Symantec™ Enterprise Security Manager™ Release Notes

ISO 17799 standard-based security policies for Symantec AntiVirus™ servers on Windows 2000 servers

Symantec ESM Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

Trademarks

Symantec, the Symantec logo, Symantec AntiVirus, Symantec Enterprise Security Manager, and Symantec Intruder Alert are trademarks of Symantec Corporation.

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

Contents

Symantec™ Enterprise Security Manager™ Release Notes

Service and support solutions

Symantec™ Enterprise Security Manager™ Release Notes

This document contains release notes for base and high-level best practice policies for Symantec™ Enterprise Security Manager™ (ESM) agents that are running Symantec AntiVirus™ version 7.5 or 7.6+ servers on Windows 2000 servers. The documented policies are provided for ESM managers and agents that are running ESM 5.1 or ESM 5.5 with Security Update 10 or later module releases.

Introducing best practice policies

ESM best practice policies are configured by members of the Symantec Security Response team to protect specific applications and operating system platforms from security vulnerabilities that could compromise the confidentiality, integrity, and/or availability of data that is stored and transmitted on your computer network.

Best practice policies are designed to enforce “common best practices” as described in the ISO/IEC 17799 international standard, “Information technology - Code of practice for information security management,” and defined through research by trusted security experts and clearing houses.

ESM best practice policies are based on sections of the ISO 17799 standard that address logical access controls and other security issues pertaining to electronic information systems. Symantec recommends that you review the ISO 17799 standard in its entirety to identify other issues, such as physical access controls and personnel training, that need to be addressed in your organization’s information security policy.

How best practice policies differ from ESM default policies

The Phase 1, 2, and 3 default policies that are installed with the ESM core product and Security Update releases are intended to be modified by users to enforce relaxed, cautious, and strict security policies in enterprises that include mixes of clients, servers, and applications that cannot be anticipated by ESM developers.

Best practice policies are preconfigured by members of the Symantec Security Response team to harden operating system platforms and protect specific combinations of applications and OS platforms from known security risks. These policies use preconfigured values, name lists, templates, and word files that directly apply to the targeted applications and platforms.

Best practice policies use the modules and templates from ESM Security Update releases to check OS patches, password settings, and other vulnerabilities on the targeted operating system. These policies may also introduce new, application-specific modules and templates to check conditions related specifically to the targeted application.

ESM best practice policies represent the collective wisdom of security experts, and they should not be modified by ESM users. In ESM 5.5, they are installed as read-only policies that cannot be edited by ESM users.

Warning: Do not attempt to modify an ESM best practice policy. Instead, copy and rename the policy, then edit the new version. This preserves the original best practice policy and also protects your customized policy from being overwritten by policy updates to the best practice policy.

How base policies differ from high-level policies

ESM best practice policies are configured as base policies, as high-level policies, or as sets that include both base and high-level policies.

Base policies are configured using the 80-20 rule of security. The 80-20 rule states that 80 percent of successful compromise comes from 20 percent of a system's vulnerabilities or misconfiguration.

To detect critical system vulnerabilities, base policies are configured to:

- Identify unneeded services
- Identify missing OS patches
- Enforce password strength rules
- Check for application-specific vulnerabilities that are deemed most critical by security experts

High-level policies incorporate checks for additional best practices that are prescribed by the ISO 17799 standard and recommended for specific application and OS platform combinations by trusted information security experts.

Industry research sources

Many of the security vulnerabilities that are addressed by the ISO 17799 standard and ESM best practice policies have been researched by security experts in our industry. Best practice recommendations that result from this research are posted to numerous Web sites and published as advisories by a variety of organizations that act as security information clearing houses.

Research resources for ESM best practice policies include, but are not limited to, the following:

- Symantec Security Response team
- CERT Coordination Center
- SANS Institute
- Computer Incident Advisory Center (CIAC)
- Center for Internet Security (CIS)
- National Infrastructure Protection Center (NIPC)
- National Security Agency (NSA)
- Information Systems Audit and Control Association (ISACA)
- Application and operating system vendors

Note: ESM best practice policies were researched using information that was released into the public domain by the organizations listed above. Recognition of these organizations does not indicate official endorsement of ESM best practice policies by any of these organizations.

Symantec AntiVirus–W2K base policy

The Symantec AntiVirus–W2K base policy runs the following ESM security checks on Windows 2000 servers that are running Symantec AntiVirus version 7.5 or 7.6+ servers to ensure compliance with the best practices described below. See the *ESM Security Update 10 User's Guide for Windows 2000 Modules* for more information about specific security checks.

Note: Both policies described in these Release Notes are preconfigured to run on Symantec AntiVirus 7.5 or 7.6+ application servers and Windows 2000 servers. These policies are not intended for Symantec AntiVirus clients.

Login Parameters checks

- **Account lockout enabled.** Account lockout should be enabled in the Windows 2000 account policy. The number of failed logon attempts that triggers account lockout should be set to 5. See ISO 17799 section 9.5.2(e).
- **Lockout time**. The account lockout time setting in the Windows 2000 account policy should not be less than 30 minutes unless it is 0, which indicates that accounts must be unlocked by the system administrator. See ISO 17799 section 9.5.2(e).
- **Time before bad logon counter is reset**. The setting that determines how soon the bad logon counter is reset after an account lockout should be set to at least 30 minutes in the Windows 2000 account policy. See ISO 17799 section 9.5.2(e).
- **Hide last user ID from Logon dialog box.** Disable the User Manager account policy setting that displays the last input user name in the Logon dialog box on your Windows 2000 server. See ISO 17799 section 9.5.2(a).
- **Do not allow shutdown from Logon dialog box**. The command that lets users shut down the system should be disabled in the Logon dialog box on your Windows 2000 server. See ISO 17799 section 9.5.

Network Integrity checks

- **List shared directories giving full control to Everyone.** The Everyone security group should be removed from the access lists for all shared directories. See ISO 17799 sections 9.2.1(a), 9.2.2, and 9.4.
- **Anonymous Lanman access disabled.** Anonymous access to LAN Manager information such as user names and shares should be disabled using the rbfix utility in the ...\ESM\bin\W2K-ix86 directory. See ISO 17799 section 9.4.
- **Check for plain text authentication.** Plain text authentication should be disabled by setting the EnablePlainTextPassword: REG_DWORD value to 0 or blank in the Windows 2000 Registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rdr\Parameters. See ISO 17799 sections 9.2.3, 9.4, and 9.5.
- **RRAS enabled.** You should remove Microsoft's Routing and Remote Access Service (RRAS) from your Windows 2000 Server. See ISO 17799 sections 8.1.5(c) and 9.4.

OS Patches checks and templates

Windows 2000 servers should be running Microsoft Service Pack 2 with the patches that are defined by patch IDs and descriptions in ESM's default Patch template for Windows 2000 servers. See ISO 17799 section 10.4.1.

Note: Make sure you have installed the patch.ps5 template file that was last updated by ESM Security Update 10. If you have edited this template, you should restore it to its previous state. You should also copy and rename any Patch templates that you decide to edit for ESM's Phase 1, 2, or 3 policies before you edit those templates in the future.

Password Strength checks

- **Minimum password length**. Windows 2000 account policy settings should require passwords to include at least 8 characters. See ISO 17799 section 9.3.1(d).
- **Accounts without passwords**. All active and disabled user accounts should be required to enter passwords to log on to your systems. See ISO 17799 sections 9.3.1 and 9.5.3.

  Assign secure passwords to all active accounts and select **User must log on to change password** and **User must change password at next logon** in the Windows 2000 security policy. You should also remove all disabled accounts from your systems. See ISO 17799 section 9.2.1.
- **Password = username**, **Password = any username**, and **Password = wordlist word.** Passwords should not be allowed to match any user name on your system or any commonly-used dictionary word. The Symantec AntiVirus–W2K base policy checks passwords against 11 dictionary word files. See ISO 17799 section 9.3.1(d)(2).
- **Password must expire**. All user accounts except the %GUEST% and %ADMINISTRATOR% accounts should use passwords that are required to expire. Clear the **Password never expires** check box in the Windows 2000 account policy. See ISO 17799 section 9.3.1(e).
- **Maximum password age**. Windows 2000 account policy settings for password expiration periods should not exceed 60 days. See ISO 17799 section 9.3.1(e).
- **Check for syskey encryption**. Password encryption by the Windows 2000 security account manager (SAM) should be enabled on your systems. Run syskey.exe and select **Encryption enabled.** See ISO 17799 sections 9.5.3 and 10.3.2.

Registry checks and templates

The Symantec AntiVirus–W2K base policy runs the **Check key and value existence** check to verify that the Symantec AntiVirus server configuration complies with records in the navce2kb.rs5 Registry template file that define mandatory and forbidden registry keys and Data Existence Sublist records that define required key settings. See ISO 17799 sections 8.3, 10.4.1, and 10.5.4.

The following best practices are enforced on Symantec AntiVirus application servers:

- Client file system realtime protection should be on and locked.
- Client realtime protection option to protect all file types should be enabled and locked.
- Client realtime protection option to clean macro viruses from files should be enabled and locked.
- Client realtime protection option to clean non-macro viruses from files should be enabled and locked.
- Client Bloodhound™ virus detection technology should be enabled and locked.
- Client sensitivity level for heuristic scanning settings should not be set to minimum level of protection.
- Clients should retrieve virus definition updates from the parent server.
- Client virus scans should be scheduled to occur automatically.
- Client uninstalls should be password-protected.
- Server file system realtime protection should be on.
- Server realtime protection option to protect all file types should be enabled.
- Server realtime protection option to clean macro viruses from files should be enabled.
- Server realtime protection option to clean non-macro viruses from files should be enabled.
- Server Bloodhound™ virus detection technology should be enabled.
- Server virus scans should be scheduled to occur automatically.
- Primary server updates should be scheduled to occur automatically daily.
- Primary server should be configured to distribute virus definition updates to servers within its server group.

The Symantec AntiVirus-W2K base policy also checks Registry keys and values against records in the w2kservb.rs5 template file to verify that the Windows 2000 member server baseline Security Options policy includes the following settings:

- Set the number of days before a password expires that signals a prompt to change user passwords to 14 days.
- Set Unsigned driver installation behavior to Do not allow installation.
- Set Unsigned non-driver installation behavior to Warn but allow installation.
- Disable the Recovery Console setting: Allow automatic administrative logon.
- Disable the Recovery Console setting: Allow floppy copy and access to drives and folders.
- Disable the setting: Allow server operators to schedule tasks.
- Set the LAN Manager Authentication Level to Use NTLMv2 session security if negotiated.
- Enable the setting: Digitally sign client communication (when possible).
- Enable the setting: Digitally sign server communication (when possible).
- Enable the Secure channel setting: Digitally encrypt secure channel data (when possible).
- Enable the Secure channel setting: Digitally sign secure channel data (when possible).

Startup Files checks

- **Check for required services**. Make sure that the following services are installed and running on the Windows 2000 servers that are running Symantec AntiVirus application servers. See ISO 17799 section 8.3.

  COM+ Event System
  Distributed Link Tracking Client
  DNS Client
  Enterprise Security Agent
  Event Log
  Logical Disk Manager
  Net Logon
  Network Connections
  Norton AntiVirus Server
  Plug and Play
  Protected Storage

Remote Procedure Call (RPC)
Security Accounts Manager
Server
System Event Notification
TCP/IP NetBIOS Helper Service
Windows Management Instrumentation Driver Extension
Windows Time
Workstation

- **Check for disallowed services**. Remove the following services from Windows 2000 servers that are running Symantec AntiVirus application servers. See ISO 17799 section 8.1.5 (c).

  Alerter
  Boot Information Negotiation Layer
  Certificate Services
  ClipBook
  Computer Browser
  DHCP Client
  DHCP Server
  Distributed Link Tracking Server
  Distributed Transaction Coordinator
  DNS Server
  Fax Service
  File Replication
  File Server for Macintosh
  FTP Publishing Service
  Gateway Services for NetWare
  Gopher Publishing Service
  IIS Admin Service
  Indexing Service
  Internet Authentication Service
  Internet Connection Sharing
  Intersite Messaging
  License Logging Service
  Messenger
  NetMeeting Remote Desktop Sharing
  Network DDE
  Network DDE DSDM

Network Monitor
Network News Transfer Protocol
Online Presentation Broadcast
Performance Logs and Alerts
Print Server for Macintosh
Process Control Service
QoS Admission Control
Qos RSVP
Remote Access Auto Connection Manager
Remote Access Server
Remote Procedure Call (RPC) Locator
Remote Registry Service
Remote Storage Engine
Remote Storage File
Remote Storage Media
Remote Storage Notification
Routing and Remote Access
RunAs Service
SAP Agent
Simple Mail Transfer Protocol
Simple TCP/IP Services
Single Instance Storage (SIS) Groveler
Site Server ILS Service
SNMP Service
SNMP Trap Service
Still Image Service
Task Scheduler
TCP/IP Print Server
Telephony
Telnet
Terminal Services
Terminal Services Licensing
Trivial FTP Daemon
Uninterrruptible Power Supply
Utility Manager
Volume Snapshot
Windows Internet Name Service

Windows Media Monitor Service
Windows Media Program Service
Windows Media Station Service
Windows Media Unicast Service
World Wide Web Publishing Service

- **Check for unknown services.** Carefully review all services that are reported as "unknown services" to determine whether they should be added to Required Services, Disallowed Services, or Optional Services name lists. This check does not report any of the services that are listed in the Optional Services name list as unknown services. See ISO 17799 sections 8.1.5(c) and 8.3.

Note: Before you add services that are reported as "unknown services" to the name lists for Required Services, Disallowed Services, or Optional Services, you should copy and rename the Symantec AntiVirus-W2K base policy.

Application Management
DefWatch
Distributed File System
Intel Alert Handler
Intel Alert Originator
Intel File Transfer
Intel PDS
IPsec Policy Agent
Kerberos Key Distribution Center
Logical Disk Manager Administrative Service
Norton AntiVirus Client
NT LM Security Support Provider
Remote Access Connection Manager
Removable Storage
Smart Card
Smart Card Helper
Symantec Central Quarantine
Symantec Quarantine Agent
Symantec Quarantine Scanner
Symantec System Center Discovery Service
Windows Installer
Windows Management Instrumentation

- **List changed services** and **List new services**. Services changes should be carefully monitored. You can update the services snapshot file to include all authorized changes from the ESM console grid. If any of the reported services changes were not authorized, you should restore the correct configuration on your Windows 2000 server. See ISO 17799 sections 8.1.2 and 8.3.1(d).
- **Remote procedure call (RPC) disabled**. Disable the remote procedure call (RPC) locator and service on Windows 2000 servers where the Symantec AntiVirus application server is running. See ISO 17799 section 8.1.5(c).
- **Remote registry access disabled**. Restrict access to the system registry to the Administrators security group. Any user that is granted read or write access to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg key has remote access to the registry.

  After a user has established a remote connection to the registry, the security on the individual keys is the only thing that restricts the user's access, regardless of what permissions the user is granted on the Winreg key. See ISO 17799 sections 9.2.2 and 9.4.2.

Symantec AntiVirus–W2K high-level policy

The Symantec AntiVirus-W2K high-level policy runs all of the security checks that are included in the base policy as well as the following checks to ensure compliance with the best practices described below. See the *Symantec ESM Security Update 10 User's Guide for Windows 2000 Modules* for more information about specific security checks.

Note: Both policies described in these Release Notes are preconfigured to run on Symantec AntiVirus 7.5 or 7.6+ application servers and Windows 2000 servers. These policies are not intended for Symantec AntiVirus clients.

Account Integrity checks

- **Rename Admin account**. Rename the account named “Administrator” on Windows 2000 and Symantec AntiVirus servers to ensure that the Administrator account is not used to break in to your system. Windows 2000 cannot lock out this account during repeated break-in attempts. See ISO 17799 sections 9.2.2 and 9.5.4(j).
- **Rename Guest account**. Rename the account named “Guest” on Windows 2000 and Symantec AntiVirus servers to ensure that this account does not provide privileged access to your system. See ISO 17799 sections 9.2.2 and 9.5.4(j).
- **List disabled/expired/locked accounts**. Review all reported accounts that have been disabled, expired, or locked for more than 90 days after the date that they were first identified as disabled, expired, or locked in the agent's user snapshot file. Either reactivate the reported accounts with new, secure passwords or delete them from the system so they cannot be used in break-in attempts. See ISO 17799 section 9.2.1(i).
- **Report new, deleted, and changed users and new, deleted, and changed security groups**. Review all changes to user accounts and security groups on Windows 2000 and Symantec AntiVirus servers to ensure that only authorized users are granted access. See ISO 17799 sections 9.2 and 9.4.

  Note: Run the Symantec AntiVirus-W2K high level policy one time on each ESM agent that is checked by the policy to create user and group snapshot files on the agent. Then periodically rerun the policy to detect changes on those agents. You can update the agent snapshot files to include authorized changes in the ESM console grid.

User rights checks

Restrict the following user rights on your Windows 2000 and Symantec AntiVirus servers to the %Administrator% account and members of the %Administrators% and %System Operators% security groups in addition to restrictions stated below. See ISO 17799 section 9.2.2.

- Access this computer from network — remove from %Guest% account
- Act as part of operating system
- Add workstations to domain — may also grant to %Domain Administrators%
- Back up files and directories — may also grant to %Backup Operators%
- Bypass traverse checking — may also grant to %Backup Operators%
- Change the system time
- Create a pagefile
- Create a token object
- Create permanent shared objects
- Debug programs
- Force shutdown from remote system — may also grant to %Power Users%
- Increase scheduling priority
- Load and unload device drivers
- Manage auditing and security log
- Modify firmware environment values — may also grant to %Server Operators%
- Replace a process level token
- Restore files and directories — may also grant to %Backup Operators%
- Shut down the system — remove from %Guest% account
- Take ownership of files or other objects

File Attributes checks and templates

- **Template file list**. The Symantec AntiVirus-W2K high-level policy uses two File template files to identify files that should reside on the Symantec AntiVirus and Windows 2000 servers: navce2ka.s50 and navce2kb.s50. Carefully investigate any files that are reported as missing by the File Attributes template checking function. See ISO 17799 sections 8.3 and 10.4.1.
- **Check file ACL**. Carefully check all reported file access permissions increases to determine whether unauthorized access is being granted to your system. See ISO 17799 section 9.2.2.
- **Perform file signature**. Carefully check all reported files with MD5 signature changes since the ESM snapshot was last updated on the agent system. A file signature change indicates a file modification that may not have been authorized. See ISO 17799 sections 10.3.3 and 10.4.1.

Note: Run the Symantec AntiVirus-W2K high level policy one time on each ESM agent that is checked by the policy to create file snapshot files with file signature records on the agent. Then periodically rerun the policy to detect changes to file signatures on those agents. You can update the agent snapshot files to include authorized signature changes in the ESM console grid.

File Watch checks and templates

The Symantec AntiVirus-W2K high-level policy uses the checks, **Enable new file checks** and **Enable removed file checks**, in the File Watch module to check all directories except *\tmp and *\temp on the C: volume for files that have been added or removed since the ESM snapshot was last updated on the agent system.

The policy enables the navce2kh.fw File Watch template file to identify the directories and changes that are watched. Carefully investigate all reported changes to identify whether the integrity of your file system has been compromised. See ISO 17799 sections 8.3, 10.4.1, and 10.5.4.

Note: Run the Symantec AntiVirus-W2K high-level policy one time to create the fwatch.dat snapshot file on each ESM agent where files will be watched before periodically rerunning the policy to identify new and removed files.

Login Parameters checks

The Symantec AntiVirus-W2K high-level policy runs all of the enabled checks in the base policy as well as the **Display legal notice during logon** check. All of your Symantec AntiVirus and Windows 2000 servers should display upon logon a legal warning that the system is private and unauthorized access is not permitted. See ISO 17799 sections 9.5.2(b) and 12.1.5.

Object Integrity checks

The Symantec AntiVirus-W2K high-level policy runs the security check, **Check for volumes without ACL control**, to identify volumes with file systems that do not support persistent ACLs. These volumes are inherently insecure because they allow anyone to add, modify, or delete files and directories. Convert the reported volumes to NTFS and set access controls for files and directories. See ISO 17799 section 9.2.

Password Strength checks

The Symantec AntiVirus-W2K high-level policy runs all of the checks in the base policy as well as the following checks to enforce the best practices described below:

- **Minimum password age**. Set the minimum password age in the Windows 2000 account policy to 14 days to prevent more frequent password changes, which could cause users to forget their passwords. See ISO 17799 sections 9.3.1 and 9.5.4.
- **Password uniqueness**. Set the number of passwords to be remembered as password history to 10 in the Windows 2000 account policy. With this setting, users cannot reuse favorite passwords until they have used 10 new, unique passwords. See ISO 17799 section 9.3.1(e) and 9.5.4(f).

Registry checks and templates

- **Check key ownership**. This check verifies that the registry key owners on examined servers match the owners that are specified in the navce2kh.rs5 and w2kservh.rs5 Registry template files that are enabled by the Symantec AntiVirus-W2K high-level policy. See ISO 17799 sections 8.3 and 10.4.

- **Check key and value existence**. This check verifies that the Symantec AntiVirus server configuration complies with records in the navce2kh.rs5 Registry template file that define mandatory and forbidden registry keys. The check also compares registry key values with required key settings that are defined in template sublist records. See ISO 17799 sections 8.3, 10.4.1, and 10.5.4.

Records in the navce2kh.rs5 template file enforce the following best practices in addition to the best practices enforced by the Symantec AntiVirus-W2K base policy:

- Client virus definitions should be updated from the parent server every 60 minutes.
- Clients should not be allowed to unload Symantec AntiVirus services. The LockUnloadServices key should be set on the server.
- Clients should be asked for a password to scan unmapped network drives.
- Server sensitivity level for heuristic scanning settings should not be set to minimum level of protection.
- Quarantine or Scan and Deliver should be enabled.
- Quarantine option should be set to Automatically repair and restore silently when new virus definitions arrive.

Records in the w2kservh.rs5 template file enforce the following best practices in addition to the best practices enforced by the Symantec AntiVirus-W2K base policy:

- Set the Number of previous logons to cache to 0.
- Enable the settings: Restrict CD_ROM access to locally logged-on users only and Restrict floppy access to locally logged-on users only.
- Allow only the %Administrator% to eject removable NTFS media.
- Turn off the setting that disables the CTRL-ALT-DEL requirement for logon.
- Disable the settings: Audit the access of global system objects and Audit use of Backup and Restore privilege.
- Enable the setting: Prevent users from installing printer drivers.
- Enable the setting: Clear virtual memory page file when system shuts down.
- Disable the Secure channel settings: Require strong (Windows 2000 or later) session key and Digitally encrypt or sign secure channel data (always).
- Disable the setting: Prevent system maintenance of computer account password.

- Set “Additional restrictions for anonymous connections” to “Do not allow enumeration of SAM accounts and shares.”
- Set the ProtectionMode value of the Session Manager key to 1 to prevent users from gaining administrative rights by way of DLLs.
- Set the RestrictGuestAccess values for the Application, Security, and System Event Log keys to 1 to prevent unauthorized access to event logs.
- Enable the setting, Digitally sign server communication (always), and disable the setting, Digitally sign server communication (when possible). Set the amount of idle time required before disconnecting a session to 15 minutes.
- Set the AutoShareServer value of the LanManServer\Parameters key to 0 to turn off the setting that allows administrative shares to be automatically created.
- Enable the setting, “Digitally sign client communication (when possible), and disable the setting, “Digitally sign client communication (always).
- Disable the setting: Send unencrypted password to connect to third-party SMB servers.

System Auditing checks

- **Security events success auditing.** The following successful security events should be audited on Windows 2000 servers that are running the Symantec AntiVirus application server. Auditing of successful events helps you detect system break-ins and provides valuable tracking information during and after a break-in. See ISO 17799 section 9.7.2.1(a).

  Account logon events
  Account management
  Logon events
  Policy change
  System events

- **Security events failure auditing.** The following failed security events should be audited on Windows 2000 servers that are running the Symantec AntiVirus application server. Auditing of failed events helps you identify break-in attempts and provides valuable tracking information during and after such attempts. See ISO 17799 section 9.7.2.1(c).

  Account logon events
  Account management
  Logon events
  Object access

Policy change
Privilege use
System events

- **Security events do not overwrite security log**. Make sure that Windows 2000 Event Viewer security log properties do not allow the system to overwrite events in your security log that are not older than the archive period, which should be defined by your security policy. See ISO 17799 section 9.7.2.3(d).
- **Security event log size**. Make sure the size of your security event log is at least 10,496 kilobytes. See ISO 17799 section 9.7.2.3.

Policy installation procedures

ESM's best practice policies should be installed on the ESM managers that will run the policies on ESM agents with the applications and operating system platforms that are targeted by specific best practice policies.

Installation prerequisites

Before you run the executable program that installs the best practice policies that are documented in these Notes, you need to complete the following prerequisites:

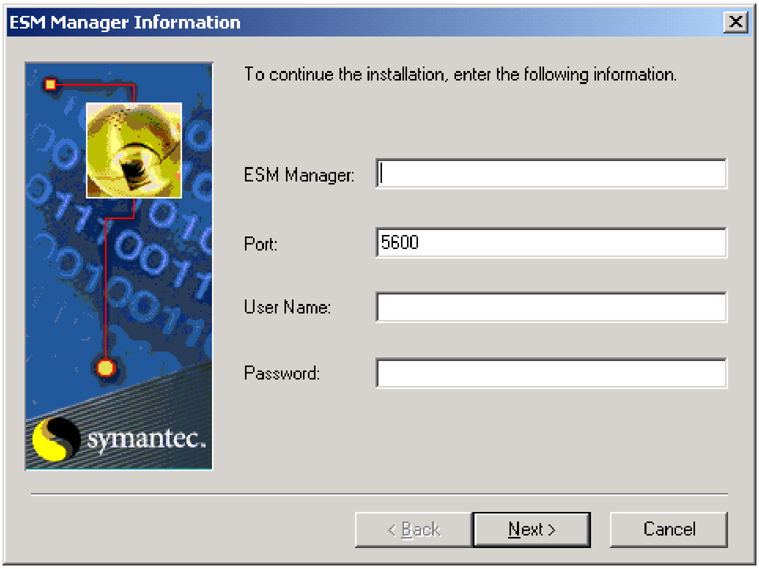
- Upgrade all ESM manager and agent systems that will use the best practice policies to ESM version 5.1 or later.
- Upgrade the Windows 2000 modules on all ESM manager and agent systems that will use the best practice policies to Security Update 10 or later.
- Download the **BestPractice_Windows_2000_Server_Symantec_AV_Server** executable file from the SWAT Web page at:

  http://securityresponse.symantec.com.
- Identify the ESM account name, the ESM account password, and the communication port that must be used to connect to each ESM manager you intend to install.

Installation steps

1. Run the **BestPractice_Windows_2000_Server_Symantec_AV_Server** executable file from a system that has network access to the ESM manager you want to install.
2. Click **Next** to close the InstallShield Welcome dialog box.
3. Click **Yes** to accept the Symantec Corporation Software License Agreement.
4. If the installation program does not find the required Java™ 2 Runtime libraries on your system, you will be prompted to install the Java 2 Runtime Environment. Click **Yes** to start the installation, click **Yes** to accept the Software License Agreement, then click **Next** to install the Java 2 Runtime Environment.

5 Click **Yes** to continue installation of the best practice policies.



ESM Manager Information

To continue the installation, enter the following information.

ESM Manager:

Port: 5600

User Name:

Password:

6 Enter requested ESM Manager Information, then click **Next**.

Note: If the modules installed on the specified manager system have not been upgraded to SU10 or later, ESM returns an error message and aborts the installation of the best practice policies. Upgrade the manager to SU10 or later and rerun the install program.

7 Click **Finish** to exit the installation program after a successful installation.

Known restrictions

Registration of new agents to ESM 5.1 managers

When you register a new ESM 5.1 agent with an operating system that was not registered to your ESM 5.1 manager before you installed a best practice policy, the new agent's operating system inaccurately displays in the policy's expanded module lists in the ESM enterprise tree.

For example, when you first install the Symantec AntiVirus-W2K best practice policies on an ESM 5.1 manager, the tree correctly displays only "WIN2000" branches for each module in these policies. If you later register a Windows NT agent to the same manager, the tree incorrectly displays an "NT" branch for each module in the policies. This is misleading because these policies do not run on Windows NT agents.

These are cosmetic errors that are fixed in the ESM 5.5 console release. If you are using the ESM 5.1 console, remember that each set of ESM best practice policies is intended to run only on ESM agents that are running the operating systems, versions, and applications that are identified by the policy titles.

Service and support solutions

Symantec’s Technical Support Group of skilled Technical Engineers can provide platform-specific information about Symantec products. Our staff has in-depth expertise in both client/server computing and information security technology.

Contacting technical support

To contact Symantec’s technical support

North America, Latin America, or Asia Pacific

Telephone:(888) 727-8671

Web:http://www.symantec.com/techsupp/

Outside North America but supported from the United States (i.e., APLA)

Telephone:(781) 663-2686

Web:http://www.symantec.com/techsupp/

Europe, Middle East, Africa, (EMEA)

Telephone:+44 (0) 1372 214321

FAX:+44 (0) 1372 751815

E-mail:eurbox_epsom@symantec.com

Licensing

Telephone:(888) 584-3925

FAX:(781) 487-9818

E-mail:license@symantec.com

World Wide Web site

Web:http://www.symantec.com/techsupp/

Service and support offices

North America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401
U.S.A.

http://www.symantec.com/
Fax: (541) 984-8020

Automated Fax Retrieval
(800) 554-4403
(541) 984-2490

Argentina, Chile, and Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

http://www.symantec.com/region/mx
+54 (11) 4315-0889
Fax: +54 (11) 4314-3434

Asia/Pacific Rim

Symantec Australia Pty. Ltd.
408 Victoria Road
Gladesville, NSW 2111
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 9850 1000
Fax: +61 (2) 9817 4550

Brazil

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

http://www.symantec.com/region/br/
+55 (11) 3048-7515
Fax: +55 (11) 3048-7510

Colombia, Venezuela, the Caribbean, and Latin America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401
U.S.A.

http://www.symantec.com/region/mx/
+1 (541) 334-6054 (U.S.A.)
Fax: (541) 984-8020 (U.S.A.)

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032
Fax: +353 (1) 811 8033

Automated Fax Retrieval
+31 (71) 408-3782

Mexico

Symantec Mexico
Blvd Adolfo Ruiz Cortines,
No. 3642 Piso 14
Col. Jardines del Pedregal
Ciudad de México, D.F.
C.P. 01900
México

http://www.symantec.com/region/mx
+52 (5) 661-6120

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

March 2002