By default, these are 1 week and 1 day, respectively.

For more information on managing certificate revocation, consult the links provided in Manage certificate revocation.

Troubleshooting Certificate Revocation

When an application or service checks a CRL, it must be able to locate the CRL or it cannot authenticate the certificate holder. You may need to troubleshoot one or more of the following CRL problems:

- *Outdated CRLs* – Changes made to CRLs are not reflected in the context of an application until a cached CRL or delta CRL expires. For up-to-date information on revoked certificates to be available, choose a short delta CRL publication interval.
- *Unavailable CRLs* – Ensure that copies of the CRLs are published to locations (files or URLs) accessible to applications that require them. In addition, ensure that all CRLs in a CA hierarchy are accessible, in particular those published by an offline root CA.
- *Moved CRLs* – Information on the location of a moved CRL is not added to certificates published before the move. Do not move a CRL unless absolutely necessary.

For more information on additional certificate revocation problems and their troubleshooting, consult Troubleshooting Certificate Status and Revocation.

Configuring Key Archival and Recovery

Windows Server 2003 enables you to archive the private key associated with a certificate, so that you can recover it later should it be lost. Key archival involves storing the private keys in a secure database. Key recovery involves retrieval of the encrypted certificate and private key and submission of a request to the CA by a key recovery agent that possesses a key recovery agent certificate from the CA.

The process of key archival and recovery involves the following steps:

1. Create a key recovery agent account. This involves configuring the key recovery agent certificate template with permissions for the recovery agent.
2. Acquire the certificate. This involves creating a console containing the Certificates snap-in and running the Certificate Request Wizard to request a key recovery agent certificate. You can also use the Certificate Enrollment Web pages to request this certificate by selecting the **Advanced certificate request** option and specifying the **Key Recovery Agent** template.
3. Configure the CA for key recovery. This involves configuring the recovery agent with the key recovery agent certificate from the Certificates console focused on the computer from which key recovery will be performed.
4. Use the **Certificate Templates** snap-in to create a new certificate template that provides for key archival.
5. Use the **Certification Authority** snap-in to enable the issuance of a certificate based on this template, and then use the Certificate Request Wizard to request the certificate and install it in the Personal certificate store.
6. Use **Certutil.exe** to perform the key recovery into a BLOB output file that contains the certificate chain and its associated private key, and then recover the original public/private key pair.
7. Use the **Certificates** snap-in to import the recovered private key to the user's Personal certificate store. You can then verify that the serial number of the certificate matches the original from the Details tab of the certificate's Properties dialog box.

For more information on managing key archival, consult Key Archival and Management in Windows Server 2003.

Deploying and Revoking Certificates to Users, Computers, and CAs

- After you have configured the appropriate templates and their associated properties, it is simple to make them available. From the Certification Authority snap-in, right-click **Certificate Templates** and choose **New** > **Certificate Template to Issue**. Select the appropriate template from the **Enable Certificate Templates** dialog box, and then click **OK**.
- Users requiring certificates can obtain them by going to http://*server*/certsrv, where *server* is the name of the CA server. This starts the Web Enrollment pages, which guide the user through the process of obtaining the appropriate certificate. For more information, see Using Windows Server 2003 Certificate Services Web pages and links cited therein.
- Mapping certificates involves associating a certificate with a user account. You can configure either one-to-one mapping, which associates a single certificate to a single user account, or many-to-one mapping, which associates several certificates to a single account. You can also use Directory Service certificate mapping to authenticate users in Active Directory with client certificates. For more information on certificate mapping and how-to links, consult About Mapping.
- You can use Group Policy to configure autoenrollment of computer or user certificates based on version 2 certificate templates. In a GPO linked to the appropriate Active Directory container, navigate to **Computer Configuration\Windows Settings\Security Settings\Public Key Policies**. Double-click **Autoenrollment Settings** and select the **Enroll certificates automatically** option. If required, select the additional options shown in *Figure 30*.

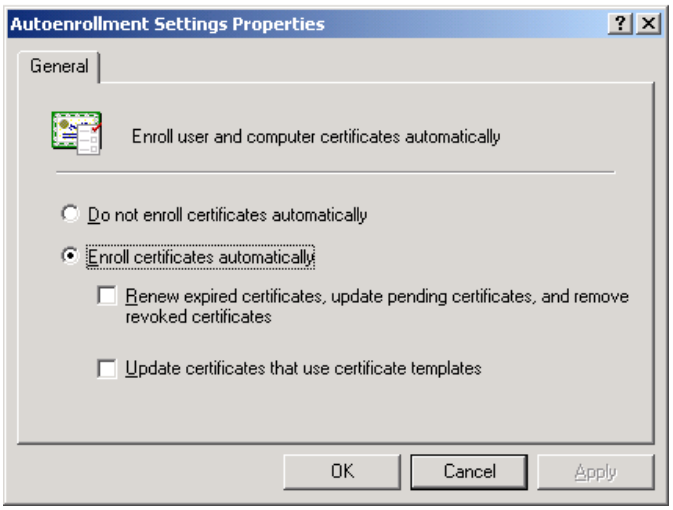


Figure 30 – The Autoenrollment Settings Properties Dialog Box Enables You to Configure Certificate Autoenrollment

- You can revoke certificates from the Certification Authority snap-in. Right-click the certificate to be revoked and select **All Tasks** > **Revoke Certificate**. In the Certificate Revocation dialog box, specify a reason code and then click **Yes**. If there is a possibility that you may want to reinstate the revoked certificate later, select **Certificate hold** as the reason.

Backing Up and Restoring the CA

- Certificate Services is included in the System State data, which you can back up as a unit from the Backup or Restore Wizard through the Windows Backup application.
- You can back up Certificate Services separately by right-clicking the server in the Certification Authority snap-in and choosing **All Tasks** > **Back up CA**. Follow the instructions provided by the Certification Authority Backup Wizard.
- You can restore Certificate Services by right-clicking the server and choosing **All Tasks** > **Restore CA**. Click **OK** to stop Certificate Services and then follow the instructions provided by the Certification Authority Restore Wizard.

Practice Questions

Chapter 1 Implementing, Managing, and Troubleshooting Security Policies

1. You are a network administrator for a large manufacturing firm. You have seven servers, which you recently upgraded from Windows 2000 Server to Windows Server 2003. You plan to add the IAS server role to one of your existing Windows Server 2003 servers that is underutilized. |

   You want to ensure that the new IAS server is configured to be as secure as possible with the least amount of administrative effort until you have time to manually address the security and configuration of the server.

   What should you do?

   - ❍ A. On the new IAS server, apply the default security template Secure.inf and restart the system.
   - ❍ B. On the new IAS server, apply the default security template Hisec.inf and restart the system.
   - ❍ C. On the new IAS server, apply the default security template Notssid.inf and restart the system.
   - ❍ D. On the new IAS server, apply the default security template DC security.inf and restart the system.

2. You manage network security for a growing building management company. Your domain consists of six servers running Windows Server 2003, which include two domain controllers, one remote access server, and three file and print servers. In addition, the firm has 150 workstations running Windows XP Professional, which are all members of the domain.

   Management has become increasingly concerned about security on the company's network and wants you to frequently check and ensure that all servers and workstations are kept up to date and are configured securely. You decide to install and use Microsoft Baseline Security Analyzer (MBSA) to accomplish the inspection and workstation compliance tasks.

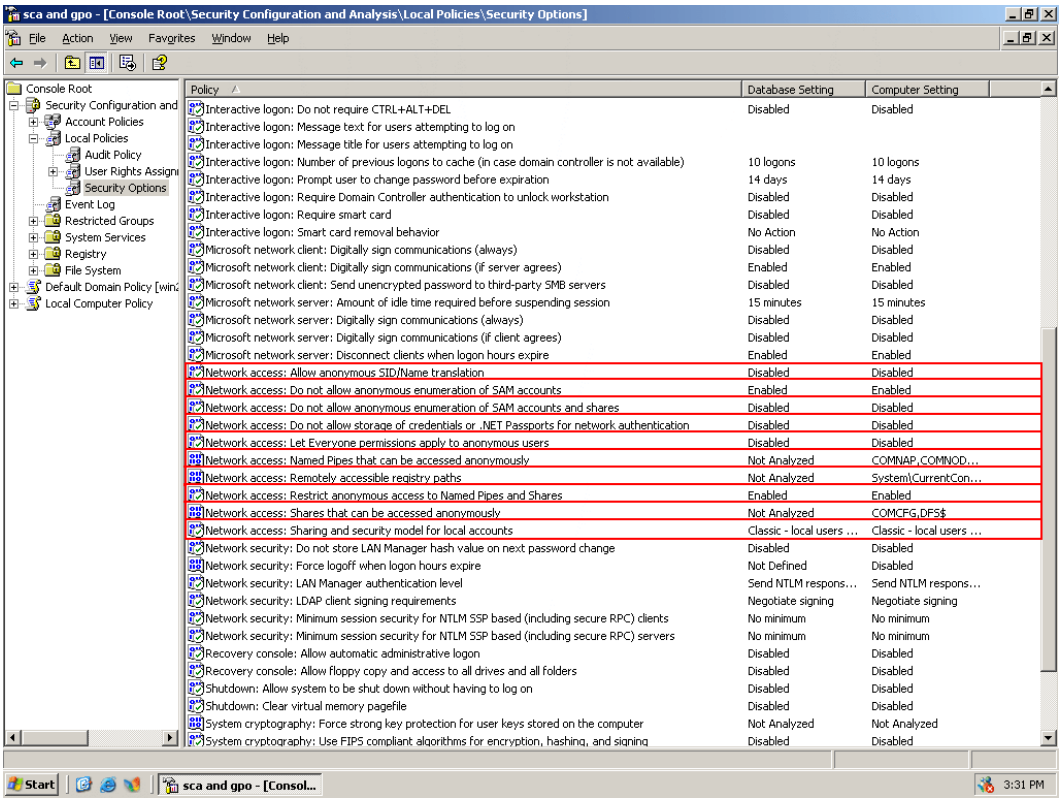
   After installing MBSA, you attempt to scan one of your test computers using its fully qualified domain name. However, despite repeated attempts, MBSA will not allow you to connect to or scan the computer. What could be the source of this problem?

   Select the correct answer.

   - ❍ A. MBSA cannot use fully qualified domain names to find and scan workstations.
   - ❍ B. WINS is not enabled on the destination computer you are trying to scan.
   - ❍ C. The version of MBSA you are running is out of date and lacks the most current update for the utility.
   - ❍ D. The account you used to log on to your computer is not a member of the Domain Admins group and therefore cannot use the fully qualified domain name to access other workstations.

3. The Windows 2000 Additional Restrictions for Anonymous connections managed the registry value called Restrict Anonymous in the HKLM/CurrentControlSet/Control/Lsa/ registry key. This value has been replaced in Windows Server 2003 with which policies?

   To answer, select the appropriate policies in the exhibit.

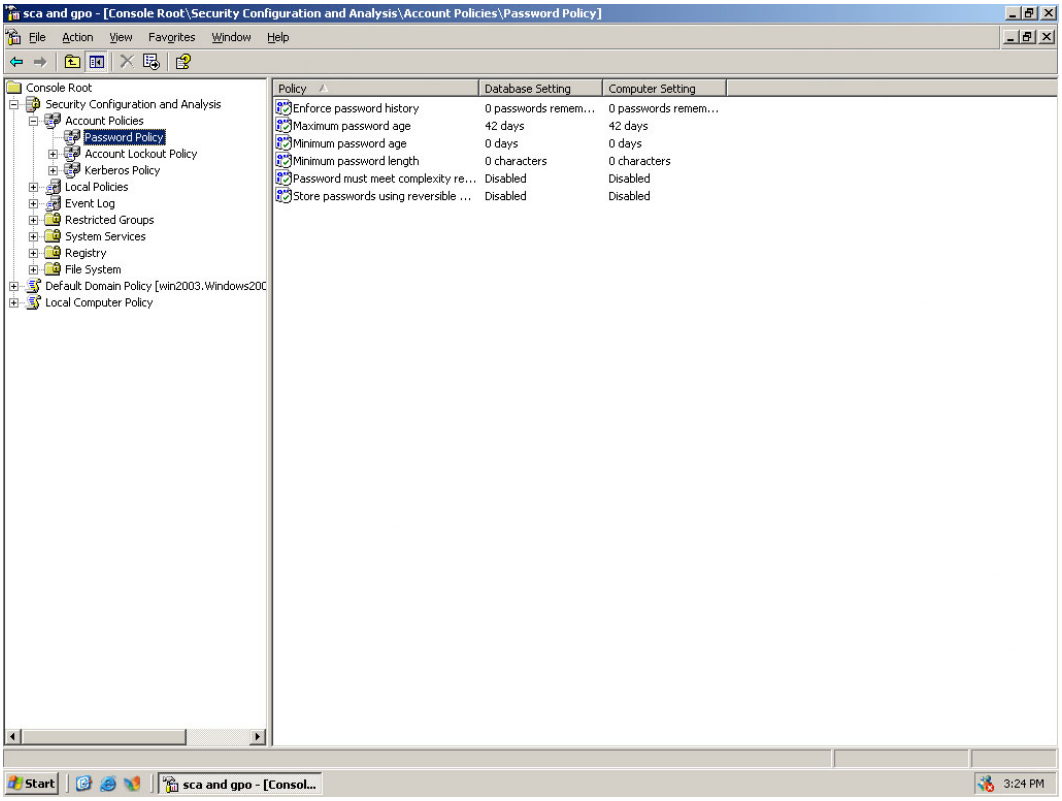


4. You are the network administrator for the Test domain, which consists of a Windows 2003\ domain with computers running Windows XP Professional. Company policy states that all passwords must be complex and secure to reduce the likelihood of a successful password attack. The exhibit shows your current password policy. How would you change it to meet company policy and become more secure? Each answer presents part of the solution.

   Choose three.

   - ❑ A. Enforce password history = 24
   - ❑ B. Maximum password age = 120
   - ❑ C. Minimum password age = 0
   - ❑ D. Minimum password length = 8
   - ❑ E. Password must meet complexity requirements = Enabled
   - ❑ F. Store passwords using reversible encryption = Enabled

Exhibit(s):



Chapter 2 Implementing, Managing, and Troubleshooting Patch Management Infrastructure

1. You are an administrator for a mid-size investment management firm, Your Money Investments. Your network consists of 10 servers running Windows Server 2003 and 400 desktop computers running Windows XP Professional.

   To keep up with the latest fixes and security patches, you decide that you want to upgrade your workstations to Windows XP Professional Service Pack 1. After successfully deploying a service pack upgrade through a GPO to workstations in your domain, you are faced with the problem of what to do with new systems that are built. You aren't always able to attend to every installation of every desktop and you want to make sure the latest service pack is installed on every workstation deployed to the network before it is connected or logged on to.
   What can you do to ensure these needs are met in an effective manner and with as little administrative effort as possible going forward?

   Select the correct answer.

   - ❍ A. On your workstation, copy the Windows XP source files to a folder on your hard disk called C:\WinXP.

     Obtain the latest service pack and place the files into a subfolder on your hard disk called C:\WinXP\SP.

     Create a CD that contains the files in the C:\WinXP directory.

     Use this CD to install future workstations.
   - ❍ B. On your workstation, copy the Windows XP source files to a folder on your hard disk called C:\WinXP.

     Obtain the latest service pack and extract the files into a folder on your hard disk called C:\SP.

     While logged on as Administrator on that system, run the command c:\SP\i386\update\update.exe /s:c:\WinXP at a command prompt.

     Create a CD that contains the files in the C:\WinXP directory.

     Use this CD to install Windows XP on new workstations.
   - ❍ C. Create a new OU on your domain called New Workstations.

     On your domain controller, copy the Windows XP source files to a folder on your hard disk called C:\WinXP.

     Obtain the latest service pack and extract the files into a subfolder called C:\WinXP\SP.

     Create a new GPO that assigns these files to the New Workstations OU.

     When new workstations are added to the domain, put them in the OU.
   - ❍ D. On your workstation, copy the Windows XP source files to a folder on your hard disk called C:\WinXP.

     Obtain the latest service pack and extract the files into a folder on your hard drive called C:\SP.

     While logged on as Administrator on that system, run the command c:\SP\i386\update\update.exe /s:c:\WinXP at a command prompt.

     Copy the WinXP directory to a share on one of your file servers, such as \Server1 Win2000SP2.

     Run all future installations from this directory using a DOS network boot disk.

2. You are the network administrator for the Test domain, which consists of a Windows 2003 domain with client computers running Windows XP Professional. It is your responsibility to test update content before applying it to computers in your production environment.

   Because you want the ability to test content in a test environment and then be able to push the content that you have tested to your production environment, you decide to use a manually configured distribution point. Which of the following steps should include in this process? Each answer presents part of the solution.

   Choose three.

   - ❑ A. Create a folder named \Content on the manually created content distribution point.
   - ❑ B. Get a valid digital certificate for server authentication from your organization. This certificate should be stored on the server that you would like to administer.
   - ❑ C. Copy all the files and folders under the \Content\cabs directory from the source server running SUS to the \Content directory on the server with the manually created content distribution point.
   - ❑ D. Create a VROOT called Content and point to the \Content\Cabs directory.
   - ❑ E. Right-click the Web site where SUS is installed, and then click Properties. SUS is typically installed under the Default Web site. On the Web Site tab, set the SSL port to 443.

Chapter 3 Implementing, Managing, Troubleshooting Security for Network Communications

1. You are one of three administrators for a medium-size firm, Packit Inc. The network features eight servers running Windows Server 2003, including two domain controllers, three file servers, and one Exchange Server 2003 server. Two servers are configured as RAS servers, which accept incoming dial-up connections from employees using portable computers running a mix of Windows 2000 and Windows XP.

   You configure a remote access policy that allows members of the Domain Users group to dial in to your RAS servers between 7:00 a.m. and 5:00 p.m. every day. At your recommendation, management approves the use of smart cards for remote users.

   You need to configure your remote access policy to allow the mobile users to log on using their new smart cards. What authentication method do you need to implement to accomplish this?

   Select the correct answer.

   - ❍ A. EAP-TLS
   - ❍ B. MS-CHAPv2
   - ❍ C. SPAP
   - ❍ D. IAS

2. You work for a mid-size development firm in California called Talent Not Required. Your network consists of 15 servers running Windows Server 2003 and 230 workstations running Windows XP Professional.

   Management is adding a wing to the office building and, although the new addition is fully outfitted with network connections, they want to be able to take advantage of 802.11b wireless technology from their notebook computers in the boardrooms and other casual meeting areas. The wireless-enabled users don't need access to files on the company network, but they need Outlook Web Access and access to the Internet.

   Knowing that much of the data the wireless-enabled users deal with is sensitive in nature, you must ensure that the systems are as secure as possible from a network traffic sense. You also must prevent unauthorized users from using your wireless network.
   What should you do? Each answer presents part of the solution.

   Choose two.

   - ❑ A. Split the network at your Internet connection. Connect the wireless access point on its own connection separate from your regular network.
   - ❑ B. On one of your more robust workstations on the network, install a second NIC and enable Internet Connection Sharing (ICS). Connect the wireless access point to this ICS-enabled NIC.
   - ❑ C. Configure the wireless access point unit to use 64-bit WEP and enable broadcasting of the SSID.
   - ❑ D. Configure the wireless access point unit to use 128-bit WEP and disable the broadcasting of the SSID. Manually configure each wireless user's laptop with the appropriate WEP and SSID settings.

3. When a computer first starts up, before GPOs take effect, the startup behavior of the IPSec driver determines how traffic is handled. What is the startup mode of the IPSec driver by default?

   Select the correct answer.

   - ❍ A. The IPSec driver startup mode defaults to the behavior of the last GPO.
   - ❍ B. The IPSec driver defaults to a permit startup mode. This means that all traffic is permitted inbound and outbound.
   - ❍ C. The IPSec driver defaults to a deny startup mode. This means that all traffic is dropped inbound and outbound.
   - ❍ D. The IPSec driver defaults to a stateful startup mode. This means that all outbound computer-initiated traffic is permitted. Additionally, inbound traffic is permitted only if in response to outbound traffic.

4. In which of the following four scenarios would you be required to use IPSec in tunnel mode?

Select the correct answer.

- ❍ A. You are tasked with using IPSec to protect traffic between two computers. A third-party firewall exists between the computers. Traffic moving through the firewall must be decrypted.
- ❍ B. Your boss asks you to build an endpoint-to-endpoint tunnel between two gateways, which both support L2TP/IPSec VPN connections.
- ❍ C. Your boss wants you to employ packet filtering. Specifically, she wishes to permit or block certain traffic based on source address, destination address, IP protocol, or specific TCP or UDP ports.
- ❍ D. You need to protect the traffic between two systems that use static IP addresses on both sides.

5. You are the network administrator for the Test domain, which consists of a Windows 2003 domain with client computers running Windows XP Professional.

You are responsible for configuring digital certificates. You are using Secure Sockets Layer (SSL) connections between clients and the Web servers.
Which steps are included in the process?

To answer, drag each correct answer to the right side ofthe screen in the proper order.

A. The client creates a unique session key to be used for the session.
B. The client keeps a copy of the key unencrytpted and creates another copy of the key encrypted with the public key that it received from the server.
C. The client connects to a Web site using the https protocol and port 80.
D. The server sends the client a copy of its certificate containing its public key.
E. The client connects to a Web site using the https protocol and port 443.

_____
_____
_____
_____
_____

Chapter 4 Planning, Configuring, and Troubleshooting Authentication, Authorization, and PKI

1. You are an administrator for a large manufacturing firm, HomeSecOrg. The network consists of 250 workstations running Windows XP Professional, and 20 servers running Windows Server 2003, including several Windows Server 2003 domain controllers, an Exchange Server 2003 server, an enterprise root CA, and a subordinate CA.

   Certificate Services has been running without incident for a length of time, but recently there has been increased attention to the security of servers in the organization. Management wants you to ensure that the CAs remain as secure as possible and that certificates issued run little risk of being compromised.

   In your current environment, you want to dramatically increase the security of your CA servers and help improve the integrity of your certificates issued to users.

   What should you do?

   - ❍ A. Install a second enterprise root CA on a new server.

     Configure the new enterprise root CA to load-balance certificate issuing to users and workstations on the domain.
   - ❍ B. Configure the existing enterprise root CA as an offline enterprise root CA.

     Install two new subordinate CAs and configure the offline enterprise root CA issue certificates to the two new subordinate CAs.
   - ❍ C. Install an offline standalone root CA on a new server.

     Configure the standalone root CA to issue certificates to subordinate CAs configured on your domain.

     Take the pre-existing enterprise root CA offline.
   - ❍ D. Configure a new server to run Windows Server 2003 with IIS v6 installed.

     Set up a Web site and configure the enterprise root CA to use it for users to request certificate updates or view the CRL.

     Enable IPSec for connections to and from the enterprise root CA and the Web site and from the Web site to workstations.

2. You are one of the administrators of a large Windows Server 2003 domain with 19 servers running Windows Server 2003 and 5000 workstations running a mix of Windows 2000 Professional and Windows XP Professional.

   A large pool of users from the engineering department work remotely from the office on laptops provided by the company. In an effort to ensure the data on these laptops is as secure as can be, you have enabled EFS on several folders that the users will save files to. Occasionally, you have to gain access to encrypted files of users who are transferred or leave the company. Currently, only the domain administrator can recover these files and he is often out of town on business. What do you recommend should be done to allow you and other administrators the ability to recover the encrypted data in these EFS-enabled folders in the most effective and secure manner?

   Select the correct answer.

   - ❍ A. Edit the lowest priority group policy in the domain and in the Computer Configuration folder under Public Key Policies\Encrypted Data Recover node. Run the Add Recovery Agent Wizard and add the necessary administrators as recovery agents.
   - ❍ B. Add administrators that you want to act as recovery agents to a new group called Recovery Agents. On each workstation on which EFS is used, modify the Folder and Share security settings on the folder where EFS is enabled so that the Recovery Agents group has Full Control to the folder and files within.
   - ❍ C. Have the domain administrator provide you with his username and password whe ever you need to recover EFS encrypted data. Have the domain administrator reset his password after each request.
   - ❍ D. Edit the highest priority group policy in the domain and in the Computer Configuration folder under Public Key Policies\Encrypted Data Recover node. Run the Add Recovery Agent Wizard and add the necessary administrators as recovery agents.

3. Your company spans the world with employees in two domains. The Marketing group in the Americas domain and the Marketing team in the AsiaPac domain would like to share network resources with the other group.

   You want to change permissions for the AMERICAS\marketing group and the ASIAPAC\marketing group to allow them access to each other's network resources.

   What should you do?

   - ❍ A. Place the AMERICAS\marketing group and the ASIAPAC\marketing group into their respective global groups.

     Nest the two global groups into one universal group, giving the new group permissions to the network resources.
   - ❍ B. Place the AMERICAS\marketing group and the ASIAPAC\marketing group into thei respective universal groups.

     Nest the two universal groups into one local group, giving the new group permissions to the network resources.
   - ❍ C. Place the AMERICAS\marketing group and the ASIAPAC\marketing group into their respective universal groups.

     Nest the two universal groups into one global group, giving the new group permissions to the network resources.
   - ❍ D. Place the AMERICAS\marketing group and the ASIAPAC\marketing group into their respective local groups.

     Nest the two local groups into one global group, giving the new group permissions to the network resources.

4. You are the network administrator for the Test domain, which consists of a Windows 2003 domain with Windows XP Professional computers. You have created a GPO that redirects users' start menus to a shared folder on a file server. Some of users are missing programs from the start menu that were there yesterday but disappeared when they logged on today.

   You verify that the users can access the shared folder, and when you log on to one of the computers, all of the programs appear fine. You must troubleshoot and resolve this problem. What should you do? Each answer presents part of the solution.

   Choose two.

   - ❑ A. Run the secedit/refreshpolicy command on one of the computers.
   - ❑ B. Run the gpupdate command on one of the computers.
   - ❑ C. In the Group Policy Management Console (GPMC), run the Resultant Set of Policy (RSoP) in planning mode.
   - ❑ D. In the Group Policy Management Console (GPMC), run the Resultant Set of Policy (RSoP) in logging mode.
   - ❑ E. Run the gpresult command on one of the computers.

5. You are the network administrator for the PrepLogic forest, which consists of several Windows 2003 domains with client computers running Windows XP Professional. You configure Windows Server 2003 to archive the private keys of certificates at the time of issuance so that you are able to recover the key should it be lost.

   You have discovered that for some reason several keys have become corrupt. Which tools can you use to recover the keys? Each answer presents part of the solution.

   Choose two.

   - ❑ A. Ntdsutil utility
   - ❑ B. Krecover utility
   - ❑ C. REdirCOMP utility
   - ❑ D. Certutil tool
   - ❑ E. Netdiag_setup tool

Answers and Explanations

Chapter 1

1. Answer: B

Explanation A. Although this would provide secure security settings quickly, Secure.inf is not the most secure template you can apply. You should apply Hisec.inf.

Explanation B. The Highly Secure (Hisec.inf) security template is the most secure template you can apply out of the box. You can manually configure your server to be more secure; however, using Hisec.inf is the best way to apply strong security settings out of the box as quickly as possible.

Explanation C. The No Terminal Server user SID template (Notssid.inf) can remove Terminal server registry entries but ultimately does not improve security beyond default security settings and certainly does not secure as well as the Hisec.inf template.

Explanation D. The Domain Controller Security (DC security.inf) template is practical only for domain controllers. Because the IAS server is not a domain controller, the DC security.inf template wouldn't be the best choice for this situation. The Hisec.inf template is the best choice.

2. Answer: A

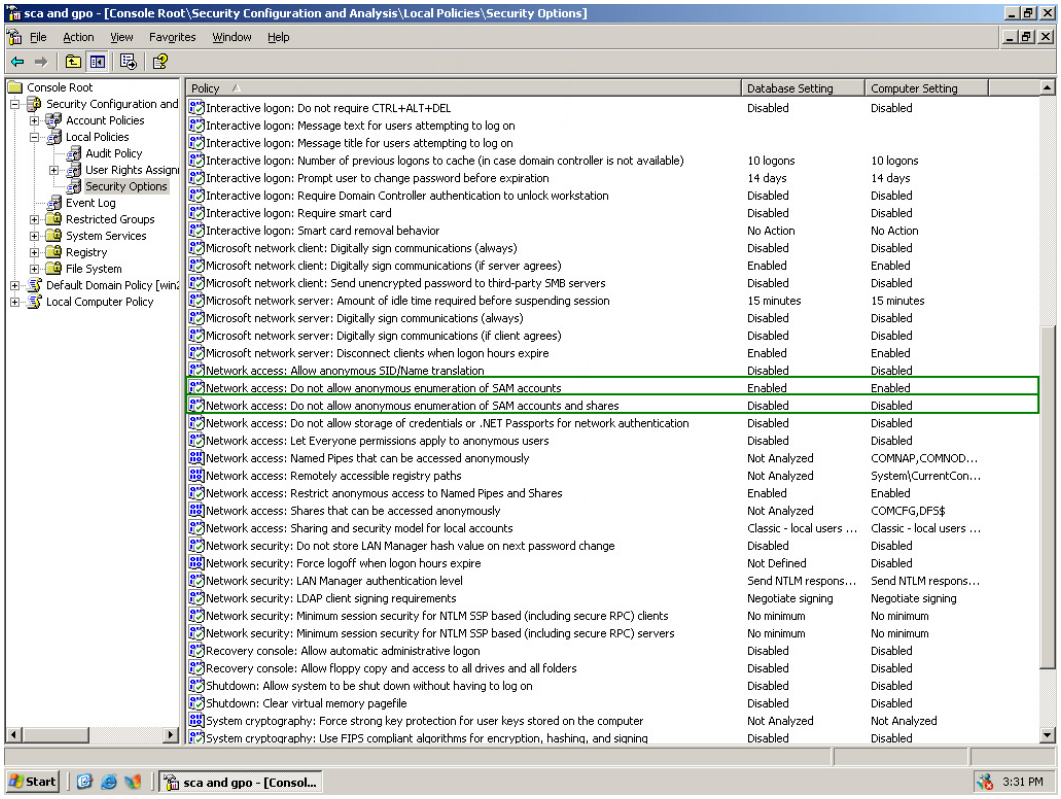
Explanation A. To scan remote computers, you can use either an IP address or the computer's NetBIOS name. MBSA does not support scanning computers using their fully qualified domain names.

Explanation B. WINS will have no effect on whether you can connect to the computer using the fully qualified domain name through MBSA. MBSA is unable to use fully qualified domain names to find and scan workstations. To scan remote computers, you can use either an IP address or the computer's NetBIOS name.

Explanation C. Regardless of the version of MBSA, the utility is unable to resolve fully qualified domain names. To scan remote computers, you can use either an IP address or the computer's NetBIOS name.

Explanation D. Being a member of the Domain Admins group does not affect whether you can use a fully qualified domain name to connect to a remote computer with MBSA. MBSA cannot use fully qualified domain names to find and scan workstations. To scan remote computers, you can use either an IP address or the system's NetBIOS name.

3. Answer:



Explanation: Network Access: Do not allow anonymous enumeration of SAM accounts and shares and Network Access: Do not allow anonymous enumeration of SAM accounts replace the Windows 2000 Additional Restrictions for Anonymous connections that managed the registry value called Restrict Anonymous.

4. Answers: A, D, E

Explanation A. The values for Enforce password history are 0 to 24. It is recommended that you set this policy value to 24 to limit password reuse.

Explanation B. The values for Maximum password age are 0 to 999. It is recommended that you set this policy to either 30 or 60 days.

Explanation C. The values for Minimum password age are 0 to 998. Set to 2 days; this disallows immediately changes.

Explanation D. The values for Minimum password length are 0 to 14. Set to at least 8.

Explanation E. The Password must meet complexity requirements setting should be set to Enabled. It requires that passwords are complex and more secure.

Explanation F. The Store passwords using reversible encryption setting should be set to Disabled. Never enable this setting unless business requirements outnumber the need to protect password information.

Chapter 2

1. Answer: B

Explanation A. Although this could make the service pack more accessible, it won't automatically install the service pack when the installation is performed. To do this, you must slipstream the service pack into the operating system installation.

Explanation B. This method is called slipstreaming. Whenever a technician installs Windows XP using that CD, the service pack updates and data will already be integrated into that installation. This can be done repeatedly and can also be used for Windows Server 2003 installations. These images can also be used on a RIS server for automated deployment.

Explanation C. This type of installation goes against one of the important guidelines, which is that the service pack must be installed prior to the workstation being mounted to the network. For updates to be distributed in this fashion, the system must be connected to the network and powered on.

Explanation D. This solution would work because it has a slipstreamed service pack installation; however, it goes against the guideline of not connecting to the network prior to having the service pack installed. You could create a sandbox network that is not connected to your regular production network where updates and installations could be performed safely and securely.

2. Answers: A, C, D

Explanation A. You take content from the \Content folder on a server running SUS that can connect to the Internet, and copy this content to the manually created content distribution point. Remember to copy the complete \Content directory.

Explanation B. This is a step used to secure administration of a server running SUS by using Internet Explorer from a remote computer.

Explanation C. You take content from the \Content folder on a server running SUS that can connect to the Internet, and copy this content to the manually created content distribution point. Remember to copy the complete \Content directory.

Explanation D. You take content from the \Content folder on a server running SUS that can connect to the Internet, and copy this content to the manually created content distribution point.

Explanation E. This is a step used to administer a server running SUS by using Internet Explorer from a remote computer. By default, all administration is done over HTTP.

Chapter 3

1. Answer: A

Explanation A. EAP-TLS is the authentication method used for authenticating with smart cards over a PPTP or L2TP remote access connection. EAP-TLS can be used in situations in which data encryption is required.

Explanation B. MS-CHAPv2 does not support authentication using smart cards and therefore will not work in this scenario. EAP-TLS is the authentication method that provides the necessary support for smart cards in Windows 2000 or Windows XP.

Explanation C. SPAP does not support authentication using smart cards and therefore will not work in this scenario. EAP-TLS is the authentication method that provides the necessary support for smart cards in Windows 2000 or Windows XP.

Explanation D. IAS is not required to support smart cards and therefore has no use in this scenario. Routing and Remote Access Services with EAP-TLS authentication is all that is required to support smart cards.

2. Answers: A, D

Explanation A. Whenever possible, you should separate your wireless networks from your wired networks. Even the best wireless security is generally not acceptable especially for networks on which sensitive data is passed. Putting the wireless connection on it's own link to your Internet feed will allow the users to access the Internet and OWA while preventing them from accessing the main network.

Explanation B. This solution would be a poor choice in almost every way. Not only do you have to rely on the workstation to remain running, you are also piggybacking your wireless solution onto your production network, which should be avoided. In addition, ICS is prone to reliability issues when used with larger numbers of users and is not as secure as a good firewall or even a system configured to perform NAT. You are better off to segment your network at the connection to your Internet provider to keep your main network and wireless network separate.

Explanation C. Although your wireless users will be able to easily connect whenever they want, this will allow anyone, even unauthorized users, to connect to the access point. In addition, 64-bit encryption isn't as secure as 128-bit or 256-bit encryption found on many of today's newer wireless access points. In this scenario, disable SSID broadcasting and use the strongest WEP possible. Manually configure each laptop that needs to connect and, if possible, configure your wireless access point to filter by MAC (hardware) addresses for the laptops.

Explanation D. Your wireless users won't be able to easily connect simply by walking by an access point; however, this configuration will provide strong security. Using 128-bit encryption is acceptable by today's standards, but use 256-bit encryption if possible. Manually configuring each laptop may seem tedious but will limit the number of users on the network and minimize the chances of your sensitive WEP and SSID information being discovered by unauthorized users. If possible, configure your wireless access point to filter by MAC addresses for the laptops.

3. Answer: D

Explanation A. The IPSec driver starts up in stateful mode, by default. The mode can be changed by using the following netsh command: netsh ipsec dynamic set config bootmode value={stateful | block | permit}

Explanation B. The IPSec driver starts up in stateful mode, by default. The mode can be changed by using the following netsh command: netsh ipsec dynamic set config bootmode value={stateful | block | permit}

Explanation C. The IPSec driver starts up in stateful mode, by default. The mode can be changed by using the following netsh command: netsh ipsec dynamic set config bootmode value={stateful | block | permit}

Explanation D. The IPSec driver starts up in stateful mode, by default. The mode can be changed by using the following netsh command: netsh ipsec dynamic set config bootmode value={stateful | block | permit}

4. Answer: A

Explanation A. If you did not require the traffic to be decrypted between the two endpoints, you should use IPSec in transport mode. In this scenario, you will establish one IPSec tunnel between the first computer and the firewall. The second IPSec tunnel will run from the firewall to the second computer.

Explanation B. In this case, you would use IPSec in transport mode. If neither gateway supported L2TP/IPSec VPN connections, you would be forced to use IPSec in tunnel mode.

Explanation C. All of this functionality can be done using IPSec in transport mode.

Explanation D. This is a great example of when to use IPSec in transport mode. However, if one computer does not support IPSec, you may be able to establish an IPSec tunnel to the nearest network device that supports IPSec.

5. Answer:

A. The client creates a unique session key to be used for the session. E.
B. The client keeps a copy of the key unencrytpted and creates another copy of the key encrypted with the public key that it received from the server. D.
C. The client connects to a Web site using the https protocol and port 80. A.
D. The server sends the client a copy of its certificate containing its public key. B.
E. The client connects to a Web site using the https protocol and port 443.

Explanation: The correct order is as follows:

1. The client connects to a Web site using the https protocol and port 443.
2. The server sends the client a copy of its certificate containing its public key.
3. The client creates a unique session key to be used for the session.
4. The client keeps a copy of the key unencrytpted and creates another copy of the key encrypted with the public key that it received from the server.

The client connects to a Web site using the https protocol and port 443, not port 80.

Chapter 4

1. Answer: C

Explanation A. You can have only one enterprise root CA installed and online at a time. Therefore, this configuration would not function properly. In addition, it does nothing to improve the security of the CAs or authenticity of the published certificates because both servers are still communicating directly with users and workstations and therefore are more susceptible to attack and compromise.

Explanation B. An enterprise root CA requires connectivity with Active Directory; therefore, this configuration would not work and would disable Certificate Services on the network.

Explanation C. This solution provides very good security because the only CA issuing certificates to workstations and users is the subordinate CA, which receives certificates from the standalone offline CA. The standalone offline CA is far less susceptible to attack because it doesn't actively participate in Active Directory and it does not issue certificates to users and computers directly, making it harder to attack.

Explanation D. Simply adding IPSec to connections to and from the enterprise root CA will not guarantee authenticity of certificates issued from the CA because the server is still susceptible to attack. In addition, when configured, an enterprise root CA already has a Web site configured for the users to perform maintenance tasks as described. This configuration will only provide some protection of the data passing to and from the enterprise root CA and the users and workstations connecting to it, not for the CA itself.

2. Answer: D

Explanation A. You must configure these settings in the highest priority group policy to ensure that another group policy doesn't override it in the future. Also, for this to work properly, you need to be logged on as an administrator on the first domain controller created in the domain. After the wizard runs, you can select users or certificates to act as recovery agents.

Explanation B. Simply having rights to an EFS-encrypted folder will not provide the rights to read or modify any EFS-encrypted files in that folder unless you are the owner and original creator of the file. In this configuration, there is also no way to recover data if a certificate is completely lost.

Explanation C. Although you could recover EFS data in this manner, it is highly insecure and any domain administrator that either proposes or follows this solution would be placing the domain at a high risk for exploit regardless of whether he changed his password.

Explanation D. You must configure these settings in the highest priority group policy to ensure that another group policy doesn't override it in the future. Also, for this to work properly, you need to be logged on as an administrator on the first domain controller created in the domain. After the wizard runs, you can select users or certificates to act as recovery agents.

3. Answer: A

Explanation A. Each domain's group can be placed in a global group, giving them permissions to a resource in their domain. However, granting permissions to a group external to that domain is best served by using universal groups. Best practices states placing or nesting the global group into the universal group.

Explanation B. Each domain's group can be placed in a global group, giving them permissions to a resource in their domain. However, granting permissions to a group external to that domain is best served by using universal groups. Best practices states placing or nesting the global group into the universal group.

Explanation C. Each domain's group can be placed in a global group, giving them permissions to a resource in their domain. However, granting permissions to a group external to that domain is best served by using universal groups. Best practices states placing or nesting the global group into the universal group.

Explanation D. Each domain's group can be placed in a global group, giving them permissions to a resource in their domain. However, granting permissions to a group external to that domain is best served by using universal groups. Best practices states placing or nesting the global group into the universal group.

4. Answers: D, E

Explanation A. Gpupdate is a command-line utility that can be used if the policy needs to be refreshed immediately. Gpupdate replaces the Windows 2000 command secedit /refreshpolicy.

Explanation B. Gpupdate is a command-line utility that can be used if the policy needs to be refreshed immediately. Gpupdate replaces the Windows 2000 command secedit /refreshpolicy.

Explanation C. Planning mode performs a "what if" scenario to predict the effects of a proposed series of policies on a specified user/computer combination.

Explanation D. Logging mode obtains information on the existing Group Policy application for a specific user/computer combination. This includes the precedence of applying policy settings when the user is subject to different Group Policy objects (GPOs) containing conflicting policy settings.

Explanation E. Displays Group Policy settings and RSOP for a user or a computer.

5. Answers: B, D

Explanation A. Ntdsutil performs various Active Directory Database tasks.

Explanation B. Key recovery involves use of the Certutil tool, which is a command-line utility included with Windows Server 2003 Certificate Services that performs a large number of certificate management tasks. You can also use the Krecover utility included in the Windows Server 2003 Resource Kit.

Explanation C. REdirCOMP is a Windows Server 2003 utility that allows computers to be placed in specific organizational units.

Explanation D. Key recovery involves use of the Certutil tool, which is a command-line utility included with Windows Server 2003 Certificate Services that
performs a large number of certificate management tasks. You can also use the Krecover utility included in the Windows Server 2003 Resource Kit.

Explanation E. This command-line diagnostic tool helps isolate networking and connectivity problems by performing a series of tests to determine the state of your network client and whether it is functional.